Research paper / Оригинальная статья
https://doi.org/10.51176/1997-9967-2023-4-200-219
МРНТИ 06.81.30
JEL: G14, G12, G32, O51

The Impact of Cybersecurity Breaches on Firm's Market Value: the Case of the USA

Gulmira K. Issayeva[a], Elmira E. Zhussipova[a]*, Ainura N. Aitymbetova[a], Alma S. Kuralbayeva[b], Damira B. Abdykulova[a]

[a]M.Auezov South Kazakhstan University, 5 Tauke Khan Ave., 160000, Shymkent, Kazakhstan; [b]Central Asian Innovation University, 137 Madeli Kozha Str., 160013, Shymkent, Kazakhstan

For citation: Issayeva, G. K., Zhussipova, E. E., Aitymbetova, A. N., Kuralbayeva, A. S., & Abdykulova, D. B. (2023). The Impact of Cybersecurity Breaches on Firms' Market Value: the Case of the USA. Economics: the strategy and practice, 18(4), 200-219, https://doi.org/10.51176/1997-9967-2023-4-200-219

ABSTRACT

In the context of global digitalization trends, the problem of the impact of cyberattacks on the company is significantly relevant. This article is devoted to the impact of cyberattacks on the firms' market value since it is an indicator of firm performance. The authors used the event study methodology to study the impact of cyberattacks on the firm's market value. In addition, linear regression analysis (OLS) was applied to study the factors influencing cumulative abnormal returns (CAR). The paper's central hypothesis is the assumption that a cyberattack announcement is supposed to change market reaction, which is predicted to be harmful since cybercrime incidents can lead to high implicit and explicit costs. Therefore, an adverse market reaction reflects negative CAR during the event. The paper explores the effect of firm-specific and attack-specific characteristics of cyberattacks on the CAR with the data of cyberattacks for US firms from 2011 to 2020. Thus, the impact of cyberattacks on CAR by industry type and firm size was examined. Also, the type of cybercrime that is more harmful to the company was identified. The study results confirm the central hypothesis and show that cyberattacks negatively affect the firms' market value. In addition, it was found that the market reaction to the breach is more harmful to small firms. Thus, large firms have advantages over medium and small ones in sustaining financially during cyberattacks. Additionally, the paper defines no consistent evidence that market reaction to cyberattacks depends on firm and breach types.

KEYWORDS: Economy, Practice, Firm, Cyberattack, Cyber Incident, Cumulative Abnormal Returns

CONFLICT OF INTEREST: the authors declare that there is no conflict of interest.

FINANCIAL SUPPORT: The study was not sponsored (own resources).

Article history:
Received 25 December 2022
Accepted 29 November 2023
Published 30 December 2023

* **Corresponding author: Zhussipova E.E.** – PhD, Senior Lecturer, M.Auezov South Kazakhstan University, 5 Tauke Khan avenue, 160000, Shymkent, Kazakhstan, 87477323306, email: elmira_zhusipova@mail.ru

Кибершабуылдардың компанияның нарықтық құнына әсері (АҚШ мысалында)

Исаева Г.К.[a], Жусипова Э.Е.[a]*, Айтымбетова А.Н.[a], Куралбаева А.Ш.[b], Абдыкулова Д.Б.[a]

[a]М.Әуезов атындағы ОҚУ, даң.Тәуке хан 5, 160000, Шымкент қ., Қазақстан; [b]Орталық Азия инновациялық университеті, көш. Мәделі қожа 137, 160013, Шымкент, Қазақстан

Дәйексөз үшін: Исаева Г.К., Жусипова Э.Е., Айтымбетова А.Н., Куралбаева А.Ш., Абдыкулова Д.Б. (2023). Кибершабуылдардың компанияның нарықтық құнына әсері (АҚШ мысалында). Экономика: стратегия және практика, 18(4), 200-219, https://doi.org/10.51176/1997-9967-2023-4-200-219

ТҮЙІН

Жаһандық цифрландыру тенденциясы жағдайында кибершабуылдардың компания қызметіне қалай әсер ететіні өзекті мәселелердің қатарында болып отыр. Компанияның нарық құны оның тиімділігін анықтайтын бірден-бір көрсеткіш болғандықтан, бұл мақалада кибершабуылдардың осы көрсеткішке ықпалы зерттелді. Кибершабуылдардың фирманың нарық көрсеткіштеріне ықпалын зерттеу үшін мақалада оқиғаны зерттеу (event study) әдістемесі қолданылды. Сонымен қатар, жиынтық аномалды пайданың (CAR) мөлшеріне әсер ететін факторларды зерттеу үшін сызықтық регрессиялық талдау (OLS) жүргізілді. Жұмыстың негізгі гипотезасы кибершабуылдар компанияның айқын және жасырын шығындарын арттыра отырып, жиынтық аномалды пайдаға (CAR) теріс әсер етуі мүмкін деген болжам болып табылады. Нарықтың жағымсыз реакциясы CAR-дің теріс шамасы арқылы көрініс табады. Талдау жүргізу үшін авторлар 2011-2020 жылдар аралығындағы АҚШ фирмаларының кибершабуылдары туралы деректерді пайдаланып, CAR-ға әртүрлі кибершабуыл түрлерінің әсерін компания көлемі мен саласы бойынша зерттеп шықты. Сонымен бірге, компанияға ең көп қаржы шығындарын әкелетін кибершабуыл түрі анықталды. Зерттеу нәтижелері жұмыстың негізгі гипотезасын растап, кибершабуылдар фирмалардың нарық құнына теріс әсер ететінін көрсетті. Бұдан басқа, киберинциденттердің шағын компанияларға тигізетін кері әсері ірі компанияларға қарағанда айтарлықтай жоғары екені анықталды. Осылайша, кибершабуылдар кезінде ірі компаниялар шағын және орта компаниялармен салыстырғанда қаржылық тұрғыдан орнықтырақ деген қорытынды жасауға болады. Сонымен қатар, киберқылмыстың әкелетін қаржылық шығындар мөлшері кибершабуыл түріне және компанияның саласына тәуелді болмайтыны анықталды.

ТҮЙІН СӨЗДЕР: экономика, практика, компания, кибершабуыл, киберинцидент, жалпы аномалдық кіріс

МҮДДЕЛЕР ҚАҚТЫҒЫСЫ: авторлар мүдделер қақтығысының жоқтығын мәлімдейді.

ҚАРЖЫЛАНДЫРУ: зерттеуге демеушілік қолдау көрсетілмеді (меншікті ресурстар).

Мақала тарихы:
Редакцияға түсті 25 Желтоқсан 2022
Жариялау туралы шешім қабылданды 29 Қараша 2023
Жарияланды 30 Желтоқсан 2023

* **Хат-хабаршы авторы: Жусипова Э.Е.** – PhD, аға оқытушы, М.Әуезов атындағы ОҚУ, даң.Тәуке хан 5, 160000, Шымкент, Қазақстан, 87477323306, email: elmira_zhusipova@mail.ru

Влияние кибератак на рыночную стоимость компании (на примере США)

Исаева Г.К.[a], Жусипова Э.Е.[a]*, Айтымбетова А.Н.[a], Куралбаева А.Ш.[b], Абдыкулова Д.Б.[a]

[a]Южно-Казахстансакий университет им.М.Ауэзова, пр. Тауке хана 5, 160000, Шымкент, Казахстан; [b]Центрально-Азиатсакий инновационный университет, ул. Мадели кожа 137, 160013, Шымкент, Казахстан

Для цитирования: Исаева Г.К., Жусипова Э.Е., Айтымбетова А.Н., Куралбаева А.Ш., Абдыкулова Д.Б. (2023). Влияние кибератак на рыночную стоимость компании (на примере США). Экономика: стратегия и практика, 18(4), 200-219, https://doi.org/10.51176/1997-9967-2023-4-200-219

АННОТАЦИЯ

В условиях тенденций всеобщей цифровизации проблема влияния кибератак на деятельности компании является весьма актуальной. Данная статья посвящена влиянию кибератак на рыночную стоимость компаний, так как данный показатель определяет эффективность деятельности компании. Для изучения влияния кибератак на рыночные показатели фирмы в статье была использована методология исследования событий (event study). Кроме того, для изучения факторов, влияющих на величину совокупной аномальной прибыли (CAR) был применен линейный регрессионный анализ (OLS). Основной гипотезой работы является предположение, что кибератаки могут негативно влиять на совокупную аномальную прибыль (CAR), повышая явные и неявные затраты компании. Неблагоприятная реакция рынка отражается в отрицательном показателе CAR. Для проведения анализа авторы использовали данные о кибер-инцидентах фирм США с 2011 по 2020 годы, и исследовали влияние различных типов кибератак на CAR в разрезе видов отраслей и размеров предприятий. Также, был определен тип киберпреступления, который наносит больший ущерб компании. Результаты проведенного исследования подтверждают основную гипотезу исследования, и показывают, что кибератаки негативно влияют на рыночную стоимость фирм. Кроме этого, было выявлено, что негативное влияние кибератак на малые компании существенно выше, чем на крупные. Таким образом, можно сделать вывод о том, что крупные компании более финансово устойчивы по сравнению со средними и малыми компаниями во время кибератак. В результате исследования также выявлено, что финансовый ущерб от киберпреступления не зависит от вида кибератаки и от типа индустрии к которой принадлежит компания.

КЛЮЧЕВЫЕ СЛОВА: экономика, практика, фирма, кибератака, кибер-инцидент, совокупная аномальная прибыль

КОНФЛИКТ ИНТЕРЕСОВ: авторы заявляют об отсутствии конфликта интересов.

ФИНАНСИРОВАНИЕ: Исследование не имело спонсорской поддержки (собственные ресурсы).

История статьи:
Получено 25 декабря 2022
Принято 29 ноября 2023
Опубликовано 30 декабря 2023

* **Корреспондирующий автор: Жусипова Э.Е.** – PhD, старший преподаватель, Южно-Казахстансакий университет им.М.Ауэзова, пр. Тауке хана 5, 160000, Шымкент, Казахстан, 87477323306, email: elmira_zhusipova@mail.ru

Introduction

On the 29th of July 2019, the personal information of US bank Capital One Financial, involving the confidential data of more than 100 million customers, was exposed to the public. The company's share price dropped nearly 6% the next day. The incremental cost of this data breach is supposed to be beyond $100 million (Murphy & Bond, 2019). In December 2019, Travelex announced a hacker attack that demanded a ransom to prevent the exposure of the personal data of their users, including account names and credit card details. It resulted in £25 million in losses to Travelex, which was deteriorated by the coronavirus effect (Warrell, 2019). It is believed that cyberattacks lead to considerable financial losses. The total financial losses from cybersecurity breaches in 2020 were estimated to reach $1.8 billion, compared with $1.2 billion in 2019 (Hiscox, 2020).

The number of cyberattacks is multiplying due to the digitalisation of all activities, specifically during the pandemic period. In the digital era, every firm can be targeted as a victim of a privacy breach event. That is why it is essential to investigate cybersecurity breach incidents over the years and to study how they affect the performance of firms.

This paper focuses on whether cybersecurity breaches impact a firm's value and operating performance. Previous studies find that breaches negatively affect a firm's market value (Campbell et al., 2003; Garg et al., 2003a, 2003b; Hovav & D'Arcy, 2003, 2004; Cavusoglu et al., 2004; Kamiya, 2018). In addition, some studies have shown that negative impacts differ depending on the type of breach and firm characteristics (Cavusoglu et al., 2004; Hovav & D'Arcy, 2003; Hovav et al., 2017). Also, some empirical results have found mixed evidence that breaches impact firm revenue, profit, reputation, and financial policy (Gordon et al., 2003; Mukhopadhyaya et al., 2013; Low, 2017; Kamiya, 2018; Garg, 2020). Therefore, it is interesting to explore further how cybersecurity incidents affect a firm's performance, investment, and financial policies with updated data, following the steps and logic used in the previous research.

The first hypothesis of this paper is that cybersecurity breaches result in negative cumulative abnormal returns (CARs). The following hypothesis is that market reaction to cyberattacks depends on the firm type. The third hypothesis is that there are significant differences between the negative CAR depending on the firm size. Additionally, the fourth hypothesis of this research is that various breach types impact CAR differently.

The event study methodology is used in this research to examine CAR caused by security breach incidents. The data used in the study is collected from the Audit Analytics database, while stock prices and market returns are from the Center for Research and Securities Prices (CRSP) dataset. Furthermore, annual firm performance data is retrieved from the Compustat database.

The CAR is calculated using the main steps of the event study for (-1,+1), (-3,+3), and (-5,+5) event windows. After that, a t-test on CARs is conducted to study how CARs differ across the firm type, firm size, and breach type. Then, the regression of CARs (-1,+1) on the factors that can impact CARs is run.

The main results are consistent with the previous research. Thus, the t-test results reveal a significant negative impact of cyberattacks on the firm's value. Moreover, results show different market reactions for small firms. They experience a significant drop in the firm's value due to the cyberattack. However, the following t-tests reveal no consistent evidence between the market reaction to cyberattacks across industries, firm size, and cyberattack type.

Literature review – Hypotheses

There is a stream of research today on the relationship between cybersecurity breaches and the market value of a company. It is suggested that announcements about cybersecurity incidents negatively impact publicly traded companies' cumulative abnormal returns (CAR). Campbell et al. (2003) have found that cybersecurity incidents related to lost confidential information significantly negatively impact CAR. Goel and Shawky (2009) investigated that cyberattacks harmed the market value. Cavusoglu et al. (2004) have investigated cybersecurity breaches impact and detected a 2.1% loss in the firm's market value. Moreover, they have identified that the negative impact depends on the incident type, firm type, and size.

It was suggested that only companies that actively use websites and provide online services absorb more negative effects during cybersecurity breaches disclose (Hovav & D'Arcy, 2003). However, to date, every company is using websites to increase their market share, specifically during COVID-19 and the restriction of offline services. Cybersecurity is becoming an essential part of modern business that relates to the heavy use of Internet sources. Cyber attackers are developing methods for accessing companies' financial and personal information. Therefore, in further examining the impact of cybersecurity breaches impact, Hovav et al. (2017) have identified that the objective, specific tools used for the cybercrime, and type of the attacker, also significantly impact the company's market value. Gordon et al. (2003) revealed that cybersecurity breach announcements result in harmful to firms' revenue, profit, and reputation.

Furthermore, Mukhopadhyaya et al. (2013) and Low (2017) found that cyberattacks negatively impact profit, market capitalization, and intangible assets such as a firm's brand image. Moreover, recent studies have found changes in firm economic policy, such as increasing cash holdings (Garg, 2020) and reconsidering investment and compensation policies (Kamiya, 2018). Given that, it is essential to study how cybersecurity breaches can affect the firm's various activities.

It should be noted that some researchers distinguish cybersecurity breaches from data privacy breaches. Personal data breaches can emerge from cybersecurity incidents, and they are related to the disclosure of personal information about the company, its customers, and suppliers. Thus, many researchers are examining the impact of personal information disclosure on firm performance. According to studies by Gatzlaff and McCullough (2010) and Martin et al. (2017), the announcement about personal information breaches has a significant negative impact on the company's performance. In addition, Martin et al. (2017), Jeong et al. (2019), and Janakiraman et al. (2018) have revealed the fact that a personal data breach announcement can give competitive advantages to rival firms damaging firms that have experienced a cyber-attack. It raises a concern that collecting and storing private information about customers, shareholders, and other stakeholders can increase the risk of data vulnerability. According to the study by Martin et al. (2017), breach announcements can negatively impact customers' decisions about the goods and services of breached companies, decreasing their spending. Therefore, there is a need to research this aspect in detail and study how personal data breaches can affect the firm's stakeholders.

This study uses a dataset for the last ten years in the USA to examine how cybersecurity breaches impact various firms' activity. It is important to note that the USA is the first country that implemented mandatory breach disclosure rules under the State Security Breach Notification Laws. According to the Audit Analytics database, registered cybersecurity incidents in the USA for only six months of 2021 (107) are more than all registered cyber-crimes in 2020 (105). It should be noticed that the majority of previous studies focused on the impact of cyberattacks on US firms examining events that occurred at the beginning of the 2000s (Campbell et al., 2003; Garg et al., 2003a, 2003b; Hovav & D'Arcy, 2003, 2004; Cavusoglu et al., 2004). Given that, it becomes relevant to revise all the statements that have been made in previous years using the updated database.

How cybersecurity breaches impact the market value of firms is of interest to this research since the firm value is an indicator of firm performance. Increasing the firm's market value and relative shareholder wealth is the primary purpose of the company's managers (Martin & Murphy, 2017). A cyberattack announcement is supposed to change market reaction, which is predicted to be harmful since cyber-crime incidents can lead to high implicit and explicit costs for a firm. An adverse market reaction reflects a negative cumulative abnormal return (CAR) during the event. This study will explore this impact on different industries. It will help understand whether the specific industry firms are a target of cyber-attacks. Moreover, how cybersecurity incidents impact different-sized firms will be investigated. Finally, it will explain whether large firms have advantages over medium and small ones to sustain financially during cyber-attacks.

Furthermore, defining which type of cyber-crime is more damaging is essential. Exploring the impact of various types of cyber-crime can give a clear picture of which are more dangerous for firms and help managers implement an efficient firm's cybersecurity resilience system. In addition, it is essential to quantify the impact of cybersecurity breaches by evaluating the average financial losses from cybersecurity breaches. Do the considerable financial losses influence a significant drop in market value or not?

First, market reactions to the disclosure of cybersecurity breaches are analysed to answer these questions. It is believed that cyber-attacks lead to negative implications such as decreasing the market value of the firm, high expenses due to the recovering reputation, and financial losses after breaches. The research will attempt to identify whether there is a significant negative cumulative abnormal return or not. This consideration leads to the following hypothesis:

H1: A cybersecurity breach announcement results in a negative abnormal return

Rejection of H0 would signal market participants' response to the announcement of a data breach.

Moreover, which type of firms are likely to be affected by cyber-attacks will be determined by setting the following hypothesis:

H2: The impact of cybersecurity breach announcement on cumulative abnormal return depends on the industry type

Rejection of H0 would signal a difference in response to the cybersecurity breaches between firms according to the industry type.

Next, another firm-specific parameter, such as firm size, will explore the impact of firm size on cumulative abnormal return. For this purpose, the following hypothesis will be considered:

H3: The impact of cybersecurity breach announcement on cumulative abnormal return depends on the firm size

Rejection of H0 would again signal a difference in response to the cybersecurity breaches between firms according to the firm size.

Another way to consider the impact of cybersecurity breach announcements is to find the relationship between cyber-crime type and cumulative abnormal return. For example, Campbell et al. (2003), Cavusoglu et al. (2004), and Gatzlaff & McCullough (2010) revealed a different effect of breach type on a firm's market value. Given that, it is interesting to revise how various types of breaches can impact the firm's performance. For that reason, the following hypothesis will be set:

H4: There are significant differences between the negative cumulative abnormal return of cyber incidents depending on the breach type

Rejection of H0 would signal a different reaction to the cybersecurity breaches depending on its type.

Methodology

The event study methodology is used in this research to investigate the impact of announcements about cybersecurity breaches on a firm's market performance. The event study helps to examine cumulative abnormal returns caused by security breach incidents. We can interpret whether the event significantly impacts stock price variance (McWilliams & Siegel, 1997; MacKinlay, 1997).

The market model (MM) is used to explore the cumulative abnormal returns caused by cybersecurity incidents, as suggested by McWilliams & Siegel (1997) and MacKinlay (1997). According to the standard event study, the difference between return and expected return is determined by regression. The standard formula used for that calculation is as follows:

$$R_{it} = \alpha_i + \beta_i * R_{mt} + \varepsilon_{it} \qquad (1)$$

where, R – Return
i – the firm,
t – event data,
R_{mt} – market index,
a, ß - market model parameters
ε - residual

Identifying an event window and estimation period for the market model is required. Usually, the estimation period takes 120 trading days before the event window. The event window can be set as 1,3,5,10-days before and 1,3,5,10-days after the incident. The event windows are used in 3, 7, and 11 days overall (1, 3, and 5 days before and after the cybersecurity incident). The reason for taking [-1,+1], [-3,+3], [-5,+5] event windows is that there can be an interval between dates when the breach happens, then revealed and announced to the public. Market value might not absorb all information in the short event window in 1 or 3 trading days. That is why it is essential to see the differences between event windows results and compare them. Taking a long 21 days event window might have a confounding effect on other events. Therefore, in performing the event study, estimation windows will be set as 119-days (-120,-2), 117-days (-120,-4), and 115-days (-120,-6), while event windows will include three trading days (-1,+1), seven trading days (-3,+3), eleven trading days (-5,+5), respectively.

Then actual return will be compared with the expected return calculated by regression. This model looks as follows:

$$AR_{ik} = R_{ik} - (\alpha_i + \beta_i * R_{mk}) \qquad (2)$$

where AR – abnormal return
i – the firm,
k – is the time period of the event window, in our case, its 11 days
R – actual return of firm i in the period k
R_{mk} – market index, in k time period
a, ß - market model parameters

After that, cumulative abnormal return (CAR) is calculated by summing abnormal return for the 11-day event window. The following formula is used:

$$CAR_i = \sum_{k=-5}^{k=5} AR_{ik} \qquad (3)$$

A linear regression analysis (OLS) is implemented to investigate factors that impact cumulative abnormal returns and whether the effect of the announcement varies for different variables, such as firm size, type, cybersecurity breaches type, and financial losses. The empirical model can be presented as the following equation (3):

$$CAR_i = \alpha + \ \beta_1 * Firm\ size + \beta_2 * Firm\ type + Repeated\ Attacks + \beta_5 * Multiple\ Attacks +$$

$$+ \ \beta_3 * Incident\ type + \ + \beta_4 * + \beta_6 * ROA + \beta_7 * Ln(Revenue) + \ \varepsilon_{in} \qquad (4)$$

where, , - regression model parameters,
- residual.

The dependent variable is CAR. The regression model includes four types of independent variables. Firstly, some variables for company characteristics, such as *Firm size and firm type,* are used. The firm size is determined by the total assets of small, medium, large, and massive companies.

Then, it is considered to generate a set of dummy variables *Firm type* = {*Manufacturing, Transport, Wholesale, Retail, Finance, Services, Mining, and Construction*} according to the industry type by the SIC Code classification (SIC-NAICS, 2021).

The incident type variable is included in order to control for event characteristics. It is suggested by Cavusoglu et al. (2004), Chen et al. (2011), Das et al. (2012), Gordon et al. (2011), Hovav & D'Arcy (2003) that the prominent cybersecurity breaches can be divided as credit card information loss, hacking, personal information disclosure, software damages. Our dataset downloaded from the Audit Analytics database consists of extended types of incidents, including ransomware and unauthorised access as a separate types of hacking. It is essential to break down the incident types to examine which have a more negative impact on firm performance. Therefore, it is considered generating the set of dummy variables *Incident = {Phishing, Malware, Misconfiguration, Ransomware, Unauthorised Access and Not disclosed}*.

Moreover, it is considered to use information about repeated attacks within a year and an entire period. For that purpose, we divided firms into two groups and created dummy variables, such as repeated attacks and multiple attacks. Using these two variables in regression helps examine whether repeated attacks impact CAR or not. Further, we use another firm-specific characteristic that defines firm performance, such as Return on assets (ROA) and the natural logarithm of Revenue (*ln(Revenue)*).

Data collection and sample description

The Cybersecurity Disclosure Day is taken as an "event" to study the impact of breaches on the market value of US firms. A new dataset of US firms for the 2011-2020 period is used to verify previous studies that have found a negative impact of cyberattacks on shareholders wealth. The number of cybersecurity incidents for the USA companies is collected from the Audit Analytics database. The initial sample of the cybersecurity breaches contains 674 observations. 2 observations without indicated event date and six observations without information about firm characteristics such as sic code are deleted. The sample consists of 666 observations for that period.

Table 1 shows the annual frequency of cybersecurity breaches from 2011-2020.

Table 1 - The number of cybersecurity breaches per year

Year	Number of incidents	Percentage
2011	24	3.59
2012	29	4.35
2013	39	5.86
2014	55	8.26
2015	41	6.16
2016	49	7.36
2017	82	12.31
2018	109	16.37
2019	133	19.97
2020	105	15.77
Total	666	100
Note: developed by authors using the Audit Analytics database for 2011-2020		

The chronological distributions of 666 cyber-attacks over the period 2011 to 2020 by industry are presented in Table 2:

Table 2 - Distribution of Cyberattacks by Industry

Industry type	**Number of incidents**	**Percentage**
Mining, gas, and oil field	2	0.3
Construction	2	0.3
Manufacturing	160	24.03
Transport, communications	93	13.96
Wholesale trade	17	2.55
Retail trade	95	14.26
Finance	102	15.32
Service industries	195	29.28
Total	666	100
Note: developed by authors using the Audit Analytics database for 2011-2020		

Thirty-one observations are deleted since there are no records about firm characteristics such as cusip number. The remaining 635 cyber incidents are explored to determine whether there are repeated cyber-attacks. Three hundred thirteen firms experienced only a single attack for the 2011-2020 period, while 114 firms experienced multiple attacks (Table 3).

Table 3 - The number of not-repeated cyber-attacks for the 2011-2020 period

Number of cyber-attacks per firm	Total number of attack	Number of firms
1	313	313
2	138	69
3	75	25
4	36	9
5	30	6
6	-	-
7	7	1
8	16	2
9	-	-
10	20	2
Total	635	427
Note: developed by authors using the Audit Analytics database for 2011-2020		

This table shows 313 firms experienced only one attack from 2011-2020. Our sample consisted of 427 firms with at least one cyber incident. Then, 208 duplicated events are deleted. In summary, the dataset consists of 427 cybersecurity breaches. In addition, 24 observations with no information about total assets were deleted.

Table 4 summarises the sampling process.

Table 4 - Data set and applied filters for cyber-attack incidents

No.	Applied filters	Number of events		
		Initial	Deleted	Remaining
1	Observations collected from the Audit Analytics database	674	-	674
2	Deleted:			
	with no records of event characteristics such as event date, siccode, customer numbers	674	39	635
	duplicated events	635	208	427
	with missing values	427	24	403
	the final sample of cyber security events	403		403
Note: developed by authors using the Audit Analytics database for 2011-2020				

Moreover, the Wharton Research Data Services (WRDS) database, namely the Center for Research and Securities Prices (CRSP) dataset, has been used for retrieving daily equity data for the USA firms (i.e., closing price, cumulative adjusted price factor, number of shares outstanding, the value-weighted return including distributions as a proxy for the market return). This initial dataset consists of 18,046,296 observations, of which 8,674,525 are excluded for being related to non-public companies. Furthermore, 99,196 observations related to firms whose common stocks do not trade on the NYSE, NASDAQ, and AMEX are deleted. The remaining 9,272,575 observations are checked for duplicated events. Finally, after merging two datasets, 8,413,404 observations are deleted, and the final sample consists of 859,171 observations.

It is decided to exercise 1-, 3- and 5-day event windows to see the market's reaction and compare them since there are some delays in the discovery and public announcement of cybersecurity incidents. Therefore, the start days can differ from the announcement and disclosure days of the breaches.

Then, the initial 76,797 observations with less than 11 days of the event windows and 17,388 observations with less than 115 days of estimation windows are deleted. As a result, the total number of remaining observations matched the requirements of the chosen event study methodology consists of 764,986, and the number of observing cybersecurity breach incidents is 337. Table 5 summarises the sampling process.

Table 5 - Data set and applied filters for event study

No.	Applied filters	Number of events		
		Initial	Deleted	Remaining
1	Observations collected from the WRDS database	18,046,296	-	18,046,296
2	Deleted: non-public companies	18,046,296	8,674,525	9,371,771
	not publicly traded companies	9,371,771	99,196	9,272,575
	duplicated events	9,272,575	-	9,272,575
3	Events reported by Audit Analytics	403	-	403
4	Merging two datasets	9,272,575	8,413,404	859,171
5	Deleted:			
	Breaches that have less than 11 days of event window and less than 115 days of the estimation period	859,171	94,185	764,986
6	The final sample of observations	764,986		764,986
	the final sample of events	337		337
Note: developed by authors using WRDS and Audit Analytics database for 2011-2020				

Empirical Analysis

Impact of cybersecurity breaches on firm value

The results of the event study of cybersecurity incidents for the 2011-2020 period are presented in this section. 1-,3-, 5-day event windows and 119-,117-, 115-day estimation windows are taken to explore the market reaction.

Table 6 presents the descriptive statistics of CAR for various event windows. It shows that the mean value of CAR on the event day is negative for all three windows, i.e. -0.7%, -0.9%, and -0.8%, respectively. Also, the distribution of CARs is negatively skewed, indicating that more CAR values are negative. Thus, the value for CAR (-5,+5) has a moderate skewness of -0.88, while short event windows have higher but acceptable values as -1.83 for CAR (-1,+1) and -1.69 for CAR (-3,+3). Furthermore, the kurtosis of CAR(-1,+1) has a high value of 27.71, which is decreased to 15.59 for CAR (-3,+3) and 11.17 for CAR (-5,+5). It shows that CARs distributions are too peaked, and more CAR values are closely around the mean. Moreover, it indicates that distributions are more heavy-tailed than a normal distribution and have some extreme values.

Table 6 - Descriptive Statistics of CARs

	CAR (-1,+1)	**CAR (-3,+3)**	**CAR (-5,+5)**
Mean	-0.007	-0.009	-0.008
Median	-0.004	-0.004	-0.005
Standard Deviation	0.046	0.065	0.079
Min	-0.411	-0.434	-0.514
Max	0.277	0.267	0.321
Variance	0.002	0.004	0.006
Skewness	-1.83	-1.69	-0.88
Kurtosis	27.71	15.59	11.17
Observations	337	337	337

Note: Calculated by authors using Stata16

It is noticeable that the negative CAR for the 3-day window increases from -0.7% to -0.9%, then in the 5-day window, it slightly decreases back to -0.8%. Thus, it can be interpreted that cybersecurity incidents significantly impact the market in a short period.

To examine the significance of the negative CAR value, we run a one-tailed *t*-test for three event windows. The output of the test is shown in Table 7.

Table 7 - t-test results of CARs

	CAR (-1,+1)	**CAR (-3,+3)**	**CAR (-5,+5)**
Observations	337	337	337
Mean	-0.007***	-0.009***	-0.008**
Standard Error	0.002	0.004	0.004
Standard Deviation	0.046	0.065	0.079
[95% Conf. Interval]	-0.012	-0.016	-0.017
	-0.002	-0.002	0.0001
T	-2.810	-2.638	-1.944
degrees of freedom	336	336	336
Pr(T< t)	0.002	0.004	0.026

Notes:
1) * p<0.10, ** p<0.05, *** p<0.01
2) Calculated by authors using Stata16

The study reveals that the mean CAR (-1,+1) and CAR (-3,+3) are statistically significant at 1%. Likewise, the mean CAR (-5,+5) is also statistically significant but at 5%.

The hypothesis test makes it possible to confirm that cybersecurity attacks negatively impact the firm's market value.

Impact of firm and cybersecurity breach specific characteristics on average CAR.

To study the market reaction across the different firm types, we ran t-tests and the ANOVA-tests, where the dependent variable was CAR, and firm type was the independent variable. Table 8 presents the hypothesis test result that the firm's type impacts CAR in 1-, 3-, and 5-days event windows. According to these results, firms in the financial, transport, and communications spheres significantly damage CARs in all three event windows. The highest negative CAR is -2.8% for transport and communications firms in a 5-day window. It is statistically significant at 1%. Retail firms have -1.2% CAR (-1,+1) and -1.7% CAR (-3,+3) at 5% significance level. Furthermore, it is noticed that construction firms have -2.8% CAR (-3,+3) at 10% level of significance. However, this result is not meaningful since the number of construction firms is too small.

Table 8 - Comparison of CARs between various firm types

	Observations	**CAR (-1,+1)**	**CAR (-3,+3)**	**CAR (-5,+5)**
Mean of CARs				
Manufactory	88	-0.007 (0.137)	-0.006 (0.247)	0.002 (0.556)
Transport and communications	51	-0.009* (0.060)	-0.016* (0.060)	-0.028*** (0.005)
Wholesale	14	0.007 (0.703)	0.004 (0.609)	-0.003 (0.412)
Retail	44	-0.012** (0.019)	-0.017** (0.031)	-0.011 (0.257)
Finance	48	-0.008* (0.063)	-0.012** (0.038)	-0.011* (0.080)
Service	89	-0.005 (0.151)	-0.006 (0.120)	-0.006 (0.166)
Mining, oil, and gas	1	0.022 (N/A)	0.089 (N/A)	0.038 (N/A)
Construction	2	-0.021 (0.118)	-0.028* (0.067)	-0.023 (0.116)
Test of differences				
F-test (ANOVA)		0.39 (0.910)	0.64 (0.721)	0.71 (0.661)

Notes:
1) *P*-values reported in parentheses are based on standard errors
2) * *p* <0,10, ** *p* <0,05, *** *p* <0,01
3) Calculated by authors using Stata16

Notwithstanding the significant negative CAR values for a specific type of firm, a test of differences (ANOVA-test) defines that the p-value is more than 0.05 (0.910, 0.721, and 0.661, respectively). Therefore, we can state that CAR values do not significantly differ between various firms.

Table 9 reports the t-test results for comparing CARs of various-sized firms. The test output reveals that almost all firms except the medium have significant damaging CARs. Thus, the highest negative CAR at a 5% significance level is observed for small-sized firms, -1.4%, -2.3%, and -2.3% for 1-,3-, and 5-day event windows, respectively. The lowest negative CAR at 10% has experienced huge firms in CAR (-1,+1) and CAR (-5,+5), -0.5% and and 0.661, respectively). Therefore, we can state that CAR values do not significantly differ between various firms.

Table 9 reports the t-test results for comparing CARs of various-sized firms. The test output reveals that almost all firms except the medium have significant damaging CARs. Thus, the highest negative CAR at a 5% significance level is observed for small-sized firms, -1.4%, -2.3%, and -2.3% for 1-,3-, and 5-day event windows, respectively. The lowest negative CAR at 10% has experienced huge firms in CAR (-1,+1) and CAR (-5,+5), -0.5% and -0.7%, respectively. Big firms have significance at 1% level -0.9% and -1.3%, and at 5% level -1.4% for 1-,3-, and 5-day windows, respectively. Medium firms have positive 0.1%, 0.3%, and 1.1% CARs. However, they are insignificant.

Table 9 - Comparison of CARs between different firm sizes

	Observations	**CAR (-1,+1)**	**CAR (-3,+3)**	**CAR (-5,+5)**
Mean of CARs				
Small	85	-0.014** (0.029)	-0.023** (0.016)	-0.023** (0.032)
Medium	83	0.001 (0.552)	0.003 (0.668)	0.011 (0.924)
Big	84	-0.009*** (0.004)	-0.013*** (0.002)	-0.014** (0.041)
Very big	85	-0.005* (0.053)	-0.004 (0.198)	-0.007* (0.070)
Test of differences				
F-test (ANOVA)		1.58 (0.194)	2.57* (0.054)	2.82** (0.039)
Bonferroni test (Differences between medium and small firms)			0.026* (0.06)	0.034** (0.031)
Notes: 1) *P*-values reported in parentheses are based on standard errors 2) * *p* <0,10, ** *p* <0,05, *** *p* <0,01 3) Calculated by authors using Stata16				

Test of differences reveals some diversity in market reaction across various-sized firms since the p-value is 0.054 for CAR (-3,+3) and 0.039 for CAR (-5,+5). Thus, we can reject a null hypothesis and state that firm size can impact CAR differently. The Bonferroni test has been run to define the difference between firms. Bonferroni test reveals the difference between medium and small firms is -2.6% for CAR (-3,+3) and -3.4% for CAR (-5,+5).

Table 10 represents the t-test output for defining whether there is a different market reaction across various types of attacks.

Table 10 - Comparison of CARs between various types of attack

	Observations	**CAR (-1,+1)**	**CAR (-3,+3)**	**CAR (-5,+5)**
Mean of CARs				
Malware	66	0.002 (0.636)	0.003 (0.678)	0.009 (0.808)
Malware/Phishing	1	-0.024 (N/A)	-0.096 (N/A)	-0.074 (N/A)
Misconfiguration	15	-0.005 (0.352)	0.005 (0.607)	-0.007 (0.393)
Not Disclosed	115	-0.005* (0.062)	-0.008* (0.059)	-0.011** (0.037)

Phishing	63	-0.010** (0.034)	-0.020** (0.027)	-0.011 (0.165)
Ransomware	25	-0.013 (0.273)	-0.016 (0.243)	-0.023 (0.162)
Unauthorized Access	52	-0.015*** (0.000)	-0.016** (0.019)	-0.015* (0.058)
Test of differences				
F-test (ANOVA)		0.82 (0.552)	1.21 (0.299)	0.88 (0.513)

Notes:
1) *P*-values reported in parentheses are based on standard errors
2) * *p* <0,10, ** *p* <0,05, *** *p* <0,01
3) Calculated by authors using Stata16

The test defines that *Unauthorised Access* has the highest negative and significant CARs, -1.5% at 1% level, -1.6% at 5%, and -1.5% at 10% level for 1-,3-, and 5-day windows respectively. Furthermore, *Not Disclosed* cyberattacks also have significant negative average CAR, -0.5% at 10% level for CAR (-1,+1), -0.8% at 10% level for CAR (-3,+3), -1.1% at 5% level of significance for CAR (-5,+5). *Malware* has a cheerful insignificant CAR, while *Phishing* has a significant at 5% level -1.0% and -2.0% mean for CAR (-1,+1) and CAR (-3,+3). There is only one observation where *Malware* and *Phishing* are combined, which is why it is not a reliable result, and we cannot take into account these damaging CARs even they are very high compared with others (-2.4%, -9.6% and -7.4%).

The ANOVA-test does not reveal any differences between CARs of various cyber-attack types since the p-value is more than 0.05 (0.552, 0.299, and 0.513). Thus, we can assume that market reaction to various types of breaches is not significantly different.

Table 11- compares CARs of firms experiencing a different type of information loss.

Table 11 - Comparison of CARs between various information loss

	Observations	CAR (-1,+1)	CAR (-3,+3)	CAR (-5,+5)
Mean of CARs				
Financial	105	-0.013*** (0.004)	-0.016*** (0.003)	-0.014** (0.049)
Not Disclosed	15	0.013 (0.708)	0.008 (0.582)	-0.018 (0.234)
Other	53	-0.012* (0.096)	-0.007 (0.249)	-0.004 (0.379)
Personal	164	-0.004** (0.046)	-0.008** (0.036)	-0.005 (0.152)
Test of differences				
F-test (ANOVA)		1.93 (0.124)	0.76 (0.515)	0.37 (0.774)

Notes:
1) *P*-values reported in parentheses are based on standard errors
2) * *p* <0,10, ** *p* <0,05, *** *p* <0,01
3) Calculated by authors using Stata16

The test reveals that financial information loss significantly impacts the market. Thus, average CAR (-1,+1) is -1.3%, CAR (-3,+3) is -1.6% at 1% significance level, and CAR (-5,+5) is -1.4% at 5% level. Personal information loss also negatively impacts CAR at a 5% significance level, taking -0.4% and -0.8% in 1-day and 3-day event windows, respectively. Other information losses are also negative but insignificant in CAR (-3,+3) and CAR (-5,+5), while not disclosed information losses are positive but not significant in CAR (-1,+1) and CAR (-3,+3). However, the last result is meaningless due to the small sample size of not-disclosed information cases.

Running the ANOVA test indicated no significant difference in market reaction between various information losses since the p-value is 0.124, 0.515, and 0.774 for three windows greater than 0.05. Therefore, we can state that various information losses do not negatively impact CAR differently.

Correlation analysis among variables

Before running regression, the correlation analysis between all variables is carried out in this paper. The result is shown in Table 12.

It can be noticed that there is a strong positive linear relationship between CAR and ROA, indicating that companies with high ROA rates have more positive CAR than companies with lower ROA. Moreover, the correlation coefficient between CAR and records losses is -0.1985, which is statistically significant at 5%, showing that extensive records losses will decrease CAR. In addition, the correlation analysis reveals the linear relationship between CAR and the type of attack (0.12 at 5% significance level).

Furthermore, correlation analysis has shown a significant positive linear relationship between multiple attacks and firm size, ROA, and revenue. The correlation coefficients are 0.1882, 0.0961, and 0.2649, respectively, indicating that big, profitable firms with significant revenues can be a target for cyclically repeated cyberattacks. Also, a linear relationship between multiple attacks and firm type reveals that a specific firm type can be a target. In addition, the relationship between multiple attacks and types of attacks points out the fact that specific types of attacks tend to repeat.

Table 12 - Correlation between variables

	CAR	Firm size	Firm type	Type of attack	Type of information	ROA	Repeated attacks	Multiple attacks	Revenue	Number of records lost	Duration	Late Discovery	Late Disclosure
CAR	1.000												
Firm size	0.043 (0.436)	1.000											
Firm type	0.005 (0.921)	-0.004 (0.939)	1.000										
Type of attack	-0.117** (0.032)	-0.130** (0.017)	0.020 (0.713)	1.000									
Type of information	0.069 (0.210)	0.071 (0.192)	-0.098* (0.072)	0.188*** (0.000)	1.000								
ROA	0.232*** (0.000)	0.224*** (0.000)	0.127** (0.020)	-0.052 (0.338)	0.026 (0.639)	1.000							
Repeated attacks	-0.032 (0.558)	0.072 (0.190)	-0.001 (0.980)	0.001 (0.986)	0.064 (0.240)	0.007 (0.896)	1.000						
Multiple attacks	-0.031 (0.566)	0.188*** (0.000)	0.098* (0.073)	-0.128** (0.019)	0.046 (0.396)	0.096* (0.078)	0.462*** (0.000)	1.000					
Revenue	0.052 (0.345)	0.814*** (0.000)	-0.028 (0.611)	-0.196*** (0.000)	-0.018 (0.737)	0.396*** (0.000)	0.068 (0.214)	0.265*** (0.000)	1.000				
Number of records lost	-0.198** (0.020)	0.115 (0.183)	0.134 (0.118)	-0.146* (0.089)	0.064 (0.461)	0.125 (0.147)	-0.095 (0.272)	0.101 (0.239)	0.132 (0.125)	1.000			
Duration	-0.027 (0.754)	0.113 (0.189)	-0.032 (0.714)	-0.321*** (0.000)	-0.050 (0.561)	0.022 (0.802)	0.033 (0.704)	-0.018 (0.834)	0.020 (0.816)	0.036 (0.792)	1.000		
Late Discovery	-0.028 (0.768)	0.176** (0.061)	-0.074 (0.437)	-0.396*** (0.000)	-0.095 (0.316)	0.063 (0.509)	0.057 (0.544)	0.039 (0.680)	0.121 (0.198)	0.083 (0.572)	0.938*** (0.000)	1.000	
Late Disclosure	0.007 (0.923)	0.084 (0.252)	-0.026 (0.726)	-0.121 (0.101)	0.017 (0.814)	0.043 (0.563)	-0.018 (0.812)	-0.075 (0.307)	0.019 (0.795)	-0.128 (0.273)	0.895*** (0.000)	0.962*** (0.000)	1.000

Notes:
1) *P*-values reported in parentheses are based on standard errors
2) * p <0,10, ** p <0,05, *** p <0,01
3) Calculated by authors using Stata16

It should be noted that *type of attack* defines the *number of record losses*, *duration, late discovery, and delay* in disclosure of the breach. The last three variables have a significant strong relationship since they have almost the same basis of information.

Regression analysis of CAR

Ordinary least squares (OLS) regressions have been established to determine which factors are responsible for a negative CAR mean. This paper tries to explain the impact of various variables such as *Firm size, Firm type, Type of information, Type of attack, repeated attacks* within one year, *multiple attacks* for the decade, *Return on Assets* (ROA), and the natural logarithm of *Revenue*, *Number of Records Lost, Duration, Late Disclosure* and *Late Discovery* of the attacks on dependent variable CAR (-1,+1). Table 13 presents the output of the regression results.

ROA and Revenue are used as determinants of firm performance. Repeated attacks and multiple attacks are dummy variables that take a value equal to one if cyber-attacks are repeated and zero otherwise.

In Regression (1), we define that the coefficient of small-sized firms is significant at a 10% level, indicating that small firms have a lower average CAR than the largest ones by -2.2%. Moreover, coefficients on cyberattacks, such as *Phishing*, *Ransomware,* and *Unauthorised Access*, are negative and significant. For example, phishing decreases average CAR by 1.9% compared to malware attacks at a 5% significance level. Moreover, ransomware decreases CAR's mean by 2.3% at a 5% significance level, compared with malware. Likewise, unauthorised access can drop CAR more harmful than malware by 2.3% at a 1% significance level.

Furthermore, financial information losses can decrease CAR by 1.3% at a 5% level, compared with personal information losses. We can notice that ROA positively impacts CAR. Increasing ROA for one rate tends to increase the average CAR by 7.3% at a 1% level, indicating that, on average, firms with high ROA do not have a negative breach impact. In terms of the explanatory power of the regression model, adjusted R^2 is not large enough, revealing that independent variables explain only 7.4% of the variability CAR. Even though the *F*-statistic is significant at a 1% level since the p-value is 0.002, it indicates that the Regression (1) is meaningful.

Table 13 - OLS regressions of CAR (-1,+1)

Independent variables	**CAR (-1,+1)**					
	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**
Firm size						
-small	-0.022* (0.095)	-0.014 (0.346)	-0.030 (0.222)	-0.029 (0.276)	-0.021 (0.291)	-0.017 (0.579)
-medium	-0.004 (0.681)	0.006 (0.610)	-0.014 (0.478)	-0.004 (0.866)	-0.007 (0.625)	-0.016 (0.536)
-big	-0.012 (0.141)	-0.003 (0.731)	-0.030** (0.047)	-0.027* (0.090)	-0.022* (0.066)	-0.025 (0.219)
Firm type						
- Transport and communications	-0.009 (0.286)	0.004 (0.703)	-0.024 (0.116)	-0.030** (0.050)	-0.021* (0.084)	0.002 (0.901)
- Wholesale trade	0.015 (0.246)	0.001 (0.954)	0.028 (0.207)	0.008 (0.743)	0.027 (0.173)	0.021 (0.407)
- Retail trade	-0.006 (0.494)	0.008 (0.389)	-0.008 (0.600)	-0.017 (0.379)	-0.008 (0.524)	0.038 (0.103)
- Financial firms	-0.006 (0.503)	-0.002 (0.878)	0.005 (0.749)	0.001 (0.944)	0.003 (0.824)	-0.024 (0.345)
- Services	-0.004 (0.523)	0.004 (0.655)	0.007 (0.584)	0.012 (0.320)	0.003 (0.735)	-0.009 (0.531)
- Mining, oil, and gas	0.064 (0.156)		0.072 (0.165)	0.077 (0.130)	0.065 (0.174)	
- Construction	-0.013 (0.679)	-0.001 (0.968)	-0.038 (0.463)	-0.007 (0.888)	-0.023 (0.492)	-0.026 (0.457)

Type of attack						
Malware/Phishing	-0.048 (0.288)	-0.055* (0.081)	-0.044 (0.380)		-0.048 (0.304)	
Misconfiguration	-0.014 (0.278)	-0.023 (0.147)	-0.026 (0.297)	-0.013 (0.676)	-0.003 (0.896)	
Not Disclosed	-0.012 (0.092)	-0.012 (0.129)	-0.006 (0.659)	-0.003 (0.870)	-0.007 (0.492)	-0.029* (0.093)
Phishing	-0.019** (0.024)	-0.015 (0.121)	-0.021 (0.158)	-0.006 (0.700)	-0.019 (0.101)	-0.012 (0.537)
Ransomware	-0.023** (0.045)	-0.006 (0.789)	-0.003 (0.859)	-0.003 (0.869)	-0.009 (0.566)	0.013 (0.652)
Unauthorized Access	-0.023*** (0.009)	-0.019** (0.042)	-0.021 (0.148)	-0.021 (0.208)	-0.026** (0.026)	-0.028* (0.060)
Type of information						
Financial	-0.013** (0.040)	-0.015** (0.012)	-0.007 (0.562)	-0.005 (0.680)	-0.015 (0.110)	-0.017 (0.280)
Not Disclosed	0.031** (0.017)		0.040* (0.071)	0.082*** (0.002)	0.028 (0.143)	
Other	-0.007 (0.324)	0.021 (0.421)	-0.011 (0.533)	-0.023 (0.172)	-0.009 (0.423)	
Repeated attacks	-0.003 (0.771)	-0.012 (0.315)	0.019 (0.368)	0.013 (0.563)	0.022 (0.180)	0.039* (0.095)
Multiple attacks	-0.005 (0.499)	-0.012* (0.079)	-0.021 (0.102)	-0.035*** (0.009)	-0.021** (0.032)	-0.049*** (0.005)
Revenue	-0.004 (0.124)	0.0001 (0.971)	-0.005 (0.288)	-0.002 (0.787)	-0.003 (0.417)	-0.004 (0.502)
ROA	0.073*** (0.000)	0.040 (0.281)	0.109* (0.072)	0.152** (0.031)	0.085* (0.076)	-0.015 (0.855)
Number of Records lost		-0.002*** (0.005)				-0.002 (0.315)
Duration of the attack			4.27e-06 (0.874)			
Late discovery				5.53e-06 (0.828)		-3.18e-06 (0.931)
Late disclosure					5.54e-07 (0.967)	
Intercept	0.112* (0.078)	0.030 (0.687)	0.145 (0.230)	0.054 (0.689)	0.095 (0.301)	0.149 (0.371)
Observations	337	137	138	114	186	49
***F*-Statistic**	2.16*** (0.002)	1.46 (0.103)	1.26 (0.213)	1.86** (0.021)	1.37 (0.127)	1.60 (0.123)
Adj. R^2	0.074	0.069	0.043	0.148	0.046	0.201

Notes:
1) *P*-values reported in parentheses are based on standard errors
2) * *p* <0,10, ** *p* <0,05, *** *p* <0,01
3) Calculated by authors using Stata16

In Regression (2), we include the number of records lost as an additional explanatory variable. As a result, the sample becomes smaller due to a lack of information about losses, consisting of 137 observations. The Number of Records Lost passed the t-test at the significance level of 1%. Thus, on average, increasing the number of record losses by 1% tends to decrease CAR by 0.20%, ceteris paribus. However, the F-test does not pass the significance level, which means the regression model has no statistical meaning.

Then, it is decided to explore how the attack's longevity, the company's cybersecurity reaction to disclose it, and the delay of the public announcement will affect the stock price reaction. According to the correlation analysis, they have a strong linear relationship, and that is why they are considered to be used separately in the regression model.

In Regression (3), we add the Duration of the cyber-attack to examine whether there is a relationship between CAR and breach longevity. The number of observations is 138. The regression model does not pass the F-test since the p-value (0.203) is more than 0.05. Therefore, the regression model has no statistical meaning. Duration as a variable also has no explanatory power since the p-value is more significant than 0.05.

In Regression (4), variable Duration is replaced with variable Late Discovery to identify whether the weakness of the firm's cyber-security system can impact CAR. Although the Duration coefficient is insignificant since the p-value is more significant than 0.1, the regression passes the F-test at the significance level of 5%, indicating that the regression is meaningful. All variables in the regression model can explain about 14.8% of the variability of CAR.

In Regression (5), Late Discovery is replaced with the additional explanatory variable Late Disclosure to explore how disclosure delay affects shareholders wealth. The analysis result in Table 13 reveals that the regression model does not have a statistical meaning since the p-value of the F-test is 0.127, and it is more significant than 0.05.

Regressions 3,4,5 has a minimal number of observations since not all firms that experienced cyber-attacks publicly announce breaches' start and discovery date, and they try to hide this information as maximum as possible. Thus, we have only 138 observations indicating the incident's start and end dates for calculating the Duration variable. Moreover, there are only 114 firms in the sample when adding the Late Disclosure variable, using differences between announcement and start dates. Furthermore, we have only 186 firms with available information for a sample with Late Discovery.

In Regression (6), we combined Regression (2) with the variable Late Discovery. The sample size shrunk to 49 observations since not all the firms have the number of records lost and breach start and discovery dates. As a result, the sample becomes very small and does not have a statistical meaning since the p-value of the F-statistic is 0.123, more significant than 0.05.

Overall, it can be noticed that adjusted R^2 rates are small, and our regressions do not have sufficient explanatory power. Nevertheless, the F-statistics are large and significant at a 1% level in Regression (1) and a 5% level in Regression (4) since the P-value of F-statistics are 0.002 and 0.021, respectively. The last regression has the highest adjusted R squared (20.11%). However, the number of observations is too small (49 breaches), and the F-statistic is also small and insignificant (p-value=0.123). That is why the result of Regression (6) does not have a meaning.

Conclusions

This study explored the impact of cybersecurity breaches on the company's overall performance. A significant negative impact on the firm's value is identified. Moreover, the influence of various firm-specific parameters and characteristics on the cumulative abnormal return of the company in the cybersecurity event dates was studied. The hypotheses tests reveal that only firm size can differently impact CAR. It is determined that small firms have a significant drop in firm's value due to the cyber-attack. This can indicate that smaller firms do not invest in security technology as big ones. Consequently, small firms should try to increase their expenditures to create a reliable security system. Additionally, the paper defines no consistent evidence that market reaction to cyberattacks depends on firm and breach types.

There are some limitations in providing this research. There are different databases for collecting cybersecurity breach incidents, such as the Audit Analytics database, Privacy Rights Clearinghouse, ProQuest, ABIInforms. Moreover, they have a different number of registered cybersecurity breaches and various types of information. Therefore, the results depend on which database is used, leading to different outputs. Thus, having reliable sources of cyber-crime incidents will allow us to understand better the relationship between cyberattacks and a firm's performance.

References

1. 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

2. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70-104. https://doi.org/10.1080/10864415.2004.11044320

3. Chen, X., Bose, I., Leung, A. C. M., & Guo, C. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems*, *50*(4), 662-672. https://doi.org/10.1016/j.dss.2010.08.020

4. Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, *8*(4), 27-55. https://doi.org/10.1080/15536548.2012.10845665

5. Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: what do investors think?. *Inf. Secur. J. A Glob. Perspect.*, *12*(1), 22-33. https://doi.org/10.1201/1086/43325.12.1.20030301/41478.5

6. Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74-83. https://doi.org/10.1108/09685220310468646

7. Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*, *49*(2), 503-519. https://doi.org/10.1111/fima.12274

8. 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

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

10. Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*(6), 461-485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

11. Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, *19*(1), 33-56. https://doi.org/10.3233/JCS-2009-0398

12. Hiscox. (2020). *Hiscox cyber readiness report 2020.* [cited 10 August, 2023]. Available at: Hiscox_Cyber_Readiness_Report_2020_UK.PDF

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

14. Hovav, A. & D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security, 13*(3), 32-40. https://doi.org/10.1201/1086/44530.13.3.20040701/83067.5

15. Hovav, A., Han, J., & Kim, J. (2017). Market reaction to security breach announcements: Evidence from South Korea. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *48*(1), 11-52. https://doi.org/10.1145/3051473.3051476

16. Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of marketing*, *82*(2), 85-105. https://doi.org/10.1509/jm.16.0124

17. Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*(5), 681-695. https://doi.org/10.1016/j.im.2018.11.003

18. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). *What is the impact of successful cyberattacks on target firms?* (No. w24409). National Bureau of Economic Research.

19. Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security*, *2017*(4), 18-20. https://doi.org/10.1016/S1361-3723(17)30034-9

20. MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of economic literature*, *35*(1), 13-39.

21. Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58. https://doi.org/10.1509/jm.15.0497

22. Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135-155. https://doi.org/10.1007/s11747-016-0495-4

23. McWilliams, A., & Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *Academy of management journal*, *40*(3), 626-657. https://doi.org/10.5465/257056

24. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not?. *Decision Support Systems*, *56*, 11-26. https://doi.org/10.1016/j.dss.2013.04.004

25. Murphy, H. & Bond, S. (2019). Capital One data breach sparks cloud security fears. *Financial Times.* [cited 14 August, 2023]. Available at: https://www.ft.com/content/5b3046ca-b2d4-11e9-bec9-fdcab53d6959

26. SIC-NAICS. (2021). SIC Code and NAICS Code Business List. [cited 10 July 2023]. Available at: http://siccode.com

27. Warrell, H. (2019). Malicious software attacks ‘spiralling out of control’, report warns. *Financial Times*. [cited 10 July 2023]. Available at: https://www.ft.com/content/f3cc4243-5942-46d0-8d26-ee757c8f225f

Information about the authors

Gulmira K. Issayeva – Cand. Sc. (Econ.), Professor, M. Auezov South Kazakhstan University, Shymkent, Kazakhstan, email: gulmira_issaeva@mail.ru, ORCID ID: https://orcid.org/0000-0001-9459-357X
***Elmira E. Zhussipova** – PhD, Senior Lecturer, M. Auezov South Kazakhstan University, Shymkent, Kazakhstan, email: elmira_zhusipova@mail.ru, ORCID ID: https://orcid.org/0000-0001-7363-8214
Ainura N. Aitymbetova – Cand. Sc. (Econ.), Associate Professor, Head of the Department of Finance, M. Auezov South Kazakhstan University, Shymkent, Kazakhstan, email: a-ainura.81@mail.ru, ORCID ID: https://orcid.org/0000-0002-1907-8591
Alma S. Kuralbayeva – Doc. Sc. (Econ.), Professor, Central Asian Innovation University, Shymkent, Kazakhstan, email: kuralbayeva.a@gmail.com
Damira B. Abdykulova – Senior Lecturer, M. Auezov South Kazakhstan University, Shymkent, Kazakhstan, email: dami_bax@mail.ru

Авторлар туралы мәліметтер

Исаева Г.К. – э.ғ.к., профессор, М.Әуезов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан, email: gulmira_issaeva@mail.ru, ORCID ID: https://orcid.org/0000-0001-9459-357X
***Жусипова Э.Е.** – PhD, аға оқытушы, М.Әуезов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан, email: elmira_zhusipova@mail.ru, ORCID ID: https://orcid.org/0000-0001-7363-8214
Айтымбетова А.Н. – э.ғ.к., қауымдастырылған профессор, «Қаржы» кафедрасының меңгерушісі, М.Әуезов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан, email: a-ainura.81@mail.ru, ORCID ID: https://orcid.org/0000-0002-1907-8591
Куралбаева А.Ш. – э.ғ.д., профессор, Орталық Азия инновациялық университеті, Шымкент, Қазақстан, email: kuralbayeva.a@gmail.com
Абдыкулова Д.Б. – аға оқытушы, М.Әуезов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан, email: dami_bax@mail.ru

Сведения об авторах

Исаева Г.К. – к.э.н., профессор, ЮКУ им. М.Ауэзова, Шымкент, Казахстан, email: gulmira_issaeva@mail.ru, ORCID ID: https://orcid.org/0000-0001-9459-357X
***Жусипова Э.Е.** – PhD, старший преподаватель, ЮКУ им. М.Ауэзова, Шымкент, Казахстан, email: elmira_zhusipova@mail.ru, ORCID ID: https://orcid.org/0000-0001-7363-8214
Айтымбетова А.Н. - к.э.н., ассоциированный профессор, заведующая кафедрой «Финансы», ЮКУ им. М.Ауэзова, Шымкент, Казахстан, email: a-ainura.81@mail.ru, ORCID ID: https://orcid.org/0000-0002-1907-8591
Куралбаева А.Ш. – д.э.н., профессор, Центрально-Азиатский инновационный университет, Шымкент, Казахстан, email: kuralbayeva.a@gmail.com
Абдыкулова Д.Б. – старший преподаватель, ЮКУ им. М.Ауэзова, Шымкент, Казахстан, email: dami_bax@mail.ru