Role of Cyber-Risk on shaping the movement of stock returns: An event study on T-Mobile Company

دور المخاطر السيبرانية في تشكيل حركة عوائد الأسهم :
دراسة حدث لشركة T-Mobile

Dr. Samira M. Allam

Faculty of Business, Ain Shams University- ASU, Egypt.
Faculty of Business, Badr University in Cairo- BUC, Egypt

samira.allam@bus.asu.edu.eg

Dr. Mohamed Abdelraouf

Faculty of Business, Badr University in Cairo- BUC, Egypt
Faculty of Management & Technology, Arab Academy for Science and Technology and Maritime Transport- AAST, Egypt
mohamedabdelraouf04@gmail.com

مجلة الدراسات التجارية المعاصرة

كلية التجارة – جامعة كفر الشيخ
المجلد الثامن . العدد الخامس عشر- الجزء الثاني
يناير ٢٠٢٣م
رابط المجلة : **https://csj.journals.ekb.eg**

Abstract

Cyber risk has become a major concern for companies as the frequency and severity of cyber-attacks have increased. Giving the actual data, the current study aims to investigate the impact of the cyber-risk on T-Mobile company stock returns. T-Mobile company has suffered from six data breaches between the period of 2015 and 2023. The event study was used to test the impact of data breach announcements on T-Mobile Company's stock returns. The findings show that data breaches have a significant impact on companies' financial performance, as indicated by the abnormal returns observed following the announcement of data breaches which were observed in 2015, 2018, and 2021; alternatively, it vanished in 2019, 2020, and 2023.The study may be valuable for practitioners and academics interested in how cyberattacks influence the financial industry. Moreover, results have a significant implication for businesses, investors, and politicians in terms of enhancing risk management techniques and reducing potential, financial and reputational harm caused by such attacks. However, more research is needed to understand the factors driving the variation in timing and magnitude of abnormal returns following data breach announcements.

Keywords: Cyber-risk, Data breach, Event study, Stock returns.

المستخلص:

أصبحت المخاطر السيبرانية مصدر قلقاً كبيراً للشركات نتيجة ازدياد شدة تلك الهجمات وتكراراها ، وذلك بالرجوع إلى بيانات فعلية ، وبالتالي فأن الدراسة الحالية تهدف إلى التحقق من تأثير هذه المخاطر على حركة عوائد أسهم شركة T-Mobile. عانت الشركة محل الدراسة من ستة عمليات استهدفت اختراق البيانات الخاصة بها في الفترة من ٢٠١٥ حتى ٢٠٢٣ وقد تم استخدام دراسة الحدث من أجل اختبار تأثير الإعلان عن تلك الاختراقات التي عانت منها الشركة على عوائد الأسهم الخاصة بها ، وقد تم التوصل إلى أن هناك تأثيرا ً معنويا ً لتلك الاختراقات على الأداء المالي لتلك الشركة محل الاختبار. وقد أُثبت معنوية هذا التأثير استنادا ً إلى ظهور العوائد غير العادية التابعة لعملية الإعلان عن اختراق البيانات في الأعوام ٢٠١٥ ، ٢٠١٨ و ٢٠٢١. على النقيض أن تلك العوائد قد تلاشت في الأعوام ٢٠١٩، ٢٠٢٠ و ٢٠٢٣ . تنبع أهمية الدراسة الحالية من كونها تعد ذا أهمية لكلٍ من الأكاديمين ، والممارسين المعنيين بتأثير المخاطر السيبرانية على الأسواق المالية. علاوةً على ذلك فأن النتائج تعد ذا أهمية جوهرية لمجالات الأعمال من مستثمرين و سياسيين فيما يخص تعزيز تقنيات إدارة المخاطر وتقليل الضرر المحتمل سواء على الصعيد المالي أو السمعة التي قد تنجم عن تلك الهجمات. وبالرغم من ذلك فهناك إحتياج إلى المزيد من البحث لفهم العوامل التي تؤدي إلى التباين في حجم وتوقيت العوائد غير العادية الناجمة عن الإعلان عن وجود عملية إختراق.

الكلمات المفتاحية : المخاطر السيبرانية ، إختراق البيانات ، دراسة حدث ، عوائد الأسهم .

1. Introduction

In recent decades, the globe has seen a remarkable transformation. The ability to keep up with the rapid pace of change and technological innovation is an outstanding instrument for advancement (Panetta, 2018).

The conventional approaches to providing financial services have been altered by fintech developments. Greater business efficiency, market diversification, decentralization, and reshaped communication channels between financial service providers and customers have all made room for more transparency and financial inclusion. Faster, less expensive, and more readily available digital financial services are another example. Fintech does, however, have flaws and may pose serious risks to the financial system. The negative aspects of fintech include cyber danger, dependency on Internet connectivity, the possibility of data and privacy breaches, lack of regulatory frameworks, the volatility of cryptocurrencies, and lack of competition as a result of Big Tech's significant impact (Vučinić & Luburić, 2022).

The increasing use of fintech has led to an increased need for corporations to pay attention to cyber risk. While fintech has revolutionized the financial industry, it has also made financial transactions more vulnerable to cyber-attacks Kopp *et al*. (2017), Ryu (2018), Vučinić *et al*. (2022) the cyber world is getting increasingly sophisticated, and so are the risks it faces MCITP (2019) ,widespread and intricate Kraus, Kraus, & Shtepa (2022) . As a result, the impact of cyber-attacks on the movement of stocks corporations has become an important concern for investors and companies alike (Khakan, Mostafiz and Najaf, 2021).

Fintech includes a variety of services and activities; moreover, technological innovations have altered the lines of communication between financial service providers and customer bringing with them new behaviors Panetta (2018) ,Vučinić *et al*. (2022). The effect showed that financial technology is considered a significant factor that can cause redrawing the movement in financial markets.

The globe is becoming a potential target for cyberattacks as the usage of digital technologies expands; they merely take a worldview. It is incorrect to believe that just a small number of nations are responsible for these cyberattacks, and that, as a result, additional limitations may be placed on them. Indeed, cybercriminals may launch an assault from anyplace (Vučinić *et al*. 2022).

In many ways, cyber risk has been around since the dawn of the internet itself. Technology has progressed and so have the techniques employed by hackers to bypass protections. In addition to financial losses, cyberattacks may have an effect on a company's reputation, create a drop in consumer confidence, halt operations, steal data, and lead to the theft or loss of intellectual property Leroy (2022) , Aldasoro *et al*. (2022), inflict severe harm Panetta (2018) . Cybersecurity issues used to be a problem for the banking sector's corporate operations Gai, Qiu, & Elnagdy (2016), and are categorized as an operational risk (Bouveret, 2018).

Cyber risk refers to the chance of suffering damage or loss as a consequence of a breach in cybersecurity measures implemented by an organization or of malicious behaviour conducted online. Companies in today's interconnected world are forced to defend themselves against a wide range of cyberattacks (Jaiswal *et al*. 2021; Chaudhary *et al*. 2022).

According to Baldoni (2019) one of the most common kinds of online danger is called malware, and it refers to a kind of software that is designed to interfere with, damage, or gain unauthorized access to a computer system or network. Malware occurs in many different forms, including viruses, trojan horses, and worms. In addition to that, it has the potential to do significant damage to an organization's processes as well as its data.

Phishing is a different kind of cyber-attack that includes deceiving individuals into disclosing sensitive information like passwords, credit card numbers, or other personal data. To obtain sensitive data, cybercriminals frequently use email or other communication channels to pretend to be reputable organizations (Prakash *et al*. 2019).

Cyber risks frequently include Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks. In these assaults, a computer system or network is overloaded with traffic or requests resulting in a crash or user unavailability (Cetinkaya, Ishii & Hayakawa, 2019).

Another sort of cyber risk is social engineering, which includes persuading someone to divulge private information or take a step that might jeopardize a network or computer system. Hence, social engineering techniques pose a serious risk to company security since they might be hard to spot (Smith, Papadaki, & Furnell, 2013).

Moreover, Advanced Persistent Threats (APTs) are persistent, targeted assaults against certain people or organizations with the goal of obtaining unauthorized access to confidential data or intellectual property. For many businesses, these assaults provide a substantial issue since they can be very complex and hard to identify (Chowdhary, 2019).

An insider threat may be particularly harmful to a company's cybersecurity since the perpetrators will already have easy access to sensitive information and infrastructure. Employees, vendors, or other trusted parties may be the source of a data breach if they intentionally or recklessly handle the sensitive information they have access to. Among the many kinds of cybercrime is intellectual property theft (IP) (Hadlington, 2018).

Another threat is that hackers use ransomware encrypt data belonging to an organization and demand payment, generally in cryptocurrency, in return for the decryption key. Since it may disrupt operations and result in considerable financial losses, this kind of assault can be disastrous for enterprises. Ransomware attacks may also lead to the loss of confidential information or IP, which might have long-lasting effects on a company (Brewer, 2016).

A data breach occurs when an unauthorized party gains access to sensitive or confidential information. This type of security incident can take place in a variety of ways, such as hacking, phishing, or physical theft of data storage devices. The sensitive information that is typically targeted in a data breach includes personal data such as names, addresses, social security numbers, and financial information, as well as intellectual property, trade secrets, and other confidential business data (Cease, 2014).

Therefore, when managing cyber risk, corporations must overcome a number of obstacles. The main difficulty is that the danger landscape is always changing. So, corporations must be ahead of the curve to secure their assets since cybercriminals are continuously coming up with new ways for penetrating security systems. The second obstacle is the lack of qualified employees to handle the cyber risk inside the corporation (Kosub, 2015).

The announcement of a cyber-attack on a corporation can have a significant impact on its stock price, as investors may panic and sell off their shares, leading to a drop in the stock price. The cost of remedying the damage can also affect the financial performance of a corporation; thus, a further decline in stock prices may occur Tosun (2021). The impact of cyber-attacks on stock prices and financial performance may not be immediately apparent. Sometimes this impact can take months or even years to become fully apparent. Hence, it will become difficult for companies to accurately assess the true extent of the damage and take appropriate action (Paté-Cornell *et al*. 2018).

In addition, it is difficult to accurately quantify the potential financial impact of cyber-attacks, which hinders predicting the exact cost of this type of risk as this impact can depend on a wide range of factors such as the type of data that is compromised, the level of disruption caused, and the company's reputation Zhan *et al*. (2015) , Reddick (2009), Carayon & Kraemer, (2006). In addition to the loss of customer trust or reputational damage, the above mentioned consequences can have long-lasting impacts on a company's performance (Chowdhury, 2016; Agrafiotis *et al*. 2016).

In a letter that he wrote in September 2015, T-Mobile CEO John Legere addressed a data breach that had happened at their vendor, Experian, which handled credit applications for T-Mobile. Claims that the breach affected almost 15 million customers who applied for T-Mobile service or device finance between September 1, 2013, and September 16, 2015, (Legere, 2015).

Once more, in August 2021, T-Mobile was the target of a cyberattack that had a negative impact on 76.6 million Americans. Customers of T-Mobile filed the class action case, which was resolved for $500 million. Of that money, $150 million will be used to upgrade T-Cybersecurity Mobile's technologies and defences, while $350 million will be used to address customer claims. No one payment to a T-Mobile customer should be more than $2,500 according to the proposed settlement (Corkery, 2022).

Lastly, in the discovery that occurred in 2023, almost 37 million T-Mobile customers have been affected by the data breach. The amount paid by T-Mobile in reaction to the 2022 data breach is not specified in the official statement, although the company paid $350 million to settle customer claims from a class action lawsuit coming from an earlier data leak. Google Fi, which lists T-Mobile as one of its network partners, was also affected by the same hack in terms of client data. (Condon, 2023).

2. Research motivation

Cyber-attacks have become a significant threat to businesses, and their impact on stock price is a crucial area of research. As the financial industry increasingly relies on technology, fintech services have emerged to improve accessibility and innovation. However, they also pose new risks that need to be addressed which reflects the motive of current study. Thus, cyber risk in particular, is a critical challenge for businesses, as it can result in significant financial and reputational costs. As technology continues to evolve, businesses must remain vigilant and take proactive measures to mitigate the risks associated with cyber-attacks and other forms of cyber risk.

3. Literature review

Cyber-attacks have become a growing concern for businesses in recent years. This literature review explores the relationship between cyberattacks and the movement of stock prices. It provides an overview of the independent variable, which is cyber-attacks, including their types, causes, and consequences. It then delves into the dependent variable, which is the movement of stock prices, including the methods used to study this relationship and the factors that influence the extent of stock price fluctuations.

Mention (2019) explored the field of fintech by studying its impact on the financial landscape. Fintech encompasses both innovative financial services made possible by technology and the organizational frameworks that support them. Any invention that seeks to improve the production, delivery, and the use of financial services can be considered fintech in a broader sense. Additionally, regulators are taking notice of fintech as it presents new challenges and opportunities for oversight, including protecting customer data privacy and promoting financial inclusion.

According to Ernst and Young (2017) investigation, the legacy financial institutions in developed economies will be forced to clarify their strategies, build new capabilities, and change their cultures as a result of this trend, even though its effects have so far been most noticeable in developing economies like China and India. While Gobble (2018) discovered that fintech businesses have arisen as industry disruptors by using technology to provide fresh, cutting-edge financial services that are often more practical, effective, and affordable than conventional financial services. Treleaven (2015) found that many sorts of fintech exist, including payments and transfers, lending and financing, personal finance, and cryptocurrencies.

Jenik and Lauer (2017) found that fintech has several positive aspects, including enhanced accessibility, cost-effectiveness, and innovation. Jaksic and Marinc (2019) fintech does, however, also have significant drawbacks, like security issues, lack of regulation, and inadequate customer assistance. Hence, cyberattacks may target fintech services, putting users' financial and personal information at risk. Since fintech services are often exempt from the same rules as conventional financial services, fraud may occur. Therefore, fintech services may be fully digital denying clients the chance to get the in-person assistance they need in certain circumstances.

According to Haizler (2017) the concept of cyber risk is a relatively new phenomenon, with the term only gaining traction following the rise of the internet in the 1990s. The first notable incident of cybercrime occurred in 1988, when a computer science student named Robert Morris released a worm that infected thousands of computers across the United States. Eisenberg explained that since this incident, cyber threats have continued to evolve and become more sophisticated, making them increasingly difficult to detect and prevent.

Strupczewski (2021), Hossain *et al*. (2022), investigated the cyber risk and found that it referred to the potential damage, loss, or disruption to an organization's operations or assets resulted from a breach or attack on its computer systems or networks. It encompassed a broad range of potential threats, including data breaches, hacking, malware, phishing attacks, and distributed denial of service (DDoS) attacks Suryateja (2018). Abu Bakar et al (2020) found that the problem of cyber risk is one that is continually developing, and as technology develops, so do the potential threats that come with it.

According to Xuan, Dao, & Nguyen (2020), Advanced Persistent Threats (APTs) and Intellectual Property (IP) theft are two specific types of cyber risk that can pose significant threats to organizations. APTs are described as sophisticated and stealthy attacks carried out by skilled and persistent adversaries who aim to gain access to a system or network and remain undetected for a prolonged period of time. This caused severe damage to the organization under attack by stealing sensitive data, disrupting operations, or even using the compromised network as a launching pad for further attacks. On the other hand, IP theft refers to the stealing of an organization's proprietary information, such as trade secrets, designs, and other intellectual property.

Ghafir and Prenosil (2014) argued that APTs and IP theft are serious cyber risks that can result in significant financial, competitive advantage losses, and reputational damage for organizations. They also recommend training employees on cybersecurity best practices and investing in appropriate technologies and solutions to effectively manage these specific types of cyber risks.

Leuprecht, Skillicorn, and Tait (2016) and Solhaug *et al*. (2015) argued the history and types of cyber risk, as well as the costs, challenges, and obstacles associated with it and explained that cyber risk can take many forms from data breaches to hacking attacks, and it can have significant financial and reputational costs for businesses.

Li and Liu (2021) noted that cyber risk can take many different forms, including targeted assaults on particular firms as well as more extensive and pervasive attacks on entire sectors. They suggested that understanding the various forms of cyber risk and their potential impacts is essential for organizations to effectively manage these risks and develop appropriate cybersecurity strategies.

Nathan and Scobell (2020) pointed out that cyber risk can result in significant financial and reputational costs for businesses. IBM Security stated that the average cost of a data breach in 2020 was $3.86 million, which includes expenses such as lost income and damage to brand reputation. Direct costs related to the incident, such as legal fees and computer repairs, are also factored into this figure. Utzig, Mane, and Mikua (2023) highlighted that cyber risk can have far-reaching consequences, including a loss of customer confidence and trust, which can be difficult to restore. Even if a company took a swift action to mitigate the impact of a cyber incident, customers may be hesitant to do business with them again due to concerns about the safety and security of their personal information.

Serra-Ruiz *et al*. (2016) argued that the constantly evolving threat landscape is a significant barrier to effectively managing cyber risk. Cybercriminals are continuously devising new tactics to exploit vulnerabilities and access sensitive information, which necessitates a proactive approach to cybersecurity. However, many businesses faced the challenge of limited resources and a shortage of skilled personnel, which can hinder their ability to implement effective cybersecurity measures. Hammoudeh *et al*. (2017) asserted that the constantly evolving nature of cyber threats and protective measures makes it challenging for many small and medium-sized organizations to keep up. As a result, these organizations may lack the resources or expertise required to effectively prevent and respond to cyberattacks.

Akande (2021) highlighted the problem of ransomware attacks as an example of the constantly evolving nature of cyber risk and the challenges they pose for businesses. To explain, ransomware is a virus that encrypts an organization's data and makes it inaccessible until a ransom is paid. Payne and Mienie (2021) indicated that cyber attackers are constantly developing new tactics to make ransomware attacks more sophisticated, such as the use of double extortion where data is not only encrypted but also stolen and threatened with public release until the ransom is paid. Which reflected the ever-evolving nature of cyber risk and the need for businesses to stay up to date with the latest protective measures to avoid potential financial and reputational damage.

Coburn, Leverett, and Woo (2018) highlighted the potential impact of cyber risk on a corporation's stock price, as investors may lose confidence in the firm after a cyber event, such as a data breach or ransomware attack. Moreover, the potential reputational damage that could result from a widely reported cyberattack can cause long-term harm to the brand's image, further impacting stock values. This was in line with Zou and Schaub (2018), the news of the breach caused investor anxiety about the possible financial and reputational repercussions of the event, which caused Equifax's stock price to decline by around 14% in the days after the breach. Similar to this, Manworren, Letwat, & Daily (2016), concluded that data breach at Target in 2013 resulted in the exposure of some 40 million consumers' credit card details. In the days after the breach notification, the company's stock price decreased by almost 10%.

In the same regard, Wojcik (2012) explained that in addition to the direct financial costs associated with a cyber incident, such as legal fees and IT remediation, companies may also experience indirect costs such as lost business and damage to their reputation. While Uma and Padmavathi (2013) inferred that customers might lose trust in the company's ability to protect their sensitive data resulting in a loss of sales and revenue. This can have a long-term impact on the company's stock prices (Huang, Ye, and Stuart Madnick, 2019).

Say and Vasudeva (2020) suggested that investors may view cyber risk as an indication of a company's overall risk management and governance practices. They noted that a cyber incident can lead to a decline in investor confidence and a drop in stock prices if the company is seen as having inadequate risk management practices. This effect may be particularly pronounced if the company has a history of cyber incidents or if the incident is seen as resulting from negligent or inadequate cybersecurity practices.

Durbin (2017) proved that in the current digital era, with the increasing prevalence and sophistication of cyber-attacks, businesses need to adopt a proactive and comprehensive approach to cybersecurity. He concluded that to mitigate the risks associated with cyber incidents and protect their stock prices, companies should invest in the latest tools and technology, establish robust cybersecurity policies and procedures, and regularly test and update their systems.

Al-Zaben *et al.* (2018) defined a data breach as the unauthorized access, exposure, or theft of personally identifiable information (PII). On the other hand, Lagazio, Sherif, and Cushman (2014), suggested that data breaches can occur due to a variety of factors, including hacking, phishing, and malware attacks. Sensitive data can be compromised resulting in significant financial losses and reputational damage for those affected.

Solove, Liu, & Citron (2017) highlighted the fact that identity theft, in which personal details like names, addresses, and account numbers are exploited, is a common outcome of data breaches. Identity theft may have devastating effects, including harm to a person's income, credit, and reputation.

Zou and Schaub (2019) suggested that there are several actions that both individuals and businesses can take to prevent data breaches, including using strong passwords, implementing two-factor authentication, regularly updating software, and providing personnel with training on data security best practices. Daly (2018) indicated that in the event of a data breach, prompt steps should be made to adopt remedial actions such as informing potentially impacted persons, investigating, and enhancing data security protocols. The harm from the breach may be reduced by taking these measures, and future instances can be avoided. Luijf, Besseling, & De Graaf (2013) emphasized that in today's digital world, data breaches are a common risk that individuals and businesses must be aware of. It is crucial to take proactive measures to safeguard private data and prevent potential threats. Jones *et al*. (2019) conducted research on the impact of cybercrime on publicly traded companies' stock values by gathering financial data from companies that had been identified as victims of cybercrime in news publications. Then they emphasized the gravity of cybercrime, not only in terms of lost profits and stolen property but also in terms of reputational damage to a company, which can eventually cause its stock market value to decline.

The results of the study showed that stock prices had a detrimental effect during each of the time periods examined, with one of them having a particularly significant influence, which demonstrated how cybercrime impacts the company's stock market value (Smith *et al.* 2019).

In conclusion, it has been shown that cyber-attacks significantly lower a company's stock price. As technology advances, organisations confront an increasing risk of data breaches, hacking, malware, and phishing attacks. Fintech, or the financial technology sector, has become a significant industry disruptor by offering unique financial services that are both more accessible and more affordable than the alternatives. As a result, fintech has flaws as well, such as poor security, a lack of regulation, and subpar customer service. In order to lessen the likelihood of being hacked or suffering other losses related to financial technology, organisations need to take preventative measures against cybersecurity threats, such as performing regular risk assessments, maintaining constant monitoring, and developing strong incident response plans. The literature emphasised the significance of understanding the relationship between cyberattacks and stock prices, as well as the importance for businesses to take a proactive approach to cybersecurity in order to secure their operations, assets, and sensitive data. This calls for attention and sheds light on the defects and damages that may result, not only for the disadvantages that are cyber risk considered one of them.

4. Developing Hypotheses & Research Methodology

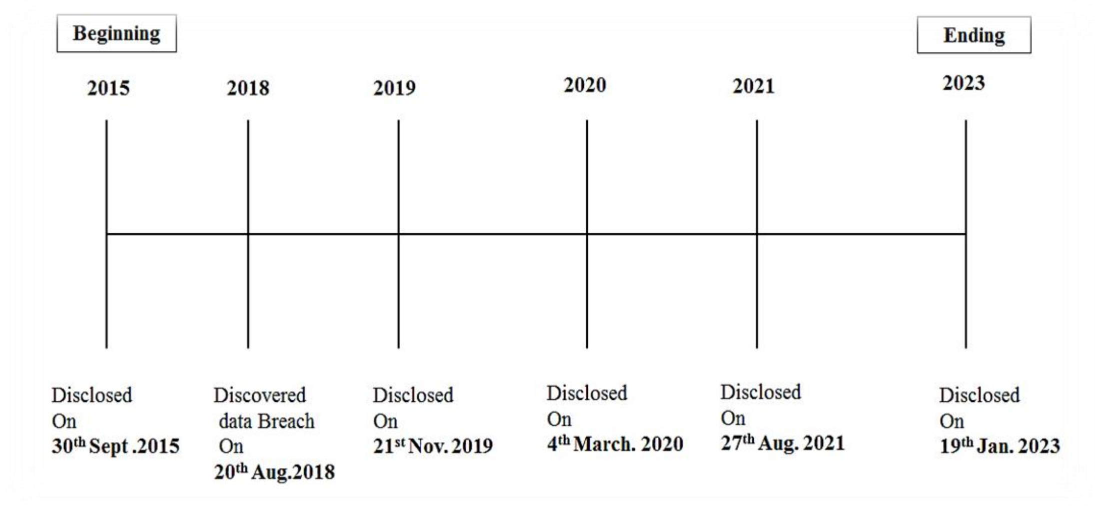
Despite the rising concern over data breaches, few studies have assessed the financial impact of cyber-attacks on a company's reputation or even on the market value of its shares. The cost of data breaches has received most attention in the literature, but the effects on a company's stock have not been well explored. So, this study seeks to concentrate on how the financial market reacts to this operational risk by tracking the movement of stock returns before and after the data breach announcement. One way to measure the impact of cyberattacks on a company is to conduct an event study of stock price fluctuations, which is a statistical method used to determine the impact of a specific event on the value of a company's stock. Hence, the study aims to test the following hypothesis:

There are no statistically significant differences between abnormal returns before announcing data breaches and those after these announcements in the company (T-Mobile US).

T-Mobile US is a telecommunications company headquartered in Bellevue, Washington, USA, where it provides wireless voice and data services, as well as mobile broadband services to over 100 million customers in the United States, Puerto Rico, and the U.S. Virgin Islands. T-Mobile US, Inc. is one of the largest providers of wireless communication services in the United States and has a market capitalization of over $170 billion as of March 2023. The company operates a nationwide 5G network and has partnerships with major technology companies such as Apple, Samsung, and Google to offer a wide range of devices and services to its customers. The study population includes all events of the announcement about data breaches for T-Mobile US, (TMUS) from 2015 to 2023.

Figure (1) shows these announcements as follows:

Figure (1): Announcement of Data Breaches


Beginning
Ending
2015
2018
2019
2020
2021
2023
Disclosed On 30th Sept .2015
Discovered data Breach On 20th Aug.2018
Disclosed On 21st Nov. 2019
Disclosed On 4th March. 2020
Disclosed On 27th Aug. 2021
Disclosed On 19th Jan. 2023

Source: T-Mobile letter (2015,2021,2023)

According to figure (1), there are six data breach announcements made between 2015 and 2023. The hypothesis which mainly focused on the market response to these events could be tested using the event study methodology to test the significance between abnormal returns using Wilcoxon Signed-Rank Test. The calculation for the Z value in a Wilcoxon Signed-Rank Test is dependent on the specific data being analyzed. The general process of conducting a Wilcoxon Signed Rank Test.

The null hypothesis is that:
`` There are no statistically significant differences between abnormal returns before announcing data breaches and those after these announcements in the company (T-Mobile US)``.

The alternative hypothesis is that:

`` There are statistically significant differences between abnormal returns before announcing data breaches and those after these announcements in the company (T-Mobile US)``.

Therefore, the differences between the two related variables are calculated and ranked by absolute value, and the sign of the difference is then ignored. The Wilcoxon Signed-Rank Test involves calculating the sum of the positive and the negative ranks, while the test statistic is the smaller of these two sums. Finally, the Z value is calculated using the test statistic and the sample size. The p-value is then calculated using a standard normal distribution table, and the null hypothesis is rejected if the p-value is less than the significance level.

4. Results of Empirical Work

After calculating the actual returns, we estimate the normal returns using the market model using the NASDAQ index, then we estimate the abnormal returns. To test the normality of abnormal returns, the following table summarizes testing normality using Kolmogrov-Smirnov test:

Table (I): Testing normality of the abnormal returns using Kolmogrov-Smirnov Test.

DAY	2015		2018		2019		2020		2021		2023	
	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.
-40	0.144	0.036	0.171	0.005	0.083	.200*	0.235	0.000	0.105	.200*	0.087	.200*
-35	0.157	0.029	0.169	0.013	0.091	.200*	0.237	0.000	0.139	0.085	0.095	.200*
-30	0.124	.200*	0.145	0.109	0.094	.200*	0.224	0.001	0.153	0.072	0.090	.200*
-25	0.149	0.160	0.157	0.114	0.114	.200*	0.213	0.005	0.146	0.180	0.089	.200*
-20	0.140	.200*	0.173	0.120	0.118	.200*	0.209	0.022	0.129	.200*	0.119	.200*
-15	0.138	.200*	0.255	0.010	0.181	.200*	0.149	.200*	0.145	.200*	0.143	.200*
-10	0.143	.200*	0.194	.200*	0.219	0.189	0.207	.200*	0.192	.200*	0.183	.200*
-5	0.233	.200*	0.304	0.147	0.259	.200*	0.316	0.115	0.286	.200*	0.331	0.077
Event Day	30, Sept		6, Sept		21, Nov		4, March		27, Aug		19, Jan	
5	0.255	.200*	0.245	.200*	0.408	0.007	0.214	.200*	0.231	.200*	0.400	0.009
10	0.191	.200*	0.236	0.121	0.328	0.003	0.138	.200*	0.219	0.189	0.188	.200*
15	0.124	.200*	0.210	0.073	0.189	0.156	0.140	.200*	0.121	.200*	0.132	.200*
20	0.117	.200*	0.161	0.184	0.170	0.134	0.126	.200*	0.105	.200*	0.146	.200*
25	0.111	.200*	0.119	.200*	0.152	0.140	0.153	0.137	0.108	.200*	0.137	.200*
30	0.100	.200*	0.131	0.197	0.170	0.027	0.104	.200*	0.124	.200*	0.133	0.183
35	0.118	.200*	0.110	.200*	0.129	0.147	0.108	.200*	0.121	.200*	0.123	0.198
40	0.107	.200*	0.098	.200*	0.135	0.064	0.097	.200*	0.127	0.105	0.154	0.017

As indicated by the significance levels associated with Z values, for all research periods during the years before and after the announcement of the T-Mobile data breach, daily abnormal returns deviate from normal.

Table II summarizes the descriptive statistics of abnormal returns for various time periods before and after the data breach announcement, ranging from 5 to 40 days. The table displays the mean and standard deviation for each time period.

Table (II): Testing the descriptive statistics of abnormal returns.

DAY	2015		2018		2019		2020		2021		2023	
	Mean	Std.	Mean	Std.	Mean	Std.	Mean	Std.	Mean	Std.	Mean	Std.
-40	0.002	0.012	0.001	0.016	0.002	0.010	-0.004	0.020	-0.002	0.010	0.000	0.016
-35	0.002	0.012	0.002	0.017	0.002	0.011	-0.005	0.021	-0.003	0.011	0.000	0.017
-30	0.002	0.012	0.003	0.017	0.003	0.011	-0.006	0.023	-0.003	0.011	0.000	0.017
-25	0.001	0.013	0.002	0.018	0.003	0.012	-0.006	0.025	-0.003	0.010	0.001	0.016
-20	0.003	0.013	0.000	0.007	0.004	0.013	-0.009	0.027	-0.003	0.010	0.000	0.015
-15	0.003	0.014	-0.001	0.006	0.006	0.013	-0.004	0.014	-0.002	0.011	0.000	0.017
-10	0.003	0.016	-0.003	0.007	0.006	0.014	-0.002	0.013	-0.006	0.011	0.000	0.019
-5	-0.003	0.018	0.001	0.006	-0.002	0.011	0.000	0.016	-0.010	0.006	-0.009	0.012
Event Day	30, Sept		6, Sept		21, Nov		4, March		27, Aug		19, Jan	
5	-0.005	0.009	0.007	0.018	0.004	0.010	-0.006	0.037	-0.007	0.006	-0.007	0.021
10	-0.004	0.013	0.004	0.013	0.005	0.011	-0.007	0.032	-0.006	0.007	-0.011	0.025
15	-0.002	0.012	0.004	0.011	0.005	0.010	-0.003	0.029	-0.005	0.009	-0.007	0.022
20	-0.005	0.016	0.003	0.011	0.004	0.009	-0.005	0.030	-0.003	0.010	-0.004	0.020
25	-0.005	0.017	0.004	0.011	0.002	0.009	-0.001	0.028	-0.002	0.011	-0.002	0.020
30	-0.005	0.017	0.004	0.010	0.002	0.009	-0.001	0.025	-0.004	0.012	-0.003	0.018
35	-0.004	0.020	0.003	0.011	0.002	0.008	-0.001	0.024	-0.004	0.012	-0.002	0.017
40	-0.004	0.020	0.003	0.014	0.001	0.008	0.001	0.023	-0.005	0.014	-0.001	0.018

Table (III) illustrates the significance of variation among abnormal returns comparing those of days -40: -5 with those of days 5: 40, using Wilcoxon Signed Rank Test, as follows:

Table (III): Testing Hypothesis using Wilcoxon Signed Rank Test.

Period	**2015**		**2018**		**2019**		**2020**		**2021**		**2023**	
	30, Sept		**6, Sept**		**21, Nov**		**4, March**		**27, Aug**		**19, Jan**	
	Z	**Sig.**	**Z**	**Sig.**	**Z**	**Sig.**	**Z**	**Sig.**	**Z**	**Sig.**	**Z**	**Sig.**
Day -5: Day 5	-.135-^{b}	0.893	-.674-^{b}	0.500	-.674-^{b}	0.500	-.135-^{b}	0.893	-.944-^{b}	0.345	-.135-^{b}	0.893
Day -10: Day10	-1.070-^{b}	0.285	-1.682-^{c}	0.093	-.051-^{b}	0.959	-.255-^{c}	0.799	-.866-^{b}	0.386	-.415-^{c}	0.678
Day -15: Day 15	-1.306-^{b}	0.191	**-1.931-^{c}**	**0.043**	-.114-^{c}	0.910	-.057-^{c}	0.955	**-1.647-^{b}**	**0.040**	-1.079-^{c}	0.281
Day -20: Day 20	**-2.016-^{b}**	**0.044**	-.821-^{c}	0.411	-.112-^{c}	0.911	-.448-^{b}	0.654	-1.344-^{b}	0.179	-.261-^{c}	0.794
Day -25: Day 25	-.605-^{b}	0.545	-.982-^{c}	0.326	-.471-^{c}	0.638	-.982-^{b}	0.326	-1.440-^{b}	0.150	-.444-^{c}	0.657
Day -30: Day 30	**-2.026-^{b}**	**0.043**	-.876-^{c}	0.381	-.134-^{b}	0.894	-.668-^{b}	0.504	-.586-^{b}	0.558	-.648-^{c}	0.517
Day -35: Day 35	-1.425-^{b}	0.154	-.622-^{c}	0.534	-.311-^{c}	0.756	-1.163-^{b}	0.245	-.753-^{b}	0.451	-.106-^{b}	0.915
Day -40: Day 40	-1.438-^{b}	0.150	-1.143-^{c}	0.253	-.242-^{c}	0.809	-1.479-^{b}	0.139	-1.317-^{b}	0.188	-.343-^{c}	0.732

[1] Illustration of a, b and c

Table III shows the results of the Wilcoxon Signed Rank Test used to test the hypothesis of significant abnormal returns before and after the data breach announcements. The table presents the Z-score and significance level (Sig.) for each time period, separated by the year and date of the announcement.

The findings indicate that data breaches have a significant impact on the companies' financial performance as demonstrated by the abnormal returns observed across different years. Abnormal returns were observed at different

[1] Note: denotes a. Wilcoxon Signed Ranks Test, denotes b. Based on positive ranks, and denotes c. Based on negative ranks.

time intervals following the announcement of data breaches in 2015, 2018, and 2021.

In 2015, abnormal returns were observed both 20 and 30 days following the data breach announcement, while in 2018, they were observed only 15 days after the announcement. This finding suggests that investors in 2018 may have been more sensitive to the news of the data breach than in 2015, potentially, due to the severity or scope of the breach, or market conditions prevailing at the time.

Additionally, in 2021, abnormal returns were observed only 15 days after the announcement of the data breach. This result implies that the market may have become more efficient in responding to data breaches over time, potentially, due to increasing awareness of cyber risk and improving risk management practices by companies.

The absence of abnormal returns in 2019, 2020, and 2023 suggests that investors did not perceive those breaches to have a significant impact on the company's stock return. It is possible that the company's response to the breaches was more effective, or that those breaches were less severe than those occurred in the years where abnormal returns were observed. However, more research is needed to understand the factors driving the variation in the timing and magnitude of abnormal returns following data breach announcements.

Overall, the findings underscore the importance of timely and transparent disclosure of data breaches to investors and stakeholders, as well as the need for companies to have effective response and remediation plans in place to minimize the impact on their stock performance.

5. Conclusions

Based on the efficient market hypothesis, there is an effect of information on prices and returns. This study highlights the significance of cyber-attacks as a growing operational risk for companies. It finds that data breaches can have a significant impact on the companies' financial performance as evidenced by abnormal returns observed following the announcement of data breaches in different years for T-Mobile Company. The results demonstrate that data breaches have a clear role on shaping the movement of stock returns, as seen by the abnormal returns in 2015, 2018, and 2021 following the declaration of data breaches; alternatively, it disappeared in 2019, 2020, and 2023.

This indicates that companies that experience a cyber-attack or data breach often experience a significant decrease in their stock price due to the damage to their reputation, financial performance, and investor confidence. The study's findings might be valuable for practitioners and academics interested in learning more about how cyberattacks influence the financial industry. Moreover, the results have significant implications for businesses, investors, and politicians in terms of enhancing risk management techniques and reducing the potential financial and reputational harm caused by cyber-attacks. This aim requires an early upfront notification of data breaches, effective response, repair procedures, continual monitoring and assessment of cyber risk with the fast growth of fintech and the rising complexity of cyber-attacks. To prevent stock price swings, corporations must take necessary precautions to defend against cyber-attacks and data breaches. Further research is necessary to comprehend the factors responsible for the differences in the size and timing of abnormal returns subsequent to the disclosure of data breaches. These factors can help in explaining why financial markets react differently to such events. To elucidate the market response, a new research approach combining traditional and behavioral finance can be pursued. This amalgamation can be extended to other fields such as customer loyalty, where it can serve as an explanatory variable for distinct reactions.

References

Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Roberts, T. and Upton, D.M., 2016. Cyber harm: concepts, taxonomy and measurement, doi: 10.2139/ssrn.2828646

Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T., 2022. The drivers of cyber risk. *Journal of Financial Stability*, *60*, p.100989, doi: 10.1016/j.jfs.2022.100989

Ali, A., Septyanto, A.W., Chaudhary, I., Al Hamadi, H., Alzoubi, H.M. and Khan, Z.F., 2022, February. Applied Artificial Intelligence as Event Horizon Of Cyber Security. In *2022 International Conference on Business Analytics for Technology and Security (ICBATS)* (pp. 1-7). IEEE, doi: 10.1109/ICBATS54253.2022.9759076

Alshamrani, A., Myneni, S., Chowdhary, A. and Huang, D., 2019. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), pp.1851-1877, doi: 10.1109/COMST.2019.2891891

Al-Zaben, N., Onik, M.M.H., Yang, J., Lee, N.Y. and Kim, C.S., 2018, August. General data protection regulation complied blockchain architecture for personally identifiable information management. In *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 77-82). IEEE, doi: 10.1109/iCCECOME.2018.8658586

Arcuri, M.C., Brogi, M. and Gandolfi, G., 2017, January. How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns. In *ITASEC* (pp. 175-193).

Arcuri, M.C., Brogi, M. and Gandolfi, G., 2018. The effect of cyber-attacks on stock returns. *Corporate Ownership & Control*, *15*(2), pp.70-83, doi: 10.22495/cocv15i2art6

Barati, M. and Yankson, B., 2022. Predicting the Occurrence of a Data Breach. *International Journal of Information Management Data Insights*, *2*(2), p.100128, doi: 10.1016/j.jjimei.2022.100128

Beaman, C., Barkworth, A., Akande, T.D., Hakak, S. and Khan, M.K., 2021. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, p.102490, doi: 10.1016/j.cose.2021.102490

Biener, C., Eling, M. and Wirfs, J.H., 2015. Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*, pp.131-158, doi: 10.1057/gpp.2014.19

Biju, J.M., Gopal, N. and Prakash, A.J., 2019. Cyber attacks and its different types. *International Research Journal of Engineering and Technology*, *6*(3), pp.4849-4852.Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*, *2016*(9), 5-9.

Bouveret, A., 2018. *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Cease, C.C., 2014. Giving out your number: A look at the current state of data breach litigation. *Ala. L. Rev.*, *66*, p.395.

Cetinkaya, A., Ishii, H. and Hayakawa, T., 2019. An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy*, *21*(2), p.210, doi: 10.3390/e21020210

Chowdhury, A., 2016. Recent cyber security attacks and their mitigation approaches–an overview. In *Applications and Techniques in Information Security: 6th International Conference, ATIS 2016, Cairns, QLD, Australia, October 26-28, 2016, Proceedings 7* (pp. 54-65). Springer Singapore, doi: 10.1007/978-981-10-2741-3_5

Cimpanu, (2020) *T-Mobile says Hacker gained access to employee email accounts, User Data, ZDNET*. Available at: https://www.zdnet.com/article/t-mobile-says-hacker-gained-access-to-employee-email-accounts-user-data/?ftag=COS-05-10aaa0h (Accessed: March 21, 2023).

Cimpanu, (2021) *T-mobile discloses its fourth data breach in three years*, *ZDNET*. Available at: https://www.zdnet.com/article/t-mobile-discloses-its-fourth-data-breach-in-three-years/ (Accessed: March 22, 2023).

Coburn, A., Leverett, E. and Woo, G., 2018. *Solving cyber risk: protecting your company and society*. John Wiley & Sons.

Condon (2023) *T-mobile reports another data breach, impacting 37 million customers, ZDNET*. Available at: https://www.zdnet.com/article/t-mobile-reports-another-data-breach-impacting-37-million-customers/ (Accessed: March 22, 2023).

Corkery, M. (2022) *T-mobile reaches $500 million settlement in huge 2021 data breach, The New York Times*. The New York Times. Available at: https://www.nytimes.com/2022/07/22/business/t-mobile-hacking-settlement.html (Accessed: March 22, 2023).

Corkery, M. (2022) *T-mobile reaches $500 million settlement in huge 2021 data breach, The New York Times*. The New York Times. Available at: https://www.nytimes.com/2022/07/22/business/t-mobile-hacking-settlement.html (Accessed: March 22, 2023).

Daly, A., 2018. The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law & Security Review*, *34*(3), pp.477-495, doi: 10.1016/j.clsr.2018.01.005

Do Xuan, C., Dao, M.H. and Nguyen, H.D., 2020. APT attack detection based on flow network analysis techniques using deep learning. *Journal of Intelligent & Fuzzy Systems*, *39*(3), pp.4785-4801, doi: 10.3233/JIFS-200694

Durbin, S., 2017. Identifying, Analyzing, and Evaluating Cyber Risks. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, pp.97-107, doi: 10.1002/9781119309741.ch7

Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., Lynn, M.S. and Santoro, T., 1989. The Cornell commission: on Morris and the worm. *Communications of the ACM*, *32*(6), pp.706-709, 10.1145/63526.63530

Ey (2018) *EY Fintech Adoption Index: Fintech services poised for mainstream adoption in the US with 1 in 3 digitally active consumers using FinTech, PR Newswire: press release distribution, targeting, monitoring and marketing*. Available at: https://www.prnewswire.com/news-releases/ey-fintech-adoption-index-fintech-services-poised-for-mainstream-adoption-in-the-us-with-1-in-3-digitally-active-consumers-using-fintech-300481126.html (Accessed: March 15, 2023).

Gai, K., Qiu, M. and Elnagdy, S.A., 2016, April. A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 171-176). IEEE, doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.65

Ghafir, I. and Prenosil, V., 2014. Advanced persistent threat attack detection: an overview. *Int J Adv Comput Netw Secur*, *4*(4), p.5054.

Gobble, M.M., 2018. Digitalization, digitization, and innovation. *Research-Technology Management*, *61*(4), pp.56-59, doi: 10.1080/08956308.2018.1471280

Greig, (2021) *T-mobile hack: Everything you need to know*, *ZDNET*. Available at: https://www.zdnet.com/article/t-mobile-hack-everything-you-need-to-know/ (Accessed: March 23, 2023).

Hackers help themselves to data belonging to 2 million T-Mobile customers (no date) *ZDNET*. Available at: https://www.zdnet.com/article/international-hackers-help-themselves-to-data-belonging-to-2-million-t-mobile-customers/ (Accessed: March 20, 2023).

Hadlington, L.J., 2018. Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom, doi: 10.5281/zenodo.1467909

Huang, K., Ye, R. and Madnick, S., 2019. Both Sides of the Coin: The Impact of Cyber Attacks on Business Value, doi: 10.2139/ssrn.3699756

Haizler, O. (2017). The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking. *Cyber, Intelligence, and Security*, *1*(1), 31-45.

Islam, U., Muhammad, A., Mansoor, R., Hossain, M.S., Ahmad, I., Eldin, E.T., Khan, J.A., Rehman, A.U. and Shafiq, M., 2022. Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. *Sustainability*, *14*(14), p.8374, doi: 10.3390/su14148374

Jakšič, M. and Marinč, M., 2019. Relationship banking and information technology: The role of artificial intelligence and FinTech. *Risk Management*, *21*, pp.1-18, doi: 10.1057/s41283-018-0039-y

Jenik, I. and Lauer, K., 2017. Regulatory sandboxes and financial inclusion. *Washington, DC: CGAP*.

Kopp, E., Kaffenberger, L. and Jenkinson, N., 2017. Cyber Risk, Market Failures, and Financial Stability, International Monetary Fund.

Kosub, T., 2015. Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*, pp.615-634, doi: 10.1007/s12297-015-0316-8

Kraemer, S.B., 2006. *An adversarial viewpoint of human and organizational factors in computer and information security*. The University of Wisconsin-Madison.

Kraus, K., Kraus, N. and Shtepa, O., 2022. Practice of the implementation cyber security and financial inclusion at the micro-, macro-and global levels of the economy. *VUZF review*, *7*(2), pp.25-40, doi: 10.38188/2534-9228.22.2.03

Lagazio, M., Sherif, N. and Cushman, M., 2014. A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, pp.58-74, doi: 10.1016/j.cose.2014.05.006

Legere, J. (2015) *A letter from CEO John Legere on experian data breach - t-mobile newsroom*, *T*. Available at: https://www.t-mobile.com/news/blog/experian-data-breach (Accessed: March 19, 2023).

Leroy, I., 2022. The relationship between cyber-attacks and dynamics of company stock: the role of reputation management. *International*

Journal of Electronic Security and Digital Forensics, *14*(4), pp.309-317, doi: 10.1504/IJESDF.2022.123891

Leuprecht, C., Skillicorn, D.B. and Tait, V.E., 2016. Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, *33*(2), pp.250-257, doi: 10.1016/j.giq.2016.01.012

Li, Y. and Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, pp.8176-8186, doi: 10.1016/j.egyr.2021.08.126

Luiijf, E., Besseling, K. and De Graaf, P., 2013. Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6*, *9*(1-2), pp.3-31, doi: 10.1504/IJCIS.2013.051608

Manworren, N., Letwat, J. and Daily, O., 2016. Why you should care about the Target data breach. *Business Horizons*, *59*(3), pp.257-266, doi: 10.1016/j.bushor.2016.01.002

MCITP, M., 2019. The risk of artificial intelligence in cyber security and the role of humans.

Mention, A.L., 2019. The future of fintech. *Research-Technology Management*, *62*(4), pp.59-63, doi: 10.1080/08956308.2019.1613123

Najaf, K., Mostafiz, M.I. and Najaf, R., 2021. Fintech firms and banks sustainability: why cybersecurity risk matters?. *International Journal of Financial Engineering*, *8*(02), p.2150019, doi: 10.1142/S2424786321500195

Nathan, A.J. and Scobell, A., 2020. Off-Grid Solar Market Trends Report 2020. *Int. Financ. Corp*, *91*(5), p.215.

Panetta, F., 2018. Fintech and banking: today and tomorrow. *Speech of the Deputy Governor of the Bank of Italy, Rome*, *12th May*.

Paté-Cornell, M.E., Kuypers, M., Smith, M. and Keller, P., 2018. Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, *38*(2), pp.226-241, doi: 10.1111/risa.12844

Payne, B. and Mienie, E., 2021, June. Multiple-Extortion Ransomware: The Case for Active Cyber Threat Intelligence. In *ECCWS 2021 20th European Conference on Cyber Warfare and Security* (p. 331). Academic Conferences Inter Ltd, doi: 10.34190/EWS.021.075

Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N. and Jaiswal, A.K., 2021. A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), pp.669-710, doi: 10.18535/ijsrm/v9i12.ec04

Reddick, C.G., 2009. Management support and information security: an empirical study of Texas state agencies in the USA. *Electronic Government, an International Journal*, *6*(4), pp.361-377, doi: 10.1504/EG.2009.027783

Refsdal, A., Solhaug, B., Stølen, K., Refsdal, A., Solhaug, B. and Stølen, K., 2015. *Cyber-risk management* (pp. 33-47). Springer International Publishing, doi: www.10.1007/978-3-319-23570-7_5.com

Ryu, H.S., 2018. What makes users willing or hesitant to use Fintech?: the moderating effect of user type. *Industrial Management & Data Systems*, *118*(3), pp.541-569, doi: 10.1108/IMDS-07-2017-0325

Sabillon, R., Cavaller, V., Cano, J. and Serra-Ruiz, J., 2016, June. Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1-9). IEEE, doi: 10.1109/ICCCF.2016.7740434

Saleem, J., Adebisi, B., Ande, R. and Hammoudeh, M., 2017, July. A state of the art survey-Impact of cyber attacks on SME's. In *Proceedings of the international conference on future networks and distributed systems*, doi: 10.1145/3102304.3109812

Say, G. and Vasudeva, G., 2020. Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches. *Strategy Science*, *5*(2), pp.117-142, doi: 10.1287/stsc.2020.0106

Smith, Aaron, Maria Papadaki, and Steven M. Furnell. "Improving awareness of social engineering attacks." In *Information Assurance and Security Education and Training: 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Zealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brazil, July 27-31, 2009, Revised Selected Papers 8*, pp. 249-256. Springer Berlin Heidelberg, 2013, doi: 10.1007/978-3-642-39377-8_29

Smith, K.T., Jones, A., Johnson, L. and Smith, L.M., 2019. Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1), pp.42-60, doi: 10.1108/JICES-02-2018-0010

Sohime, F.H., Ramli, R., Rahim, F.A. and Bakar, A.A., 2020, August. Exploration study of skillsets needed in cyber security field. In *2020 8th International Conference on Information Technology and Multimedia (ICIMU)* (pp. 68-72). IEEE, doi: 10.1109/ICIMU49871.2020.9243448

Solove, D.J. and Citron, D.K., 2017. Risk and anxiety: A theory of data-breach harms. *Tex. L. Rev.*, *96*, p.737.

Strupczewski, G., 2021. Defining cyber risk. *Safety science*, *135*, p.105143, doi: 10.1016/j.ssci.2020.105143

Suryateja, P.S., 2018. Threats and vulnerabilities of cloud computing: a review. *International Journal of Computer Sciences and Engineering*, *6*(3), pp.297-302, doi: 10.26438/ijcse/v6i3.298303

T-Mobile Newsroom (2021) *T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack.* Available at: https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation (Accessed: March 23, 2023).

Tosun, O.K., 2021. Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, p.101795, doi: 10.1016/j.irfa.2021.101795

Treleaven, P., 2015. Financial regulation of FinTech. *Journal of Financial Perspectives*, *3*(3).

Ucci, D., Aniello, L. and Baldoni, R., 2019. Survey of machine learning techniques for malware analysis. *Computers & Security*, *81*, pp.123-147, doi: https://doi.org/10.1016/j.cose.2018.11.001

Uma, M. and Padmavathi, G., 2013. A Survey on Various Cyber Attacks and their Classification. *Int. J. Netw. Secur.*, *15*(5), pp.390-396.

Utzig, M., Mane, A.K. and Mikuła, A., 2023. Digital trust and information and communication technology usage in households: The case of European countries. In *Trust, Digital Business and Technology* (pp. 169-184). Routledge.

Vučinić, M. and Luburić, R., 2022. Fintech, risk-based thinking and cyber risk. *Journal of Central Banking Theory and Practice*, *11*(2), pp.27-53, doi: 10.2478/jcbtp-2022-0012

Wash (2023) *T-mobile informing impacted customers about unauthorized activity*, *T-Mobile Business*. Available at: https://www.t mobile.com/news/business/customer-information (Accessed: March 23, 2023).

Wojcik, J., 2012. Cyber insurance not always enough. *Business Insurance*, *46*(16), p.4.

Zhan, Z., Xu, M. and Xu, S., 2015. Predicting cyber attack rates with extreme values. *IEEE Transactions on Information Forensics and Security*, *10*(8), pp.1666-1677, doi: 10.1109/TIFS.2015.2422261

Zou, Y. and Schaub, F., 2018, April. Concern But No Action: Consumers' Reactions to the Equifax Data Breach. In *Extended abstracts of the 2018 CHI conference on human factors in computing systems* (pp. 1-6), doi: 10.1145/3170427.3188510

Zou, Y. and Schaub, F., 2019. Beyond mandatory: Making data breach notifications useful for consumers. *IEEE Security & Privacy*, *17*(2), pp.67-72, doi: 10.1109/MSEC.2019.2897834

Appendix

Table (I): Testing normality of the abnormal returns using Kolmogrov- Smirnov Test.

DAY	2015		2018		2019		2020		2021		2023	
	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.
-40	0.144	0.036	0.171	0.005	0.083	.200*	0.235	0.000	0.105	.200*	0.087	.200*
-35	0.157	0.029	0.169	0.013	0.091	.200*	0.237	0.000	0.139	0.085	0.095	.200*
-30	0.124	.200*	0.145	0.109	0.094	.200*	0.224	0.001	0.153	0.072	0.090	.200*
-25	0.149	0.160	0.157	0.114	0.114	.200*	0.213	0.005	0.146	0.180	0.089	.200*
-20	0.140	.200*	0.173	0.120	0.118	.200*	0.209	0.022	0.129	.200*	0.119	.200*
-15	0.138	.200*	0.255	0.010	0.181	.200*	0.149	.200*	0.145	.200*	0.143	.200*
-10	0.143	.200*	0.194	.200*	0.219	0.189	0.207	.200*	0.192	.200*	0.183	.200*
-5	0.233	.200*	0.304	0.147	0.259	.200*	0.316	0.115	0.286	.200*	0.331	0.077
Event Day	**30, Sept**		**6, Sept**		**21, Nov**		**4, March**		**27, Aug**		**19, Jan**	
5	0.255	.200*	0.245	.200*	0.408	0.007	0.214	.200*	0.231	.200*	0.400	0.009
10	0.191	.200*	0.236	0.121	0.328	0.003	0.138	.200*	0.219	0.189	0.188	.200*
15	0.124	.200*	0.210	0.073	0.189	0.156	0.140	.200*	0.121	.200*	0.132	.200*
20	0.117	.200*	0.161	0.184	0.170	0.134	0.126	.200*	0.105	.200*	0.146	.200*
25	0.111	.200*	0.119	.200*	0.152	0.140	0.153	0.137	0.108	.200*	0.137	.200*
30	0.100	.200*	0.131	0.197	0.170	0.027	0.104	.200*	0.124	.200*	0.133	0.183
35	0.118	.200*	0.110	.200*	0.129	0.147	0.108	.200*	0.121	.200*	0.123	0.198
40	0.107	.200*	0.098	.200*	0.135	0.064	0.097	.200*	0.127	0.105	0.154	0.017

Table (II): Testing the descriptive statistics of abnormal returns.

DAY	2015		2018		2019		2020		2021		2023	
	Mean	Std.	Mean	Std.	Mean	Std.	Mean	Std.	Mean	Std.	Mean	Std.
-40	0.002	0.012	0.001	0.016	0.002	0.010	-0.004	0.020	-0.002	0.010	0.000	0.016
-35	0.002	0.012	0.002	0.017	0.002	0.011	-0.005	0.021	-0.003	0.011	0.000	0.017
-30	0.002	0.012	0.003	0.017	0.003	0.011	-0.006	0.023	-0.003	0.011	0.000	0.017
-25	0.001	0.013	0.002	0.018	0.003	0.012	-0.006	0.025	-0.003	0.010	0.001	0.016
-20	0.003	0.013	0.000	0.007	0.004	0.013	-0.009	0.027	-0.003	0.010	0.000	0.015
-15	0.003	0.014	-0.001	0.006	0.006	0.013	-0.004	0.014	-0.002	0.011	0.000	0.017
-10	0.003	0.016	-0.003	0.007	0.006	0.014	-0.002	0.013	-0.006	0.011	0.000	0.019
-5	-0.003	0.018	0.001	0.006	-0.002	0.011	0.000	0.016	-0.010	0.006	-0.009	0.012
Event Day	**30, Sept**		**6, Sept**		**21, Nov**		**4, March**		**27, Aug**		**19, Jan**	
5	-0.005	0.009	0.007	0.018	0.004	0.010	-0.006	0.037	-0.007	0.006	-0.007	0.021
10	-0.004	0.013	0.004	0.013	0.005	0.011	-0.007	0.032	-0.006	0.007	-0.011	0.025
15	-0.002	0.012	0.004	0.011	0.005	0.010	-0.003	0.029	-0.005	0.009	-0.007	0.022
20	-0.005	0.016	0.003	0.011	0.004	0.009	-0.005	0.030	-0.003	0.010	-0.004	0.020
25	-0.005	0.017	0.004	0.011	0.002	0.009	-0.001	0.028	-0.002	0.011	-0.002	0.020
30	-0.005	0.017	0.004	0.010	0.002	0.009	-0.001	0.025	-0.004	0.012	-0.003	0.018
35	-0.004	0.020	0.003	0.011	0.002	0.008	-0.001	0.024	-0.004	0.012	-0.002	0.017
40	-0.004	0.020	0.003	0.014	0.001	0.008	0.001	0.023	-0.005	0.014	-0.001	0.018

Table (III): Testing Hypothesis using Wilcoxon Signed Rank Test.

Period	2015		2018		2019		2020		2021		2023	
	30, Sept		6, Sept		21, Nov		4, March		27, Aug		19, Jan	
	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.	Z	Sig.
Day -5: Day 5	-.135-^{b}	0.893	-.674-^{b}	0.500	-.674-^{b}	0.500	-.135-^{b}	0.893	-.944-^{b}	0.345	-.135-^{b}	0.893
Day - 10: Day10	-1.070-^{b}	0.285	-1.682-^{c}	0.093	-.051-^{b}	0.959	-.255-^{c}	0.799	-.866-^{b}	0.386	-.415-^{c}	0.678
Day - 15: Day 15	-1.306-^{b}	0.191	**-1.931-^{c}**	**0.043**	-.114-^{c}	0.910	-.057-^{c}	0.955	**-1.647-^{b}**	**0.040**	-1.079-^{c}	0.281
Day - 20: Day 20	**-2.016-^{b}**	**0.044**	-.821-^{c}	0.411	-.112-^{c}	0.911	-.448-^{b}	0.654	-1.344-^{b}	0.179	-.261-^{c}	0.794
Day - 25: Day 25	-.605-^{b}	0.545	-.982-^{c}	0.326	-.471-^{c}	0.638	-.982-^{b}	0.326	-1.440-^{b}	0.150	-.444-^{c}	0.657
Day - 30: Day 30	**-2.026-^{b}**	**0.043**	-.876-^{c}	0.381	-.134-^{b}	0.894	-.668-^{b}	0.504	-.586-^{b}	0.558	-.648-^{c}	0.517
Day - 35: Day 35	-1.425-^{b}	0.154	-.622-^{c}	0.534	-.311-^{c}	0.756	-1.163-^{b}	0.245	-.753-^{b}	0.451	-.106-^{b}	0.915
Day - 40: Day 40	-1.438-^{b}	0.150	-1.143-^{c}	0.253	-.242-^{c}	0.809	-1.479-^{b}	0.139	-1.317-^{b}	0.188	-.343-^{c}	0.732