UNIVERSITY
OF TURKU
Turku School of
Economics

The effect of information security breaches on publicly listed companies' business performance

Research about the impact of distinct information security breach types on stock market value of publicly listed companies.

Turku School of Economics
Master's thesis

Author:
B. Hendrix

Supervisors:
Dr. J. Järveläinen
Dr. E. Caron

19.07.2023
Turku

Master's thesis

Subject: Information System Security / Economics
Author: Bram Hendrix
Title: The effect of ISBs on publicly listed companies’ business performance
Supervisors: J. Järveläinen & E. Caron
Number of pages: 68 pages + appendices twelve pages
Date: 19.07.2023

Keywords: Information security breach, cyber attack, stock market response, long-term effect, abnormal returns, event study methodology.

Abstract

The negative repercussions of cyber threats on business entities are substantial. However, the existing body of research on this topic presents contradictory or imprecise findings, impeding the establishment of a consensus on effective prevention or mitigation strategies. Compounding this issue is the lack of precision and standardization in measuring and categorizing information security breaches.

This study aims to enhance our understanding of the direct and long-term impacts of information security breaches on business performance, specifically by utilizing a novel classification to measure differential impacts on the stock market value of publicly listed companies. To achieve this, the following research question is posed: What are the respective impacts of disruptive and exploitative information security breaches on the stock market value of publicly listed companies, and how do these impacts evolve over time? Drawing on prior research indicating the relevance of disruptive and exploitative characteristics in understanding the effects of information security breaches on victim companies, this study seeks to improve precision and standardization in breach measurement.

To answer the research question, an extensive quantitative analysis is conducted using the Cyber Event Database from the University of Maryland and historical stock market data. The investigation focuses on identifying correlations between information security breaches and stock market responses. The findings reveal that information security breaches significantly harm business performance in the short- and long-term, particularly when breaches exhibit exploitative characteristics. Moreover, these adverse effects persist long after the occurrence of the breach.

The outcomes of this research provide decision-makers with valuable insights to better comprehend, anticipate, and prepare for the persistent threats posed by information security breaches. Additionally, this study contributes to existing research by expanding upon previous works. Nevertheless, further research is warranted to gain a more comprehensive understanding of the intricate dynamics within cyberspace.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

In the years 2013 to 2014, Yahoo, a leading internet service provider, fell prey to a series of damaging data breaches. The breaches resulted in unauthorized access to over three billion user accounts, causing considerable harm to Yahoo's reputation and financial health. (Shankar & Mohammed, 2020.) The devastating consequences of these cyber attacks led to a nearly 20% decline in Yahoo's stock value, culminating in its acquisition by Verizon at a significantly depreciated price (Daswani & Elbayadi, 2021).

Such incidents highlight the escalating cyber threat landscape characterized by increased frequency, diversity, and associated costs (Gupta & Agarwal, 2017). The alarming rise in the magnitude of the cyber threat is also reflected in Gartner's annual report (2019), which showed a twofold increase in the average annual per-employee spending on IT security from 2012 to 2018, with leading technology companies like Microsoft or ASML dedicating more than a billion dollars to cybersecurity. According to Jovanovic (2022), the direct costs of information security breaches (hereafter, ISBs) in 2021 exceeded a staggering 6 trillion dollars. The potential fallout from these breaches, while difficult to quantify, has definitely the potential to bring organizations to the brink of bankruptcy (Tosun, 2021).

As public and private sectors grapple with the escalating cyber threats, a consensus on the best course of action remains elusive (Harry & Gallagher, 2018.). According to these researchers, this stems from the lack of precision and standardization in how cyber events are measured and categorized. The ensuing debate on the impact of ISBs on firm performance, as gauged by stock market responses, brings to light contrasting viewpoints. Most studies, such as those by Tosun (2021) and Spanos and Angelis (2016), indicate a significant short-term effect on a company's trading value following a data breach. Conversely, other studies like Kannan et al. (2007) suggest a minimal or statistically insignificant impact.

The question of long-term impacts of ISBs remains a subject of ongoing debate. Research on this topic is relatively limited, which makes it even more intriguing and worthy of investigation (Chang et al., 2020). Some researchers, such as Lewis (2002) and Chang et al. (2020), argue that these breaches can have lasting effects on a company's performance. On the other hand, studies by Tosun (2021) and Cavusoglu et al. (2004) suggest that the long-term impacts are negligible or non-existent.

Furthermore, existing research indicates that the nature of a breach influences its impact on the stock market. However, scholars often hold conflicting perspectives on this matter, such as the debate surrounding whether Denial of Service (DoS) attacks are detrimental to the stock market value of publicly listed companies. (Garg et al., 2003; Yayla & Hu, 2011.)

According to Harry and Gallagher (2018), the presence of conflicting viewpoints regarding the effects of different types of attacks on targets, organizations, and society lead to ineffective resource allocation and a failure to discern the true consequences, potentially resulting in significant harm to business performance. These authors propose a new taxonomy, which categorizes ISBs into disruptive and exploitive based on their effect on the victim organisation. The authors assert a strong argument for the efficacy of their classification system in identifying threats and elucidating their impact on businesses. By employing this classification, they provide insights into the various ways businesses are affected by these threats and further enhance the understanding of the specific nature of threats and their implications for different aspects of business operations.

1.1 Research question

By utilizing the taxonomy proposed by Harry and Gallagher (2018), this study aims to investigate whether this classification can help elucidate the conflicting literature. The primary goal is to explore if the type of ISB -whether disruptive or exploitive- influences the severity of the impact on business performance, and how these impacts evolve over time, measured by the stock market reaction. Consequently, the following research question has been formulated:

What are the respective impacts of disruptive and exploitive information security breaches on the stock market value of publicly listed companies, and how do these impacts diverge over time?

1.2 Thesis outline

The introductory chapter serves to provide an overview of the topic and furnish background information pertaining to the research questions. The second chapter, titled "Theory and Hypothesis Development," commences with a paragraph that introduces key concepts and definitions related to cyberspace, ISBs and their impact on business performance. In the subsequent paragraph, the taxonomy proposed by Harry & Gallagher (2018) is presented, elucidating its potential influence on the impacts of ISBs. Thereafter is hypothesized how ISBs impact the stock market as time progresses. Lastly, the two subsequent paragraphs delve into the significance of these impacts, while bifurcated by disruptive and exploitive characteristics. The third chapter provides a detailed overview of the methodologies employed to measure the formulated hypotheses. In the subsequent chapter, this study presents the results obtained from the analysis. The fifth and last chapter concludes with a summary of the findings and concluding remarks.

2 Theory and hypothesis development

The theoretical framework provides the conceptual and methodological foundation for this study. The relevant literature establishes a theoretical basis for the research question and hypotheses in this section. This chapter aims to demonstrate a deep understanding of the topic and establish the significance of the research by situating it within the broader theoretical context. The review of the literature will also highlight the gaps in existing knowledge, which will guide the development of hypotheses for the empirical part of the thesis.

2.1 Concepts and definitions

This section of the thesis will define and clarify the key concepts and terms relevant to the research question and hypotheses. By providing clear definitions and distinctions, the reader will be able to follow the argument and avoid confusion.

2.1.1 Events in the cyberspace

Given the varying definitions employed by authors in cyberspace, including terms like cyber attacks, cyber intrusion, cyber breach, security breaches, and others, it is essential to provide clarity regarding the key definitions that hold significance in this paper.

Cyberspace, as articulated by academics such as Liff (2012), is a globally interconnected digital environment that facilitates communication and transactions through the internet. This complex domain, as highlighted by Deibert and Rohozinski (2010), encompasses not only the physical infrastructure, such as servers and networks, but also the software, data, and human users that interact within it. It's an ever-evolving landscape, with continuous innovations and evolving threats, making its governance and security management a challenging but crucial task (Deibert & Rohozinski, 2010; Liff, 2012). One essential function of cyberspace is to serve as a platform for various cyber operations, from routine data exchange to sophisticated cyber attacks (Dunn Cavelty, 2013).

Information security events and cyber events, while closely related, have distinctive characteristics. According to the National Institute of Standards and Technology (NIST, 2018), an information security event is defined as "an occurrence indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant". It encompasses a broad range of incidents, such as unauthorized access, data breaches, system malfunctions, insider threats, or physical theft of information assets. Information security events can be caused by both internal and external factors and may or may not involve cyber-related elements. (NIST, 2018.)

On the other hand, a cyber event, as articulated by Householder (2017) from the Carnegie Mellon University's Software Engineering Institute, is a more specific subset of information security events that pertains to "disruptions of cyberspace that create noticeable impacts in the physical world". This usually entails attacks on computer systems, networks, or internet-connected devices, aiming at compromising data integrity, causing service disruption, or gaining unauthorized access. So, while all cyber events can be considered information security events, not all information security events are cyber events. (Householder, 2017.)

While information security events and cyber events are often perceived as negative incidents, it is important to note that this is not always the case, as highlighted by Spanos and Angelis (2016). Their research, aligned with prior definitions, indicates that information security incidents can encompass both favourable occurrences like IT investments, as well as unfavourable events such as cyber attacks. While an ISB or attack falls under the umbrella of cyber events, other occurrences like IT investments, information security incidents, and IT outsourcing can also be categorized as information security events (Spanos & Angelis, 2016).

Similarly, ISBs and cyber attacks, although sometimes used interchangeably, bear different implications. According to the International Organization for Standardization (2018), an ISB is a situation where there is a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data." This usually aligns with any incident or occurrence that has an impact on the confidentiality, integrity, or availability of information or information systems (Samonas & Coss, 2014). It's a broader term that includes not just intentional attacks but also inadvertent mishandling, such as an employee mistakenly emailing sensitive data to the wrong person (von Solms & van Niekerk, 2013). On the other hand, a cyber attack, as defined by the National Institute of Standards and Technology (NIST, 2018), is a malicious and deliberate attempt by an individual or an organization to exploit computer systems, infrastructure, or networks with the intention to create harmful effects or to compromise the integrity, confidentiality, or availability of information residing in these systems

(Stevens, 2012). Therefore, while a cyber attack is a deliberate action aiming to cause harm, an ISB can be either accidental or intentional, and it pertains more to the outcome than the intent. However, important to note, both are associated with negative consequences.

Figure 1 provides a clear illustration of how each definition leads to a more specific subgroup. While there may be instances where certain authors utilize these four definitions interchangeably, this paper strictly adheres to the definitions outlined here.

The taxonomy proposed by Harry and Gallagher (2018) holds significant relevance in this study, thus warranting explicit mention. Their definition of cyber events states, "Cyber events are defined as the result of any single unauthorized effort or the culmination of many such technical actions that threat actors, through the use of computer technology and networks, use to create a desired primary effect on a target." It is worth mentioning that their conceptualization of cyber events is solely applicable at the level of cyber attacks. However, the focus of this study lies specifically within the realm of ISBs.

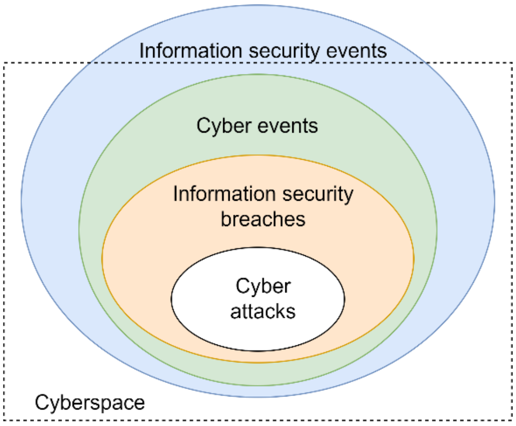

Figure 1: Events within cyberspace

2.1.2 Cyber Triad

A breach of information security fundamentally involves a compromise of the Confidentiality, Integrity, and Availability (CIA) Triad, which is the cornerstone of information security (Pfleeger et al, 2006; Samonas & Coss, 2014; Whitman & Mattord, 2012). The CIA Triad is a widely-accepted model that encapsulates the primary objectives of information security and forms the basis for various security policies, procedures, and controls (Bishop, 2003).

Confidentiality refers to the principle that information should only be accessed by authorized individuals, systems, or entities, ensuring that sensitive information is not disclosed to unauthorized parties (Pfleeger et al., 2006). A breach of confidentiality, such as a data leak, can result in unauthorized parties gaining access to sensitive information, which can lead to serious consequences, including reputational damage, financial loss, and legal implications (Campbell et al., 2003).

Integrity ensures that information and systems are protected from unauthorized modification, ensuring that data remains accurate, consistent, and trustworthy over its entire lifecycle (Pfleeger et al., 2006). Breaches of integrity, such as data tampering, can corrupt data and disrupt the functionality of systems and processes, leading to operational inefficiencies, erroneous decision-making, and a loss of trust (Harry & Gallagher, 2018).

Availability guarantees that the information systems are accessible to authorized users when required, which is essential for maintaining business continuity (Pfleeger et al., 2006). Breaches of availability, such as a denial-of-service attack, can disrupt business operations and result in financial losses and a decrease in customer satisfaction (Harry & Gallagher, 2018).

In essence, a breach in any aspect of the CIA Triad constitutes an ISB, potentially leading to significant impacts on an organization's process, reputation, and financial performance (Whitman & Mattord, 2012).

2.1.3 Cyber attacks

A diverse range of manifestations characterizes cyber attacks, and multiple definitions have been proposed to delineate their nature (e.g., Garg et al., 2003; Harry & Gallagher, 2018). The subsequent examples represent a subset of widely acknowledged instances that will be referenced in this paper.

Denial-of-Service (DoS) attack: A DoS attack is an attack that attempts to make a website, server or network unavailable by overwhelming it with traffic or requests (Gupta & Badve, 2017). According to them, a DoS attack can be carried out by a single attacker using a single computer or multiple attackers using multiple computers. The goal of a DoS attack is to disrupt the targeted service and make it unavailable to its intended users. While there are many variances of the Dos attacks, for example, SYN flood (sending so many connections requests that it either half opens or closes completely for other users), CMP flood (sending too much echo-request server, which forces a network to reply over its capacity, which results in a shutdown) or the Ping of death (sending abnormal large packets that disrupt the web server) the most common is the Distributed Denial-of-Service (DDoS) attack, which uses multiple compromised computers to flood the targeted service with traffic. (Harry and Gallagher, 2018; Gupta & Badve, 2017.)

Phishing attack: A phishing attack uses fraudulent messages or emails to deceive the recipient into providing sensitive information, for example, credit card data or login credentials (Siew Kei, 2020). He explains that a phishing attack aims to deceive the recipient into believing that the message is from a trustworthy source, such as an e-commerce or bank website. The attacker can then use the provided information for malicious purposes. As per Siew Kei's research, an overwhelming 91% of all cyber attacks initiate with a phishing email directed towards an unsuspecting victim.

Website defacement: An attack in which an attacker alters the visual appearance of a website without the owner's consent. This attack is often used to convey a political or social message, embarrass the website owner, or redirect visitors to other websites (Romagna & van den Hout, 2017). According to Romagna and van den Hout (2017), the attacker may change the website's content, add or remove images, or replace the entire website with a different page or message. In addition to causing damage to the website owner's reputation, website defacement can also be used as a stepping stone to carry out more severe attacks such as phishing, malware injection, and data theft (Garg et al., 2003; Harry & Gallagher, 2018). According to them, website defacement is a relatively common form of cyber attack, especially against websites that lack proper security measures.

Malware (injection): Malware is software developed to harm, disrupt, or gain unauthorised entry to systems, networks or computers (Roseline & Geetha, 2021). Following Roseline and Geetha (2021), malware is a broad software category that includes viruses, worms, trojans, spyware, and ransomware. Malware can infect a computer system through various means, such as email attachments, downloaded files, or infected websites. Once the malware is on the system, it can carry out various malicious activities, including stealing sensitive information, monitoring user activity, damaging files, and taking control of the system. (Roseline & Geetha, 2021.)

In this paper, the taxonomy developed by Harry and Gallagher (2018) will be presented as a framework that comprehends all cyber attacks. The taxonomy will be further examined in subsequent paragraphs.

2.1.4 Cyber events impact business performance

Business performance refers to the analysis of a company's effectiveness in achieving its goals and objectives. It includes several aspects such as financial performance, operational efficiency, market share and value, and customer satisfaction, among others. (Neely, 2005.)

In the digital age, business performance is significantly impacted by cyber events. Specifically, cyber attacks can disrupt business operations, damage reputation, and result in significant financial losses. (Böhme & Moore, 2016; Romanosky, 2016.) According to Yayla and Hu (2011), the challenge in measuring the impact of cyber events on business performance stems from the absence of accurate metrics and adequate instruments for financial analysis, as pointed out by Harry and Gallagher (2018). What complicates this analysis further is that ISBs can result in both tangible and intangible expenses (Yayla & Hu, 2011).

Tangible costs are direct, measurable expenses. These costs can include expenses such as loss of revenue, loss of productivity or cost of soft and hardware. (Yayla & Hu, 2011.) For instance, a company might need to pay professionals to restore systems, recover lost data, or defend against lawsuits resulting from the ISB (Romanosky, 2016).

Intangible costs, on the other hand, are indirect and harder to quantify. They include damage to a company's reputation, loss of consumer trust, loss of competitive advantage, and loss of investor confidence, which all could subsequently lead to a decrease in future revenue. (Yayla & Hu, 2011.) The long-term impact of these intangible costs can severely exceed the immediate tangible costs (Romanosky, 2016).

Despite numerous trade and media reports estimating the total tangible and intangible cost of ISBs, most of these numbers are merely estimations, and their reliabilities and accuracies are seldom empirically validated (Yayla & Hu, 2011). This further underscores the complexity of quantifying the impact of cyber events on business performance.

A widely employed approach for measuring business performance is the utilization of stock market data (Chang et al., 2020). Given the abundance of data sources associated with stock markets, which exhibit direct or indirect responses to diverse real-world occurrences, the task of quantifying and conducting statistical analyses on the economic ramifications of cyber events becomes increasingly concrete (Spanos & Angelis, 2016). Moreover, in accordance with the Efficient Market Hypothesis (EMH), the stock market is considered "informationally efficient", implying that the market value of a company reflects all accessible information, thus being a valid representation of a company’s performance. (Fama, 1970).

2.1.5 Stock market impact

The stock market is a platform where buyers and sellers trade shares of publicly held companies. The price of a company's stock (also referred to as a firm’market value) is influenced by numerous factors including company performance, market events, economic indicators, and market sentiment. (Madura, 2008.)

Tangible losses incurred from ISBs, such as costs associated with system recovery or legal fees, directly impact a company's economic performance. This is often reflected in the firm’s financial statements through increased expenses or reduced revenues. Investors and market analysts closely monitor these financial indicators to assess a company's profitability and growth potential. (Yayla & Hu, 2011.) Consequently, when tangible losses are significant, they lead to a decrease in the company's stock price as investors may perceive the company to be less profitable or financially stable (Cavusoglu et al., 2004; Tanimura & Wehrly, 2009).

On the other hand, intangible losses, such as damage to the company's reputation or loss of customer trust, indirectly impact the stock market value. While these losses may not be immediately evident in a company's financial statements, they can lead to a decrease in future revenues and profits, as customers may choose to take their business elsewhere. (Yayla & Hu, 2011.) This potential for future financial impact causes investors to re-evaluate the organisation's long-term options, resulting in a significant decrease in market value over time (Gatzlaff & McCullough, 2010; Yayla & Hu, 2011).

Furthermore, the disclosure of an ISB also negatively impact investor confidence and sentiment, leading to a decrease in stock price even before the tangible or intangible losses are fully realized (Campbell et al., 2003; Ali, 2021). This underlines the multi-faceted impact of cyber events on a company's stock market performance.

To calculate the effect of incidents on the stock market, an event study will be done. This is a research method used to analyse the impact of specific events (such as announcements) on the stock market. It involves examining the behaviour of stock prices and returns surrounding an event to understand how the market reacts to that event. (Chang et al., 2020.)

Returns refer to the changes in the value of a stock or investment over a specific period of time. Returns represent the gain or loss in the investment's value relative to its initial or reference price. Returns can be calculated on a daily, weekly, monthly, or any other desired time interval basis. They are typically expressed as percentages and are computed by comparing the ending value of the investment to its initial or reference value. (Bodie, 2010.)

The market model is a frequently used model in event studies that estimates the expected or normal performance of a stock based on its historical relationship with a market index, such as the S&P 500. It assumes that stock's returns are linearly related to the returns of the market index. The difference between actual returns and expected returns is known as the abnormal return. (Chang et al., 2020.)

Cumulative Abnormal Return (hereafter, CAR) is an often-used method in event studies to analyse the cumulative impact of an event on stock's returns over a specific measurement period, such as the event window (e.g., Campbell et al., 2003; Gatzlaff & McCullough, 2010; Yayla & Hu, 2011). It is acquired by summing the abnormal returns over the measurement period.

Buy-and-Hold Abnormal Return (hereafter, BHAR) is another measure used in event studies to evaluate the abnormal returns over a more extended period, typically one year. BHAR accounts for the buy-and-hold strategy, considering the changes in stock prices and reinvestment of any dividends or distributions over the specified period. (Barber & Lyon, 1997; Chang et al., 2020; Ritter, 1991.) Like CAR, BHAR is acquired by summing the abnormal returns over the measurement period.

Lastly, the Fama-French Three-Factor model (hereafter, FFTF) is a widely recognized asset pricing model that extends on the market model. It incorporates three factors: market risk (captured by market returns), size (captured by the size of the company), and value (captured by the book-to-market ratio). FFTF provides a more comprehensive explanation of stock returns by considering additional factors beyond just the overall market return. It helps determine whether the abnormal returns are statistically significant and whether the abnormal returns can be attributed to the event itself rather than general market movements.

(Chang et al., 2020.; Fama, 1970). All approaches will be further elaborated on in the method chapter.

2.2 Exploitive and disruptive ISBs

The nature of an ISB encountered by an organization holds a significant influence on the impact it has on a company's business performance and the response of the stock market. DoS attacks, theft of customer data, and website defacement attacks each yield distinct effects on the stock market value of publicly listed companies. (Garg et al., 2003; Yayla & Hu, 2011.) For instance, a malware attack primarily focused on the theft of non-essential information results in minimal disruptions to the firm's operations, thereby likely prompting a less severe market reaction. Conversely, a ransomware attack that immobilizes the organization's IT infrastructure and brings its operations to a standstill can have a significantly more devastating impact on its target's business performance. (Harry & Gallagher, 2018; Yayla & Hu, 2011.)

While the type of ISB is a significant factor, it is more critical to assess how the attack impacts the firm's ability to conduct business (Yayla and Hu, 2011). This notion aligns with the classification system proposed by Harry and Gallagher (2018), which focuses on the effect on the victim. The researchers argue that the impact of an ISB on the victim's operations more directly dictates the business's immediate and potential future performance, and as such, is likely to be a more relevant indicator of how the stock market reacts.

Harry and Gallagher's (2018) classification system bifurcates ISBs into two primary categories, with every five subcategories, based on the effect on the victim: disruptive and exploitive (see Figure 2). Disruptive ISBs (hereafter, D-ISBs) are those that interrupt or degrade the victim's ability to conduct business. These could include ransomware attacks that lock down a company's digital infrastructure, DoS attacks that overwhelm servers and halt online services or sabotage that damages physical or digital assets. On the other hand, exploitive ISBs (hereafter, E-ISBs) lead to a loss of data. Most often is this done with malicious intent where perpetrators aim to steal, disclose, or otherwise misuse a victim's data or resources, such as cyber attacks that expose sensitive customer information or espionage that steals proprietary technology. (Harry & Gallagher, 2018.)

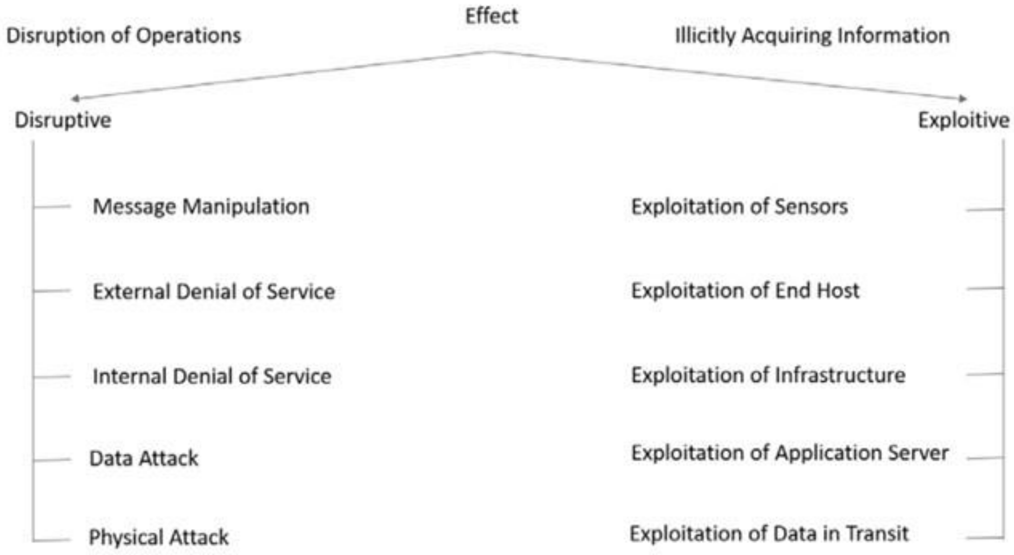
Effect
Disruption of Operations
Illicitly Acquiring Information
Disruptive
Exploitive
Message Manipulation
External Denial of Service
Internal Denial of Service
Data Attack
Physical Attack
Exploitation of Sensors
Exploitation of End Host
Exploitation of Infrastructure
Exploitation of Application Server
Exploitation of Data in Transit

Figure 2: Cyber event taxonomy (Harry & Gallagher, 2018)

The classification of ISBs as either disruptive or exploitive, as proposed by Harry and Gallagher (2018), could provide an insightful framework for understanding variations in short-term and long-term stock market reactions. For instance, D-ISBs probably trigger immediate and significant declines in stock value due to the inability to conduct operations, which results in immediate revenue losses (Yayla & Hu, 2011).

Conversely, when considering E-ISBs characterized by data theft or misuse, immediate operational disruptions may not be evident (Harry & Gallagher, 2018). Consequently, the initial market reaction may be less severe, given that it may not be immediately apparent that an incident has occurred, and business operations can continue as usual. However, the long-term consequences can be significant due to factors such as reputational damage, loss of customer trust, potential legal penalties, and the expenses involved in enhancing security measures (Chang et al., 2020).

Therefore, understanding whether an ISB is disruptive or exploitive can help anticipate the likely timing and extent of the stock market's reaction. The classification of Harry and Gallagher (2018) is further explained in the subsequent paragraphs.

Two notions are important to acknowledge: firstly, perpetrators regularly combine cyber attacks for a desired result, resulting in both disruptive and exploitive effects (Harry & Gallagher, 2018). However, this paper does not delve into the examination of such attacks but rather focuses on clearly delineating the distinction between these two effects.

Secondly, Harry and Gallagher (2018) describe a single cyber attack as an attack which can consist of either one or multiple unauthorised technical actions. For instance, when a hacker conducts a spear-phishing message attack to penetrate a computer network and subsequently removes information on four other devices, that will qualify as a single incident.

2.2.1 Disruptive ISBs

D-ISBs have the potential to cause significant harm to business operations, leading to deterioration in the victim's integrity and availability. Moreover, these breaches are typically carried out with deliberate intent. Malicious actors can adopt a myriad of strategies with wide-ranging disruptive consequences, contingent upon the extent to which an organisation relies on information technology to undertake its essential operations. These strategies could involve erasing information from one or multiple networks, deploying ransomware, undermining physical equipment utilised in manufacturing goods by tampering with Supervisory Control And Data Acquisition (SCADA) systems, blocking consumers from gaining access to the company's website or obstructing entry to a social media account. (Harry & Gallagher, 2018.) The following represent the five types of D-ISBs.

1. Message manipulation

Message manipulation refers to a type of cyber attack where an organisation's communication channels are tampered with, disrupting its ability to accurately convey messages to its intended audience, such as users or customers (Harry & Gallagher, 2018). This form of a cyber attack can take numerous shapes, from social media hijacking to website defacement, and it primarily aims at spreading misinformation, generating chaos, or damaging the reputation of the targeted entity (Hadnagy & Fincher, 2015). An illustrative example of a message manipulation attack occurred in 2015 when hackers affiliated with the extremist group ISIS managed to infiltrate the US Central Command's Twitter and YouTube accounts. The attackers posted threatening messages and changed the account graphics to reflect their affiliation, causing widespread alarm and confusion. (Broadhurst et al., 2014.)

2. External Denial of Service (EDoS)

This category includes cyber attacks executed from appliances outside the target organisation's systems that degrade or deny the victim's capacity to communicate with other systems (Harry & Gallagher, 2018). For instance, an attacker might coordinate a botnet (an army of compromised computers) to transmit an enormous volume of traffic to a specific website. This sudden influx of requests can overwhelm the website's servers, causing it to slow down significantly or even crash, thus denying service to legitimate users (Peng, Leckie, & Ramamohanarao, 2007).

3. Internal Denial of Service (IDoS)

If a cyber attack is conducted from inside a victim's network that restricts entry to different internal systems, it is categorised as an Internal Denial of Service attack (Harry & Gallagher, 2018). Unlike traditional EDoS attacks, IDoS attacks are harder to detect as they utilize legitimate network credentials and often mimic normal system behaviour (Zargar, Joshi, & Tipper, 2013). For example, an employee might inadvertently download malicious software onto their workstation. This software could be programmed to send an abnormally high number of requests to an internal server, such as a file server or a database server. As a result, the server becomes overwhelmed with illegitimate requests and unable to service the legitimate ones, leading to disruption of service to other employees. (Mirkovic & Reiher, 2004.)

4. Data attack

This category includes cyber attacks that manipulate, destroy, or encrypt data in a victim's network. Frequently used techniques include ransomware, wiper viruses, or administrative credentials to alter information. (Harry & Gallagher, 2018.) A notable example of a data attack is the 2017 Maersk ransomware cyber attack where hackers encrypted files and systems, requesting 300 dollars for its release. Maersk, responsible for roughly one-fifth of global trade shut down completely within a day, and estimated losses of 250 million dollars. Moreover, the disruption in the entire supply chain is believed to be costing over a billion dollars. (Capano, 2021.)

Data attacks exhibit similar traits to exploitative attacks, with data attacks often manifesting a combination of disruptive and exploitative effects. A data attack is only classified as disruptive if data theft or data distribution is not involved. Data attacks primarily focus on compromising data integrity rather than confidentiality, which distinguishes them from exploitative attacks. Distinctively, uncombined exploitative attacks exclusively lack disruptive attributes. (Harry & Gallagher, 2018.)

5. Physical attack

The classification of a cyber attack as a physical attack occurs when it manipulates, destroys or degrades physical systems. Tactics employed to achieve such effects may include using Programmable Logic Controllers (PLC) to open or close electrical breakers or leveraging user passwords to access and adjust settings in a human-machine interface, thereby causing physical equipment to malfunction, consequently leading to damages. (Harry & Gallagher, 2018.) An instance of this occurred in December 2015 when a hostile actor exploited the control interface of a Ukrainian utility, tripping several breakers in power substations. This led to a loss of power for tens of thousands of consumers for a extended time. (Lee, Assante & Conway 2016.)

2.2.2 Exploitive ISBs

In certain scenarios, information security events lead to the loss, destruction, or manipulation of sensitive data, violating the confidentiality of an organisation. More often, these events are perpetrated by criminals. The aim of these adversarial entities could encompass the procurement of customer records, intellectual property, classified national security documents, or proprietary information about the target organisation. While the methodologies employed by cybercriminals can differ, the nature of the data they target remains consistent. (Harry & Gallagher, 2018.) The following represent the five types of E-ISBs:

1. Exploitation of Sensors

This form of cyber attack is characterised by the theft of data from peripheral devices like credit card scanners, intelligent lighting systems, network-connected thermostats, or cars. Unlawful acquisition of technical, consumer, personal, or corporate data from devices such as CCTV cameras, smart TVs, or baby monitors also falls under exploitation of Sensors. (Harry & Gallagher, 2018.)

2. Exploitation of End Hosts

In this category of cyber attacks, hackers seek to pilfer data housed on user devices, such as desktop computers, laptops, or mobile devices (Harry & Gallagher, 2018). An example, in the 2016 Democratic National Committee (DNC) hacking incident, Russian hackers used spear-phishing emails to trick DNC employees into revealing their credentials, leading to the theft of sensitive emails and documents (Rid, 2020).

3. Exploitation of Network Infrastructure

Hackers exploit direct access to network equipment, like routers, switches, and modems, to compromise data in this category of cyber attacks (Harry & Gallagher, 2018). In 2014, a group of hackers called the Equation Group, allegedly linked to the NSA, was reported to have infected hard drive firmware across multiple countries. This sophisticated attack allowed them to have persistent access to the networks of their targets. (Kaspersky, 2015.)

4. Exploitation of Application Server

This type of cyber attack involves malicious actors gaining access to data within a server-side application or directly on the server through misconfigurations or vulnerabilities (Harry & Gallagher, 2018). According to Perlroth (2015), the U.S. Office of Personnel Management (OPM) suffered a major breach when hackers exploited a vulnerability in the application server to gain access to records of over 22 million federal employees and contractors (Perlroth, 2015).

5. Exploitation of Data in Transit

This type of cyber attack occurs when hackers intercept data during its transmission between devices (Harry & Gallagher, 2018). For instance, in 2017, the KRACK (Key Reinstallation Attack) demonstrated how vulnerabilities in the WPA2 protocol could allow attackers to intercept network traffic between a device and a wireless access point, leading to data-in-transit exploitation (Vanhoef & Piessens, 2017).

2.3 ISBs' impact on stock market value

This paragraph aims to assess the implications of ISBs on the stock market value of publicly listed companies. Adding to the intrigue, the effects will be assessed for both the short- and long-term, which will be cross-referenced in the subsequent paragraphs with two effects ISBs have.

Furthermore, assessing the influence of ISBs on the stock market typically involves measuring the impact from the day of the announcement (the day a company discloses that it has been breached), as demonstrated by studies such as Campbell et al. (2003), Chang et al. (2020), and Hinz et al. (2015). This is because the stock market relies on information to react, as stated by Fama (1970). In the case of many ISBs, measuring from the event date (the day the ISB actually happened, classified as date zero) would be impractical since breaches are often disclosed much later, or not at all, as noted by Amir et al. (2018). Exploitive attacks, in particular, can go undetected for an extended period, as highlighted by Harry & Gallagher (2018). Consequently, in this study, the comparison between disruptive and exploitive attacks will primarily be based on the announcement date. However, considering arguments suggesting that D-ISBs can immediately impact the stock market (measured from date zero), this hypothesis will also be considered.

2.3.1 ISB's short-term impact

There is substantial research concerning the immediate aftermath of announcements of cyber events on the stock market value of publicly listed companies (e.g., Campbell et al. 2003; Kannan et al. 2007; Hinz et al. 2015). These authors offer compelling insights into the significant negative stock price reactions that frequently occur in the short-term following corporate data breaches (measured in a three- and seven-day window).

Campbell et al. (2003) provide cogent empirical evidence suggesting that firms experiencing breaches of confidentiality undergo a pronounced depreciation in stock value within a day following the announcement. This finding is echoed by Cavusoglu et al. (2004), who establish a negative correlation between the disclosure of security breaches and a subsequent 2.1% decline in stock prices within the two days of the event.

Similarly, Goel and Shawky (2009) demonstrate that the revelation of ISBs has a damaging effect of approximately 1% on the stock market value in the immediate aftermath of the announcement. This evidence was further corroborated by Tosun (2021), who confirmed that ISBs continue to result in considerable short-term losses. Tripathi and Mukhopadhyay (2020) lend additional support to this perspective, arguing that the effect of ISBs on negative cumulative abnormal returns is more prominent within a briefer timeframe than a more extended one.

Gatzlaff and McCullough (2010) further advanced this narrative by showing that ISBs resulted in immediate significant negative abnormal returns within their one-day and two-day windows. Their study further showed that companies with more severe data breaches suffered larger negative abnormal returns.

A study by Tanimura and Wehrly (2009) investigated the impact of confidential data breaches on market value and whether they result in negative consequences. They found that, on average, a firm's market value decreased significantly within three days following the announcement of a security breach. However, according to their findings, the market value losses are in similar magnitudes to an ISB's direct costs (tangible costs). Based on these observations, they concluded: "Direct costs, and not reputational penalties, are the primary deterrents to information security breaches".

Hinz et al. (2015) focused on the effect of data stealing by electronics businesses. They found that such companies faced a significant decline in share prices in the short-term. Their research further indicated an increase in systematic risk following the data theft, suggesting a wider market apprehension related to the breached firm's future prospects.

However, not all studies align with these findings. Kannan et al. (2007) and Huang and Madnick (2020), for example, reported an absence of significant negative abnormal returns in the short-term following a security breach. Even after considering diverse variables such as breach types, company types, and study timeframes, the results remained insignificant. Huang and Madnick (2020) noted the inherent difficulty in quantifying losses resulting from ISBs and the unclear impact of these losses on firm performance.

In an extensive literature review, Spanos and Angelis (2016) concluded that information security events exert a considerable impact on the stock market, primarily in a negative direction. Their systematic examination of bibliographic sources yielded 45 studies within 37 relevant papers. The majority of these studies (75.6%) conveyed statistical significance concerning the effect of ISBs on companies' market value. Of these, 71.1% indicated a negative stock market response, 24.4% reported a positive reaction, 2.2% presented mixed reactions, and 2.2% reported impartial reactions. The findings predominantly manifested within a few days preceding and following the event.

The research of Spanos and Angelis (2016) is supported by Ali et al. (2021), who performed a systematic literature study of the effect of information security events on stock market reactions. Their research focused on both favourable and unfavourable security events, with a special emphasis on understanding the effects of cyber events.

The findings of Ali et al. (2021) revealed that cyber events have not only a direct financial impact on businesses but also affect investor confidence and company reputation. This, in turn, results in a stock market reaction. Specifically, the research indicated that in 75% of the studies, information security events had a significant impact on a firm's stock market performance. These results were largely observed within two days before and after the announcement. The research of Ali et al. (2021) is consistent with earlier research that has found a negative stock exchange response to ISBs.

Taken together, these findings suggest that ISBs are likely to provoke a negative stock market response in the short-term for publicly listed companies. This pattern is consistently observed across different industry sectors, breach types, and geographies, lending robust empirical support to the hypothesis that ISBs lead to a decline in short-term stock market value. The accumulated evidence from the existing literature points towards the formulation of the following hypothesis:

H1: Announcements of ISBs have a negative impact on the short-term stock market value of publicly listed companies.

2.3.2 ISBs’ impact over time

While there is substantial research concerning the immediate aftermath of cyber events on the stock market value of publicly listed companies, academic work focusing specifically on the gradual implications is relatively limited (Chang et al., 2020). Despite this, the available literature offers valuable insights into the possible enduring impact of such breaches.

The first perspective views the long-term impact in a relatively short timeframe, extending to weeks post-breach. Considering that longer timeframes are susceptible to external factors unrelated to the preceding event, it is argued that shorter timeframes yield more dependable and reliable results (Telang & Wattal, 2007).

For instance, Gatzlaff and Mccullough (2010) reported that the adverse effect on stock prices continued for two days following a security breach announcement. However, the magnitude of this effect slowly diminished compared to the immediate aftermath, measuring several timeframes up to sixty days after the event. Tripathi and Mukhopadhyay (2020) further validated this observation. They reported significant losses only within a one-to-three-day window following the ISB disclosure. However, in only one of the three years they analysed did these losses persist within their 21-day window, suggesting that the severity of the stock market reaction declines over time.

According to the findings of Yayla and Hu (2011), it was observed that within a 10-day window, only Denial of Service (DoS) attacks demonstrated an increase in the severity of losses as time progressed. On the other hand, unauthorized access to customer data, unauthorized access to employee and company data, as well as website defacement, did not yield significant results in terms of changes over time.

As most literature suggests that the effects of most ISBs on the stock market diminish over time (within a measurement period of up to twenty days following the announcement), the following hypothesis is formulated:

H2: The impact of announcements of ISBs on the stock market value of publicly listed companies diminishes within twenty days.

Some researchers interpret the long-term impact over a more extended timeframe, ranging from 180 days to five years post-breach. Tosun (2021) reported significant losses within a five-day window following the disclosure of an ISB. However, this study did not observe significant losses at one, three, or five years after the event, indicating a possible recovery or normalization of stock prices in the long run.

In contrast, Chang et al. (2020) concluded that ISB announcements had a significant negative impact on both short-term and long-term market value. Their study observed a substantial average abnormal return of -10.21% 12 months post-event, with even larger significant abnormal returns of -32.68% and -34.36% at 24 and 36 months, respectively. These results suggest that the impact of ISBs may indeed be sustained over an extended period.

Furthermore, Romanosky, Hoffman, and Acquisti (2014) emphasized that organizations experience long-term negative effects on their business performance following data breaches, especially those that involve sensitive personal data, primarily due to litigation. They further assert that the costs associated with market value losses serve as the primary driver of these adverse consequences.

Taken together, these studies suggest that the fallout from an ISB on a company's stock market value is not transient but has a chance to persist for an extended period. Therefore, the following hypothesis is made:

H3: Announcements of ISBs have a negative impact on the long-term stock market value of publicly listed companies.

2.4 Disruptive and exploitive ISB announcements' short-term impact

Harry and Gallagher's (2018) conceptualization of ISBs as either disruptive or exploitive could provide a robust framework for understanding the stock market's reaction to these events. Although both categories of breaches have negative consequences for the affected organization, existing literature overwhelmingly suggests that disclosures of E-ISBs have a significantly more short-term impact on the stock market value of publicly traded companies.

As previously shown, several studies have examined the impact of E-ISBs on stock market value. Campbell et al. (2003) found that breaches compromising confidentiality led to a 2.1% decline in stock value within a day of the disclosure, while breaches not violating confidentiality had no significant effect. Similarly, Tanimura and Wehrly (2009) discovered that confidential data breaches resulted in an average decrease of market value within three days of the announcement. Hinz et al. (2015) focused on data theft in the electronics industry and found a significant short-term decline in share prices for affected companies. Garg et al. (2003) determined that the theft of customer data had a more substantial negative impact on stock market value compared to disruptive events. All these authors argue that theft and breaches that violate confidentially, which both are characteristics of Harry & Gallagher's (2018) description of E-ISBs, have a strong impact on a firm's market value on the day or within a couple of days preceding the event.

Research on D-ISBs presents conflicting findings. For instance, Grag et al. (2003) discovered that the theft of credit card information or customer data had a significantly higher impact (ranging from 9.6% to 15%) compared to DoS incidents (ranging from 2.6% to 3.9%) and website defacement, which resulted in a negative impact of 1.1% to 2%. Hovav and D'Arcy's (2003) research indicated that, in general, the market does not penalize firms that have experienced DoS attacks, as their results did not show any significant stock market losses. In contrast, Yayla and Hu (2011) found that DoS attacks explicitly caused substantial damage to the stock market value, with the impact persisting over a ten-day period, compared to unauthorized access. Contradicting all these findings, Cavusoglu et al. (2004) found no significant difference in stock market reaction based on the type of attack. This is further supported by Das et al. (2012), who found no significant differences in stock market reaction following incidents of data theft, DDoS attacks, phishing attacks, and website defacement.

Given that most research concludes that E-ISBs have a severe negative impact on the stock market, while fewer studies reach the same conclusion for D-ISBs, the following hypothesis is formulated:

H4: Announcements of E-ISBs have a bigger negative impact on the short-term stock market value of publicly listed companies than D-ISBs.

However, it can be argued that D-ISBs provoke more a severe short-term stock market reaction than E-ISBs based on date zero.

D-ISBs are characterized by the halting or degrading of an organization's ability to conduct business. This category includes breaches like ransomware attacks that lock down a company's digital infrastructure, DoS or DDoS attacks that overwhelm servers and halt online services, and sabotage that damages physical or digital assets. (Harry and Gallagher, 2018.) The immediate impact on operations, and consequently on revenue and profit, is often significant and very visible as websites, servers and services are down or unavailable (Yayla & Hu, 2011). These tangible effects on business performance make D-ISBs highly visible to investors, resulting in immediate uncertainty which leads to drops in stock prices as investors attempt to price in the new risk (Dixit & Pindyck, 1994).

Moreover, the uncertainty associated with D-ISBs can exacerbate their impact on stock prices (Dixit & Pindyck, 1994). The duration of service disruption is often unknown at the onset, leading to uncertainty about the full extent of revenue loss (Harry & Gallagher, 2018).

Furthermore, the costs associated with the remediation of D-ISBs can be substantial. These costs could include the expenses for restoring services, implementing stronger security measures, compensating affected customers, and potential legal costs. These immediate and direct costs can substantially impact an organization's financial performance, leading to a downward revision of the company's value. (Romanosky, 2016.) As Tanimura and Wherly (2008) have argued that direct costs are the primary deterrents in ISBs, these direct costs are likely visible in the stock market response. Building upon this theory is Garg et al. (2003), who found that it is likely that insiders and individuals directly impacted by the breach had access to significant information prior to the public disclosure. The size of this group is considerably larger due to the visibility of the ISB (Yayla and Hu, 2011). Even with limited information, this could stimulate considerable market speculation regarding the company's market value, ultimately leading to the observed negative decline in the firm's market value on the day preceding the official announcement (Dixit & Pindyck, 1994; Fama, 1970; Garg et al. 2003).

Given the frequent occurrence of undetected or overlooked exploitative incidents during the ISB, along with the uncertain identification of the exact day within a particular week or month, or even the possibility of their complete absence, it is illogical to measure their impact based on date zero (Amir et al., 2018; Harry & Gallagher, 2018). However, in line with the literature, it is probable that ISBs generate a response on the stock market on the very same day. Consequently, the following hypothesis is put forth:

H5: D-ISB have a negative impact on the short-term stock market value of publicly listed companies (measured from date zero).

2.5 Disruptive and exploitive ISB announcements’ long-term impact

E-ISBs, characterized by the theft, disclosure, or misuse of sensitive data, may not initially impact a company's operations, but their long-term intangible effects can be very severe for business performance (Chang et al., 2020). These events can damage a company's reputation, a critical asset in the information economy, leading to a sustained decrease in stock value (Harry & Gallagher, 2018).

Research has shown that reputation and trust play essential roles in a company's ability to attract and retain customers, which in turn influence revenue and profit (Yayla & Hu, 2011). This assertion is backed by the findings of Chang et al. (2021) that companies experiencing confidentiality violated publicized data breaches suffered a decrease in their market value due to the loss of customer trust and damaged reputation, which increases over time.

Moreover, E-ISBs often lead to regulatory penalties and increased future costs for security enhancement and compensating affected parties (Yayla & Hu, 2011). These costs can substantially impact a company's future cash flows, leading to a downward revision of its value by the stock market over time (Romanosky, 2016).

E-ISBs can also create competitive disadvantages, especially in cases where proprietary information or intellectual property is stolen (Harry & Gallagher, 2018). Following the theory of Yayla & Hu (2011), erosion of a company's competitive advantage can decrease its future earning potential, reflected in a sustained drop in its stock price.

All these consequences can do serious harm in the long-term, but maybe even more severely, can lead to a ‘slow burn’ effect on stock prices. The slow burn effect refers to a gradual, yet steady deterioration of a certain aspect over time. In the context of the stock market, it can refer to a consistent downward trend in a company's stock value over a period of time, often due to certain circumstances or events that instil doubt in investors' minds about the company's future prospects. (Bodie et al., 2011.)

When a company suffers an E-ISB, the impact on its stock market value may not be immediate. Instead, the negative implications of the attack may unfold gradually over time, leading to a slow burn effect. Slow burns are feared in the stock market world, as this effect results in a negative feedback loop. (Bodie et al., 2011.) This happens as investors become increasingly concerned about the potential ramifications of the attack, such as financial losses, reputational damage, and future vulnerability to similar events (Chang et al., 2016). This can lead to a gradual withdrawal of investment, which in turn depresses the company's stock value over a sustained period, which in turn adds to the concern of the investors (Bodie et al., 2011).

The downfall of the stock market value and the uncertainty around an ISB, whether revealed or not, can further exacerbate this slow burn effect. Uncertainty is a significant driver of investor behaviour, and the perceived risk related to an event like an ISB can prompt a withdrawal of investment (Dixit & Pindyck, 1994). If an information breach is publicly disclosed, it can create uncertainty about the company's ability to manage its cybersecurity risks and its future resilience to such events. On the other hand, if an information breach remains undisclosed but is later discovered, the resulting loss of trust can increase uncertainty and further depress the company's stock value (Amir et al., 2018).

Conversely, the impacts of D-ISBs are often more immediate and short-lived (Harry & Gallagher, 2018). Once operations are restored, the company can quickly start generating revenue again, and although some customers may be lost due to the disruption, the immediate and visible nature of D-ISBs allows companies to communicate remedial actions to stakeholders, potentially limiting uncertainty and the long-term damage to their reputation (Yayla & Hu, 2011).

In conclusion, the long-term effects of E-ISBs seem to be more significant. The sustained decrease in a company's stock price over time can be attributed to the damage to reputation and trust, anticipated future costs, uncertainty about the full extent of the breach, and potential loss of competitive advantage (Yayla & Hu, 2011). Hence, the following hypothesis is developed:

H6: Announcement of E-ISBs have a bigger negative impact on the long-term stock market value of publicly listed companies than D-ISBs.

2.6 Hypotheses summary

In Table 1 the hypotheses are presented in a summarized format. The focal independent variable is ISBs, while the dependent variables include the short-term stock market value and the long-term stock market value of publicly listed companies. Additionally, these relationships are influenced by the moderating factor of whether the security breach is disruptive or exploitive.

Table 1: Hypotheses summary

Hypothesis	Description
1.	Announcements of ISBs have a negative impact on the short-term stock market value of publicly listed companies.
2.	The impact of announcements of ISBs on the stock market value of publicly listed companies diminishes within twenty days.
3.	Announcements of ISBs have a negative impact on the long-term stock market value of publicly listed companies.
4.	Announcements of E-ISBs have a bigger negative impact on the short-term stock market value of publicly listed companies than D-ISBs.
5.	D-ISB have a negative impact on the short-term stock market value of publicly listed companies (measured from date zero).
6.	Announcements of E-ISBs have a bigger negative impact on the long-term stock market value of publicly listed companies than D-ISBs.

3 Method

3.1 Data collection

The objective of this research is to examine the impact of ISBs on the stock market value of publicly listed companies, taking into account the moderating effect, whether the security breach has a disruptive or exploitative effect. To achieve this, a quantitative research approach will be employed.

The primary data source for this study will be the Cyber Event Database from the University of Maryland CISSM (CISSM Cyber Events Database, n.d.). The dataset, retrieved on May 12th, 2023, comprises a comprehensive compilation of information security breach events, amounting to a total of 11,098 records. Records are divided by various variables, Notable for this study, whether the attack had a disruptive, exploitive or mixed (both disruptive and exploitive) impact.

Remarkably, within this extensive dataset, a significant proportion of 5,243 incidents transpired within the United States of America (hereafter, U.S.), involving companies, institutes, or individuals located within the U.S. Hence, to limit the scope of the study and ensure homogeneity, the analysis will focus solely on events occurring within the U.S.

Furthermore, the market model, the calculation of CAR for the short-term, and BHAR and FFTF for the long-term, will be performed using historical stock market data from the Wharton Research Data Services (WRDS, n.d.). The data utilized in this research will cover the period from 2015 to 2022.

The sample of this study has the following restrictions:

(1) The victim organisation is a firm from the U.S.
(2) The cyber event happened at the latest a year before 31-5-2023.
(3) The cyber event is classified as either disruptive or exploitive.
(4) All observations with missing variables are deleted from the sample.
(5) All firms are publicly listed (subsidiaries will be listed under their parent company).
(6) All the events must have a clear announcement date (and a date zero if it is a D-ISB).
(7) The study requires that the firm under investigation does not have any confounding factors that could potentially impact the stock market value ten days surrounding the event

day. Examples of such confounding factors include mergers & acquisitions, debt or earnings announcements, dividend announcements, and other similar events.

The final sample contains 219 observations, of which 45 are D-ISBs and 174 are E-ISBs (shown in Appendix 1 List of ISBs).

3.2 Event study

Finance theory has traditionally posited that market prices incorporate all pertinent information and future expectations regarding a company's prospects. This foundational notion allows researchers to assess the impact of specific events on a firm's outlook by examining their effects on the firm’s market value. (Fama, 1970.) Event study analysis serves as the statistical method employed to conduct such evaluations. The underlying principle of event study analysis involves comparing the disparity between the normal returns that would have been anticipated had the event not taken place and the actual returns (i.e., abnormal returns) resulting from the occurrence of the event. (Chang et al., 2020.)

3.2.1 The market model

The market model is a widely utilized tool in financial research for assessing a company's prospects, by measuring the abnormal returns resulting from the events. (Chang et al., 2020.) It enables the estimation of the relationship between a firm's stock returns and the broader market returns. This model operates on the assumption that the stock returns of a company exhibit a stable linear relationship with the systematic movements observed in the overall market. (WRDS, n.d.) The market model requires an estimation period, which is explained further below, a publicly listed company (retrieved from the CISSM Cyber Events Database), and availability of historical data (retrieved from WRDS): sufficient historical data is needed for both the individual stock and the market index to estimate the parameters (α_i and β_i) of the model accurately. The market model utilizes historical data of a specific stock to create a linear model that depicts the stock's evolution in a linear fashion relative to the overall market. This linear model serves as a valuable tool for understanding and predicting how the specific stock is likely to behave in relation to the overall market conditions in the future. The formula for the market model is:

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

In this model, i represents the firm while t represents the timeframe (estimation period). R_{it} represents the return of the individual stock. It is the variable used to denote the return a specific firm’s stock market value (i) during a given period (t). α_i is the intercept or constant term specific to the stock. It represents the expected return of the stock when the market return is zero. β_i is the beta coefficient. It measures how sensitive the stock's returns are to changes in the market. A higher beta indicates the stock tends to move more in line with the market, while a lower beta means it's less influenced by market movements. R_{mt} represents the return of the market index. It serves as an indicator of overall market performance. ε_{it} is the error term or residual. It represents the random or unexplained portion of the stock's return.

To estimate the predictable changes in the market that reflect the expected and typical performance of a company's stock market value, it is important to define a specific period of time, known as an estimation window (t). As depicted in Figure 3, the estimation window, measured prior to the announcement date or date zero, enables the calculation of the company's stock normal performance within that specific timeframe. In cases where the stock market is closed on this date, date zero is shifted to the first trading day thereafter.

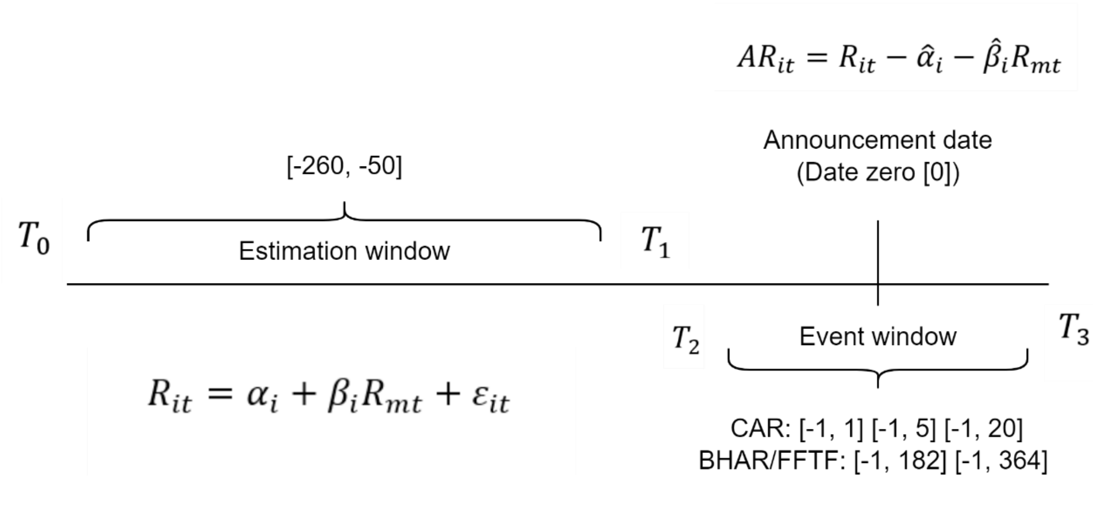
$AR_{it} = R_{it} - \hat{\alpha}_i - \hat{\beta}_i R_{mt}$
Announcement date
(Date zero [0])
[-260, -50]
T_0
Estimation window
T_1
T_2
Event window
T_3
$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$
CAR: [-1, 1] [-1, 5] [-1, 20]
BHAR/FFTF: [-1, 182] [-1, 364]

Figure 3: Estimation window and event window

T is denoted as a specific point in time, with T_0 and T_1 representing the estimation window T_2 and T_3 representing the event window. Time windows are denoted between brackets, as [x, y]. Where x represents the number of days before or after date zero that marks the beginning of the timeframe, while y represents the number of days before or after date zero that indicates the end of the timeframe. R_{it} is denoted as the average return within a time window, and AR_{it} is denoted as the abnormal return in the event window. The formula for AR_{it} is further explained in paragraph 0.

In this study, the estimation window is defined as [-260, -50], indicating that the measurement period begins 260 days before date zero and ends 50 days prior to date zero. The decision to measure up to 50 days prior to date zero is a common practice to mitigate the influence of leaks or other factors associated with the announcement. (WRDS, n.d.) This approach aims to ensure the reliability of the analysis by minimizing any potential impact resulting from prior knowledge of the announcement.

Previous studies examining the impact of varying estimation window lengths on the results have indicated that as long as the window lengths exceed 100 days, there is minimal effect on the findings (Armitage, 1995; Park, 2004). However, Campbell et al. (2010) found that longer estimation windows slightly enhance accuracy. In this study, the choice of a 210-day estimation window is based on practical considerations. When the estimation window exceeds 210 days, two records are lost from the dataset due to potential invalidity of stock market information for the respective event dates. Thus, to ensure data completeness and reliability, the estimation window is set at 210 days.

Figure 3 also displays the event window, which, like the estimation window, estimate the returns within that window. However, this window specifically surrounds date zero to measure the abnormal returns following the event. This window is needed for calculating the market model and FFTF. This study aims to evaluate the impact of ISBs by employing various measurement intervals: three days [-1, 1], seven days [-1, 5], 22 days [-1, 20], 184 days [-1, 182], and 366 days [-1, 364]. To measure the short-term impact, the three-day window is essential. Including the day before the event day enables capturing any market reaction resulting from potential information leakage and accounts for scenarios such as the initiation of an event like a DoS attack before the market closure. Likewise, in cases where an event or announcement occurs after market closure, the day immediately following the event is essential in capturing its impact (Campbell et al., 2003).

Additionally, a second short-term measurement of seven days is considered valuable to ensure the entire market receives valid information (Yayla & Hu, 2011). Furthermore, to comprehend the evolving effects of ISBs over time, a mid-term measurement of 22 days and long-term measurements spanning approximately six months and one year will be conducted. It has been observed that using CAR over significantly longer periods, such as 20 days in this instance, yields less reliable results when assessing event development (Telang & Wattal, 2007). Considering the study's focus on examining the evolving effects of different types of ISBs over time, a maximum measurement period of one year is considered appropriate. This will be measured by employing BHAR and FFTF as the evaluation metric.

3.2.2 Cumulative Abnormal Returns (CAR) Model

The short-term stock market reaction will be assessed using the CAR within the market model. CAR measures the disparity in stock prices between the normal returns and the returns observed during the event window. This occurrence is a common phenomenon in events studies (e.g., Campbell et al., 2003; Gatzlaff & McCullough, 2010; Yayla & Hu, 2011). The expected return, denoted as $E(R_{it})$, is based on the market model parameters and is computed with the formula:

$$E(R_{it}) = \hat{\alpha}_i + \hat{\beta}_i R_{mt} \tag{2}$$

CAR builds upon the outcomes generated by the market model, thus sharing the same requirements. However, CAR has additional requirements: every data record must include an event date (retrieved from the CISSM Cyber Events Database) that serves as the trigger for calculating abnormal returns and stock data surrounding this date in a three-day and seven-day window (retrieved from WRDS). Date zero is surrounded by these time windows (T_2 and T_3), from which the data is used to compute the actual stock returns (R_{it}), which are subtracted from the expected returns (see Figure 3). Consequently, the abnormal return of firm i for period t is derived from this analysis:

$$AR_{it} = R_{it} - E(R_{it}) \tag{3}$$

During the event periods (T_2, T_3), as outlined in section 3.2.1, CAR is calculated by summing up all abnormal return of the stock in their respective timeframes.

$$CAR_i = \sum_{t_2}^{t_3} AR_{it} \tag{4}$$

Therefore, when considering a sample of N firms, the calculated mean of the event-window effect is estimated as:

$$\overline{CAR_{it}} = \frac{1}{N} \sum_{i=1}^{N} CAR_{it} \tag{5}$$

For clarification: in the context of analysing the stock performance during a specific event period, such as the release of firm X's quarterly earnings report, CAR can be applied. The following steps outline an example of how CAR can be calculated:

First, select a pre-defined estimation window before the event. For instance, let's consider an estimation window of [-20, -10], which represents 20 days before the event day up to 10 days before the event.

Secondly, utilize a market model to estimate the expected returns for each day within the estimation window (formula 1 *and* 2*) for firm X. This estimation of expected returns provides a reference for the stock's performance under normal market conditions. Let's say firm X experienced a growth rate of 0,5% on average per day during the estimation period.*

Thirdly, observe the actual returns of firm X for each of the three event days: day -1 (one day prior to the event), day 0 (announcement day or date zero), and day +1 (one days after the event). These actual returns reflect the stock's performance during the event period and are shown in the historical stock market data. Let's say firm X actual returns were 0% growth on day -1, -1% on day 0 and -2% on day +1.

Fourthly, calculate the abnormal return for each event day by subtracting the expected return (derived from the market model) from the actual return observed on that specific day (formula 3*). The abnormal return represents the deviation of firm X's stock performance from what was expected during the event period. Calculations shows that the abnormal return on day -1 is a decrease of 0,5%, (0 – 0,5), day 0 is -1,5%, and -2,5% on day +1.*

Finally, sum up the three individual abnormal returns (for day -1, date zero 0, and day +1) to obtain CAR for the three-day window (formula 4*). This measure provides insight into the overall impact of the event on firm X's stock performance over the specified event period. Therefore, firm X's CAR were -5% in a three-day window.*

This process can be applied to multiple firms that have experienced the same event, allowing for a comparative analysis of their respective CARs. By dividing the CARs of these firms, valuable insights can be gained regarding the impact and effect of the event in question.

3.2.3 Buy-And-Hold Abnormal Returns (BHAR) Model

BHAR is a method that helps evaluate a stock's performance over a significant period, specifically focusing on the sustained impact of an event on the market value. Unlike CAR, which examines the cumulative abnormal returns over a specific event window, BHAR looks at the absolute performance of stocks or portfolios over an extended period, regardless of market conditions. (Chang et al., 2020.) BHAR incorporates a buy-and-hold strategy, considering the returns earned from holding the stock or portfolio throughout the entire period. By comparing the actual returns with the expected returns based on a market model, BHAR captures the abnormal returns resulting from the event from an investment perspective. This approach is a valuable tool for understanding the unique performance dynamics and identifying abnormal patterns associated with the event of interest. (Ritter, 1991; Barber & Lyon, 1997.) The formula enhances the reliability of the long-term analysis by providing a more comprehensive perspective on the stock's performance, irrespective of market fluctuations or noise (WRDS, n.d.).

As BHAR builds upon the outcomes derived from the market model, it necessitates the same requirements, but it also needs an event date (retrieved from the CISSM Cyber Events Database) and the stock data in the 184-day and 366-day windows (retrieved from WRDS). The formula for BHAR is as follows:

$$BHAR_{it} = \prod_{T_2+1}^{T_3}(1 + R_{it}) - \prod_{T_2+1}^{T_3}\left(1 + E(R_{it})\right) \tag{6}$$

In this formula, R_{it} constitutes the actual return of the stock during the holding period, and $E(R_{it})$ represents the expected return. R_{it} and $E(R_{it})$ are computed in the same manner as in CARs model with the equations (1) and (2), respectively. The periods for BHAR are T = 182 days and T = 364 days. Mean BHAR is computed by adding all the abnormal returns and splitting it by the number of records, as shown in the following equation:

$$\overline{BHAR}_{it} = \frac{1}{N}\prod_{i=1}^{N} BHAR_i \tag{7}$$

3.2.4 Fama-French Three-Factor (FFTF) model

Establishing a correlation between a specific event and long-term stock market behaviour can be challenging due to the influence of various factors, trends, and events. To enhance the robustness and validity of the findings, this study not only applies the BHARs model on the market model to compute long-term abnormal returns but also incorporates FFTF. The inclusion of the FFTF allows for an examination of the performance of long-term abnormal returns and provides additional insights into the factors that may influence these returns. (Chang et al., 2020.) It aims to explain the excess return of a portfolio or stock by considering three factors: market risk, size, and value (Fama & French, 1997).

1. Market Return Rate (R_{mt}) is a measure of the overall performance of the stock market. It represents the return an investor can expect from investing in the broad market. It is calculated as the surplus return of a market index, which means it takes into account the returns above and beyond a risk-free rate.

2. Size (SMB), also known as Small Minus Big, is a factor that considers the impact of company size on stock performance. It implies that smaller firms tend to exceed bigger firms. SMB is calculated by taking the surplus return of a portfolio of small-cap stocks and subtracting the surplus return of a portfolio of large-cap stocks.

3. Value (HML), or High Minus Low, is a factor that captures the effect of a stock's valuation on its performance. It indicates that stocks with low value ratios, such as a low price-to-book ratio, tend to outperform stocks with higher valuation ratios. HML is determined by subtracting the surplus return of a portfolio with lower book-to-market stocks from the surplus return of a portfolio with higher book-to-market stocks.

FFTF is used to explain the expected return of a stock or portfolio exactly as the market model (by creating a linear model to establish the parameters) but is based on the exposure to these three factors. It suggests that the excess return can be attributed to the risk associated with these factors rather than simply market risk. The model is more focused on the specific characteristics and behaviour of a particular stock, rather than being heavily influenced by broader market movements. (Chang et al., 2020; Fama & French, 1997.)

In terms of data requirements, FFTF requires historical data for the market returns, as well as the size and value portfolios. This includes daily data for the market index, as well as the necessary data to construct the size and value portfolios. The size portfolios are constructed based on the market capitalization of stocks, while the value portfolios are formed based on valuation ratios. All this data is retrievable in the Wharton Research Database (WRDS, n.d.). Also similar to BHAR, FFTF needs an event date (date zero) and the stock data in the 184-day and 366-day windows (retrieved from the CISSM Cyber Events Database). Similarly in the market model, sufficient historical data is needed for to estimate the parameters (α_i, β_i, s_i and h_i) of the model accurately. FFTF is represented by the following equation:

$$R_{it} = \alpha_i + \beta_i R_{mt} + s_i SMB_t + h_i HML_t + \varepsilon_{it} \tag{8}$$

In this model, R_{it} is the rate of return on firm i during period t expressed as a function of several variables. These variables include the rate of return on the market index (R_{mt}) during timeframe t, the distinction between the average return on small market-capitalization portfolios and large market-capitalization portfolios during timeframe t (SMB_t), the difference between the average return on high book-to-market equity portfolios and low book-to-market equity portfolios during period t (HML_t), and an error term represented by ε_{it}. The estimation of the expected return is conducted using the three-factor model. This involves utilizing the estimated parameters $\hat{\alpha}_i$, $\hat{\beta}_i$, $\hat{s}_i$, and $\hat{h}_i$, along with the market return rate factor, the size risk factor, and the value factor ratio. (WRDS, n.d.) The formula employed for this estimation is as follows:

$$E(R_{it}) = \hat{\alpha}_i + \hat{\beta}_i R_{mt} + \hat{s}_i SMB_t + \hat{h}_i HML_t \tag{9}$$

Subsequently, the anticipated return derived from the three-factor model is employed within BHAR formula (6 & 7) to compute the long-term abnormal returns, but for clarification purposes these results will still be referred to as FFTF.

The BHAR and FFTF results will be subject to data trimming, the deletion of outliners from the dataset (-5%). MacKinlay (1997) explains that outliers can have a disproportionate impact on the estimation of BHAR due to the compounding nature of returns over the event window. Extreme observations can contribute significantly to the cumulative abnormal return calculation, thereby influencing the overall results of the event study (Yayla, and Hu, 2011).

3.3 Validity, reliability, and objectivity

3.3.1 Internal validity

Ensuring the quality of the data was a paramount consideration throughout this rigorous research study, to improve the internal validity. To maintain integrity and reliability, a comprehensive data management plan (see Appendix 2 Data management plan) was developed, outlining the procedures for handling data in a reliable and ethical manner. The plan incorporated specific criteria to ensure the utilization of relevant and trustworthy data sources.

In particular, great care was taken to establish accurate event dates and announcement dates while mitigating the influence of confounding events surrounding the target event. The CISSM Cyber Events Database (n.d.), which provided event dates (date zero), served as a valuable source for validating the occurrence of ISBs. The university of Maryland, provider of the database, ensures data reliability and validity, as shown in the Appendix 3 CISSM data collection. Additionally, the validation of announcement dates was undertaken through a triangulation approach. This rigorous process involved meticulous cross-referencing of information obtained from the CISSM Cyber Event Database (n.d.) and diverse sources (such as articles and financial statements), predominantly through comprehensive internet searches utilizing search engines like Google and following hyperlinks from news articles to their primary sources. Only events with multiple clearly mentioned and validated announcement dates were considered for analysis. Thorough data validation procedures were implemented, including triangulation of checks for inconsistencies and errors, and missing data points were removed from the dataset.

Furthermore, a rigorous data cleaning process was employed to identify and eliminate any anomalies that had the potential to distort the analysis. To address potential outliers, 5% of the extreme values on both ends of the distribution were removed for the long-term results, as these are particularly problematic (MacKinlay, 1997).

Moreover, internal validity relies on the accuracy, completeness, and reliability of the data used for analysis. By meticulously documenting the data collection, validation, and cleaning procedures, transparency was maintained, ensuring the overall quality and reliability of the data used in this study (Armitage, 1995). Nonetheless, it should be noted that the tests utilized in this study rely on certain assumptions, including the independence of observations, the normality of data distribution, and the homogeneity of variances. Failure to meet these assumptions may jeopardize the internal validity of the tests. Therefore, these assumptions were carefully examined and considered throughout the study to minimize any potential impact on internal validity.

Independence of observations: In this study, a sample of 219 observations was collected, each representing a unique (ISB) event, in several industries, within a window of seven years. The events were selected to cover a diverse range of timeframes, ensuring that they are spread out evenly over the entire duration. This approach provides evidence for data independence in the analysis. By including events from different timeframes and industries, the study encompasses a wide range of market conditions, economic factors, and other potential influences that could affect stock returns. The non-overlapping nature of the events eliminates any direct correlation or dependence between them and avoids any bias or influence from previous or subsequent events, as they are distinct, unrelated, time varied occurrences. (Rosenblatt, 1965.)

The large sample size further supports the assertion of data independence. With a substantial number of independent observations, the likelihood of random correlations or dependencies between events is reduced. This allows for more reliable and robust conclusions to be drawn from the analysis. (Armitage, 1995.)

Normality of data distribution: Parametric tests, such as the Cross-section t-Test (hereafter, CSect T) and Patell’s Z, are only suitable for data that is normally distributed. If data is not normally distributed, additional significance tests (nonparametric tests) are required to validate the data. (IBM documentation, 2021; Yayla & Hu, 2011.) However, the central limit theorem argues that a distribution of sample with a sufficient number of data points (if N > 30), will approximate a normal distribution. (Rosenblatt, 1965). This is particularly relevant in event studies where the focus is on examining the distribution of abnormal returns rather than the underlying return distribution (Yayla & Hu, 2011). Moreover, these researches indicated that nonparametric tests lose their effectiveness when the sample size exceeds 50.

Given the substantial number of records well exceeding 200, it can be reasonably assumed that normality is assured. However, to fully ensure the validity of the data, the Shapiro-Wilk test is once applied to the full dataset on the long-term results observed within a 366-

day window (BHAR) as longer-term results are known to exhibit wider ranges of outcomes (MacKinlay, 1997). The formula for the Shapiro-Wilk test is:

$$W = \frac{(\sum_{i=1}^{n} \alpha_i x_{(i)})^2}{\sum_{i=1}^{n}(x_i - \bar{x})^2} \tag{10}$$

Where W is test statistics which can be compared to Shapiro-Wilk significance table to indicate significance. n is the sample size, a is the significance level (0.05) and x are the sample results. As expected, the Shapiro-Wilk test did not reveal a significant departure from normality, with a test statistic W of 0.9896 falling within the 95% acceptance region. This is further illustrated in the accompanying Figure 4 and Figure 5.

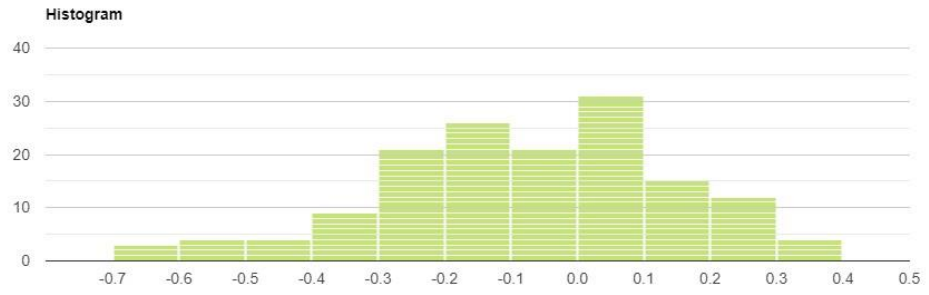

Figure 4: Histogram Shapiro-Wilk test results (N=219, Mean BHAR in 366-day window)

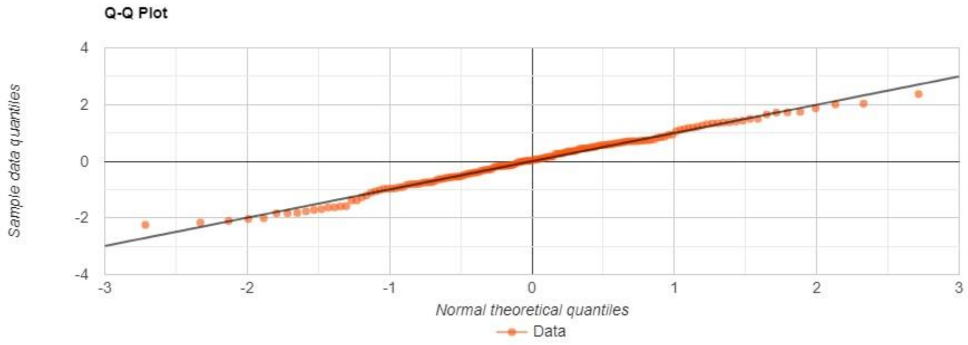

Figure 5: Q-Q plot Shapiro-Wilk test results (N=219, Mean BHAR in 366-day window)

Given that there are only 45 D-ISBs, they are subjected to the Shapiro-Wilk test as they fall below the sample size threshold of 50. Nonetheless, for the D-ISBs observed on both the date zero and the announcement day within the three-day windows, the Shapiro-Wilk test did not indicate a significant departure from normality, with W values of 0.9883 and 0.9732, respectively (As displayed in Figure 6, Figure 7, Figure 8, and Figure 9). Since the CSect T and Patell's Z tests did not yield significant results for the remaining D-ISB windows, it would be redundant to perform the Shapiro-Wilk tests for normality.

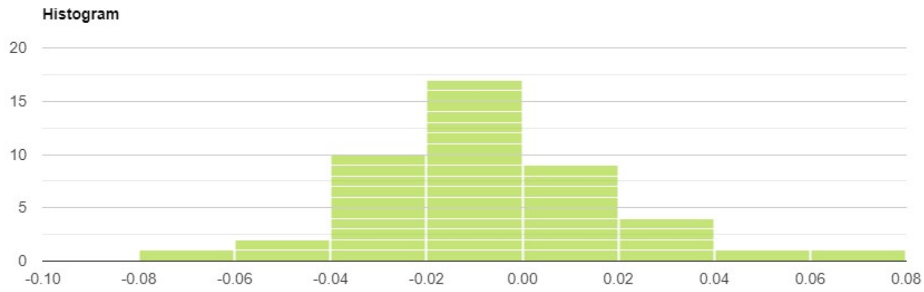

Figure 6: Histogram Shapiro-Wilk test results (N=45, Date zero Mean CAR in three window)

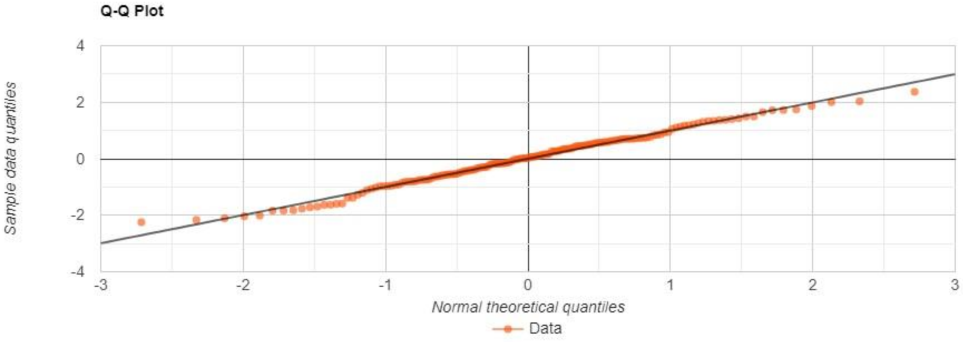

Figure 7: Q-Q plot Shapiro-Wilk test results (N=45, Announcement Mean CAR in three window)

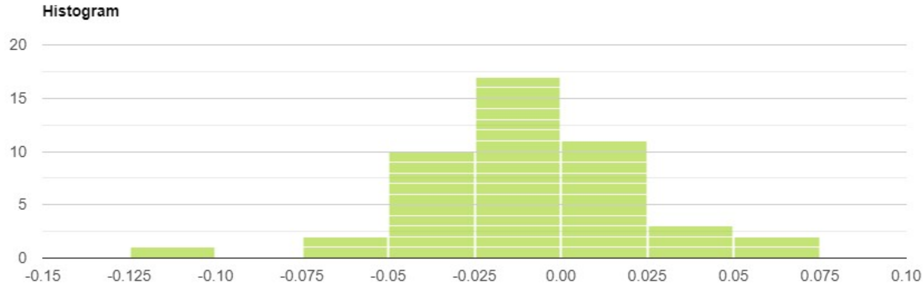

Figure 8: Histogram Shapiro-Wilk test results (N=45, Announcement Mean CAR in three window)

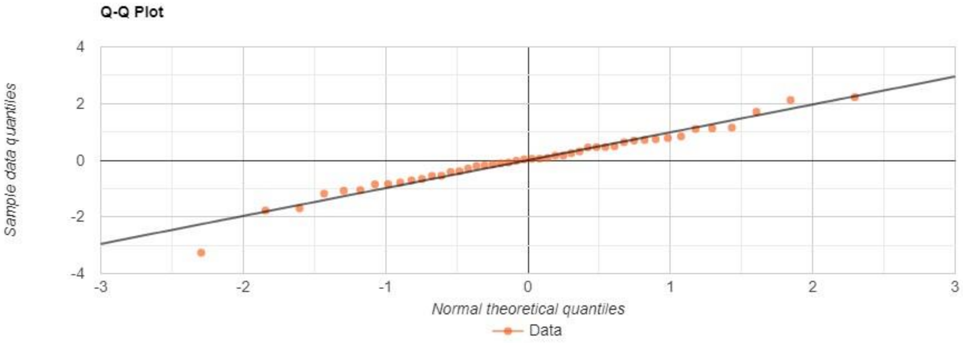

Figure 9: Q-Q plot Shapiro-Wilk test results (N=45, Announcement Mean CAR in three window)

Homogeneity of variances: In this study, the comparison of one-sample tests to a specific value (0% change in a stock's value) precludes the direct testing for homogeneity of variances. Instead, it is assumed that the data within the sample exhibit similar levels of variability, unless there are compelling reasons to believe otherwise. This assumption plays a vital role in ensuring the reliability of our statistical test. (Armitage, 1995.) Moreover, there are strong arguments in favour of the claim of homogeneity of variances based on the comprehensive evidence provided by the 219 samples of stock market data. This assertion is bolstered by several key factors that lend support to the assumption of similar variability.

Firstly, the Central Limit Theorem assures us that as sample size increases, the variability of stock returns tends to converge towards a consistent level (Rosenblatt, 1965). Additionally, the Law of Large Numbers suggests that with a sample size of this magnitude, the observed values closely approximate the true population parameters. The statistical reliability of the dataset is enhanced by the large sample size, which diminishes the influence of random fluctuations and outliers, resulting in more accurate variance estimates. Furthermore, the efficient nature of the stock market (hereafter, EMH), characterized by high trading volumes, extensive investor participation, and constant price adjustments, lends further support to the assumption of homogeneity of variances. (Fama, 1970.) While it is important to consider unique events or structural breaks that may impact the data, the sizeable sample of 219 observations in this dataset strongly suggests the presence of homogeneity of variances in stock market data.

3.3.2 External validity

Generalizability: The generalizability of the research, which focuses on samples from various industries within the U.S., covering the period from 2015 to 2022 and specifically includes publicly listed companies, is notable for several reasons. Firstly, by incorporating samples from multiple industries, the research encompasses a broad representation of the U.S. economy, enhancing the potential applicability of your findings to other similar industries within the country. Secondly, given the U.S.' status as a prominent global economy, the economic trends and market dynamics observed within this context often have implications beyond its borders. As a result, research conducted within the U.S.’s market can offer valuable insights and serve as a reference for other economies facing similar circumstances.

Furthermore, the extensive time period covered by the research allows for a comprehensive analysis due to a strong assumption that specific market conditions do not play a significant role, further bolstering its generalizability. Nevertheless, it is important to note that the applicability of the research may vary across different countries or regions due to variations in market structures, regulations, and cultural factors. Additionally, the focus on publicly listed companies further narrows the scope, as it excludes private companies and organizations not listed on stock markets. Caution should be exercised when attempting to generalize the findings beyond these specific parameters.

Sensitivity of the data: The use of sensitivity tests in this research is evident through the incorporation of various event windows and the application of both the market model and the Fama-French three-factor model. (Armitage, 1995.) The exploration of different event windows, including three-day, seven-day, 22-day, 184-day, and 366-day windows, allows for the examination of effects over different time periods, ensuring the robustness and consistency of the observed results. Additionally, by utilizing both the market model and the Fama-French three-factor model, the research incorporates different analytical frameworks to assess the sensitivity of the findings to various methodologies and variable considerations. (Fama, 1970.) This comprehensive approach strengthens the validity and reliability of the research by accounting for different scenarios and variations, ultimately enhancing our understanding of the relationship between the variables of interest.

3.3.3 Reliability & objectivity

The study exhibits a strong commitment to ensuring reliability and objectivity through a rigorous implementation of data procedures, comprehensive sensitivity tests, alignment with prior research, and the consistency of results. The meticulous data collection, validation, and cleaning procedures employed by the study minimize potential biases and subjective influences, contributing to enhanced objectivity. Furthermore, the transparent documentation of these processes facilitates the replication and verification of the results by other researchers, strengthening the reliability of the research.

The inclusion of sensitivity tests, such as the examination of various event windows and the utilization of both the market model and the Fama-French three-factor model, reinforces both reliability and objectivity by evaluating the robustness and consistency of the findings across diverse scenarios and methodologies. The consistent results observed across these sensitivity tests provide further evidence of the stability and dependability of the research outcomes.

The study also builds upon existing knowledge by drawing from reputable scholarly works, such as Campell et al. (2003) and Romanosky, S. (2016), which bolsters the reliability and objectivity of the research by aligning with established findings and methodologies. Moreover, the adherence to standardized approaches and established research frameworks helps mitigate personal biases, fostering objectivity throughout the research process.

3.3.4 Significance tests

Considering that the underlying assumptions of the models employed in the event study hold true, it is deemed appropriate to utilize parametric tests for evaluating the significance of the obtained results (Yayla & Hu, 2011). In this regard, two parametric tests, namely the CSect T and the Patell's Z test, will be carried out. Both tests aim to assess whether the mean of abnormal returns, regardless of whether they are cumulative, standardized, or of other types, exhibits statistically significant differences from zero. The resulting T- or Z-statistic is then compared to the critical values from the T- and Z-distribution tables to determine the statistical significance. This comparison assesses whether the observed difference is due to chance or if it represents a true difference. (WRDS, n.d.)

The data requirements for conducting these statistical tests in the context of CAR, BHAR, and FFTF analysis are based on the previous results obtained from these methods. Specifically, the required data includes the computed abnormal returns, and their respective means. Patell's Z test also requires the standard deviation of sample, which is derived from number of valid observations and degrees of freedom. It is important to note that these tests assume certain underlying assumptions, including data independence, normality of the data distribution, and homogeneity of variances, which have been elaborated in the previous paragraphs.

The CSect T is widely utilized in event studies, for example, by Cavusoglu et al. (2004), Kannan et al. (2007) and Tosun (2021), and has demonstrated excellent performance, making it a valuable tool for confirming the consistency and dependability of the results (Campbell et al., 2010). However, event study analysis commonly deals with endogeneity issues, where the explanatory variables may be correlated with unobservable factors or lagged dependent variables. The CSect T does not provide a framework to address endogeneity concerns adequately. (WRDS, n.d.)

Therefore, to overcome endogeneity concerns, CAR, Patell’s Z test is applied. Patell's Z statistic is also commonly utilized, for example, by Chang et al. (2021) and Tanimura and Wehrly (2009), to measure that standardizes abnormal returns during the event window by dividing them by the standard deviation of abnormal returns observed during the estimation period. This test enables reliable estimation and hypothesis testing while considering the data structure, individual differences, and potential time-dependent effects. By incorporating instrumental variables, Patell's Z test effectively deals with endogeneity concerns that may arise due to correlated omitted variables or lagged dependent variables in relation to the explanatory variables. (WRDS, n.d.) However, according to Campbell et al. (2010), it has been observed that Patell's Z test tends to reject the null hypothesis too easily. Hence, to ensure robustness and reliability, both CSect T and Patell's Z test will be employed, following the method of Gatzlaff & Mccullough, (2010).

The formula for the CSect T is as follows:

$$t = \frac{\frac{1}{M}\sum_{i=1}^{M} RetVar_{it}}{\sqrt{\frac{1}{M(M-1)}\sum_{i=1}^{M}(RetVar_i - \frac{1}{M}\sum_{i=1}^{M} RetVar_i)^2}} \tag{11}$$

Where

$$RetVar = CAR, or\ BHAR$$

M represents the mean of the abnormal return observed in the sample. This are derived from CAR, BHAR, or FFTF, respectively. The formula for Patell’s Z test is:

$$t_{Patell} = \frac{\sum_{i=1}^{M} SAR_{i,t}}{\sqrt{\sum_{i=1}^{M}\frac{K_j-2}{K_j-4}}} = \frac{mean\left(SAR_{i,t}\right)}{\frac{\left(\sqrt{\sum_{i=1}^{M}\frac{K_j-2}{K_j-4}}\right)}{M}} \tag{12}$$

Where SAR is

$$SAR_{i,t} = \frac{CAR_{i,t}}{\sqrt{S_{AR_i}^2}} \tag{13}$$

Where $S_{AR_i}^2$ is

$$S^2_{AR_i} = \frac{1}{W_i - K} \sum_{T_2}^{T_3} AR^2_{it} \tag{14}$$

W_i represents the count of non-missing returns within the estimation window. For instance, in the absence of any missing observations, W_i would be equal to $T_1 - T_0 + 1$ where T_0 and T_1 indicate the starting and ending periods, respectively. K represents the degrees of freedom, which correspond to the number of free parameters in the benchmark model utilized for calculating the abnormal returns. In the market model, K is equal to 2.

It is worth noting that the formulation of Patell's Z test is not designed for analysing BHAR (WRDS, n.d.). However, the FFTF helps mitigate endogeneity concerns. By including the size and value factors in the model, it aims to capture some of the systematic risks associated with these characteristics, which helps control for potential endogeneity arising from omitted variables. Additionally, the use of FFTF can provide a framework for testing the relationship between risk factors and abnormal returns. This can help identify whether abnormal returns are truly driven by specific factors or if there are other underlying endogenous variables at play. (Chang et al., 2020; Fama & French, 1997.) Therefore, solely the CSect T is deemed appropriate for testing BHAR.

3.4 Ethicality

This thesis adheres to the principles of ethical research and data usage. The information is solely from open sources, ensuring zero breaches of privacy and confidentiality. Throughout the research process, I have maintained honesty, integrity, and transparency, accurately representing my objectives, methods, and findings. I have respected intellectual property rights and copyright by appropriately citing and referencing all external sources. By upholding these ethical standards, I have ensured the integrity and validity of this thesis. The ethical handling of data is further described in Appendix 2 Data management plan. Furthermore, AI have been used in this thesis in the following manner:

The utilization of ChatGPT (https://platform.openai.com/overview) has served as an aid in providing suggestions and assistance during the writing process. The prompts used with ChatGPT involved tasks such as sentence or paragraph rewriting, concept explanations, or acquiring information on specific topics. For instance, examples of prompts include requests like "Rewrite this in a paragraph: [...]", "How do you prove homogeneity of variances with one sample?", or "Explain the CIA triad in an academic sense".

Additionally, the study employed the AI Elicit (https://elicit.org/) as a research tool. Elicit leverages language models to automate various aspects of research workflows, such as parts of the literature review process. It possesses the capability to identify pertinent papers even without exact keyword matches, provide concise summaries of the papers' insights pertaining to your specific inquiry, and extract essential information from those papers.

However, it is essential to emphasize that the ideas, analysis, and conclusions presented in this thesis are entirely my own. The assistance received from ChatGPT or Elicit should be considered as educational in nature. It is important to acknowledge that these AI’s generates responses based on patterns and information from its training data. While it can offer guidance and generate ideas, it does not guarantee the accuracy, reliability, or comprehensiveness of the information provided. To ensure the academic integrity of this thesis, I have taken additional measures. This includes meticulously scrutinizing the credibility of every author mentioned and personally validating each statement with reputable sources. Every external source used in this thesis, including ideas or information suggested by these AI’s, has been appropriately cited and referenced. I have attributed the contributions of others appropriately to acknowledge their work and to prevent any potential issues of plagiarism.

Lastly, I have employed ResearchRabbit (https://www.researchrabbit.ai/) to gather research papers. ResearchRabbit allows users to add research papers, and the AI then selects relevant papers that reference each other, creating a network of interconnected research. This AI tool has been valuable in identifying pertinent literature.

By including this disclaimer, I affirm that I have utilized AI as a tool to support the thesis writing process while maintaining full responsibility for the final content and academic integrity of this work.

4 Results

4.1 Descriptive Statistics

A total of 219 samples from the dataset were selected for analysis, covering the period from 2014 to 2022. The distribution of samples across each year is presented in Table 2. The data appeared to be relatively evenly distributed across most years, with the exception of 2018 and 2020. It is worth noting that the smaller number of samples in 2022 is consistent with the rest of the dataset, as data collection did not go beyond June 2022.

Table 2: D-ISBs and E-ISBs per year (N=219)

Year	Samples	Disruptive ISBs	Exploitive ISBs
2022	9	4	5
2021	20	4	16
2020	42	14	28
2019	21	3	18
2018	38	7	31
2017	25	5	20
2016	19	2	17
2015	23	4	19
2014	22	2	20

Figure 10 and Figure 11 depict how D-ISBs and E-ISBs were divided based on the classification explained in paragraph 2.2, respectively. The findings indicated that D-ISBs primarily consisted of data attacks and EDoS attacks, while E-ISBs were predominantly associated with the exploitation of the application server.

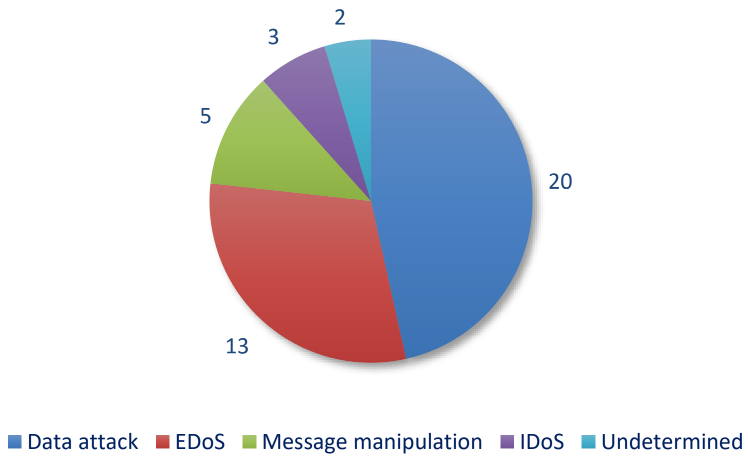

Figure 10: D-ISBs bifurcated per type

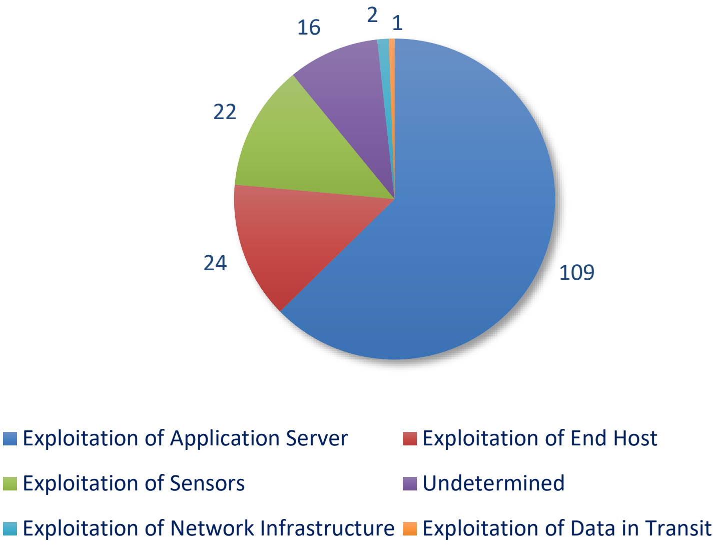

Figure 11: E-ISBs bifurcated per type

Lastly, Figure 12 displays the distribution of the sample by industry, with exploitative ISBs represented by the blue bars and D-ISBs represented by the red bars. The 'Information' industry stood out as the most prevalent in the dataset, accounting for 21.9% of the ISBs. Following closely was the 'Professional, Scientific, and Technical Services' industry, comprising 15.5% of the incidents. Notably, the D-ISBs depicted a relatively even distribution across the industries, with the exception of 'Transportation and Recreation' and 'Real Estate and Rental and Leasing,' where they appeared to be more dominant.

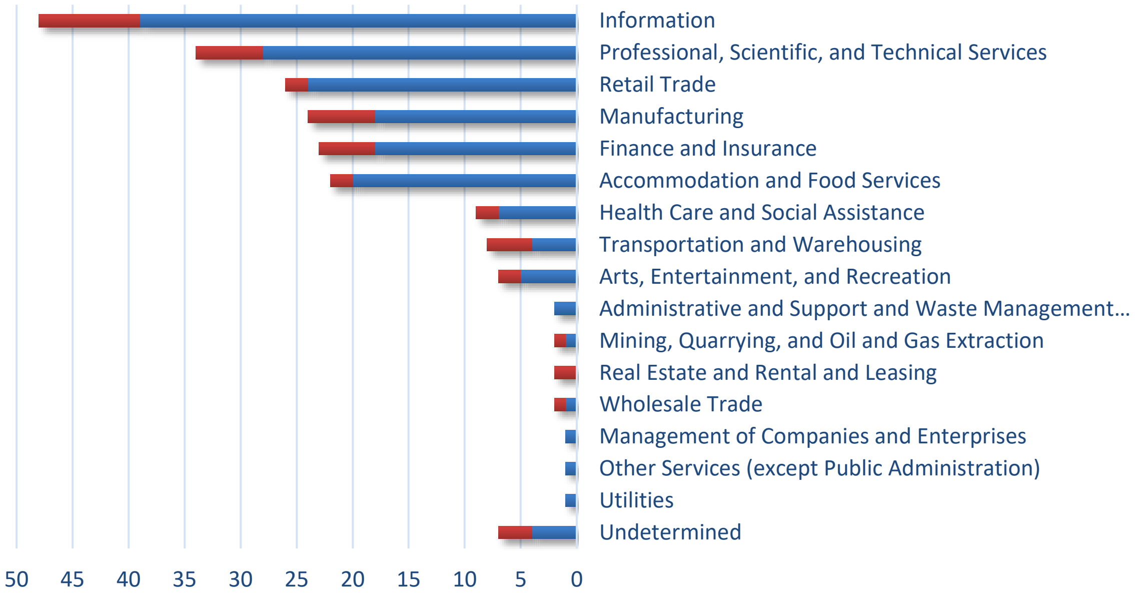

Figure 12: ISBs bifurcated between D-ISBs and E-ISBs per industry (N=219)

4.2 ISBs announcements' overall impact

4.2.1 ISB announcements' impact up to 20 days

Hypothesis 1 predicted that announcements of ISBs would have a negative impact on the short-term stock market value of publicly listed companies. Table 3 presents the results of this test. All results were statistically significant at level 0.01. The analysis demonstrated significant negative abnormal returns observed within the event windows of [-1, 1], [-1, 5], and [-1, 20], as confirmed by both the CSect T and Patell's Z tests. On average, when an event company disclosed an ISB, it led to stock price declines of -1.14%, -1.64%, and -2.39%, respectively.

Table 3: ISB announcements' impact (up to 20 days) (N=219)
Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Event window	Mean CAR	CSect T	Patell's Z test
[-1, 1]	-0.0114	-3.9425***	-4.3797***
[-1, 5]	-0.0164	-3.4337***	-4.4086***
[-1, 20]	-0.0239	-2.6709***	-3.8355***

The empirical results indicated that the organization encountered immediate financial setbacks following the incident, as investors reassessed the company's market worth within the stock market. The noteworthy presence of substantial negative abnormal returns during the specified event periods presented compelling evidence regarding the detrimental influence of an ISB on the stock prices of publicly traded companies. Consequently, these findings lent support to hypothesis 1, which asserted that the revelation of a data breach significantly diminished the breached company's short-term market value.

However, these results contradicted hypothesis 2, which predicted that the impact of announcements of ISBs on the stock market value of publicly listed companies diminished within twenty days. The analysis of Figure 13 revealed an interesting trend: rather than diminishing over time, the observed pattern indicated an increasingly negative trend after the announcement of ISBs, extending up to a period of twenty days. This implied that the effect of ISB disclosure does not decrease, but increases as time progressed, contrary to the initial hypothesis. The results per day are visible in Appendix 4 Tables .

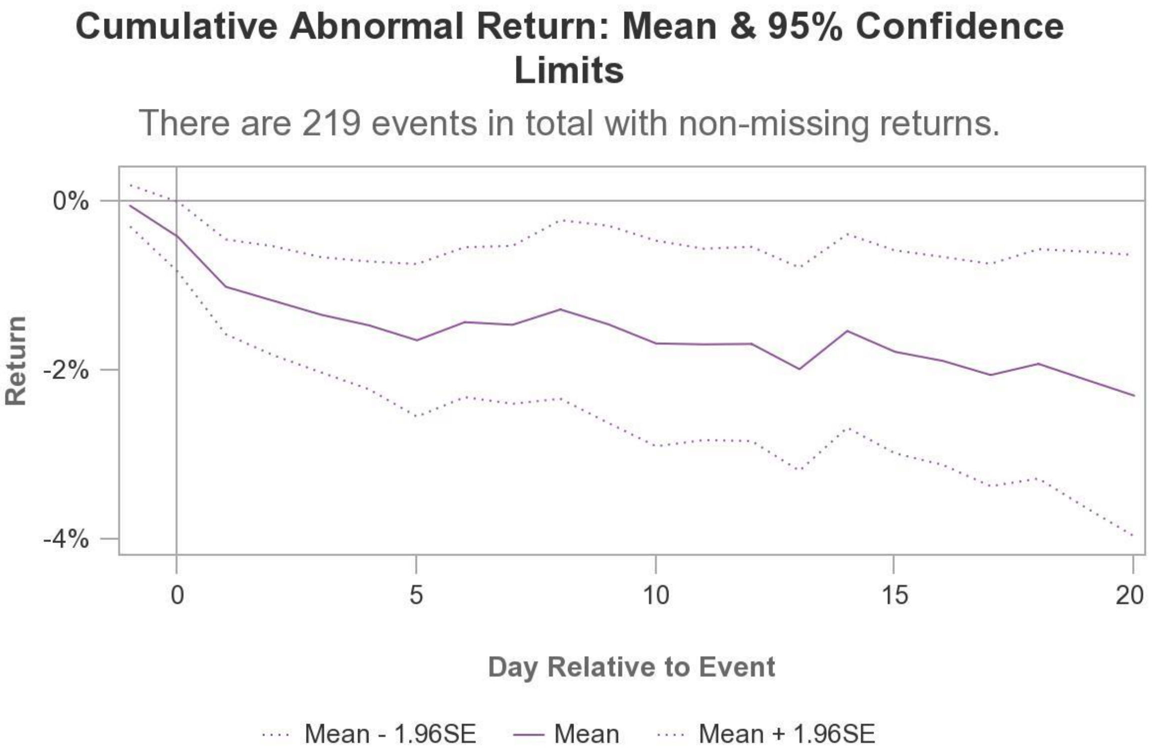

Figure 13: Mean CAR development of ISBs impact within a 22-day window (N=219)

4.2.2 ISB announcements’ long-term impact

Table 4 presents the results of hypothesis 3, which tested if announcements of ISBs have a negative impact on the long-term stock market value of publicly listed companies (after 182 and 364 days), using both the market model and the FFTF. It should be noted that the sample size was slightly decreased due to the exclusion of companies with incomplete information within the specified windows. After assessing the outcomes, an additional 5% of the data was subjected to trimming to enhance the reliability of the analysis.

Table 4: ISB announcements’ impact after 182 days (N=191) and 364 days (N=185)
Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Event window	Mean BHAR	CSect T
Market Model		
[-1, 182]	-0.0895	-4.8234***
[-1, 364]	-0.1593	-3.6923***
Fama-French Three-Factor model		
[-1, 182]	-0.0790	-4.0761***
[-1, 364]	-0.2260	-3.0682***

The findings of the empirical analysis indicated highly statistically significant negative abnormal returns within the 184-day and 366-day windows, validated by the CSect T. Specifically, if investors had held any stocks out of the sample following an ISB, they would, on average, experience losses ranging from -8.95% after six months to -15.93% after a full year. The results obtained from FFTF also demonstrated that the announcement of data breach events had a significant adverse impact on the company's long-term market value. The average cumulative abnormal returns after 182 days after an ISB amount to -7.90%, which further declined to -22.60% after a full year. These findings provided substantial evidence supporting hypothesis 3.

4.3 Disruptive and exploitive ISBs announcements' impact up to 20 days

This paragraph presents the findings related to hypothesis 4. Hypothesis 4 posited that announcements of E-ISBs would have a bigger negative impact on the short-term stock market value of publicly listed companies than D-ISBs. Table 5 presents the differentiated outcomes of disruptive and exploitative ISBs up to 20 days following their disclosure.

Table 5: Disruptive (N=45) and exploitive (N=174) ISB announcements impact (up to 20 days) Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Event window	Mean CAR	CSect T	Patell's Z test
Disruptive ISBs			
[-1, 1]	-0.0108	-2.2829**	-1.5406*
[-1, 5]	-0.0078	-0.9173	-0.7341
[-1, 20]	0.0078	0.6289	0.3943
Exploitive ISBs			
[-1, 1]	-0.0116	-3.3560***	-4.1333***
[-1, 5]	-0.0186	-3.3338***	-4.5816***
[-1, 20]	-0.0324	-3.0013***	-4.5187***

The results revealed that announcements of D-ISBs did not yield statistically significant effects within the seven- and 22-day windows. However, a three-day window analysis indicated a significant decrease of -1.08%, as was determined by the CSect T at level 0.05 and Patell's Z test at level 0.1. Conversely, announcements of E-ISBs exhibited highly statistically significant results across all examined windows in both tests. Disclosures of E-ISBs resulted in losses of -1.16% in the three-day window, -1.86% in the seven-day window, and -3.24% in the 22-day window, demonstrating a progressively declining trend over time, as depicted in Figure 14.

These findings partially supported hypothesis 4, suggesting that the disclosure of E-ISBs had a more pronounced negative impact compared to D-ISBs. As D-ISBs showed weak significance solely in the three-day, in contrary to E-ISBs that showed highly significant results in all three windows, E-ISBs posed a greater threat to the short-term stock market value of firms. The results per day are visible in Appendix 4 Tables .

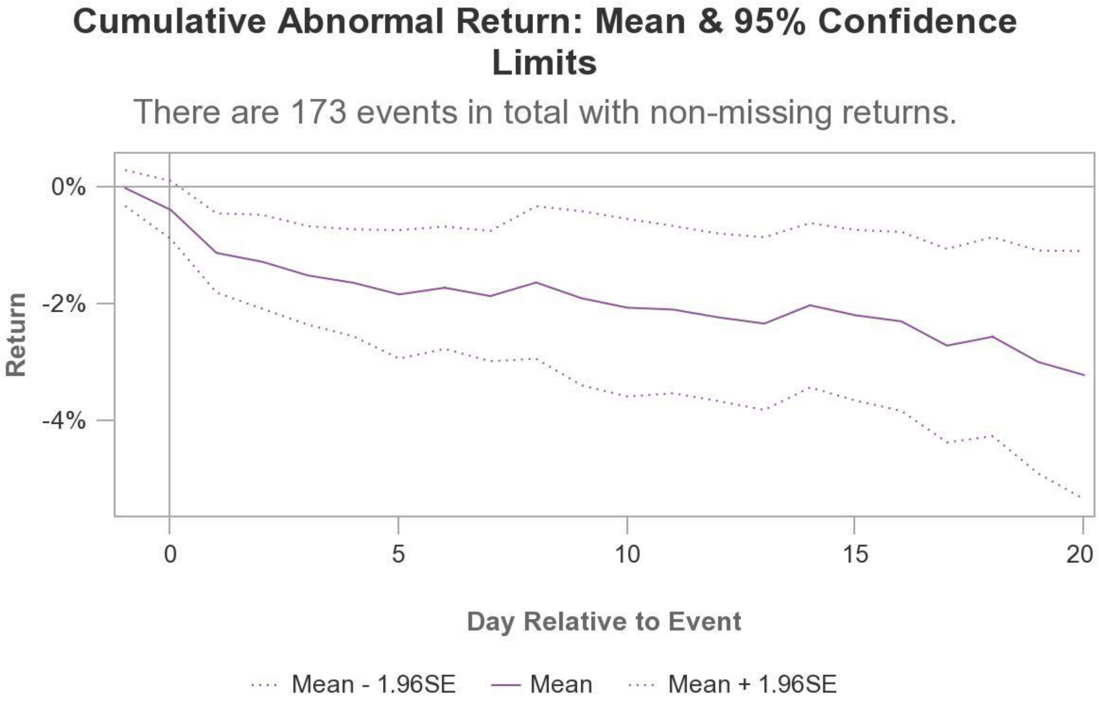

Figure 14: Mean CAR development of E-ISBs’ impact within a 22-day window (N=219)

4.4 Disruptive ISBs’ impact on date zero

This paragraph presents the results of hypothesis 5, which predicted that D-ISB have a negative impact on the short-term stock market value of publicly listed companies (measured from date zero).

Table 6 presents the results. The findings revealed a loss of 0.79% within a three-day window, which was supported by the CSect T at level 0.05 and Patell’s Z test at level 0.1.

In the seven-day event window, the results were not significant. Given that the literature only suggested an immediate impact, the study focused only on the short-term effects within three-day and seven-day windows. The results aligned with this notion, as the impact became less pronounced and statistically insignificant after five days. These findings partially supported hypothesis 5. The results per day are visible in Appendix 4 Tables

Table 6: D-ISBs' impact on date zero (N=45)
Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Event window	Mean CAR	CSect T	Patell's Z test
[-1, 1]	-0.0079	-2.0802**	-1.2214*
[-1, 5]	-0.0068	-0.9940	-0.7546

4.5 Disruptive and exploitive ISBs announcements' long-term impact

The results of hypothesis 6 are presented in this paragraph, testing if announcements of E-ISBs had a bigger negative impact on the long-term stock market value of publicly listed companies than D-ISBs. Table 7 presents the results of the analysis focusing on the long-term impact of announcing D-ISBs on a firm's market value. However, none of the obtained results were statistically significant, neither when using the market model nor the FFTF.

It is important to note that in the measurement spanning 184 days, data completeness issues resulted in the exclusion of two events. Similarly, in the measurement spanning 366 days, an additional two events were not recorded due to incomplete data. After assessing the outcomes, an additional 5% of the data were subjected to trimming to enhance the reliability of the analysis.

Table 7: D-ISB announcements' impact after 182 days (N=39) and 364 days (N=37)
Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Event window (D-ISBs)	BHAR	CSect T
Market Model		
[-1, 182]	0.0166	-0.0543
[-1, 364]	-0.0404	0.6864
Fama-French Three-Factor model		
[-1, 182]	-0.0348	-1.2668
[-1, 364]	-0.1519	0.4264

Table 8 displays the findings of the investigation examining the long-term consequences of disclosing E-ISBs on the market value of a company. The results indicated statistically significant outcomes after 182 days, with a decline of -12.89% and -10.44% using the market model and the FFTF, respectively. Moreover, the results after 364 days also exhibited significance, revealing a -26.95% decrease according to the market model and a -25.34% decline using the FFTF. All results were significant at 0.01 level.

It is worth noting that in the measurement spanning 182 days, four events were excluded due to incomplete data. Similarly, in the measurement spanning 364 days, an additional six events were not recorded due to data incompleteness. After assessing the outcomes, an additional 5% of the data were subjected to trimming to enhance the reliability of the analysis.

Table 8: E-ISB announcements' impact after 182 days (N=153) and 364 days (N=147)
Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Event window (E-ISBs)	Mean BHAR	CSect T
Market Model		
[-1, 182]	-0.1289	-3.8550***
[-1, 364]	-0.2695	-2.3838***
Fama-French Three-Factor model		
[-1, 182]	-0.1044	-3.8066***
[-1, 364]	-0.2534	-3.0973***

As the impact of D-ISBs does not yield any significant results, particularly in terms of negative effects, the findings support hypothesis 6. This suggests that the disclosure of E-ISBs has a more pronounced and negative influence on the long-term market value of publicly listed companies. This impact is both evident within a 184-day window and a 366-day window.

The results of all the hypotheses tests are summarized in Table 9.

Table 9: Summary of findings

Hypothesis	**Description**	**Supported**
1.	Announcements of ISBs have a negative impact on the short-term stock market value of publicly listed companies.	Yes
2.	The impact of announcements of ISBs on the stock market value of publicly listed companies diminishes within twenty days.	No
3.	Announcements of ISBs have a negative impact on the long-term stock market value of publicly listed companies.	Yes
4.	Announcements of E-ISBs have a bigger negative impact on the short-term stock market value of publicly listed companies than D-ISBs.	Partially supported
5.	D-ISB have a negative impact on the short-term stock market value of publicly listed companies (measured from date zero).	Partially supported
6.	Announcements of E-ISBs have a bigger negative impact on the long-term stock market value of publicly listed companies than D-ISBs.	Yes

5 Conclusion and discussion

This chapter aims to present a comprehensive summary and conclusions based on the results obtained in this study. In addition, it provides a thorough discussion, highlights the managerial implications, and addresses the limitations inherent in the research design.

Despite extensive research on ISBs, the literature is still inconsistent and contradictory on the effects and the best course of action for prevention (Harry & Gallagher, 2018; Spanos & Angelis, 2016). As highlighted in the introduction, the threats in cyberspace are growing and evolving (Gupta & Agarwal, 2017). To address the problem following problem statement is formulated: "What are the respective impacts of disruptive and exploitive information security breaches on the stock market value of publicly listed companies, and how do these impacts diverge over time?". This study added on the literature by exploring whether the type of ISB -disruptive or exploitive- influenced the severity of the impact on business performance, and how these impacts evolved over time, measured by the stock market reaction.

5.1 Summary of results and concluding remarks

5.1.1 ISB's Short-term impact

Numerous studies, such as Campbell et al. (2003) and Spanos & Angelis (2016), suggested that announcements of ISBs have a negative impact on the short-term stock market value of publicly listed companies. However, there were contrasting findings, for instance Kannan et al. (2007), who reported insignificant results. The findings of this study were in line with the earlier studies and provided robust evidence that, within a three-day and seven-day timeframe, announcements of ISBs led to a significant decrease in the stock market value.

5.1.2 ISB's impact over time

While there is a considerable amount of existing literature that examines the disclosure of short-term reactions of the stock market to ISBs, there is less research on the long-term stock market response following such incidents (Chang et al., 2021). Most studies in this domain indicated that the impact of ISBs tends to diminish in the weeks following the breach, with results becoming less statistically significant over time (e.g., Gatzlaff & McCullough, 2010; Yayla & Hu, 2011). Therefore, the second hypothesis in this study suggested that the impact would be less significant twenty days after the breach. However, the findings revealed that the stock market value loss more than doubles when measured within a twenty-day window, contradicting the initial hypothesis.

Furthermore, the results indicated that the impact of ISBs disclosure continues to grow significantly over a 184-day period and once again more than doubles within a 366-day period. While the literature remains limited about the long-term impact, based mostly on the research of Chang et al. (2020) and Romanosky, Hoffman, and Acquisti (2014), some arguments were made that a significant effect could persist within these timeframes. Surprisingly, the results of the study demonstrated highly significant impacts, highlighting the considerable threat that ISBs pose to business performance in the long-term.

5.1.3 Bifurcated results short-term

The existing literature provided evidence that the taxonomy proposed by Harry and Gallagher (2018) could potentially resolve some of the contradictions observed in prior studies regarding the impact of announcing ISBs. This taxonomy reclassified ISBs based on their effect on the victim organization. By doing so, it offers better alignment with the actual harm caused to business performance. Specifically, the taxonomy categorized ISBs into two primary groups: D-ISBs and E-ISBs. (Harry & Gallagher, 2018.) Prior research indicated that more significant results are observed when ISBs exhibit characteristics more closely aligned with the exploitive group. Building upon this insight, this study hypothesized that the impact of ISBs would be more pronounced if they are in the exploitive category. The results partially supported this notion, as both D-ISBs and E-ISBs demonstrated a similar level of harm to the business within the three-day window, but the results for the D-ISB were at lower significant levels (CSect T at 0.05 and Patell’s Z at 0.1 level). Moreover, D-ISBs lost their significance in the seven-day and 22-day windows, indicating a diminishing impact over time, in contrast to E-ISBs.

In addition, a hypothesis was put forth that D-ISBs may have an immediate negative impact on business performance, measured from date zero. The literature supported this theory, but to the best of my knowledge, this specific aspect has not been studied before. D-ISBs can be more visible, which adds to the uncertainty surrounding the event, potentially affecting the stock market value of companies (Bodie et al., 2011; Harry & Gallagher, 2018). The findings of this study partially supported this hypothesis, as the results indicate a significant impact within the three-day window. However, the significance levels of the results were low (CSect T at the 0.05 level and Patell's Z at the 0.1 level) and became insignificant in the seven-day window.

5.1.4 Bifurcated result long-term

Given the existing scarcity of research on the long-term effects of announcing ISBs on the stock market, there is even less evidence regarding the relative severity of D-ISBs versus E-ISBs. However, there was some research that provides a foundation for a theoretical argument suggesting that exploitive events have a greater negative impact on business performance in the long run compared to disruptive events (Romanosky, 2016; Yayla & Hu, 2011). Based on these theories, a hypothesis suggesting that E-ISBs do more harm than D-ISBs on the long-term was put forth in this study.

The results of this study supported the hypothesized notion in both the 184-day window and the 366-day window. Specifically, E-ISBs demonstrated strong statistical significance in these longer timeframes, indicating a significant negative impact on business performance. In contrast, D-ISBs did not exhibit any significant results, implying a lack of long-term effects on the stock market. These findings provided evidence that supported the hypothesis, suggesting that exploitive events have a more severe and enduring impact on business performance than disruptive events.

5.2 Theoretical contribution

The findings of this study demonstrated a significant and negative impact on the stock market value of publicly listed companies following the announcement ISBs, both in the short-term and over an extended period. These results contradicted some previous papers that either found no significant negative losses, observed a diminishing impact over time, or suggested a lack of long-term consequences (Kannan et al., 2007; Tosun, 2021; Yayla & Hu, 2011).

Additionally, the study introduced the concept of the moderating effect by classifying ISBs as either disruptive or exploitive, providing insights into their differential impacts on business performance. The study discovered significant moderating effects in nearly all timeframes, thus providing valuable insights into understanding which type of ISBs was more damaging and had a more significant influence on business performance, as well as how the resulting damage evolved over time, extending up to a year following the breach.

Additionally, this study uncovered a noteworthy finding that D-ISBs had a significant impact on the stock market value on the day of the event. To the best of my knowledge, previous studies has not examined the impact of ISBs specifically measured from the day of the breach itself. This finding suggests that threat that D-ISBs posses should not be disregarded, because the literature suggesting that it inflicts lesser damage (measured from the announcement day), as this study highlights the importance of considering immediate effects as well.

Furthermore, the study provided support for the value of the taxonomy proposed by Harry and Gallagher (2018). The research findings indicated a relationship between their classification groups and the severity of impacts, underscoring the value of the differentiation in the taxonomy, which in turn helps in understanding and assessing the consequences of types ISBs.

Overall, this thesis enhanced theoretical understanding by unravelling complex dynamics and consequences of ISBs in the context of stock market value and business performance.

5.3 Managerial relevance

The findings of this thesis hold managerial relevance for shareholders, cyber security specialists, and other decision-makers primarily in the U.S. Understanding the impact of ISBs on stock market value provides valuable insights for risk management and strategic planning. The identification of short-term and long-term effects of ISBs allows managers to better anticipate and mitigate potential financial losses. Moreover, the recognition of the differential impacts of disruptive and exploitive events enables managers to allocate resources and prioritize security measures effectively. By considering the immediate effects of ISBs, organizations can develop timely response strategies to minimize reputational damage and restore investor confidence.

The thesis also emphasized the importance of adopting the taxonomy proposed by Harry and Gallagher (2018) as a framework for classifying ISBs, providing managers with a practical tool to assess the severity of different threats and tailor their risk management approaches accordingly. Ultimately, the managerial implications derived from this thesis contribute to enhancing the resilience of organizations in the face of ISBs and safeguarding their long-term performance and market value.

5.4 Limitations & discussion

This study had several limitations that should be acknowledged. Firstly, the research scope was focused solely on ISBs that occur within the cyberspace, excluding the possibility of exploring ISBs in other contexts. Consequently, the findings did not capture the broader range of ISBs that can occur outside of the digital realm. Moreover, it is noteworthy that Harry & Gallagher (2018) exclusively labelled ISBs as cyber attacks in their research. However, upon closer examination of their database, it became evident that it also included ISBs that occurred accidentally. Thus, in this paper, the definitions proposed by Harry & Gallagher (2018) have been rectified accordingly, as outlined in paragraph 2.1.1.

Secondly, the dataset used in this study exclusively concentrates on businesses located within the U.S., which possessed a limitation to the generalizability of the findings to other regions.

Thirdly, due to the relatively smaller number of disruptive events included in the study, the results may have become insignificant more quickly. The diminished number of D-ISBs compared to E-ISBs undermines the validity and significance of hypotheses 4 and 6, thereby reducing their value as conclusive findings.

Fourthly, the overlap between disruptive announcements and zero-day events may have introduce ambiguity when attributing the observed effects solely to the ISBs or their corresponding announcements.

Fifthly, measuring the impact of an event in an event study based on the Efficient Market Hypothesis (EMH) has certainly limitations that should be considered (Fama, 1970):

1. The EMH assumes that investors are rational and make unbiased decisions based on all available information. However, human behaviour and cognitive biases can influence investment decisions, leading to market anomalies and deviations from the efficient market hypothesis.

2. Another limitation is that the EMH assumes that all relevant information is publicly available. However, there may have been instances where certain information about ISBs is not widely disseminated or is only accessible to a select group of market participants. This may have created information asymmetry and impact the efficiency of the market.

3. EMH relies on the assumption that any abnormal returns observed can be attributed solely to the event. However, stock markets may have exhibited various inefficiencies and complexities that can influence returns, such as market-wide trends, macroeconomic factors, or other company-specific events. This is limited by deletion confounding factors but can not be fully overcome. Thus, isolating the exact impact of ISBs on stock returns using CAR and BHAR is limited to some degree.

4. Additionally, utilizing the EMH to measure the impact on business performance may not capture other important dimensions of the impact of ISB, for example physical or emotional damage to employees. These non-financial consequences are aspects that can influence the overall effect of ISBs on business performance and may not be fully captured by the chosen measurements.

Finally, the used methods in an event study have certain limitations that should be considered (Armitage, 1995):

1. The use of event windows to capture the impact of ISBs may introduce potential biases. The selection of the event window duration can significantly affect the calculated CAR and BHAR values. Different event window lengths may have led to different interpretations of the impact and make it difficult to compare the results across different studies. This is mitigated by the use of various event windows but can not be fully overcome.

2. The measurements used in the study, the market model, CAR, BHAR, and FFTF exhibit differences in formula and may not perfectly align with each other. Consequently, drawing definitive conclusions about whether the impact of ISBs has worsened or improved over time is challenging due to discrepancies between these measurements.

5.5 Future research

Building upon the insights and limitations identified in this study, future research can contribute to a deeper understanding of the impacts of ISBs on businesses. One potential avenue for further exploration is to extend the geographical scope beyond the U.S. and include other regions, such as Europe or Asia. This broader perspective would allow for a comparative analysis of the impacts of ISBs across different contexts, taking into account variations in regulatory frameworks, cultural factors, and industry characteristics.

In addition, future studies can explore alternative methodologies to measure the financial consequences of ISBs, considering the limitations associated with CAR and BHAR measurements. For instance, researchers can investigate the applicability of event study methodologies that incorporate different benchmarks or control groups. This approach would provide a more nuanced analysis of abnormal stock returns, helping to capture the specific impacts attributable to ISBs.

Furthermore, the taxonomy proposed by Harry and Gallagher (2018) offers a promising avenue for future research. This taxonomy introduces five subgroups within the overarching categories of disruptive and exploitive events. Investigating these subgroups could yield valuable insights into the varying levels of threat severity posed by different types of ISBs. This research would contribute to a more nuanced understanding of the specific characteristics and dynamics that influence the impacts of ISBs on business performance.

By pursuing these future research directions, scholars can further refine our understanding of the multifaceted implications of ISBs, extend the geographical and conceptual boundaries of the current knowledge base, and provide practical insights for policymakers and practitioners in effectively managing and mitigating the risks associated with ISBs.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 proceedings, 94.*

Ali, S. E. A., Lai, F. W., Dominic, P. D. D., Brown, N. J., Lowry, P. B. B., & Ali, R. F. (2021). Stock market reactions to favorable and unfavorable information security events: A systematic literature review. *Computers & Security,* 110, 102451.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies,* 23, 1177-1206.

Armitage, S. (1995). Event study methods and evidence on their performance. *Journal of Economic Surveys,* 9(1), 25-52.

Barber, B. M., & Lyon, J. D. (1997). Detecting long-run abnormal stock returns: The empirical power and specification of test statistics. *Journal of Financial Economics,* 43(3), 341-372.

Bishop, M. (2003). *Computer security: Art and science.* 2003. Westford, MA: Addison Wesley Professional, 4-12.

Bodie, Z., Kane, A., & Marcus, A. J. (2011). *Investments*. McGraw-Hill/Irwin.

Böhme, R., & Moore, T. (2016). The “iterated weakest link” model of adaptive security investment. *Journal of Information Security,* 7(02), 81.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. An analysis of the nature of groups engaged in cyber crime, *International Journal of Cyber Criminology,* 8(1), 1-20.

Campbell, C. J., Cowan, A. R., & Salotti, V. (2010). Multi-country event-study methods. *Journal of Banking & Finance*, 34(12), 3078-3090.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breach: Empirical evidence from the stock market. *Journal of Computer Security,* 11(3), 431–448.

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.

Chang, K. C., Gao, Y. K., & Lee, S. C. (2020). The effect of data theft on a firm's short-term and long-term market value. *Mathematics*, 8(5), 808.

CISSM Cyber Events Database. (n.d.). Center for International and Security Studies at Maryland. <https://cissm.umd.edu/cyber-events-database>, retrieved 30.5.2023.

Capano, D. E. (2021). *Throwback attack: How NotPetya accidentally took down global shipping giant Maersk.* Industrial Cybersecurity Pulse. <https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/>, retrieved 24.5.2023.

Daswani, N., & Elbayadi, M. (2021). The Yahoo breaches of 2013 and 2014. *In Big Breaches* (pp. 155-169). Apress, Berkeley, CA.

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.

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, 21(4), 43-57.

Dixit, A. K., & Pindyck, R. S. (1994). *Investment under uncertainty.* Princeton University Press.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, 15(1), 105-122.

Fama, E. F., & French, K. R. (1992). The cross-section of expected stock returns. *The Journal of Finance,* 47(2), 427-465.

Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance,* 25(2), 383-417.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2), 74–83.

Gartner. (2018, December). *IT key metrics data 2019: Executive summary.* <https://www.gartner.com/en/documents/3895271>, retrieved 18.3.2023.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review,* 13(1), 61-83.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7), 404–410.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS quarterly*, 567-594.

Hadnagy, C., & Fincher, M. (2015). *Phishing dark waters: The offensive and defensive sides of malicious emails.* John Wiley & Sons.

Harry, C., & Gallagher, N. (2018). Classifying cyber events. *Journal of Information Warfare*, 17(3), 17–31.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, 52(3), 337-347.

Householder, A. D., Wassermann, G., Manion, A., & King, C. (2017). *The cert guide to coordinated vulnerability disclosure*. Carnegie-Mellon Univ Pittsburgh Pa Pittsburgh United States.

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, 97–121. https://doi.org/10.1046/j.1098-1616.2003.026.x

Huang, K., & Madnick, S. (2020). A cyberattack doesn’t have to sink your stock price. *Harvard Business Review.*

IBM Documentation. (2021, August). Statistics - parametric and nonparametric. <https://www.ibm.com/docs/en/db2woc?topic=procedures-statistics-parametric-nonparametric>, retrieved 29.05.2023.

International Organization for Standardization. (2018). ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. <https://www.iso.org/standard/73906.html>, retrieved 21.3.2023.

Jovanovic, B. (2022, 2 november). *Better safe than sorry: Cyber security statistics and trends for 2022*. Dataprot. <https://dataprot.net/statistics/cyber-security-statistics/>, retrieved 22.2.2023.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce,* 12(1), 69–91. https://doi.org/10.2753/jec1086-4415120103

Kaspersky. (2015). *Equation group: The crown creator of cyber-espionage*. <https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage>, retrieved 11.5.2023.

Liff, A. P. (2012). Cyberwar: a new ‘absolute weapon’? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, 35(3), 401-428.

Madura, J. (2008). *Financial institutions and markets*. Thomson.

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

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53.

National Institute of Standards and Technology. (2012). Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology (NIST SP 800-61). <https://csrc.nist.gov/glossary>, retrieved 29.05.2023.

Neely, A. (2005). The evolution of performance measurement research: developments in the last decade and a research agenda for the next. *International Journal of Operations & Production Management*, 25(12), 1264-1277.

Park, N. K. (2004). A guide to using event study methods in multi-country settings. *Strategic Management Journal*, 25(7), 655-668.

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, 39(1), 3-es.

Perlroth, N., Shane, S., & Sanger, D. E. (2017). Security breach and spilled secrets have shaken the NSA to its core. *New York Times*, 12, 214-228.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, M. (2006). *Security in computing, prentice hall*. Boston–MA, USA.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Ritter, J. R. (1991). The long-run performance of initial public offerings. *The Journal of Finance*, 46(1), 3-27.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, 11(1), 74-104.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121-135

Rosenblatt, M. (1956). A central limit theorem and a strong mixing condition. *Proceedings of the National Academy of Sciences*, 42(1), 43-47.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3).

Shankar, N., & Mohammed, Z. (2020). Surviving data breaches: A multiple case study analysis. *Journal of Comparative International Management*, 23(1), 35–54.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216-229.

Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary security policy*, 33(1), 148-170.

Tanimura, J. K., & Wehrly, E. W. (2009). The market value and reputational effects from lost confidential information. *International Journal of Financial Management*, Vol, 5, 18-35.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, p. 76, 101795.

Tripathi, M. & Mukhopadhyay, A. (2020). Financial loss due to a data privacy breach: An empirical analysis. *Journal of Organisational Computing and Electronic Commerce*, 30 (4), s. 381–400. doi:10.1080/10919392.2020.1818521

Vanhoef, M., & Piessens, F. (2017, October). Key reinstallation attacks: Forcing nonce reuse in WPA2. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1313-1328).

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

Wharton Research Data Services. "WRDS". (n.d.) <wrds.wharton.upenn.edu>, from retrieved 2023.05.30.

Whitman, M. E., & Mattord, H. J. (2012). *Roadmap to information security: For IT and infosec managers*. Cengage Learning.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, 26(1), 60-77.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. In: *IEEE Communications Surveys & Tutorials*, 15(4), 2046-2069.

Appendices

Appendix 1 List of ISBs

Table 10: List of companies that experience an ISB including the announcement date

Announcement date	Publicly listed company	ISB-Type
23-5-2022	MGM Resorts	Exploitive
23-5-2022	General Motors	Exploitive
11-5-2022	Omnicell	Disruptive
6-5-2022	AGCO	Disruptive
22-4-2022	T-Mobile	Exploitive
27-4-2022	Tenet Healthcare Corporation	Disruptive
18-4-2022	Devon Energy Corporation	Disruptive
22-3-2022	Microsoft	Exploitive
25-2-2022	Nvidia	Exploitive
15-12-2021	Acorda Therapeutics	Exploitive
4-1-2022	USCellular	Exploitive
12-11-2021	Costco Wholesale Corporation	Exploitive
11-11-2021	Hewlett Packard Enterprise	Exploitive
11-6-2021	Mcdonald's	Exploitive
10-6-2021	Electronic Arts	Exploitive
14-6-2021	Maximus	Exploitive
30-4-2021	First Horizon Corporation	Exploitive
22-4-2021	CNA Financial	Disruptive
26-4-2021	Honeywell	Disruptive
17-6-2021	Carnival Corporation	Exploitive
10-3-2021	Molson Coors	Disruptive
9-3-2021	Tesla	Exploitive
9-2-2021	T-Mobile	Exploitive
16-2-2021	Pfizer	Exploitive
19-2-2021	Kroger	Exploitive
25-2-2021	WestRock	Disruptive
25-1-2021	Walmart	Exploitive
11-1-2021	Ubiquiti	Exploitive
4-2-2022	News Corp	Exploitive
29-12-2020	T-Mobile	Exploitive
24-12-2020	Citrix	Disruptive

Announcement date	Publicly listed company	ISB-Type
11-12-2020	SolarWinds	Exploitive
21-12-2020	VMware	Exploitive
18-12-2020	Cisco	Exploitive
17-12-2020	Microsoft	Exploitive
8-12-2020	FireEye	Exploitive
25-11-2020	Belden	Exploitive
17-11-2020	Americold	Disruptive
26-10-2020	Steelcase	Disruptive
29-9-2020	Arthur J, Gallagher & Co,	Disruptive
24-9-2020	Tyler Technologies	Disruptive
21-9-2020	Activision	Exploitive
20-8-2020	MoneyGram	Disruptive
25-8-2020	MoneyGram	Disruptive
27-8-2020	NCR Corporation	Exploitive
24-8-2020	PayPal	Disruptive
18-8-2020	Santander	Exploitive
14-8-2020	R1 RCM	Disruptive
6-8-2020	Intel	Exploitive
30-7-2020	Moderna	Exploitive
3-11-2020	Mattel	Disruptive
24-7-2020	Garmin	Disruptive
22-7-2020	Twilio	Exploitive
28-5-2020	Cisco	Exploitive
11-5-2020	Diebold Nixdorf	Disruptive
8-5-2020	Gilead Sciences	Exploitive
7-5-2020	Microsoft	Exploitive
11-5-2020	Genworth Financial	Exploitive
20-4-2020	Cognizant	Disruptive
31-3-2020	Marriott International	Exploitive
25-3-2020	AMD	Exploitive
23-3-2020	General Electric (GE) via Canon Business Process Services	Exploitive
5-3-2020	Carnival Corporation	Exploitive
4-3-2020	T-Mobile	Exploitive
20-3-2014	Microsoft	Exploitive
19-2-2020	MGM Resorts	Exploitive
27-2-2020	EMCOR Group	Disruptive

Announcement date	Publicly listed company	ISB-Type
12-2-2020	Altice USA Inc.	Exploitive
3-2-2020	Golden Entertainment	Exploitive
28-1-2020	Tissue Regenix Group PLC	Exploitive
21-1-2020	100 UPS Store Locations	Exploitive
27-11-2019	Adobe	Exploitive
21-11-2019	T-Mobile	Exploitive
14-11-2019	Macy's	Exploitive
31-10-2019	Marriott International	Exploitive
29-10-2019	Bed Bath & Beyond	Exploitive
16-10-2019	Ingredion Incorporated	Disruptive
15-10-2019	Pitney Bowes	Disruptive
18-10-2019	Mission Health	Exploitive
2-10-2019	Zendesk	Exploitive
17-9-2019	Magellan Health	Exploitive
13-8-2019	Choice Hotels	Exploitive
5-8-2019	AT&T	Exploitive
29-7-2019	Capital One	Exploitive
27-6-2019	PCM Inc.	Exploitive
8-5-2019	Amazon	Exploitive
30-4-2019	Charles River Laboratories International, Inc.	Exploitive
17-4-2019	Chipotle	Exploitive
11-3-2019	Citrix	Exploitive
6-3-2019	Zillow	Disruptive
11-2-2019	Dunkin' Donuts	Exploitive
28-1-2019	Discover Financial Services	Exploitive
28-1-2019	DXC Technology	Exploitive
28-1-2019	Huntington Ingalls Industries	Exploitive
28-1-2019	Hewlett Packard Enterprise	Exploitive
28-1-2019	IBM	Exploitive
28-1-2019	Sabre	Exploitive
17-12-2018	The Wall Street Journal's website	Disruptive
30-11-2018	Marriott International	Exploitive
28-11-2018	Dunkin' Donuts	Exploitive
16-11-2018	HealthEquity	Exploitive
12-11-2018	LPL Financial	Exploitive
2-11-2018	HSBC	Exploitive

Announcement date	Publicly listed company	ISB-Type
1-10-2018	Apollo	Exploitive
28-9-2018	Toyota (North America)	Exploitive
28-9-2018	Facebook	Exploitive
25-9-2018	Chegg	Exploitive
24-9-2018	T-Mobile	Exploitive
22-8-2018	Cheddar Scratch Kitchen	Exploitive
6-8-2018	Vantiv	Exploitive
16-7-2018	LabCorp	Disruptive
9-7-2018	Macy's Inc.	Exploitive
9-7-2018	Blizzard Entertainment	Disruptive
28-6-2018	Adidas	Exploitive
27-6-2018	Ticketmaster	Exploitive
21-6-2018	Humana	Exploitive
14-6-2018	HealthEquity	Exploitive
28-5-2018	Arlo	Exploitive
25-5-2018	American Family Life Assurance Company of Columbus (Aflac)	Exploitive
10-5-2018	Nuance	Exploitive
4-5-2018	Fleetcor Technologies	Exploitive
17-4-2018	Sangamo Therapeutics	Exploitive
13-4-2018	Inogen	Exploitive
2-4-2018	Boardwalk Pipeline Partners LP	Disruptive
2-4-2018	Oneok Inc	Disruptive
29-3-2018	Under Armour	Exploitive
28-3-2018	Boeing	Disruptive
16-3-2018	Frost Bank	Exploitive
20-2-2018	Tesla	Exploitive
18-1-2018	Allscripts	Disruptive
17-10-2017	Microsoft	Exploitive
11-10-2017	Equifax	Exploitive
12-10-2017	Hyatt Hotels Corp.	Exploitive
6-10-2017	Forrester Research	Exploitive
26-9-2017	Sonic Drive-In	Exploitive
14-8-2017	Blizzard Entertainment	Disruptive
31-7-2017	FireEye	Exploitive
28-7-2017	Wix.com	Exploitive
7-9-2017	Equifax	Exploitive

Announcement date	Publicly listed company	ISB-Type
27-6-2017	Mondelez International	Disruptive
27-6-2017	Merck	Disruptive
27-6-2017	Nuance Communications	Disruptive
23-6-2017	Microsoft	Exploitive
16-6-2017	The Buckle Inc.	Exploitive
12-5-2017	FedEx	Disruptive
3-5-2017	Gannett Co.	Exploitive
27-4-2017	Facebook	Exploitive
27-4-2017	Google	Exploitive
25-4-2017	Chipotle	Exploitive
7-4-2017	Gamestop	Exploitive
14-3-2017	Dun & Bradstreet	Exploitive
7-3-2017	Verifone	Exploitive
23-2-2017	Apple	Exploitive
27-1-2017	Sunrun	Exploitive
25-1-2017	U.S. Cellular	Exploitive
28-12-2016	Intercontinental Hotel Group (IHG)	Exploitive
12-12-2016	Quest Diagnostics	Exploitive
22-11-2016	Madison Square Garden	Exploitive
12-10-2016	Vera Bradley	Exploitive
16-9-2016	SS&C Technologies	Exploitive
11-8-2016	PAR Technology	Exploitive
14-6-2016	HSBC	Disruptive
8-7-2016	Amazon	Exploitive
28-6-2016	Noodles & Company	Exploitive
21-6-2016	Carbonite	Exploitive
15-6-2016	Multi-Color Corporation	Exploitive
7-6-2016	Twitter	Exploitive
1-6-2016	FOX News	Disruptive
6-5-2016	Equifax	Exploitive
4-5-2016	Brunswick Corp.	Exploitive
3-5-2016	ADP	Exploitive
7-3-2016	Seagate	Exploitive
27-1-2016	Wendy's	Exploitive
13-1-2016	Citrix	Exploitive
24-12-2015	EA	Disruptive

Announcement date	Publicly listed company	ISB-Type
19-1-2015	Juniper Networks	Exploitive
15-10-2015	EA	Exploitive
1-10-2015	T-Mobile US (via Experian)	Exploitive
25-9-2015	Hilton Hotel	Exploitive
24-8-2015	Auto Zone	Exploitive
7-8-2015	American Airlines Group Inc.	Exploitive
7-8-2015	Sabre Corporation	Exploitive
31-7-2015	Hanesbrands Inc.	Exploitive
29-7-2015	United Airlines	Exploitive
17-7-2015	CVS	Exploitive
17-7-2015	Rite Aid	Exploitive
14-7-2015	Walgreens	Exploitive
28-5-2015	copart.com	Exploitive
7-5-2015	Intercontinental Hotel Group	Exploitive
4-5-2015	Sally Beauty Supply	Exploitive
27-4-2015	Tesla	Disruptive
22-4-2015	Hyatt Hotels Corporation	Exploitive
3-3-2015	ASML	Exploitive
2-3-2015	Natural Grocers	Exploitive
10-2-2015	Delta Airlines	Disruptive
9-2-2015	Chipotle	Disruptive
4-2-2015	Anthem	Exploitive
27-10-2014	Fidelity National Financial	Exploitive
21-10-2014	Staples	Exploitive
14-8-2014	Supervalu	Exploitive
30-9-2014	Microsoft	Exploitive
23-9-2014	Activision Blizzard	Disruptive
2-9-2014	The Home Depot	Exploitive
29-9-2014	JPMorgan	Exploitive
22-8-2014	MeetMe	Exploitive
20-8-2014	UPS	Exploitive
19-8-2014	Community Health Systems	Exploitive
15-8-2014	Supervalu	Exploitive
17-7-2014	Dominion Resources	Exploitive
16-7-2014	AECOM	Exploitive
14-7-2014	Boeing	Exploitive

Announcement date	Publicly listed company	ISB-Type
14-7-2014	Lockheed Martin	Exploitive
17-6-2014	Move, Inc,	Disruptive
13-6-2014	AT&T	Exploitive
9-6-2014	Rowan Companies	Exploitive
21-5-2014	eBay	Exploitive
10-2-2014	Boston Scientific	Exploitive
5-2-2014	Comcast	Exploitive

Appendix 2 Data management plan

The CISSM Cyber Events Database (n.d.) is a valuable resource for understanding cyber threats across industries and regions. As a researcher, it is important to have a well-structured data management plan in place to ensure that data is managed in a secure, organised, and ethical manner. This plan outlines the steps that will be taken to manage data obtained from the Cyber Events Database.

Data Collection: The data used in this study is collected from the CISSM Cyber Event Database (n.d.) from the University of Maryland, which contains information on cyber events from 2014 to the present. The data is updated monthly and contains information on the threat actor, motive, victim, industry, and end effects of the attack. The database was created to address the lack of consistent, well-structured data necessary for making strategic decisions about how to invest resources to prevent and respond to cyber events. (CISSM Cyber Event Database, n.d.) The dataset is freely available to the public. However, I have gained personal access to download the full dataset (as this not generally permitted).

Data Storage: All data obtained from the Cyber Events Database will be stored on a secure, password-protected computer. Access to the data will be restricted to me only. The data will be organised in a systematic and consistent manner to ensure easy access and retrieval (version controlled). Backup copies of the data will be made regularly to prevent data loss and prevent definite faulty changes. The data will be deleted after completion of the thesis work. All original data will be kept in separate files from the files where changes will be made.

Ethical Considerations: All data obtained from the Cyber Events Database will be used in an ethical manner. Personal information is not stored or collected, and all data will be kept confidential.

Appendix 3 CISSM data collection (CISSM Cyber Event Database, n.d.)

The CISSM gathers data for its cyber event database using a mixed-methods approach that combines automated data scraping and manual review and coding by a research team. The process involves the following steps (see Figure 15) (CISSM Cyber Event Database, n.d.):

Data Scraping: A Python script is used to scrape data from relevant cyber sources, including websites on the open internet and dark web. The script accesses each site's main landing page and retrieves information such as the date published, title, URL, and article preview. This data is saved in comma-separated values (.csv) files. (CISSM Cyber Event Database, n.d.)

Review and Validation: The research team of the university of Maryland meticulously reviews and codes the gathered data. They meticulously assess whether the identified events align with the established definition of a cyber event. Furthermore, they categorize the type of threat actor, discern their motives, determine the country of origin of the threat actor, ascertain the targeted country, and classify the industry affected by the event along with its specific impacts. Finally, the researchers exercise their expertise to make conclusive judgments regarding the validity of the events as eligible members of the dataset. (CISSM Cyber Event Database, n.d.)

Validity, reliability and objectivity:

Validity: The database aims to ensure the validity of the events by defining a cyber event as the end result of unauthorized efforts or technical actions that achieve a desired primary effect on a target using computer technology and networks. The researchers trace each event back to an underlying source to gather details surrounding the event itself. This helps establish the validity of the events included in the dataset. (CISSM Cyber Event Database, n.d.)

Reliability: The reliability of the data can be assessed in several ways. The use of a Python script for data scraping adds a level of consistency and reduces the potential for human error. The manual review and coding process by the research team also contribute to the reliability of the data as they exercise judgment and expertise in categorizing and classifying the events. However, it's important to note that the reliability is dependent on the accuracy of the source material and the effectiveness of the review process. (CISSM Cyber Event Database, n.d.)

The objective of the data collection process is to create a comprehensive and structured database of cyber events. The data is collected using a mixed-methods approach, combining automated scraping with manual review and coding. By employing a Python script to gather data from various sources and subsequently reviewing and coding the collected data, the CISSM aims to ensure a comprehensive and reliable representation of cyber events in their database. (CISSM Cyber Event Database, n.d.)

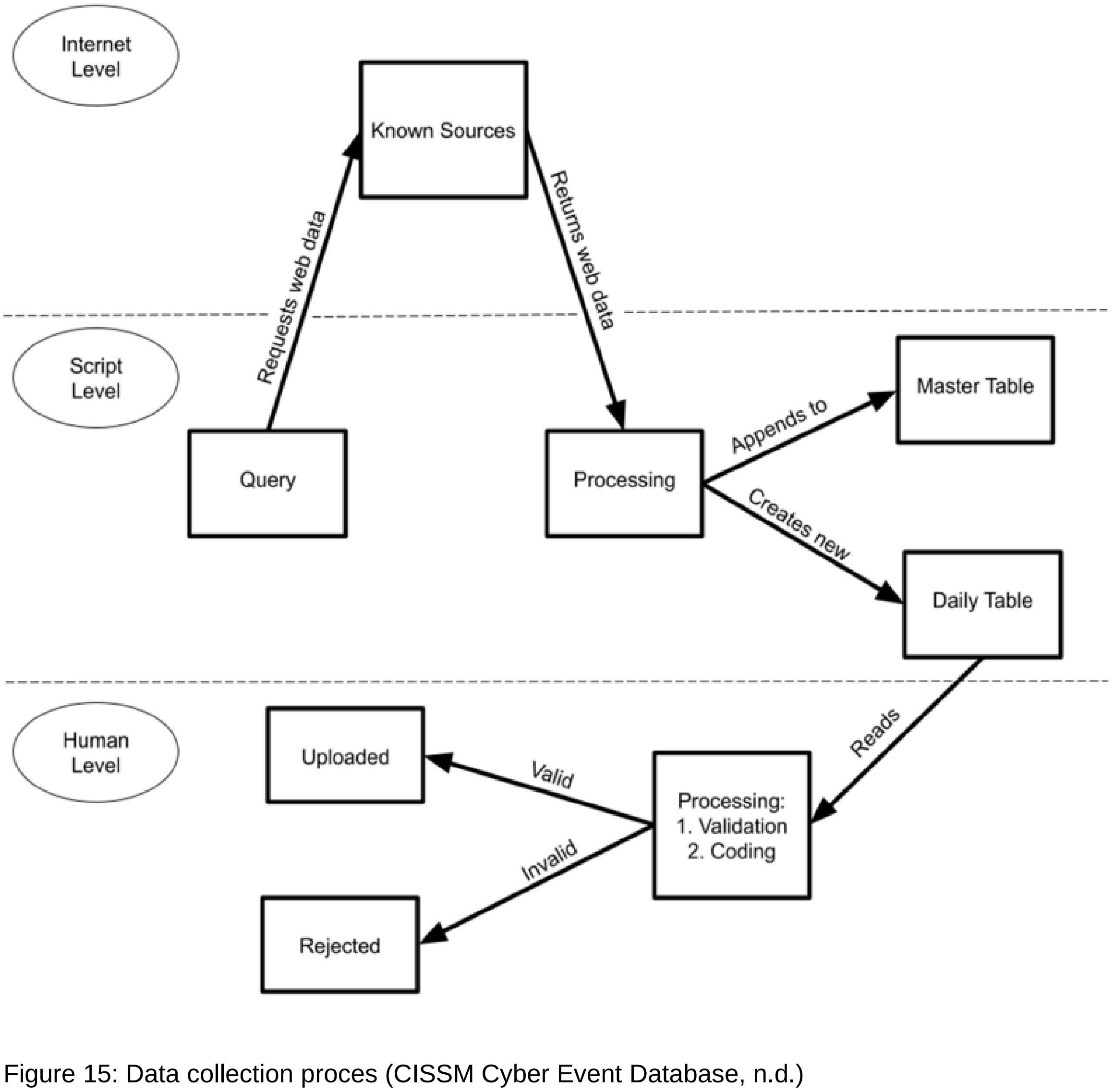

Figure 15: Data collection proces (CISSM Cyber Event Database, n.d.)

Appendix 4 Tables ISB announcements’ impact up to twenty days

Day = days distance to event date

Negative = Number of negative records per day

Total = Total number of records per day

Mean CAR = Mean CAR per day

Mean R = Mean return per day

Mean AR = Mean abnormal return per day

CAR – T = CAR T-statistic value per day

CAR – P = CAR probability per T value per day

Table 11: ISB announcements’ impact up to twenty days (N=219)

Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Day	negative	Mean CAR	Mean R	Mean AR	CSect T	CSect T - P
-1	105	-0.001157355	0.001559	-0.00116	-0.89287031***	0.372911
0	122	-0.004767549	-0.00351	-0.00361	-2.210161943***	0.028134
1	122	-0.011403466	-0.00498	-0.00664	-3.942488403***	0.000109
2	117	-0.01253808	-0.00059	-0.00113	-3.708688464***	0.000264
3	117	-0.014314964	-3.41E-06	-0.00178	-3.9653623***	9.94E-05
4	114	-0.01544671	-0.00046	-0.00113	-3.853755366***	0.000153
5	114	-0.016354137	-0.00128	-0.00091	-3.433778509***	0.000712
6	111	-0.01428546	0.002987	0.002069	-3.046927603***	0.002597
7	118	-0.015850062	-0.00172	-0.00156	-3.163899124***	0.001779
8	98	-0.013590382	0.002788	0.00226	-2.38632945***	0.017872
9	115	-0.015745978	-0.00311	-0.00216	-2.469005927***	0.014317
10	124	-0.017323746	-0.00083	-0.00158	-2.641427504***	0.008854
11	118	-0.0170747	0.001139	0.000249	-2.791448054***	0.005713
12	114	-0.017796356	-0.00043	-0.00072	-2.881008811***	0.00436
13	111	-0.020410175	-0.00112	-0.00261	-3.158397973***	0.001811
14	102	-0.016013654	0.003754	0.004397	-2.588866094***	0.010277
15	114	-0.01742874	-0.00017	-0.00142	-2.712148273***	0.007218
16	113	-0.018893915	-0.00089	-0.00147	-2.848518297***	0.004813
17	114	-0.021051589	-0.00315	-0.00216	-2.937606246***	0.003663
18	105	-0.020325382	0.003105	0.000726	-2.771238154***	0.006067
19	103	-0.022145083	0.000454	-0.00182	-2.707544031***	0.007316
20	124	-0.023941805	-0.0014	-0.0018	-2.670909727***	0.008135

Table 12: Short-term disruptive events (N=45)

Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Day	Negative	Mean CAR	Mean R	Mean AR	CSect T	CSect T - P
-1	27	-0.00364	-0.00235	-0.00364	-1.880616723*	0.066505
0	27	-0.00679	-0.00675	-0.00316	-1.718455346*	0.092588
1	26	-0.01083	-0.00102	-0.00404	-2.282899811**	0.027212
2	23	-0.01058	0.000712	0.000254	-2.162961882**	0.035895
3	22	-0.01026	-0.00011	0.000314	-1.711000042*	0.093967
4	26	-0.01093	0.00045	-0.00066	-1.416295114	0.163574
5	24	-0.0078	0.005679	0.00313	-0.917305194	0.363873
6	18	-0.00223	0.004707	0.005568	-0.227224572	0.821278
7	25	-0.00433	-0.0009	-0.00211	-0.406626764	0.68621
8	19	-0.00229	0.002135	0.002048	-0.215769056	0.830143
9	28	-0.00243	-0.00251	-0.00014	-0.23262228	0.81711
10	24	-0.0039	-0.00283	-0.00147	-0.342542061	0.733538
11	18	-0.00151	0.00725	0.002388	-0.155836784	0.876859
12	22	6.37E-05	-0.00046	0.001578	0.006105877	0.995155
13	25	-0.0084	-0.00511	-0.00847	-0.689764693	0.493884
14	18	0.000781	0.008144	0.009185	0.065972993	0.947692
15	23	0.000467	-0.00145	-0.00031	0.037870798	0.969958
16	26	-0.00261	-0.00365	-0.00307	-0.222119701	0.825226
17	20	0.002688	0.00332	0.005294	0.219176138	0.827504
18	21	0.000408	0.002763	-0.00228	0.033007729	0.973814
19	16	0.007965	0.008718	0.007556	0.618554282	0.539329
20	25	0.007767	0.002995	-0.0002	0.628869134	0.532614

Table 13: Short-term Exploitive (N=174)

Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Day	Negative	Mean CAR	Mean R	Mean AR	CSect T	CSect T - P
-1	78	-0.0005	0.002598481	-0.0005	-0.31973	0.74956101
0	95	-0.00423	-0.002649602	-0.00373	-1.67546*	0.095660653
1	96	-0.01156	-0.006034373	-0.00733	-3.35598***	0.0009733
2	94	-0.01306	-0.00093183	-0.0015	-3.19895***	0.001642289
3	95	-0.01539	2.47583E-05	-0.00233	-3.5909***	0.000429746
4	88	-0.01665	-0.000706017	-0.00126	-3.58251***	0.000442796
5	90	-0.01863	-0.003134553	-0.00198	-3.33382***	0.00104905
6	93	-0.01749	0.002529218	0.001138	-3.28799***	0.001223557
7	93	-0.01891	-0.001933135	-0.00142	-3.33783***	0.001034951
8	79	-0.0166	0.002961741	0.002316	-2.50261**	0.013261193
9	87	-0.01929	-0.003269833	-0.00269	-2.54739**	0.01172911
10	100	-0.02089	-0.000304589	-0.00161	-2.70552***	0.007506278
11	100	-0.02121	-0.000485938	-0.00032	-2.91412***	0.004041361
12	92	-0.02255	-0.000422912	-0.00133	-3.09637***	0.002287984
13	86	-0.0236	-0.000061774	-0.00106	-3.14303***	0.001969634
14	84	-0.02048	0.002586735	0.003123	-2.86529***	0.00468606
15	91	-0.02219	0.000171498	-0.00171	-2.99075***	0.003191636
16	87	-0.02322	-0.000152892	-0.00104	-2.98605***	0.003238548
17	94	-0.02736	-0.00487445	-0.00414	-3.25128***	0.001382412
18	84	-0.02584	0.003196316	0.001525	-2.98718***	0.003227267
19	87	-0.03015	-0.001743523	-0.00431	-3.10945***	0.002194262
20	99	-0.03237	-0.002567686	-0.00222	-3.00133***	0.003088168

Table 14: ISBs' impact after date zero (N=45)

Statistical significance is indicated with *, ***, and *** at the 0.1, 0.05, and 0.01 levels, respectively.

Day	Negative	Mean CAR	Mean R	Mean AR	CSect T	CSect T - P
-1	23	-0.001256407	0.003594496	-0.00126	-0.49112176	0.62578116
0	24	-0.001751208	-0.003303261	-0.00049	-0.49838204	0.62069705
1	30	-0.007891787	-0.003543591	-0.00614	-2.08018299**	0.043365037
2	18	-0.004356423	0.001161912	0.003535	-0.83131126	0.410286563
3	28	-0.006665232	-0.001139228	-0.00231	-1.14400121	0.258808822
4	21	-0.008060354	-0.004880477	-0.0014	-1.21100397	0.23235841
5	26	-0.00678007	0.000771131	0.00128	-0.99401563	0.32565053