UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M. FANNO"

CORSO DI LAUREA MAGISTRALE IN ECONOMICS AND FINANCE

TESI DI LAUREA

"THE EFFECT OF CYBERATTACKS ON EUROPEAN FINANCIAL INSTITUTIONS: AN EVENT STUDY APPROACH"

RELATORE:

CH.MO PROF. FABIO MANENTI

LAUREANDO: FILIPPO GERVASUTTI

MATRICOLA N. 2036093

ANNO ACCADEMICO 2023 – 2024

Dichiaro di aver preso visione del "Regolamento antiplagio" approvato dal Consiglio del Dipartimento di Scienze Economiche e Aziendali e, consapevole delle conseguenze derivanti da dichiarazioni mendaci, dichiaro che il presente lavoro non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere. Dichiaro inoltre che tutte le fonti utilizzate per la realizzazione del presente lavoro, inclusi i materiali digitali, sono state correttamente citate nel corpo del testo e nella sezione 'Riferimenti bibliografici'.

I hereby declare that I have read and understood the "Anti-plagiarism rules and regulations" approved by the Council of the Department of Economics and Management and I am aware of the consequences of making false statements. I declare that this piece of work has not been previously submitted – either fully or partially – for fulfilling the requirements of an academic degree, whether in Italy or abroad. Furthermore, I declare that the references used for this work – including the digital materials – have been appropriately cited and acknowledged in the text and in the section 'References'.

Firma (signature)

“The chances that we would have a breakdown that looked anything like that where you had banks making terrible loans and investment decisions and needing and having low levels of liquidity and weak capital positions, and thus needing a government bailout, the chances of that are very, very low. [...] But the world changes. The world evolves. And the risks change as well. And I would say that the risk that we keep our eyes on the most now is cyber risk. That's really where the risk I would say is now, rather than something that looked like the global financial crisis. [...] There are cyber-attacks every day on all major institutions now. That's a big part of the threat picture in today's world.”

— Jerome Powell, Federal Reserve Chairman, CBS News on April 11, 2021

TABLE OF CONTENTS

ABSTRACT

Cyber risk has been a widely debated issue in recent years. The financial world could prove particularly vulnerable when it comes to cyberattacks, given the high level of interconnection between all of the sector's players. This paper uses the event study methodology to assess the reaction of 15 European financial institutions' share prices to direct cyberattacks. The same methodology is used for testing the reaction of a sample of 22 financial institutions, based in the Eurozone, to a series of systemic cyberattacks with potential worldwide repercussions. Our research represents an original contribution to the literature in two ways. Firstly, to the best of our knowledge, no authors have previously applied the event study methodology to a sample of shares pertaining exclusively to financial institutions. Even less so to financial institutions exclusively based in the Eurozone. Secondly, to the best of our knowledge, no existing research applied our subdivision between direct and systemic cybersecurity events in a single study. Overall, our study provides empirical evidence on the effect of 14 direct and 3 systemic cyberattacks. These attacks were announced by newspapers between October 2014 and August 2023. This represents an opportunity to update the results of the older event study cybersecurity literature, as well as an opportunity to test the results by more recent studies. The results can also be useful in the interpretation and anticipation of current and future European legislation on cybersecurity. In the case of direct cyberattacks, which explicitly target banks, insurance companies or electronic money institutions, we find that stock prices exhibit negative and significant cumulative abnormal returns. Furthermore, these negative effects become more relevant when considering larger event windows after the attack date. We also divide, in accordance with other studies, direct events between ones that compromise the confidentiality of information and ones that do not. We interestingly find that attacks that do not reveal confidential information have a significant negative effect on their targets. Conversely, cyberattacks that do reveal confidential information held by financial institutions do not have a significant effect on stock prices. Regarding the three systemic events, we find contrasting but interesting results. The breach of a major US bank has an overall negative and significant effect on European companies, in particular the ones based in Italy and Spain. On the other hand, when SolarWinds was discovered to be the vector of a cyberattack on the US Government, no such negative effect was observed. Lastly in the case of the WannaCry ransomware epidemic, we find empirical evidence of negative abnormal returns only for companies based in Germany and Spain.

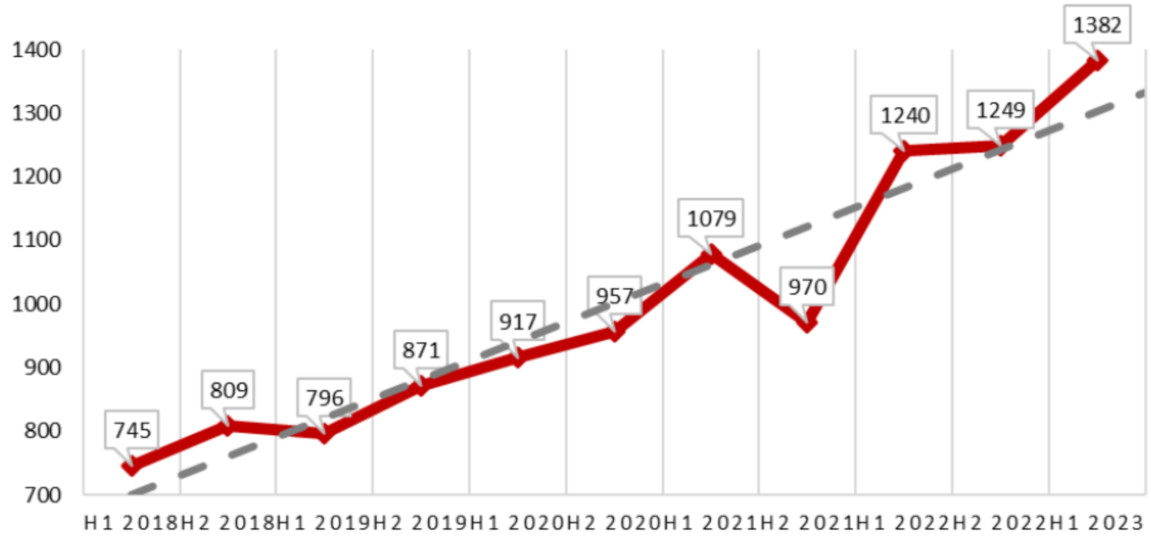
1. AN INTRODUCTION TO CYBERSECURITY

The proliferation of information technology has affected all economic sectors, and although the internet has often improved the way business is carried out, it has increased the vulnerability of critical infrastructures to information security breaches.

Nearly twenty years ago, an article published on Bloomberg (Horn, 2006) announced that for the first time "proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, according to an advisor to the U.S. Treasury Dep". The 2006 Bloomberg article and the problems it summarizes could have been written today. In 2017, the G20 warned that cyberattacks could "undermine the security and confidence and endanger financial stability" (Carnegie Endowment for International Peace, 2023). A survey from last year, aggregating the opinions of professionals working in the US financial sector (Depository Trust & Clearing Corporation, 2023), found that cyber risk was perceived as the third most important risk. The first and second position were instead respectively held by geopolitical tensions and inflation. Since the publication of the Bloomberg article, Cyber-crime has then been growing exponentially each year: according to Forbes (Brooks, 2023), the cost of cybercrime was predicted to hit 8 trillion dollars in 2023 and it was predicted to grow further to $10,5 trillion by 2025. This would mean that in the past year, the global costs associated with cybercrime were equal to 29% of the US GDP. In the specific case of data breaches, IBM calculates that the global average cost of such an attack, in 2023, is $4,45 million, 15% more than in 2020. For the financial industry, however, global statistics don't tell the whole story: firms in the financial sector lose approximately $5,9 million per data breach, 28% more than the global average (IBM, 2023). These numbers make it clear that a cyber-attack can have a disastrous impact on business. Furthermore, in the last two years, the dangers to cybersecurity worldwide have been exacerbated by the Russo-Ukrainian war (Mueller, et al., 2023).

In addition to the continuous increase in the number of attacks and the costs associated with them, the technologies and techniques used by the ill-intentioned are also being consistently improved. New attack types and tools are developed each year by attackers in order to penetrate more complex or well-controlled environments, produce increased damage and even remain untraceable (Bendovschi, 2015). In Figure 1 below we can see the number of known cyberattacks at the global level for each semester since H1 2018. The data is provided by CLUSIT in its 2023 report. As most targets of cyberattacks are reluctant to admit that they have been hit by a cyber-attack, the graph most likely only represents a fraction of the actual number of cybercrime instances that have happened in each semester.

Figure 1: Global number of known cyberattacks per semester H1 2018 – H1 2023, CLUSIT.



In the first place it is useful to give a working definition for *Cybersecurity*. The literature review by Craigen et al. (2014) suggests that the term is used broadly and, interestingly, its definitions are highly variable, context-bound, often subjective, and, at times, uninformative. In addition, it is found that there is a paucity of literature on what the term actually means and how it is situated within various contexts. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. For these reasons the authors set out to find a more broadly acceptable definition aligned with the true interdisciplinary nature of cybersecurity: they do so by reviewing the relevant literature to identify the range of definitions, to discern dominant themes, and to distinguish aspects of cybersecurity. As a first step Craigen et al. deconstruct the term cybersecurity in order to better situate the discussion within both domains of *Cyber* and *Security* and reveal some of the potential legacy issues. *Cyber* is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality (Oxford University Press, 2023). It evolved from the term *Cybernetics,* which referred to the "field of control and communication theory, whether in machine or in the animal" (Wiener, 1961). In turn *Cybernetics* comes from the Greek verb κυβερνάω, meaning "to steer" or "to govern", for example a boat or a state (Montanari, 2012). Going back to the term cyberspace, it can be defined as the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries

(National Institute of Standards and Technology, 2023). As for the term *Security*, in the literature review by Craigen et al., there appears to be no broadly accepted concept, as the term has been notoriously hard to define in the general sense. Nevertheless, according to Buzan et al. (1998), discourses in security must necessarily include and seek to understand who securitizes, on what threats, for whom why, with what results, and under what conditions. Based on nine other definitions present in the literature, Craigen et al. create a new definition, aiming to include, condense and refine all of the previous ones. The result is the following:

> *Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.*

Firstly, by avoiding the discussion of which resources, processes, or structures, the definition becomes general and recognizes the dynamic and complex nature of cybersecurity. In second place the protection of the cyberspace includes the protection in the broadest sense from all threats, including intentional, accidental, and natural hazards. Thirdly, the authors expand on the inclusion in the definition of the misalignment of property rights, which could seem as out of place at first sight. This aspect actually incorporates the two separate notions of ownership and control that dominate discussion of cybersecurity and digital assets in the literature. Any event or activity that misaligns the actual, i.e. de facto, property rights from the perceived, i.e. de jure, property rights, whether by intention or accident, whether known or unknown, is considered a cybersecurity incident.

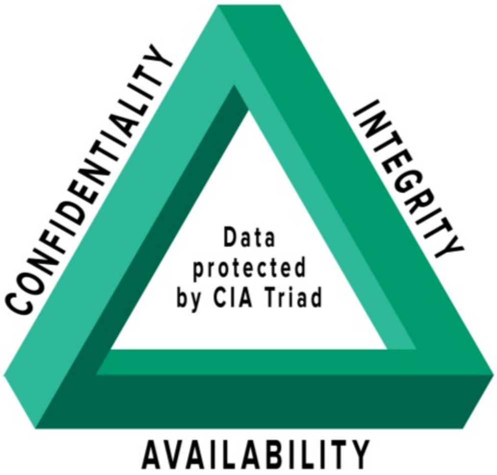
In Chapter 2 the particular dangers of cyberattacks in the context of the European financial landscape will be analyzed. This chapter on the other hand is focused on giving a summary of the world of cybersecurity, thanks to selected studies and systemic reviews. In the first part we contextualize cybersecurity in recent history. Afterwards the analysis shifts to the different types of cyberattacks, the different classes of perpetrators of such attacks and the various costs associated with them. Finally, the optimal and the actual investment levels in cybersecurity countermeasures will be discussed.

1.1 A brief history of cybersecurity

The first comprehensive published work, which became the foundation in the field of cybersecurity was a technical report named *Security Controls for Computer Systems* (Ware, 1970). This report, published in 1970, was the result of a study carried out by a task force on computer security organized by the department of defense of United States of America. The report concluded, that a comprehensive security of a computer system requires a combination of hardware, software, communications, physical, personnel and administrative controls. The first computer program that could move across a network, which also represented the first non-self-replicating benign virus in history, was written in 1971. It left a message trail, namely “I am the creeper, catch me if you can”, on whichever computing system it went through: it was understandably called as the “Creeper” (Alam, 2022). The first example of an antivirus program, which essentially performed the same functions that an antivirus does today, was instead created in the year 1973. The virus was called the Reaper and its main function consisted in chasing and eliminating the Creeper. Reaper was also the first self-replicating program, hence making it the first benign computer worm (Chen & Robert, 2004).

In 1977 the CIA introduced is a guiding model in information security, consisting in the so-called Triad (Ruthberg & McKenzie, 1977). The CIA Triad is a common model that forms the basis for the development of security systems.

Figure 2: The CIA Triad, representation by F5 Inc.



The confidentiality, integrity, and availability of information are crucial to the operation of a business, and the Triad segments these three ideas into separate focal points. This differentiation is helpful because it helps guide security teams as they pinpoint the different ways in which they can address each concern. They are used for finding vulnerabilities and methods for creating solutions. Here are the three principles described in detail (Fortinet, 2023):

- Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data, whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to the firm. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

- Integrity involves making sure that data is trustworthy and free from tampering. The integrity of the data is maintained only if the data is authentic, accurate, and reliable. For example, if a company provides information about senior managers on its website, this information needs to have integrity. If it is inaccurate, those visiting the website for information may feel that the organization is not trustworthy
- Availability consists in the fact that information and data should be available all the time. Furthermore, adaptive recovery mechanisms should be established to restore the system and the services provided by the system in case of an attack. Availability deals with the presence, accessibility, readiness, and continuity of service of system elements.

Not long after, during the 1980s ARPANET, or the Advanced Research Projects Agency Network, became the Internet (Lukasik, 2010). As computers started to become more connected, computer viruses also became more advanced. The Morris Worm was developed in 1988 and it became the starting point for the creation of more effective worms and viruses. This rise in malicious software in turn led to the development of antivirus solutions as a means for countering the worm and virus attacks (Orman, 2003). In the 1990s viruses such as Melissa caused the failure of the email systems by infecting tens of millions of computers. These attacks had mostly financial and strategic objectives. The 1990s, as a consequence of these more advanced menaces to IT systems, saw a sudden growth in the number and capabilities of antivirus companies. Nevertheless, these early antivirus products suffered of two major flaws: they used a large amount of a computer's available resources and they produced a seemingly unjustifiable number of false positives (Nachenberg, 1997).

As computers continued gaining power, the 2000s saw the emergence of new and more sophisticated malicious software (Alam, 2022). This process of coevolution has continued until the present days with exponential speed. The catalysts of such evolution are multiple. In the first place the challenge has expanded to new platforms, such as smartphones and IoT (Internet of things) devices. In the second place the rise of artificial intelligence (AI) in the last two years has opened another frontier for this ongoing struggle, with consequences that cannot yet be clearly foreseen (Guembe, et al., 2022). Lastly, as already mentioned, the increase in geopolitical instability, in particular in consequence of the Russo-Ukrainian war, has further increased the incentives for countries to invest in both cyberwarfare attack and defense capabilities.

1.2 Cyberattacks

As we have seen the world of cybersecurity and cyberattacks is a highly dynamic one. Nevertheless, in this section we aim to give a definition for cyberattacks, and afterwards propose a classification of them based on the relevant literature. This represents a necessary undertaking as, when the present study will analyze the impact of specific cyber events on European financial institutions, it will be useful to have a clear understanding of the various types of attacks and their respective characteristics.

According to Uma and Padmavathi (2013) a cyber-attack or computer network attack, consists, in accordance with the CIA Triad, in the corruption of confidentiality, integrity or availability of data or information. In more technical terms, during a cyberattack, malicious code is used in order to alter the logic of one of the programs of the defenders and this causes errors in the output of the program. The process of hacking involves in the first instance the scan of the Internet in order to identify the systems which contain poor security control. Once a hacker infects the identified system, he can remotely operate such system: in addition, a breached system can act as a silent spy on other systems or be actively used in the contagion of other realities. In summary, cyber-attacks aims to steal or hack the information of any organization or governmental entity through the use of malicious code and the exploitation of vulnerabilities. Biju et al. (2019) formalize the various phases in which a cyberattack usually develops as follows. Firstly, there is a *survey* phase, where the target is analyzed in order to find the possible ways in which the target's information or data can be threatened. In the second phase, which consists in *delivery*, the vulnerability that has been previously scouted on a machine or software gets exploited. In the third stage, defined as *breach*, the initial exploitation is effectively used in order to take advantage of the unauthorized access that has been gained. Finally, in the fourth phase of a cyberattack which is called *affect*, specific actions are taken by the attacker in the target's system and the initial goal is reached.

Uma and Padmavathi also give a list of the main characteristics that cyberattacks generally present. In particular attacks are:

- *Harmonized*: cyber attackers employ a harmonized process to infiltrate systems seamlessly. This involves the precise synchronization of multiple steps in the attack chain, ensuring a systematic and efficient approach to achieve their objectives. The coordinated execution of these steps allows hackers to attain their desired results within a predetermined timeframe and with minimal disruption to their overall plan.

- *Organized*: attackers adopt an organized methodology characterized by a logical and structured approach to compromising systems. This methodical organization enhances the effectiveness of their strategies, allowing for the exploitation of vulnerabilities with precision. By employing a well-organized approach, hackers can navigate through security measures more efficiently, maximizing the impact of their actions.
- *Massive*: cyberattacks, upon initiation, often manifest on an enormous scale, posing a significant threat to global cybersecurity. These large-scale incursions have the capability to infect billions of computers worldwide, resulting in widespread data breaches and substantial financial losses. The sheer magnitude of such attacks underscores their potential to cause extensive harm on a global scale.
- *Regimented*: attacks exhibit a regimented structure characterized by a carefully orchestrated sequence of actions. The precision and orderliness of these sequences contribute to severe and comprehensive damage, compromising the functionality of targeted organizations. The regimented nature of the attacks ensures that each step is executed with meticulous planning, leading to a more impactful and disruptive outcome.
- *Not spontaneous* nor *ad hoc*: cyberattacks are deliberately planned and executed with meticulous care, eliminating any element of spontaneity or ad hoc decision-making. Attackers invest time in strategic planning to ensure that every detail is considered, from identifying vulnerabilities to selecting the most effective attack vectors. This deliberate approach distinguishes cyberattacks from impromptu actions, emphasizing the calculated nature of these security breaches.
- *Time and resource demanding*: the orchestration of cyberattacks necessitates significant investments in both time and resources. Attackers meticulously plan and prepare, requiring ample time to conduct thorough reconnaissance, develop sophisticated strategies, and evade detection. The financial investments in acquiring advanced tools and expertise also contribute to the demanding nature of orchestrating a successful cyberattack. This deliberate allocation of time and resources underscores the complexity and seriousness of the cyber threat landscape.

The literature regarding the categorization of cyberattacks is definitely extensive and complex in the fact that it requires specific technical knowledge. The purposes of this paper do not require the knowledge of a technical taxonomy of cyberattacks. On the contrary, as we will see in the continuation of our study, only a simplified subdivision of attacks will be necessary. It is still useful, in order to have a more complete view on the world of cybersecurity and cyberattacks, to briefly discuss the nature of the taxonomies that have been proposed in the literature. For this purpose, we will make use of the literature review produced by Simmons et al. (2009): the authors create this survey as a staging ground on which to base their own proposed taxonomy. In one instance of the literature, attacks are analyzed thanks to a multidimensional basis, the four factors that are considered correspond to: the method of operation, the target, the source and the impact. Each of these factors in turns contains a number of elements with an exhaustive description. Interestingly, Simmons et al. regard this taxonomy as limited in the fact that it doesn't give proper attention to the inception component of an attack. Another taxonomy is also based on four factors, but they are significantly different from the ones that have been already mentioned. In particular this classification is based on: the attack vector, the target, the vulnerability level of the target and finally the payload or effects that are involved in the attack. Just these two examples, seen from a bird's eye view, give a picture of the complexity that this kind of literature deals with.

Uma & Padmavathi (2013), in their review, also put forward other types of classifications which are simpler, given the fact that they are based on a single characteristic of the attack. Cyberattacks can, for example, be differentiated in regards to their purpose. The three main purposes of an attack are: reconnaissance, access and denial of service. Reconnaissance involves the mapping of the target's IT system through unauthorized but undetected access. This kind of offense is similar to site inspection by thieves in a neighborhood in search for vulnerable homes, which can have absent residents or perhaps vulnerable doors and windows. The second objective is that of access: in this case the unauthorized intruder uses his capabilities to gain access to resources that should be unreachable to him. In the third case the objective consists in the disruption of a service that is provided by the target. This end is usually reached by slowing down the system in what is known as Denial-of-Service attack[1]. This kind of intrusions may also involve the deleting or corruption of information, with the intent of denying services to legitimate users of the target's services.

Another criterium for the categorization of attacks that the authors present is that of legal classification. Based on this approach attacks can be a part of four categories: cybercrime, cyber espionage, cyberterrorism and cyberwar. Cybercrime, according to Canadian law enforcement agencies, is defined as a criminal offense where a computer serves as either the target or the instrument for committing a significant part of the offense. In essence, cybercrime seeks to exploit computer systems as tools for criminal activities, with the computer itself being an incidental element of the crime. Cyber espionage instead involves the use of cracking

[1] This kind of attack will be explained in more detail afterwards, as it is part of the classification of attacks that our study uses.

techniques and malicious software, including Trojan horses and spyware, to illicitly acquire confidential information from individuals, groups, and governments. Perpetrators may execute cyber espionage entirely online, operating from professional computer desks in distant countries. Alternatively, it can entail infiltration by conventionally trained spies and moles or may result from the malicious activities of amateur hackers and software programmers. On the other hand, cyber terrorism encompasses the use of Internet-based attacks for terrorist activities, involving deliberate large-scale disruptions of computer networks through tools such as computer viruses. Lastly, cyberwar refers to the actions of a nation penetrating another nation's computers or network with the intent to cause damage or disruption. This involves strategic attacks on digital infrastructure for geopolitical purposes.

According to Uma & Padmavathi's review, cyberattacks can also be classified based on the level of involvement in the action of the attackers themselves. The first of the two resulting categories is that of active attacks. Such attacks empower the attacker to transmit data to all parties involved or unilaterally block data transmissions. The attacker, by being positioned between the communicating parties, can even opt to terminate altogether data transmission between the attacked parties. The second of these categories consists in passive attacks. This kind of strikes involves an unauthorized intruder eavesdropping on communication between two parties to illicitly obtain information stored in a system. In contrast to active attacks, passive attacks refrain from meddling with the database but may still constitute a criminal offense.

Another classification that the two researchers mention is the one based on the scope of the attacks. In the first place, attacks can be malicious and large scale. The maliciousness denotes actions taken with the deliberate intent to cause harm. A malicious attack, that is also large-scale, involves thousands of systems, leads to a firm-wide systems crash, results in the loss of substantial data and undermines the credibility of the affected company. Alternatively, attacks can be non-malicious and small scale. They typically arise from accidental actions, damages due to mishandling, or operational mistakes by inadequately trained individuals. These incidents may cause minor data loss or system crashes, with only a few systems in the network being compromised. In such cases, data is generally recoverable, and associated costs are relatively minor.

Given the fact that this paper does not seek to be a part of the technical IT literature, but of economic and financial one, the categorization of cyber incidents that will be used through the study is a result of the latter. The papers of the event study literature that have inspired the categorization of events of our study will be explored in detail in Chapter 3 (Abshishta, et al., 2017; Campbell, et al., 2003; Cavasoglu, et al., 2004; Garg, et al., 2003; Hovav & D'Arcy, 2004;

Hovav & D'Arcy, 2003; Kuo, et al., 2020). For now, it is only necessary to go into detail about the five categories into which the events will fall in.

- The *Data Breach* category refers to incidents that involve the unauthorized access, acquisition, or disclosure of sensitive information residing within a system or database. Characterized by an intrusion into secured environments, data breaches compromise the integrity and confidentiality of the compromised data. These incidents pose significant threats to individuals, organizations, and even the broader information ecosystem.
- The *Theft* class of attacks contains incidents where there is an unauthorized appropriation of currency, with the intent of economic gain or simply disruption. In order to obtain their financial goal, the perpetrators can leverage a variety of techniques to circumvent the security measures of the defender. The ramifications of cyber theft extend beyond the mere financial losses and also imply reputational damage and potential legal consequences for the affected entities.
- The *DDoS* category refers to a specific kind of attacks. Distributed Denial of Service attacks involve the orchestrated inundation of a targeted system or network with an enormous amount of traffic, thus rendering the information systems of the defender inaccessible to its legitimate users. This form of cyberattack exploits the finite resources of the target, causing service disruptions and impeding regular functionality. DDoS attacks are often executed through a network of compromised computers, amplifying their impact and rendering mitigation challenging.
- *Malware* is a portmanteau of "malicious software". This class represents a broad category of software designed to infiltrate, damage, or compromise computer systems without the user's consent. This category encompasses various subtypes, including viruses, worms, ransomware, and spyware. Malware can be disseminated through email attachments, infected websites, or compromised software, exhibiting diverse functionalities that may include data theft, system disruption, or remote control by malicious actors.
- *Phishing* is a social engineering technique wherein attackers employ deceptive tactics to manipulate individuals into divulging sensitive information, such as passwords or financial details. The attacks of this category are typically executed through fraudulent emails, messages, or websites, phishing endeavors to impersonate trustworthy entities to deceive recipients. Successful phishing attempts grant attackers access to confidential data, enabling subsequent cyber exploits. The prevalence of phishing underscores the

importance of user education and robust cybersecurity measures in safeguarding against these deceptive maneuvers.

In addition to this fist categorization, each of the 17 cyber incidents of this paper will be further subdivided into two classes. The criterium for this subdivision is provided by Arcuri et al. (2018) and Campbell et al.'s (2003) studies: namely a cyberattack may or may not involve the disclosure of confidential information. Confidential information consists in: credit card numbers, phone numbers, email addresses, addresses of residence and full names. This kind of information will be considered as confidential when it pertains to the financial institution's portfolio private and business clients. When instead the leaked data is connected with an institution's employees, the cyber-attack will not be a part of the so called confidential incidents.

1.3 Hackers, strategies and motivations

Building upon our exploration of cyberattacks in the preceding chapter, let us now delve into the details about who perpetrates such attacks and for which motivations. Understanding and predicting wrongdoing in the cyberspace is an emerging area of research. It has in particular been growing with the increase in cybercrimes and heightened awareness about cybersecurity of the recent years. The nature of cybercrimes is also becoming increasingly complex as hackers are more proficient and well-financed than earlier. Thus, our understanding of the various types of hackers and their motivations needs to be up to date. Hacker types and motivations are not part of the event study literature on cyberattacks: while different papers, as we have seen, analyze the different effect of a cyberattack based on its type, no existing research to the best of our knowledge differentiates attacks on the basis of the perpetrators. This proposal could thus represent an interesting expansion route for future event studies in this field. Attacker types and their incentives are not part of the data of this study too. Anyhow it is still useful to have an appropriate level of awareness on the topic.

For this purpose, we refer to Chng, et al.'s work (2022). These authors selected and reviewed eleven classifications and typologies of hackers and their motivations. The objective is the consolidation of the literature's understanding on this area and the summarization of the state of the art. As a result of their extensive survey the authors present, as their unique contribution to this field of research, a unified framework of 13 hacker types, each with its set of motivations. In addition, they detail the strategies that each hacker type typically employs, thus allowing for the identification of a specific hacker type based on the strategies used during the cyberattack in question.

Historically, according to Chng et al.'s review, hackers were known as one generic group. This was akin to grouping all cybercriminals into a general category, regardless of their actions and motivations. More recently, cybersecurity experts have instead formalized typologies of hackers and their motivations, which in turn provide them with a better understanding of the constellation of cybercrimes. Interestingly, in the Cheng et al.'s approach to the topic, behavioral science plays a complementary role in regard to cybersecurity. It does in fact help develop a stronger understanding of why hackers do what they do, because hackers represent economic players with their particular motivations, incentives, hopes and fears. In other words, they possess both rational and irrational cognitive processes and motivations that determine their actions. It is relevant to keep in mind that, within the authors' framework, each hacker type and the respective motivations are titled using terminologies widely used within the cybercommunity. For this reason, various attacker groups are described, in addition to the formal name given to the by the researchers, by other names present in the literature which are frequently used in the cybercommunity. In the first-place hackers can be *novices*. This class refer to hackers who are less skilled and heavily rely on online toolkits developed and provided by others. Alternative names for this type of hackers include "script kiddies" and "newbies". Novices are defined by their motivational characteristics of curiosity, notoriety, and recreation. Students have no malicious intent to hack but do so only to gain knowledge: they are in fact mainly motivated by curiosity They usually re-use malware code that they found from the Internet and they most often do not possess a proper plan of action in terms of attack steps. These hackers are also not careful enough to cover their online tracks. *Cyberpunks,* on the other hand, are low- to medium-skilled hackers who conduct attacks for their own entertainment. In particular they are focused on garnering the public and the media's attention. Some alternative names for this type of hackers include "crashers", "thugs", and "crackers". They are motivated by financial gain, notoriety, revenge, and recreation. Like novices, they may use existing codes but they usually apply some modifications or even write their own ones. The preferred attack vectors of this class of attackers include: "bricking"[2], used to cause damage to the victim's systems; exploitation of the bugs in the software running on the victim's devices; and Denial of Service attacks. *Online sex offenders* are instead sexually motivated individuals who misuse the Internet to engage in sexually deviant behaviors with underage targets. They include "cyber predators" and pedophiles. Their technique consists in the befriending of potentially vulnerable

[2] "Bricking" happens when a cyber-attack turns a piece of computer hardware into a "brick" i.e., renders it unusable to such an extent that it requires replacement.

victims on Facebook or other social media, and then in the obtainment of compromising material either directly or through chats embedded with malicious attachments. Another class is that of the *old guards*: like students, they are non-malicious hackers who have no regard for personal privacy. They can also be referred to as “white hats”, “sneakers” or “tourists”. This particular group of attackers is motivated by curiosity, notoriety, recreation, and ideology. The old guards prefer to use customized codes which are usually anticipated by penetration tests run on the objective’s systems. The function of these tests consists in revealing the actual vulnerabilities of the target. These hackers, being non-malicious, dedicate part of their time to the discovery of new malwares thanks to the employment of professional honeypots[3]. They are also able to track malicious hackers by using cyber forensic techniques. The fifth kind of cybercrime perpetrators, according to the authors, is represented by *insiders*. They are disgruntled current or ex-employees who abuse their access to get what they want. They include “internals”, “user malcontents” and “corporate raiders”. Their motivations consist in financial gain, revenge, and ideology. An insider typically makes use of his confidential knowledge on their company’s cyberinfrastructure in order to launch attacks or simply sell confidential information stored in the firm’s systems. The techniques for extracting this confidential information are essentially two: one is transferring this sensitive organizational data into one own’s devices, the other is accessing the company’s databases or cloud storage and then sharing the data. *Petty thieves* refer to criminals who have moved their nefarious activities online and are motivated by financial gain and revenge. They include extortionists, “scammers”, “fraudsters”, thieves, and digital robbers. These hackers’ attack vectors usually comprise “trojans”[4], or other types of ransomwares which are easily available on the Internet. This malicious software is almost always used with the objective of gaining credit card or bank account details. Furthermore, *digital pirates*, also known as copyright infringers, possess and engage in the illegal duplication, distribution, download, or sale of copyrighted materials. They are almost exclusively financially motivated. The technique adopted by pirates consists in stealing copyrighted content directly or indirectly and then leaking such content openly on the internet. *Crime facilitators*, including supporters, provide the necessary tools and technical know-how to cybercriminals, thus enabling them to launch sophisticated attacks which would not have been possible otherwise. They can have specific skill sets or areas of expertise and are

[3] In computer terminology, a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data that appears to be a legitimate part of the site which contains information or resources of value to attackers. It is actually isolated, monitored, and capable of blocking or analyzing the attackers

[4] A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

usually financially motivated. This sort of suppliers of malicious hackers may offer cybercrime-as-a-service to criminals: this service includes the needed support in order for the client to properly carry out phishing campaigns or employ rented malware. *Professionals* are highly skilled individuals who act as guns for hire or with the intent of furthering their criminal empire. They are motivated by financial gain and revenge. They are also known as "black hats", "elites", criminals, organized criminals, information brokers, and thieves. Professionals perform highly sophisticated attacks thanks to their extensive expertise on the full repertoire of attack vectors. They are especially careful to not leave any online trail behind: clearly their techniques lie on the opposite side of the spectrum of the ones used by novices. *Nation states* hackers are highly trained and extremely skilled attackers who work directly or indirectly for one government to destabilize, disrupt, and destroy the systems and networks of another nation or government. They are motivated by financial gain, revenge, and also ideology. This category includes "information warriors", cyber terrorists," cyber warriors", state actors, and spies. Their preferred technique implies sophisticated attacks, carefully carried out according to a series of predefined stages. *Crowdsourcers* are individuals who come together to solve a problem, often using questionable methods or chasing dubious goals. They are motivated by notoriety, revenge, recreation, and ideology. These hackers join their forces by pooling their skills together for tasks such as developing new malware or managing botnets[5]. The final group that the authors propose it that of *Hacktivists*, also known as political activists and ideologists. They use their technical skills to further their political agendas or use the Internet as a tool for political change. They are motivated by notoriety, revenge, recreation, and especially ideology. Hacktivists may employ attack vectors such as SQL injections and web server misconfigurations. Their objectives are variate and include: taking over sensitive databases and leaking their contents, defacing high-profile websites, and finally disabling widely-used public services.

1.3.1 Insider attack example: Société Générale's "rogue trader"

It is worthwhile to go through an overview of a specific attack, perpetrated by an individual that is part of the *insiders* category, detailed in the previous section. By exploring this example, we can comprehend the complexity that each class, proposed by Chng et al., brings with it: otherwise, by staying at the surface level of this classification, we risk not understanding that each cyberattack, even if includable under a set of categorizations, is essentially a category in

[5] A botnet refers to a group of computers which have been infected by malware and have come under the control of a malicious actor. The term botnet is a portmanteau from the words robot and network and each infected device is called a bot.

its own. The event we are analyzing was initially part of the dataset for our event study, but it was excluded due to its peculiar nature, that didn't allow it to properly fit inside the cyberattack categories that were proposed earlier. The attack is included by the Carnegie Endowment for International Peace in its *Timeline of Cyber Incidents Involving Financial Institutions* database, but its inclusion in the aforementioned *theft* category could have resulted unnatural.

The attack in question was conducted by an *insider*, namely Jérôme Kerviel: Jérôme was a trader employed by Société Générale. Starting from 2006 onwards, he opened a series of massive positions totaling approximately 59 billion Euros (Société Générale, 2023). The unauthorized positions were discovered by the French company only in January 2008, after a team of 20 people was set out by the firm to carry out systematic searches as a result of an initial alert by its control systems. Jérôme had until then carefully and successfully hidden the positions he opened through fictitious transactions. According to Société Générale itself, the bank found itself at risk of collapse: the positions taken by the "rogue trader" in fact represented more than the Bank's total capital. After consultation with the Governor of the Bank of France and the AMF's Secretary General, the decision was taken to close out these positions as soon as possible to secure the Bank's survival and the stability of the global financial system, which would have been threatened if the Bank had collapsed. Société Générale thus proceeded to liquidate the fraudulent positions. Once this process had been completed the firm made a public announcement of the massive fraud to which it had fallen victim, and the final loss of €4.9 billion. At the same time, the Bank announced that it had secured a capital increase enabling it to absorb this loss.

Most likely Jérôme's motivations not only consisted in financial gain but also in revenge, expressed as a desire for greater financial and professional recognition as an important employee of the firm (Société Générale, 2023). The perpetrator's technique consisted in using his privileged access to the company's trading platforms in order to make unauthorized trades: this technique did not involve the illegal sale of confidential company information. This attack is thus a peculiar instance of a cybercrime carried out by an insider.

1.3.2 Cybercrime-as-a-service

Another topic that needs a specific overview is that of cybercrime-as-a-service, which we initially found in the *crime facilitators* class of Chng et al. Tacking this kind of cybercrime was listed among the priorities for the 2022-2025 period by the Europol (2022). Analogous to cloud services in legitimate markets, like platform-as-a-service, CaaS enables criminal entrepreneurs to develop and manage their business without the complexity of building and maintaining all required expertise, infrastructure and tools themselves.

According to Manky (2013) cybercrime must be regarded as a relevant business. CaaS has in effect become a well-oiled machine, built on a wide network of players that fulfil specific functions. Just as with any other business, there are various products and services available to be sold. An example is that of consulting services, mainly about the setup of a botnet. There also exists rental services for botnets, which offer to the client the possibility of using such a tool, for a predefined amount of time, with the objective of conduction DDoS attacks. The wide range of available services also includes highly specialized "cloud cracking", which offers high-performance password cracking at a low cost and significantly reduces time it takes to uncover strong passwords. Cyber-criminals also reap profits by renting or leasing hacking tools such as trojans and ransomware to third parties. They often do so for a set price but it can be subject to negotiation, with tools offering more elaborate and evasive features commanding the highest prices.

A key area of research on CaaS is where and how the supply of these services is being matched with demand, as this question is critical for developing effective disruption strategies by law enforcement (Akyazi, et al., 2021). One of the promises of CaaS is that it is accessible for new entrants, so it cannot operate effectively within old and constrained model of closed, vetted and trust-based criminal networks. According to the review by Akyazi various studies show that cybercriminals have been using open channels like online underground marketplaces, custom websites and forums to advertise and sell their services.

1.4 The costs of a cyberattack

As we have seen in the introduction to this study, the global costs caused by cyberattacks in 2023 have been estimated at around 8 trillion dollars (Brooks, 2023). Furthermore, in the case of firms in the financial sector, according to IBM, approximately $5,9 million are lost when a data breach happens. Understandably these figures are only rough estimates and they need to be understood at a deeper level: for this purpose, this section deals with the various economic consequences that a cyberattack can have for the target firm. As a starting point, it is necessary underline that there are no standard methods for measuring the costs of cyber attacks (Cashell, et al., 2004; Park, 2010). Attacks produce many kinds of costs, some of which cannot be quantified easily, if at all. Overall, the impact of cyberattacks is hard to measure (Colivicchi & Vignaroli, 2019). In the words of Tracey Cladwell (2014) "putting a figure on the cost of data breaches is akin to nailing jelly to a wall". As a result, there is a presumed gap in private, internal data that mirrors the absence of public data on cyber-attack costs. While organizations may have good reasons not to make public disclosures regarding security breaches, one would expect their incentives to measure the costs of such incidents internally to be strong. Without accurate cost data it is difficult for organizations to assess the cyber-risks they face, make rational decisions about how much to spend on information security and evaluate the effectiveness of their security efforts. To a profit-seeking business, measurement of costs already incurred is useful primarily to the extent that it facilitates prevention or mitigation of future losses. In the cybersecurity field, as elsewhere, risk assessment is primarily a forward-looking activity. It is no less important or necessary because certain costs cannot be quantified. Thus, some methods for the evaluation of cybercrime costs have been developed in the course of the recent history of cybersecurity.

Early attempts to measure cyber-risk led to the Annual Loss Expectancy (ALE) model, developed in the late-1970s at the National Institute for Standards and Technology[6] (Cashell, et al., 2004). ALE is produced by multiplying the financial cost, or impact, of an incident by the frequency, or probability, of that incident. In other words, ALE considers security breaches from two perspectives: how much would such a breach cost, and how likely is it to occur. ALE combines probability and severity of attacks into a single number, which represents the amount a firm actually expects to lose in a given year. ALE has become a sort of standard unit of measure for talking about the cost of cyberattacks, but the model is not universally used to assess cyber-risk. The reasons of this lack of use are apparent: the ALE model assumes that cost impact and frequency of attack are known variables, when in fact they both resist quantification. The difficulties in cost measurement have been set out above, and similar uncertainties apply to efforts to specify the likelihood of an attack. Finally, attempts to calculate a value for ALE are conditioned by the "unrealistic and time-wasting assumption of numerically precise information" (Ekenberg, et al., 1995).

Another popular way to measure the economic impact of cyber-attacks is developing a risk assessment, such as the one defined in NISTIR[7] (Fung, et al., 2013). This method states that risk has to be calculated as the product of threat, vulnerability and consequences.

$$Risk = Threat \ \times Vulnerability \times Consequences$$

Threat refers to potential dangers that could exploit vulnerabilities in a system. Threats can include hackers but also natural disasters that may impact the cybersecurity of an organization.

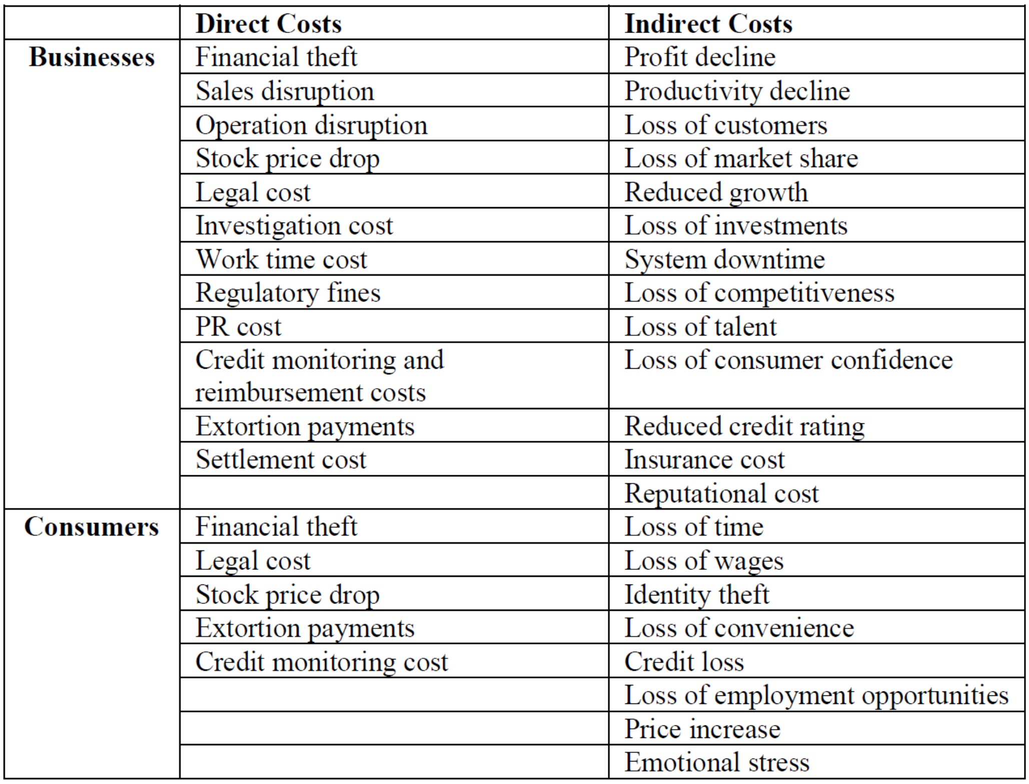
[6] The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

[7] A National Institute of Standards and Technology Interagency or Internal Report (NISTIR) is a series of publications that includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment).

On the other hand, vulnerability represents the vulnerabilities of the system. They can arise from software flaws, misconfigurations, or even human errors. Understandably, consequences involve the potential impact or harm caused by a successful exploitation of a vulnerability. Consequences can range from financial losses, damage to reputation, loss of sensitive data, or disruption of business operations. This NISITIR model has also been considered as a general model of risk not only relevant in the world of cybersecurity. As companies need to balance the costs and budget based on the quantified risks, the most challenging aspect of this approach is how to gather the information and to ensure the validity of the data. There is a lack of empirical data in the domain of cybersecurity (Wolff & Lehr, 2017), so one approach is to base the inputs on the opinions of experts or simulations.

Our overview of the economic consequences of a security breach is inspired by the subdivision of costs indicated by Cashell et al. (2004) and Wang et al. (2019). There is a consensus in the literature, namely that the costs associated with cyber-attacks can be divided into direct and indirect costs. Some specific kind of costs, on the other hand, are placed differently into the two categories depending on the authors.

Table 1: Taxonomy of the cost factors of a security breach.



	Direct Costs	**Indirect Costs**
Businesses	Financial theft	Profit decline
	Sales disruption	Productivity decline
	Operation disruption	Loss of customers
	Stock price drop	Loss of market share
	Legal cost	Reduced growth
	Investigation cost	Loss of investments
	Work time cost	System downtime
	Regulatory fines	Loss of competitiveness
	PR cost	Loss of talent
	Credit monitoring and reimbursement costs	Loss of consumer confidence
	Extortion payments	Reduced credit rating
	Settlement cost	Insurance cost
		Reputational cost
Consumers	Financial theft	Loss of time
	Legal cost	Loss of wages
	Stock price drop	Identity theft
	Extortion payments	Loss of convenience
	Credit monitoring cost	Credit loss
		Loss of employment opportunities
		Price increase
		Emotional stress

As a starting point Wang et al.'s taxonomy can be found in Table 1. The authors differentiate between the damages incurred by the breached company and the ones incurred by its customers. We won't go into detail about the losses that consumers face that are listed in the table, as from an accounting perspective, these do not count as costs to the target firm. These costs however can be significant from a policy perspective that considers the losses of society as a whole.

Direct costs in the first place include the funds, information and assets that may have been stolen or compromised during the attack. While the stolen funds and financial assets are easy to measure, stolen non-financial assets and stolen or compromised information present a more difficult scenario. The value of an information is highly dependent upon who possesses the information. Sensitive commercial R&D information in the hands of a competitor are significantly more problematic than if it were in the hands of, for example, a novice hacker. Time sensitivity can also complicate the valuation problem. In the case of a password that expires every week, because of a company's security policies, and then has to be renewed: the password itself is obviously worthless after its expiration. It is nevertheless quite valuable during its residual half-life and for this reason the attacker must act quickly if he wants to use it to gain system access. The theft of funds could also present itself in the form of an extortion, in particular in the case of ransomware. While Wang et. al do not include such costs, according to Cashell et al. expenses incurred in restoring a computer system to its original pre-attack state are to be considered as part of the direct costs. Recovery from an attack will typically require extra spending on labor and materials: these are the easiest costs to measure. But even at this basic level of cost accounting, complexities may arise. If an attack leads to increased spending on IT security it could be difficult to determine to what extent those costs are directly attributable to the attack. If a planned upgrade in hardware or software is accelerated after an attack, the upgrade cannot be classified as a security cost without doubts. Another set of direct costs arises from business interruption which results in operational and sales disruption. These costs may include lost revenue and loss of worker productivity during the disruption. Lost revenues may be easily measured by reference to a pre-attack period, but this may not tell the whole story. Lost sales may be a transitory phenomenon, limited to the attack period or they may be long-term, if, for example, some customers switch permanently to competing firms. Assigning a value to lost time depends on each individual organization's estimates of its own costs related to business opportunities forgone during the disruption or diversion of resources during the recovery effort. Finally, Wang et al. include among this first group: legal and settlement costs, regulatory fines PR costs and credit monitoring and reimbursement costs. Legal costs that may be incurred by the firm in case of lawsuits by damaged customers or third parties: in addition, if these lawsuits are successful, the company will also incur in damage compensation costs. Credit monitoring and reimbursement costs can be present if the breached firm opts to provide credit monitoring services to its affected customers. These services come with actual reimbursements in case of customers' financial losses that are directly attributable to the security breach.

The second type of costs associated with a security breach is that of indirect costs, which may continue to accrue after the immediate damage has been repaired. Many indirect costs flow from loss of reputation, or damage to a firm's brand. Customers may defect to competitors, financial markets may raise the firm's cost of capital, insurance costs may rise, and more lawsuits may be filed. A company that sees its data and information systems deeply compromised, will not only suffer reputational damages with respect to its current and potential customer base, it could also be considered a less desirable and unreliable business partner by other companies seeking commercial partnerships in the future. In summary these reputational consequences can translate to, or come together with: reductions in market share, decreased revenues, reductions in profitability and a reduction in credit rating. Some of these cost factors are readily quantifiable, but other aspects of loss of trust or confidence are intangible and difficult to measure. According to Cashell et al., some analysts even regard these indirect, intangible costs as more significant than direct costs. Indirect costs of cyber-attacks may also include economic harm to individuals and institutions other than the immediate target of an attack. Furthermore, cascade effects should also be considered as a possibility. An attack on one firm's computer networks may affect other firms up and down the supply chain. The disruption could spread from computer to interlinked computer, but quantifying the economic impact of an event of this type is undoubtedly very complex and would require a large number of assumptions. The fall in the share price of the company is placed among direct costs by Wang et al., while Cashell et al. list it among the indirect costs. Lastly submitting an insurance claim and allowing for the proper checks by the company providing cyberinsurance requires an investment in time and resources: naturally these costs come with the benefit of a delayed partial offsetting of the initial direct costs. This aspect has become more relevant in recent years as more and more companies are choosing to insure against the risks posed by cyberattacks (Marotta, et al., 2017).

1.4.1 A focus on reputational damage

In order to understand the complexity connected with the estimation of cyberattack damages with a more hands-on approach, it is useful to dig into the specifics of the estimation of at least one kind of damage. For this purpose, we offer an overview of the study by Ramkumar et al. (2018) that takes on the task of estimating reputational costs with respect to customer behavior. In their analysis, they assess the effects of a data breach announcement by a single multichannel retailer. For their experiment the researchers make use of the data provided by a real-life undisclosed US retailer that has been hit by a data breach. The individual customer transaction data from the retailer is used to conduct a detailed and systematic empirical examination of the effects of the announcement on customer spending and channel migration behavior. To identify the effects, the authors compare the change in customer behavior before and after the data breach, between a treatment group, consisting in customers whose information has been breached, and a control group, composed of customers whose information has not been breached. The authors find that, although the data breach results in a significant decrease in customer spending, customers of the firm migrate from the breached to the non-breached channels of the retailer. The findings further reflect that customers with a higher retailer patronage are more forgiving because the negative effects of the announcement are lower for customers with a higher level of patronage.

The process of estimating the reputational damages of a single data breach, in the case of a multichannel retailer, was extremely complex. Clearly, the task of estimating multiple reputational damages, each incurred by a financial institution targeted by a cyberattack, would require too much effort to allow for a comprehensive study of multiple events.

1.4.2 Number of compromised accounts as a proxy for data breach costs

For the purpose of estimating data breach costs in particular, part of the literature uses a somewhat intuitive approach: the estimated cost of each breached account is multiplied by the number of total breached accounts (Algarni & Malaiya, 2016). The estimated cost for a lost account can be found in IBM's yearly reports. On the other hand, the Data Breach Chronology website (Privacy Rights Clearinghouse, 2023) provides a detailed database of data breaches and the number of accounts involved in each of them. However, this database only provides information for US based firms.

In the European Union, private firms and the public sector are required to report the occurrence of data breaches, in the case that these breaches may involve the unauthorized access by third parties to confidential information. This rule is laid out in the General Data Protection Regulation (2016/679). Specifically, Article 33 states that "in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority". The databases maintained by these supervisory authorities are naturally not public. This results in the complexity or even impossibility of gathering the exact number of breached accounts for each data breach that occurs to a European firm. Furthermore, the absence of a public database leaves researches no other choice than to gather data with through the use of newspapers, and this process is understandably more troublesome. In addition, the amount of data itself is limited with respect to what a potential public database could allow for. In summary, the use of this methodology is not a viable path for academics who wish to quantitatively study the impact of cyberattacks for breached companies based in the European Union. Nevertheless, there is a database that could serve as a proxy for the magnitude of a data breach: the CMS[8] regularly updates an online database, namely the *GDPR Enforcement Tracker*, which chronologically lists all of the fines incurred by companies for breaches of the GDPR principles on data privacy and security. The amount of each fine could be used as a proxy for the damages actually implied by each data breach. The issue with such a database is that it reports fines relative to all kinds of data confidentiality infringements, which can range from data breaches to mere mismanagements of data that do not actually include any kind of cybercrime.

1.4.3 Relevance of the Event Study Methodology

The event study methodology will be discussed in detail in section 3.1, for now it is important to point out that it represents a useful tool for our analysis of cyberattacks. This usefulness stems from the straightforwardness of measuring the impact of cyber events based on the variations in stock price that they can cause. As mentioned before, other measures of costs associated with cyberattacks present certain characteristics, which make their use more complex. Cashell et al. point out that these complexities can lead many firms to grossly underestimate the costs of security breaches when the estimated costs are compared to the magnitude of actual stock market capitalization losses. The aforementioned complexities also importantly translate into a limitation to the number of events that can be analyzed in a single paper: we have seen that Ramkumar et. al have to focus on just one event in their endeavor to estimate reputational damage. In particular an event study requires the collection of the daily prices of a company's stock: this kind of data, unlike data involved in other types of estimations, is readily available in the online databases of Exchanges or information providers, such as Bloomberg and Yahoo Finance. For these reasons, event studies, can constitute an effective way to undergo a quantitative study on the impact of security breaches: the literature that uses such a technique in the cybersecurity field will be explored in detail in section 3.2.

In addition, stock prices represent a readily available measure of the markets and investors' valuation of a company: the market value of a firm represents the confidence that investors have in the firm itself, by measuring it we can calculate the impact of a cyber-attack. Regarding the

[8] CMS is an international law firm that offers legal and tax advisory services. It provides companies and organizations with advice on a full range of legal issues. CMS consists of 18 independent law firms with about 80 offices worldwide

value of a stock, the Dividend Discount Model proposed by John Burr Williams (1938) states that the price of a stock is determined by the present value of all its expected future dividends. Another perspective is that of the Discounted Cash Flow Model (Kruschwitz & Löffler, 2006): according to this model the value of a stock is coherent with all future expected cash flows of the company. In both cases it is easy to see why stock prices constitute such a useful tool. In effect, if an event study finds that a company's stock has registered a significant negative return, this significant negative return comes with a plethora of information. For instance, investors and markets agree on the fact that the event had significant economic repercussions, that could translate into lower future dividends paid by the stock or by lower future expected cash flows that the company can use for its operations and capital distributions. Furthermore, a significant decrease in the share price of a firm can reflect the reputational damages connected to the event: in the case of a cyberattack markets and investors may view the attacked company as more fragile and unreliable, especially if the attack was unexpected. In summary the variation in the share price of a company can incapsulate all of the different direct and indirect costs that the company faces as a result of a security breach. This advantage comes with the caveat that the costs are viewed through the lenses of investors.

1.5 Cybersecurity investments

In a threatening environment where cyberattacks are increasing in number and sophistication, investments in cybersecurity have become critical for firms in order to assure the integrity, confidentiality and availability of data assets, and in turn the survival of the business itself. Cybersecurity investments have permanently entered the set of decision variables that any firm should take into account. For this reason, in this section we offer a brief overview of the relevant literature based on the review by Fedele & Roner (2022). This paper in particular is chosen as it represents the first attempt to provide a comprehensive review of the research on the economics of cybersecurity, with a specific focus on firms' investments in cybersecurity.

In the early 2000s it was first recognized that perverse economic incentives and market failures can influence decisions regarding security, therefore economic theories were for the first time applied to cybersecurity issues. These important considerations stimulated the flourishing of a theoretical literature on firms' decisions to invest in cybersecurity. By contrast, the empirical literature is currently at an early stage, likely because of data scarcity. There are four main streams that characterize the theoretical literature. The concern for cybersecurity and, more generally, security issues was boosted in the early 2000s by the September 11th terrorist attacks. Two streams of literature that have initially emerged are particularly relevant. The first stream, examines firms' incentives to invest in cybersecurity using one-firm frameworks and, therefore, neglecting all forms of interdependence that can arise among firms. The predictions of this literature might not be of general applicability from a policy perspective because in most real-world situations firms conduct their business using common computer networks and can also be competitors in the product market. On this basis, a second and successful stream of literature investigates interdependent security, not only in the field of cybersecurity, but also, for example, in the ones of airport security, fire protection and vaccinations. This second strand of literature uses multi-firm settings. In the specific context of cybersecurity, this research focuses on the investment decisions of firms that operate their business via a common computer network, but are not competitors in the product market. This setting can be usefully illustrated by the 2013 case of the Target data breach, which involved the Target Corporation, one of biggest retail corporations in the US, and Fazio Mechanical Services Inc., a small company in the sector of heating, ventilation, and air conditioning, also based in the US. While the two companies were apparently not competitors, they were interconnected because, as part of their services, Fazio's technicians used to connect to Target's computer network to perform remote control and maintenance of the heating system. In this context, attackers managed to gain access to Target's network through Fazio, who had access credentials to Target's network for the aforementioned purposes: as a result, Target suffered one of the largest data breaches in history, with stolen sensitive information, including credit and debit card data, affecting approximately 40 million customers (The Wall Street Journal, 2014). A few years later, a third and growing strand of literature shifted the focus to the cybersecurity investment choices of firms that are competitors in the product market, but run their business using non-interconnected computer systems. Amazon. com Inc. and eBay Inc. represent a good case for this setting as they are competitors in the e-commerce sector, but rely on different computer systems for their business activity. Recently, a few papers started investigating the incentive to invest in cybersecurity of firms that use a common computer network and, at the same time, are competitors in the product market. The banking and finance sectors provide a good real-world example of such a framework. Banks tend to be direct competitors and are also closely interconnected as they take part in networks that are essential for their daily business operations. One can think of the SWIFT (Society for Worldwide Interbank Financial Telecommunications) messaging system, which banks rely on to transfer funds worldwide.

This vast and heterogeneous theoretical literature is formalized by Fedele & Roner on the basis of five crucial dimensions.

1. The dimension of *investment* can follow two alternative scenarios: either the cybersecurity investment level can take any nonnegative value in the set of real numbers or it is simply a binary decision. In the latter case there is a simple dichotomous choice of investing or not investing.
2. The dimension of *interdependence* refers to whether the investment choice is analyzed in one-firm settings, using decision theory, or in multi-firm settings, using noncooperative game theory.
3. Only for papers allowing for interdependence, the dimension *welfare* indicates whether the socially efficient investment level is calculated and compared to the equilibrium level or not.
4. Only for papers allowing for interdependence, the dimension *spillovers* describes different forms of externalities related to the three multi-firm streams of literature described before. When firms are interconnected through a common computer network, but they are not competitors in the product market, the investment by any single firm is assumed to reduce the probability of a security breach suffered by all the other firms on the network. This is referred to as *technical spillovers*. When firms are competitors, but use non-interconnected computer systems, firms suffering a cyberattack are assumed to lose clients who shift to competitors that are not hit by any attack. This is referred to as *market spillovers*. When instead firms are both interconnected and competitors, technical and market spillovers are simultaneously present.
5. Only for papers considering technical spillovers, the dimension *network* refers to whether the topology of the computer network connecting the firms is exogenously assumed or it endogenously arises as a solution to a specific optimization problem endogenous network.

Fedele & Roner assess that, in the literature that considers single-firm scenarios, generally the optimal investment in cybersecurity has an upper bound at 36.8 % of the expected loss without protection. When a multi firm scenario is considered instead, two results are observed regarding technical spillovers. Firstly, an increasing number of firms on a computer network yields a lower per-firm equilibrium investment because of free riding. Secondly this equilibrium investment is below the socially efficient level because of the positive externality created by technical spillovers: when a firm invests in its cybersecurity it not only increases its protection against security breaches, it also increases the overall security of the network of firms. In the case of papers that study market spillovers exclusively, the authors discover that the per-firm equilibrium investment is negatively affected by the number of competitors in the product market. Moreover, there is an overinvestment by each firm due to the negative externality brought about by this type of spillovers: in other words, a firm tends to invest more than would be socially optimal as it fears losing customers to competitors in the case of a cyber breach. Finally, the authors consider the literature that includes in its analysis both types of spillovers. Interestingly, the positive results due to technical and market spillovers add up, implying that the per-firm equilibrium investment decreases as the number of competitors using a common computer network increase. By contrast, the socially efficient outcome results in either underinvestment or overinvestment, depending on which spillovers prevail. This third result in particular is interesting for our study as the European financial sector, especially in the case of banks, can be considered as a multi-firm scenario with both technical and market spillovers.

2. THE EUROPEAN FINANCIAL SECTOR AND CYBERSECURITY

Since the opening of the first ATM in 1976, through the implementation of the first online banking website in 1994, to the present day, technology has played an increasingly more relevant role in the operations of banks and other companies of the financial sector (UBS, 2022). Banks now heavily rely on a multitude of hardware and software for the conduction of their daily operations and successfully delivery of their services to clients. Moreover, around half of all high-value cross-border payments worldwide use the SWIFT messaging network. This system is run from three data centers, located in the United States, the Netherlands, and Switzerland, and it uses undersea fiber-optic communications cables to transmit financial data across countries (Cipriani, et al., 2023). This level of reliance on technological systems represents a clear vulnerability when coupled with the existence of malicious individuals or groups of individuals such as the ones listed in Chapter 1.

Christine Lagarde, head of the European Central Bank, recently warned that a combined cyber attack on important banks could trigger a liquidity crisis: she stated that there are “plausible channels”, such as an operational outage that encrypted the balance accounts of a major financial institutions, though which a cyber-attack could morph into a serious financial crisis (The independent, 2020). The ECB Banking Supervision (2022) has listed the improvement in cyber risk resilience frameworks as one of the top priorities for the 2023-2025 period. The objective of such frameworks would consist in increasing the proactivity of financial institutions in tackling any unmitigated IT risks which could lead to material disruption of critical activities or services. Furthermore, in 2021 the European Systemic Risk Board has laid out recommendations on a pan-European systemic cyber incident coordination framework. According to the ESRB major cyber incidents may pose a systemic risk to the financial system given their potential to disrupt critical financial services and operations. In other words, the constantly evolving cyber threat landscape and recent increase of major cyber incidents are indicators of greater risk to financial stability in the Union. The amplification of an initial shock could either occur through operational or financial contagion or through an erosion of confidence in the European financial system. The Board states that if the financial system proves unable to absorb these shocks, the situation could evolve in a systemic cyber crisis threatening financial stability in the EU. In turn the ESRB recognizes the need for a pan-European systemic cyber incident coordination framework for relevant authorities in the Union. The aim of this framework consists in increasing the relevant authorities' level of preparedness to facilitate a coordinated response to a potentially major cyber incident, as a coordination failure could amplify the shock for the financial system by leading to an erosion of confidence in the system as a whole.

As anticipated, we chose to study the effect of direct and systemic cyber incidents on the stocks of European financial institutions. The study of direct attacks can allow to observe the markets' assessment of the risk posed by these attacks to the solidity and profitability of a single financial institution. Conversely, the study of systemic attacks can allow us to observe investors' perceptions of attacks with potential economy-wide repercussions. In other words, in the case of large-scale attacks we will hopefully be able to understand if markets present a fear of the risk of contagion or cascade effects in the instance of events with such potentially devastating consequences. The sample of companies analyzed in this paper was chosen in order to achieve the aforementioned objectives. This group of firms is comprised by banks as well as other types of firms of the financial sector. All of the considered companies are headquartered in Eurozone countries. According to the technical definitions given by European Union, this study comprises:

- Credit Institutions: an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account (575/2013).
- Insurance undertakings: a direct life or non-life insurance undertaking which has received authorization by the Member State in which it operates (2009/138/EC).

- Electronic money institutions: a legal person that has been granted authorization to issue e-money[9] (2009/110/EC).

A credit institution can also be active in other operations apart from the core one described above. For example, a bank can also provide investment and insurance services. On the other hand, a financial institution that isn't a bank can also be active in other kind of operations, but it cannot conduct the core activities of a credit institution. Further details on the financial firms part of this study are given in Chapter 4.

2.1 Regulatory landscape

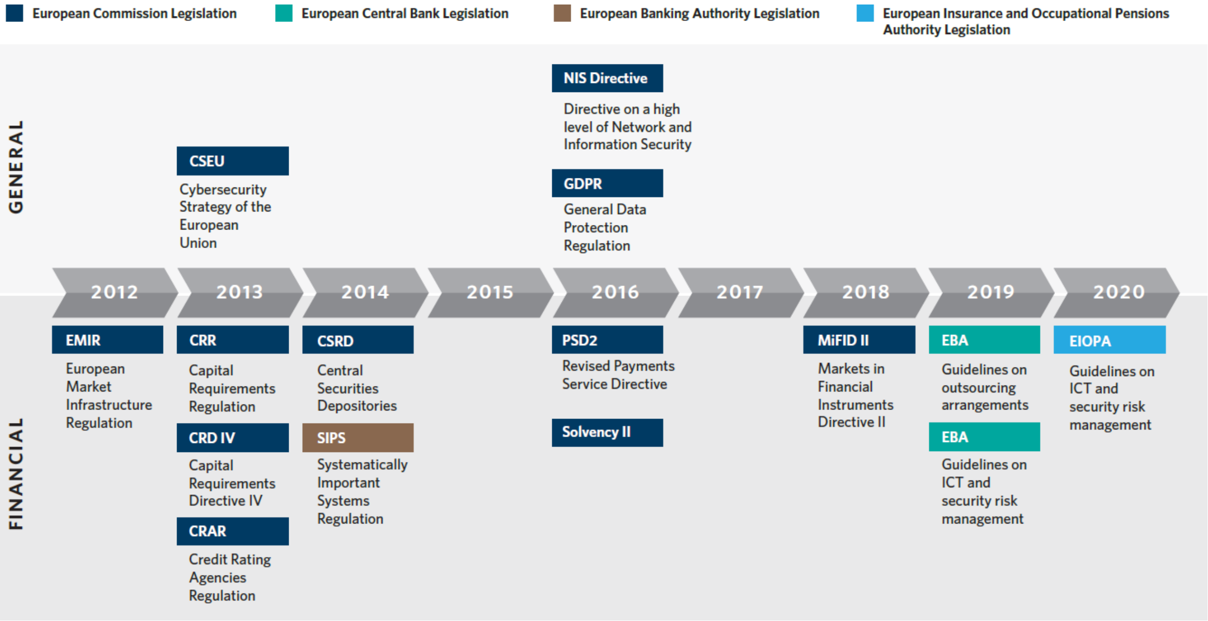
Given the relevance of cyber threats to the EU's financial system, it is important to summarize how the legislators have tackled this topic in recent years. In the 2019 edition of its regulatory digest, the World Bank identified twenty-eight pieces of legislation, standards, guidelines, and supervisory documents that have been issued by EU standard-setting bodies on cybersecurity for the financial sector. Twenty-five out of the twenty-eight existing documents were introduced since 2016. The current situation of the financial services sector in the EU, concerning cybersecurity legislation, is multilayered and complex. For this reason, we make use of Krüger & Brauchle's (2021) primer as a guideline for our summary.

Because financial institutions fall under the scope of different regulatory and supervisory areas, there is not one major European cybersecurity regime for the financial services sector, but rather a multitude of different European and national regulations and sector specific standards. In many member states, the financial sector is defined as critical infrastructure, in line with other sectors such as energy and health. Regulations concerning critical infrastructure sectors, therefore, apply to financial institutions. General European legislation surrounding topics like data protection or cybercrime applies to most companies and therefore affects financial institutions as well. Most notably, financial institutions must adhere to specific financial sector regulation and standards. Even these sector-specific standards differ between the various subsectors, such as banks, insurance companies, and financial market infrastructures. To complicate matters even further, most European standards do not apply directly in all member states, but rather must be transposed into national legislation, creating further fragmentation

[9] Electronic money means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer.

and difference. Figure 3, provided by Krüger & Brauchle, shows a timeline of the existing regulatory landscape with ICT or cybersecurity relevance for the European financial sector. As it only convers the landscape until 2021, we will expand further on newer and announced regulations in the continuation of this chapter.

Figure 3: Timeline of legislation with ICT or cybersecurity relevance for the EU's financial sector.


European Commission Legislation
European Central Bank Legislation
European Banking Authority Legislation
European Insurance and Occupational Pensions Authority Legislation
GENERAL
FINANCIAL
2012
2013
2014
2015
2016
2017
2018
2019
2020
CSEU
Cybersecurity Strategy of the European Union
NIS Directive
Directive on a high level of Network and Information Security
GDPR
General Data Protection Regulation
EMIR
European Market Infrastructure Regulation
CRR
Capital Requirements Regulation
CRD IV
Capital Requirements Directive IV
CRAR
Credit Rating Agencies Regulation
CSRD
Central Securities Depositories
SIPS
Systematically Important Systems Regulation
PSD2
Revised Payments Service Directive
Solvency II
MiFID II
Markets in Financial Instruments Directive II
EBA
Guidelines on outsourcing arrangements
EBA
Guidelines on ICT and security risk management
EIOPA
Guidelines on ICT and security risk management

In its first cyber strategy publication, titled *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (2013), the European Commission acknowledged that dealing with challenges in cyberspace should primarily be up to the member states. Therefore, there is currently no European legislation that lays down specific ICT and cybersecurity requirements for all European companies or institutions. Even if this aim, at some degree, is going to be achieved by legislation that has yet to come into force. The two most important and far-reaching pieces of current legislation are the NIS Directive and the GDPR, both passed in 2016. Both pieces of legislation are limited in scope by focusing on specific sectors, like ones that involve critical infrastructure, or topics, like data protection.

The NIS (Security of Network and Information Systems) Directive (2016/1148) was adopted in 2016 as the first EU-wide legislation on cyber security with the goal to ensure a common level of network and information security across the EU by providing legal requirements. Next to the obligation for EU member states to implement a national cybersecurity strategy and install national competent authorities (NCAs), the directive identifies seven sectors with essential services for the maintenance of critical, societal, and economic activities in the EU: the sectors of energy, health, transport, banking, financial market infrastructure, digital infrastructure, and drinking water supply. For these sectors, member states must identify national operators of essential services (OESs), namely the entities who operate the services in these sectors. The member states shall then ensure through specific critical infrastructure legislation that these entities take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems that they use in their operations. The NIS Directive describes three parameters to determine the significance of the impact of an incident: the number of users affected by the disruption of the essential service, the duration of the incident, and the geographic spread of the area affected by the incident. While past regulations mainly focused on banks, the NIS Directive adds certain types of financial market infrastructures (FMIs) to the list. It is at the discretion of member states to add further critical sectors to these. Although the NIS Directive aims to establish a common standard in the EU, as a directive it is left to the member states to transpose the directive and formulate specific requirements in their respective national legislation. The member states have to further integrate the regulations for critical infrastructures with the existing regulation for the financial sector. However, the type of integration differs between member states. Overall, the framework of the NIS Directive bears the risk of leading to varying levels of security requirements for critical institutions in different member states. With cyber risk, harmonization of security levels across countries is important because attacks can leap over from countries with lower resilience. On top of this, financial institutions that operate in multiple European countries are faced with a variety of different national legislation and responsible authorities.

The GDPR, or General Data Protection Regulation (2016/679), is the second major general existing legislation and one of the most wide-ranging pieces of regulation passed in the EU. It was adopted into law in 2016 and aims to standardize data protection law across the single market while giving individuals greater control over how their personal information is used. It applies to all organizations that control or process personal data and operate within or sell goods to the EU. The definition of processing is designed to cover practically every type of data usage and includes data collection, retrieval, alteration, storage, and destruction. The GDPR aims for a harmonization and simplification of data protection rules across the EU, widens the scope of data protection for all EU citizens, and significantly strengthens data protection enforcement and accountability by authorizing penalties for noncompliance of up to 20 million euros or 4% of global annual turnover. The GDPR, as anticipated, also formulates requirements for institutions to report breaches of personal data to the competent authorities. Financial institutions control and process a large volume of data and are therefore highly impacted by the GDPR. The regulation requires an institution to understand how it interacts with personal information and to obtain consent from individuals before taking action with that data, including consent on how and where data is stored and processed. Financial institutions have to provide new fundamental data rights to both employees and customers, such as the right to be forgotten. Even with its status as a regulation, the GDPR still leaves several significant issues to the interpretation of the member states, creating the risk of national divergence and complication for institutions operating in multiple European countries. While this divergence is smaller than with the NIS Directive, where implementation is completely up to the member states, it still leaves organizations to deal with the rules in the GDPR as well as the national member state legislation.

In the case of the financial services sector, the relevant supervisory authorities were among the first to introduce sector-specific cyber and ICT regulation in the EU, coherently with the importance of cybersecurity for this sector that we previously highlighted. In contrast to these general standards, the sector-specific standards are further specified through so called Regulatory Technical Standards (RTS) and guidelines by the ESA[10] to ensure a consistent implementation in member states. Similar to the general European regulation on ICT and cybersecurity, there is no single legislation for all financial institutions, but rather, multiple standards applying to different subsectors and in different contexts. Although regulation in the banking and payment services sphere is quite detailed and specific, standards for insurance and reinsurance are still very high-level and implicit. While this diversity is attributable to the subsectors' varying levels of maturity, it still leads to a complex and confusing regulatory landscape with overlaps and gaps.

The banking sector has traditionally been the focus of financial services regulation and accordingly has the most extensive standards concerning ICT risks and cybersecurity. The Capital Requirements Regulation (CRR), the major European banking regulation, indirectly comprises ICT risks under the broader operational risks. As these requirements are high level and rather vague, they leave a lot of room for interpretation. In order to ensure a consistent application, the EBA was mandated to specify these requirements in RTS[11] and EBA Guidelines. In these specifications, as well as in the PSD2, ICT and cyber risks are addressed explicitly. While the main focus of the CRR (575/2013) lies in establishing requirements for capital, liquidity, and counterparty credit risk, this regulation also addresses operational risks and internal governance: requirements on operational risks implicitly comprise ICT risks so the CRR is also relevant for cybersecurity requirements. Specifically, it requires the implementation of contingency and business continuity arrangements to ensure an institution's

[10] European Supervisory Agency.

[11] A Regulatory Technical Standard is a delegated technical act prepared by a European Supervisory Authority. It should further develop, specify and determine the conditions for consistent harmonization of the rules included in the basic legislative act.

ability to operate on an ongoing basis and limit losses in the event of severe business disruption. PSD2 (2015/2366) on the other hand was a specific directive for payment services providers (PSPs). In particular this directive was the first European legislative act in the financial services sector that specifically spelled out concrete requirements for cybersecurity and management of ICT risks. The directive, once translated into law, obliges PSPs to implement a strong costumer authentication (SCA) for when customer access their payment account online, make an electronic payment, or carry out any action through a remote channel. Furthermore, the PSD2 established guidelines on major incident reporting, setting out the criteria, thresholds, and methodology to be used by PSPs to determine whether or not an operational or security incident should be considered major and, therefore, be notified to the member state's competent authority.

Other legislative acts that explicitly or inexplicitly address the matter of cybersecurity for various categories of financial institutions include: the Markets in Financial Instruments Directive II (MIFIDII), the European Market Infrastructure Regulation (EMIR), the Central Securities Depositories Regulation (CSDR) and the Regulation on oversight requirements for Systemically Important Payment Systems (SIPS).

2.1.1 Legislative acts coming into force

Given the importance of cyber threats to the EU's financial sector and given the current fragmentation of national and international legislative act, the EC is still working towards further strengthening of cybersecurity measures and harmonization of such measures across countries, as well as sectors. Two major legislative acts, not included in Figure 3, are particularly relevant. In January 2023 the Digital Operational Resilience Act (DORA) regulation came into force and the institutions it covers will have to comply before January 2025. The NIS2 (Network and Information Systems 2) directive was adopted in December 2022 and it will have to be translated into law across member countries by October 2024.

With DORA (2022/2554), the EU aims to establish a universal framework for managing and mitigating ICT risk in the financial sector. By harmonizing risk management rules across the EU, DORA seeks to remove the gaps, overlaps and conflicts that could arise between disparate regulations in different EU states. A shared set of rules can make it easier for financial entities to comply while improving the entire European financial system's resilience by ensuring that every institution is held to the same standard. The requirements will be enforced proportionately through RTSs, which means smaller entities will not be held to the same standards as major financial institutions. One unique aspect of DORA is that it applies not only to financial entities but also to the ICT providers that service the financial sector. In particular the DORA makes an entity's management body responsible for ICT management. Board members, executive leaders and other senior managers are expected to define appropriate risk management strategies and stay current on their knowledge of the ICT risk landscape. Leaders can also be held personally accountable. Additionally, the involved financial entities must establish systems for monitoring, logging, classifying and reporting ICT-related incidents. Entities must also test their ICT systems regularly to evaluate the strength of their protections and identify vulnerabilities. The results of these tests, and plans for addressing any weaknesses they find, will be reported to and validated by the relevant competent authorities. Financial firms are then expected to take an active role in managing ICT third-party risk: when outsourcing critical and important functions, financial entities must negotiate specific contractual arrangements regarding exit strategies, audits and performance targets for accessibility, integrity and security, among other things. Entities will not be allowed to contract with ICT providers who cannot meet these requirements. The NIS2 directive (2022/2555) instead expands the coverage of the original NIS directive from the original 7 economic to a total of 15 sectors. In particular Essential Entities of the financial sector will be required to have contingency plans in place to ensure business continuity in the event of a cyber-attack or other incident. This requirement includes the regular testing of these plans, and the implementation of measures apt to minimizing the impact of any disruption. The involved institutions will also be required to implement robust security measures to protect their data from cyber threats. This includes the encryption of data, both in transit and at rest, the employment of access controls, and the continuous monitoring for any unauthorized access or manipulation of data. The directive also expands on the attention that financial firms must give to their Third-Party Providers (TPPs). This specific attention includes regular security assessments of third-party providers and the periodic verification that third-party providers present the adequate cybersecurity measures in accordance with the directive itself.

2.2 Systemic risk and market concentration

After having analyzed the regulatory framework, we now shift to the discussion of the European financial sector's vulnerabilities, seen through the lens of technical literature on systemic cyber risk. Firstly, within the context of financial networks, De Bandt & Hartmann (2000) have defined an event as having a systemic risk component as:

> *An event, where the release of bad news about a financial institution, or even its failure, or the crash of a financial market, leads, in a sequential fashion,*

> *to considerable adverse effects on one or several other financial institutions or markets, e.g. their failure or crash.*

Geer et al. (2020) explain how market concentration, meaning the concentration of market share in the hands of a smaller number of firms, can cause market failures and increase systemic risk. The authors highlight that trends towards market concentration are the new normal in IT systems and the Internet. The underlying catalyst of this process of concentration is that the greatest user and corporate value is often found at the most frequented places. The examples of such points of concentration range across operating systems, protocols and antivirus vendors. Arguably, the European banking sector is also gradually experiencing concentration in favor of fewer and more economically powerful credit institutions. Since 2009, the number of banks in the EU has continuously decreased in the banking sector. In 2020, there were only 5.441 banks, corresponding to a fall of 33% when compared with 2009 (Saravia, 2020). This tendency towards market concentration has a number of effects on systemic cyber risk. These effects play out at every level of the risk equation proposed by the NISTIR that we have explored in section 1.4., that is, across threat, vulnerability and impact. According to the authors concentration has predominately distributional effects on the threat component of cyber risk, namely, concentration leads to risk transference. Who gets targeted is a function of potential reward for malicious actors, which is, in turn, a function of a potential target's size or network centrality. Increased size and position correlate with malicious actor payout, whether that reward is financial, disruptive or geopolitical. As a market concentrates, the risk of being targeted by a cyberattack transfers from small, less central organizations to the major hubs or their counterparties. For smaller organizations that might not be able to assume the financial cost of greater levels of cybersecurity, the transfer of risk from small to big organizations would be a positive aspect. From the perspective of the highly concentrated organizations, the increased volume of attacks that need to be dealt with impose additional operating costs. Concentration affects the vulnerability component of the cyber risk equation. Three distinct effects emerge. First, concentration in large providers can lead to an average reduction in the individual vulnerability of users, website operators and organizations due to the greater security services provided by these major hubs. Second, since concentrated nodes tend to get targeted more often, joint probabilities suggest that they might be vulnerable across a large enough sequence of attacks. Third, platform and service concentration can also lead to increases in complexity, which can have negative effects at the level of software, increasing the proportion of vulnerable code. The first effect suggests that individuals can leverage scale to reduce their risk. The second and third suggest that at a systemic level, concentration can increase vulnerability and worsen cyber risk. Lastly the consequences of a successful cyberattack are hugely variable, but likely dependent on patterns of concentration, among other factors. In highly concentrated systems, everything is connected, especially to the big nodes in the system. Such interconnections can take a number of forms, but readily include links between organizations via data sharing agreements, common supply chains and third-party vendors. Interconnections create transmission pathways by which the negative consequences of a security incident can percolate through a whole system.

In summary Geer et al. suggest that, overall, the negative externalities of concentration with respect to cyber risk could imply that the optimal level of expenditure of an individual firm found in Chapter 1.4, equal to 37% of the expected loss, could represent a lower level than socially optimal one. This may also be true for the European financial landscape, thus the current legislation's focus on larger institutions, such as DORA's more stringent requirements for major financial firms, is justified form a theoretical standpoint at least.

Kopp et al. (2017) suggest that the market equilibrium can fail to provide a socially optimal level of security also due to information asymmetries, misaligned incentives, other externalities and coordination failures. Furthermore, the authors underline that it is still under debate which approach works best in preventing the market from failing: ex-ante regulation and ex-post liability. Ex-ante regulation aims at preventing security risks to materialize, and can take the form of rules or guidance. With ex-post liability instead, responsibility is assigned to a certain party. It is implicitly assumed that legal threats motivate the liable party to take security seriously, and invest accordingly. According to Kopp et al. information asymmetries, and the subsequent moral hazards or adverse selection problems, can take multiple forms when it comes to cybersecurity. In the first place, effective monitoring of others' activities in an anonymous and complex system like the cyberspace is either impossible or extremely costly. There are also reasons for firm actors not to share information including legitimate concerns of reputational costs or an impact on the demand for that firm's services. Additionally, with both state and non-state actors involved in cyber areas, there are strategic reasons as to why one country would prefer not to share information on the nature and size of its cyber losses or strategies in place to protect its systems from cyber-attack. A final form of information problem resides in judging the need or efficacy of particular types of cyber protection. Many firms, especially if they are smaller, lack the cyber-specific knowledge needed to make rational decisions about which software or cyber security provider to choose. When it comes to misaligned incentives an example concerns software flaws, which create common exposures to cybersecurity risk. These externalities are not often internalized by the vendors and can induce negative externalities from exposure to the same network or technologies. Software developers do not particularly emphasize security until products achieve market dominance because it is more difficult and costly to develop applications for secure products. Further down the line we will explore how the American company SolarWinds was breached, and its software Orion, used by a significant number of public sector and private customers worldwide, was compromised by attackers. This example is also potentially applicable to the European financial landscape as similar regulatory requirements across major institutions could contribute to their choice of similar security products provided by a limited number of companies. These authors too recognize the existence of positive externalities in consequence to the investment in cybersecurity of other firms. As we have seen in the previous chapter, such externalities can be defined as technical spillovers. If these externalities persist, firms have incentives to free ride by underinvesting in their own cybersecurity. If private costs are lower than social costs, with externalities not fully internalized and priced, market outcomes will not be efficient with an underinvestment in protection and the resulting negative externalities, should they be realized, being borne by the industry or society.

Kopp et al. also note that risk management in financial institutions has been mostly focused on idiosyncratic risk. This is natural given an individual firms visibility and understanding of the broader systemic effects. However, this has meant insufficient attention in countering systemic cyber risks arising from the dependence on complex infrastructure or disruptions to critical information. The predominance of cyber risk assessment on the level of individual institutions and entities signals a relatively narrow view that insufficiently considers the systemic dimension of cyber risk. In particular contagion effects on a non-technological level could represent a real threat for the financial ecosystem. Close direct connections through interbank and transfer markets, and indirect relationships, exemplified by liquidity cascades, allow shocks to spread quickly throughout the system. An institution’s inability to meet payment or settlement obligations, for example because their internal record-keeping or payments systems have been compromised, can cause crisis, which would have adverse effects on funding liquidity and knock-on effects to other institutions which were counting on the availability of these liquidity flows. Liquidity shortages can lead to fire-sales which then feed into asset valuations and spread to all kinds of market participants that are invested in or are trading a particular asset or asset class.

In sum these authors suggest that lawmakers take into consideration the various issues posed by information asymmetries to the achievement of the socially optimal level of expenditure on cybersecurity by each actor of the system.

Welburn & Strong (2022) expand on systemic risk by defining three categories of systemic failures that can occur as a result of cyberattacks: cascading, common cause, and independent. Cascading cyber failures are the result of one cyber incident propagating outward and causing many disruptions. They lead to a domino effect across firms and organizations interconnected through supply chains or other means. A DDoS cyber-attack on a TPP, where firms dependent on this TPP's services suffer outages and business disruptions due to the initial single attack can exemplify a cyber incident leading to cascading cyber failures. In this definition of cascading failure, the authors refer specifically to the propagation of firm level disruptions, not necessarily the propagation of cyber vulnerabilities. That is, the initial attack leads to cascading failures due to disrupted business services and operations. On the other hand, common cause cyber failures are the result of one cyber exploit triggered at many firms causing many cyber incidents. Unlike cascading failures, common cause failures exploit a common vulnerability held by multiple firms and organizations causing numerous cyber incidents either simultaneously or in quick succession. The WannaCry cyber-attack, that will be analyzed in the continuation of this paper, provides a well-known example of the exploitation of a software vulnerability, by a single hack to compromise thousands of machines for ransom across the world within days. It is worth noting that, in the cyberspace, cascading and common cause failures are not mutually exclusive. A quick spreading worm, for example, may exploit a widely held vulnerability on a single machine to spread from the source outward to many directly and indirectly connected systems. While this kind of incident has features of cascading failures, Welburn & Strong classify this type of failure as a common cause cyber failure with cascading consequences. For cascading failures, they focus on the cascade resulting from the direct and indirect effects of business outages where customers lose access and supplier lose revenue. Finally, independent cyber failures are the result of cyber incidents concurrently exploiting independent vulnerabilities at individual firms and organizations. In theory, numerous individual cyber incidents could happen simultaneously to create a systemic event, however in practice this type of event is currently unlikely in the authors' opinion. However, absent advances in postquantum cryptography, the advent of quantum computing could enable encryption breaking *en masse*, leading to concern over large scale independent failures Cascading and common cause cyber failures are, therefore, the main possible drivers of systemic cyber risk in present times.

Welburn & Strong, after their theoretical analysis, proceed to estimate the real costs of systemic cyber risk. They employ a quantitative method for estimating the aggregate impact of firm-level shocks with both upstream and downstream negative effect on the firm's supply chain. The results show that the potential direct costs associated with cyber incidents are greatly outweighed by the multiplier effects of up- and downstream connections. While this concern could be true for any firm-level shock, it is particularly relevant given the heavy interconnections of cyberspace. Given their analysis and estimation of potential cyber incident costs, a reliance on private sector solutions including cyber risk management and insurance may prove insufficient for the growing magnitude of risks. In other words, systemic cyber risks have the potential to exceed private sector solutions thus revealing a need for additional policy consideration. Even if the authors conduct their estimations on major US companies, their results can most likely be applied to any European firm operating in the financial sector, including major TPPs. For this reason, EU legislators in the recent years have focused on improving the risk management solutions of private institutions, which would otherwise developed at a sub-optimal level with respect to the socially efficient one. Interestingly, this cited work suggests that cyberinsurance levels may also be under their socially optimal level, when it comes to systemic attacks. Furthermore, in case of systemic attacks insurance companies providing cyber policies could be at major risk of operational failures due to the need of checking and responding to multiple claims in a short amount of time. Future sector specific legislative acts for the EU should also consider this vulnerable aspect of the insurance sector.

3. EVENT STUDIES

3.1 The Event Study Methodology

In business and finance literature, a recurring method to measure the impact of an event on a company is represented by the Event Study Methodology. In financial research in particular, event studies are used to investigate the implications of announcements of corporate initiatives, regulatory changes, or macroeconomic shocks on stock prices. These studies are often used in a single-country setting and little work has yet been conducted in an international context (El Ghoul et al., 2022).

Before going into the specific papers which have made use of such a method in the field of finance and in the cybersecurity one, it is important to give an overview of the method itself. As briefly mentioned in Chapter 1, an event study is a method used to measure the effects of an economic event on the value of firms. In other words, it is an analysis of whether there is a statistically significant reaction in financial markets to occurrences of a given type of event. The null hypothesis is that the event has no impact on the distribution of returns (MacKinlay, 1997). The method was first introduced by Fama et al. in 1969, it has since then gained popularity as an econometric technique and has become the standard method for measuring the reaction of financial asset prices to certain announcements or events (Furdui & Șfabu, 2023). The event study technique has an interesting relationship with the Efficient Market Hypothesis developed by Fama et al. (1969) and refined by Fama (1970). Before continuing with the discussion of this relationship, we delve into the specifics of the EMF. With the use of two characteristics of efficient markets, informational efficiency can be *weak*, *semi-strong*, or *strong* (Fama, 1970). The first, is how quickly and completely any new information is incorporated into asset prices. The second is which information is considered relevant and which is not.

- The *weak form* of the Efficient Market Hypothesis asserts that all historical price and volume information is already reflected in the current stock prices. In other words, past trading information, such as historical prices and volumes, is already incorporated into the current stock price. This implies that technical analysis, which involves studying historical price movements and patterns to predict future price movements, should not provide an investor with an advantage in generating consistently higher returns. If the market is weak-form efficient, it suggests that any attempt to gain an edge through the analysis of historical data, including chart patterns and technical indicators, is futile: investors cannot consistently outperform the market by relying solely on historical information. The weak form of the EMH, is sum, assumes that stock prices follow a random walk, meaning that future price movements cannot be predicted based on past prices.
- The *semi-strong form* of the Efficient Market Hypothesis builds on the weak form and adds that all publicly available information is reflected in current stock prices. This includes not only historical price and volume data, as in the weak form, but also all public information, such as financial statements, economic indicators, and news. According to the semi-strong form, it is impossible for investors to consistently achieve higher-than-average returns by using publicly available information because such information is already incorporated into stock prices. In a semi-strong efficient market, the prices of securities adjust rapidly to new information. As soon as any public information becomes available, it is reflected in the stock prices, leaving no room for investors to exploit the information for

abnormal profits. This implies that fundamental analysis, which involves studying financial statements and economic indicators, should also not provide investors with an advantage in consistently outperforming the market.

- The *strong form* of the Efficient Market Hypothesis takes the concept further by asserting that all information, whether public or private, is fully reflected in current stock prices. This means that even insider information, which is not available to the public, is already incorporated into stock prices. In a strong-form efficient market, no group of investors, including insiders, should be able to consistently outperform the market based on their private information. If the market is strong-form efficient, it challenges the notion that individuals or institutional investors can gain a sustainable advantage through possessing insider information. The strong form suggests that even those with access to non-public information cannot consistently achieve abnormal returns because the market already factors in all available information.

Now that we have summarized the three forms of the EMH, we can circle back to the its relationship with event studies. According to Kothari & Werner (2007), event studies serve an important purpose in capital market research as a way of testing market efficiency. Systematically non-zero abnormal returns by a security, that persist after a particular type of corporate event, are inconsistent with market efficiency. The measurement of such persistent abnormal returns would in fact mean that it is possible to trade profitably on the basis of public, in the case of the semi-strong form of the EMH, or private, in the case of the strong form of the EMH, information which should be already be reflected in prices. On the other hand, if prices quickly adjust in view of firm specific events, it means that the market has reacted in an efficient way. This in fact implies that the abnormal returns only persist in the short-term, instead of being persistent in the long-term. In summary, the estimation of significant abnormal returns in the short term goes in favor of proving the EMH, specifically in its semi-strong form. On the contrary, the estimation of persistent long term abnormal returns goes against the EMH. To go more into detail, short term event studies usually deal with an estimation period, after the announcement of an event, of some days, never more than a month. Long- and medium-term event studies conversely consider estimation periods in the order of multiple months or even years. The term “long-term market value”, according to Kuo et al (2020), is defined as the degree of change in stock from one to three years after the event.

The relationship between the EMH and event studies is further complicated by the *joint hypothesis problem*. According to Campbell et al. (1997) any test of efficiency must assume an equilibrium model that defines normal security returns. If efficiency is rejected, this could be attributed to one of two causes: the market could truly inefficient or an incorrect equilibrium model could have been assumed instead. The ambiguity contained in the joint hypothesis problem means that market efficiency as such can never be rejected. As this particular topic isn't central to our study, we will not explore it further. The main point that interests us, posed by the joint hypothesis problem, is that although short-term event studies, such as the one conducted in this paper, are coherent with the semi-strong form of the EMH if the resulting abnormal returns are significant, we cannot be sure that the EMH is verified.

Adding to the dichotomy between event studies with a short-term horizon and a long-term horizon, Kothari & Werner (2007) suggest that the former are overall more reliable than the latter. Long-horizon methods have seen major developments but nevertheless still present serious limitations, summarized in a lack of reliability and low power. Lyon, Barber, and Tsai (1999) went as far as stating that "the analysis of long-run abnormal returns is treacherous". Short-horizon methods are instead relatively straightforward and trouble-free. As a result, we can have more confidence and put more weight on the results of short-horizon tests than long-horizon tests. As mentioned, this paper is focused on event studies with a short-term horizon, with an analysis that does not consider more than two days after the event.

3.1.1 Event studies in financial literature

In 2007 Kothari & Warner conducted a census in order to precisely quantify the event study literature. Their census analyzed the interval between 1974 and 2000. The total number of papers reporting event study was 565. This survey only considered the articles published in 5 leading journals[12]. Since many academic and practitioner-oriented journals were excluded, these figures merely provided a lower bound on the size of the literature. Since then, the use of the ES methodology has grown so fast that an overall contemporary census would require an enormous amount of effort. This is why El Ghoul et al. (2022) provide another more recent survey, exclusively focused on the world of finance. They survey four journals[13], and find a total of 699 event-study papers, of which 545 investigated *firm-level* events (78%), 38 dealt with *peer-level events* (5,4%), and the remaining 116 focused on *country-level* events (16,6%). *Firm-level* events are events that only affect one firm. On the other hand, *peer-level* events are

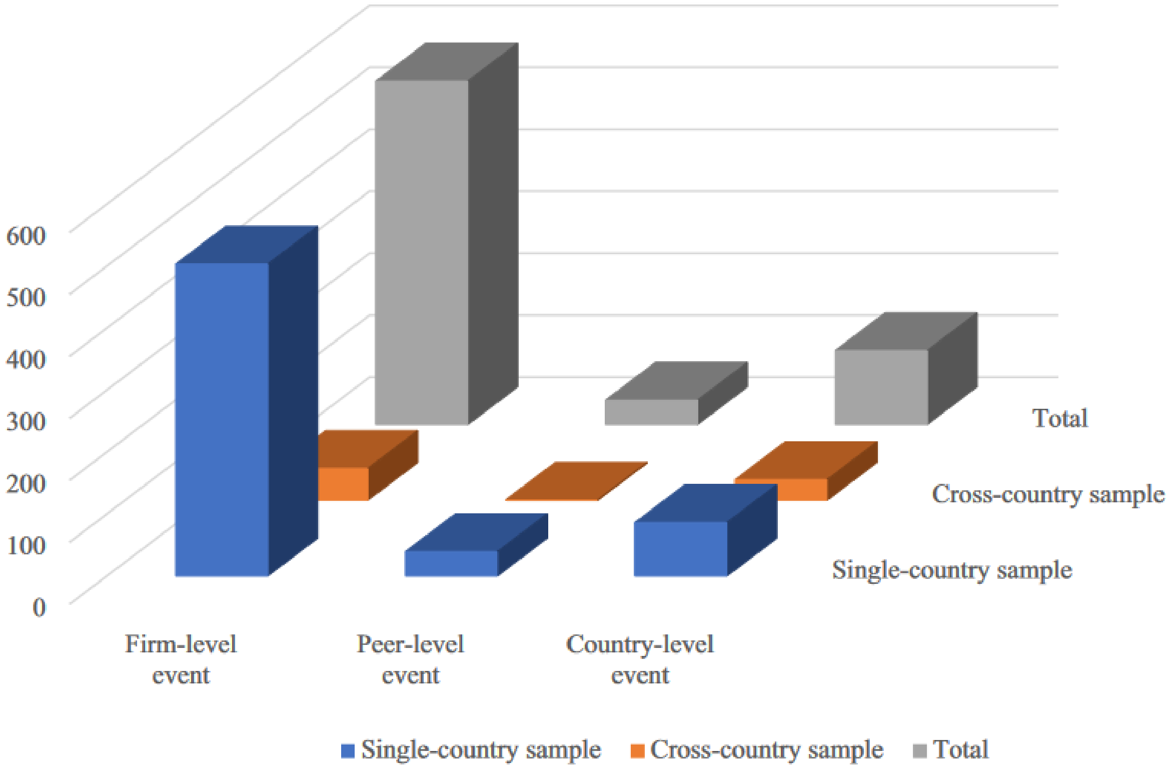
[12] Journal of Business (JB), Journal of Finance (JF), Journal of Financial Economics (JFE), Journal of Financial and Quantitative Analysis (JFQA) and the Review of Financial Studies (RFS).

[13] Journal of Financial Economics (JFE), Journal of Finance (JF), Review of Financial Studies (RFS) and Journal of International Business Studies (JIBS).

occurrences that have an impact on a multitude of companies, part of the same sector. Finally, *country-level* events are instances which affect an entire country's economy, meaning all of the firms that are either headquartered in that country, or operate in that country.

In Figure 4, El Ghoul et al. (2022) graphically divide the event studies they surveyed in six different categories, with these categories originating from two characteristics of event studies. The first characteristic is the one discussed above, namely the type of event that is considered: either firm, peer or country level. The second characteristic is instead the composition of the sample of companies, on which the effects of the aforementioned events are to be estimated. A sample of firms can in effect either be cross-country or single-country.

Figure 4: Representation of the surveyed event-studies, by event type and sample type.



In the case of our direct events or firm-level events, the sample of companies is a cross country one, as firms from different European countries have been the explicit target of attacks. On the other hand, in the case of our systemic events, while the sample is still cross-country, the events are peer-level ones. Thus, based on Figure 4, the event study of the present paper can be considered as located on two of the six different groups above. It can be seen that this paper conducts a type of analysis that has not been particularly common in the existing literature. Even more so, event studies applied to the field of cybersecurity, are themselves a niche when considering the event study world.

3.2 Event studies and cybersecurity: a literature review

In the course of this section, in the first place we go through a general review of the research that makes use of the event study methodology to assess the impact of cyber events on companies' stocks. In the second place we analyze in detail the specific papers which inspired our dissertation. As we have seen in the previous part, the assessment of the impact of unexpected events on the stock price of firms has been performed in the financial literature with event studies since the late 1960s. However, it was only in the early 2000s that the consequences of information security events were first investigated. The first incidents that were analyzed by the researchers were the information security breaches. The security breaches are essentially the successful attacks over the information systems by hackers aiming to harm the confidentiality, the integrity or the availability of a system. It is useful to summarize the approach and the results that some of the most relevant papers, part of this initial wave of specialized research, adopted and found.

The first study of this particular strand of literature is the one by Campbell et al. (2003). The authors electronically searched for terms connected to information security incidents on the websites of major US newspapers[14]. The reasoning behind this method is that, if an event related to a cybersecurity breach regarding a US company is reported by a major national newspaper, it must be relevant hand have a significant impact on the company's stock. After this research they carefully selected a total of 43 events, affecting 38 events: this means that, as in our study, some companies were the subject of multiple successful cyberattacks. The selected events all happened between January 1995 and December 2000. As a result of their study, the authors found a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data. Conversely, when the security breaches did not involve this kind of unauthorized access to confidential information, such as in the case of DDoS attacks, no significant negative reaction by the companies' shares was found. The base line of the results is that security breaches, as a generic group, have a negative effect on the stock market returns of firms, but this effect is not always statistically significant.

In 2003 Garg et al. identified a set of 22 information security breaches from 1996 to 2002. By conducting their event study on a sample of exclusively American firms they found that, on average, the stock of a company hit by a successful cyberattack presented a negative significant

[14] Wall Street Journal, New York Times, Washington Post, Financial Times, USA Today

reaction. The particularity of their research resides in their differentiation of security incidents between four types: website defacements, DDoS attacks, theft of credit card information and theft of all other customer information. Regarding the DDoS instances, the average fall in the share prices was 3,6% over a three-day period. Websites defacements caused a smaller reaction, at around minus 1,1% over the same period. Thefts of information caused a 1,5% decline in the share prices of companies over the three-day period. However, in the case of theft of credit card information, the results were more variate than the ones found for other cyber events: in general markets seem to perceive a direct correlation between the number of stolen credit card numbers and the damages to the company subject to the theft. On average, in the instance of credit card information theft, the sample companies lost 15% of their stocks' values, measured on the usual three-day period. Interestingly Garg and his collaborators also considered an aspect of cyberattacks that was not yet analyzed in similar literature. The authors measured the effect of cyber breaches on the share prices of IT security companies. As expected, in general, security stocks responded positively to security incidents targeting other companies: these stocks gained an average of 3,3% when considering all of the events in the sample. Although we do not consider this particular niche in the present study, it would surely be interesting to conduct a similar analysis utilizing the events that will be listed in chapter 4.

Another relevant early study is that by Cavasoglu et al., published in 2004. In this case the researchers, instead of manually searching online on various newspapers' websites, made use of a public database of US newspapers' articles, maintained by the LexisNexis company[15]. This allowed them to a total 66 relevant cyber events, between January 1996 and December 2001, affecting 44 US companies. As with the previous paper, we notice that the only country in which the companies of the sample are located in is the United States. Cavasoglu and his collaborators found that breached firms in the sample lost, on average, 2,1% of their market value within two days of the announcement. Their estimations are mostly significant.

In 2003 Hovav and D'Arcy focused their attention on a specific type of cyberattack: Distributed-Denials-of-Service. We are locating this paper in contrast with the chronological order of the previous two. This has to do with the fact that these authors, one year later, once again conducted a similar study but focusing on another type of attack. It is therefore coherent to describe these two studies in quick succession. Returning to the paper in question, the authors searched for relevant DDoS attacks by first using the LexisNexis database, and then applying specific selection criteria: in the end they identified a total of 23 DDoS attack announcements

[15] LexisNexis is a part of the RELX corporation (formerly Reed Elsevier) that sells data analytics products and various databases that are accessed through online portals. During the 1970s, LexisNexis began to make legal and journalistic documents more accessible electronically. As of 2006, the company had the world's largest electronic database for legal and public-records-related information.

events from 1998 through 2002. Overall, the results did not demonstrate that there is a significant impact of DDoS attacks on the capital market. However, there was some indication that such events do have an impact on companies that heavily rely on the Web for their business. Furthermore, even if the result were not significant overall the authors observe a potential correlation between the length of the downtime and the abnormal returns of a company's stock. As anticipated Hovav & D'Arcy, in 2004, focused their attention on a different type of security breaches, namely virus attacks that were publicly announced in a period of 15 years, form 1988 through 2003. The sample of firms only comprised firms that at the time were publicly traded either on the New York Stock Exchange or the NASDAQ stock exchange. The authors once again conducted their research on the relevant events through the use of the familiar LexisNexis database: this research yielded a total of 186 instances. Overall, the results found by Hovav & D'Arcy, did not demonstrate that there is a significant negative impact of virus attack announcements on the share price of the attacked companies. Specifically, viruses were associated with negative stock returns for only about 44 percent of the attacked companies.

Now that we have explored the specifics of some of the first research in this particular field, we can transition to a bird's eye view of the relevant literature that has since been published. In order to adopt this perspective, we can refer to what Spanos & Angelis found in their systemic literature review, published in 2016. These two authors, based on four quality assessment criteria identified a total of 37 relevant papers. The majority of the papers, six, were published during the year 2011 whereas during the rest of the years, starting from 2003 until September 2015, the numbers of published papers ranged between 1 and 4. The time intervals used in the papers of the systematic review started from 1988, while the most recent time interval ended in 2012. Moreover, the smallest time interval is three days while the largest is seventeen years (1995–2012). The most popular data source of information security events, that was used in 32,4% of the papers, was the LexisNexis Database that has already been mentioned. In Chapter 5, which covers the methodology of our paper, there is a brief explanation of the different estimation models that can be employed in an event study. For now, it is important to keep in mind that we are going to employ the one-factor model. Circling back to the literature review by Spanos & Angelis, regarding the model employed in the various event studies, it was found that 78,4% use the one-factor model, which is a type of market model. Instead, in 13,5% of the publications, the Fama–French three-factor model was used.

In the previous section, about the general literature on event studies, we found that El Ghoul, et al. (2022) observed a profound bias toward single country event studies, with the majority of them focused on United States firms. Coherently to this observation, Spanos & Angelis found that the vast majority of the papers (83,8%), which used event studies on cybersecurity incidents, analyzed firms that are traded in the US Stock Market. In particular only five papers (13,5%) used firms from different countries. The authors attribute this strong US bias to the availability of information regarding US firms. The number of events that have been used ranges from 4 to 306 with an average of 91,7 events. The impact of security breaches on the targeted companies is generally considered as a negative phenomenon. 89,3% of the considered papers presented a negative impact, even if not all of these papers had significant results: 71.4% of the articles found negative returns that were actually significant. It can be anticipated that in this systematic literature review the most common significance test were found to be the t-test, the Z-test, the Wilcoxon sign-ranked test and the sign test.

After this general review of the literature, covering the more recent years until 2016, we can discuss some of the latest developments in the field. A study by Kuo, et al. (2020) considers data breaches from 2003 to 2015. The relevant events are once again derived from the LexisNexis database. The novelty of the study by Kuo and his collaborators comes from the subdivision of data breaches in two different types based on their effects: the first group of breaches contains those events which impact is deemed to be short-term, conversely the second group contains those events with long-term effects. For the first kind of events a sample of 99 units is identified, for the second a sample of 52. According to the researchers themselves, this study is the first to empirically analyze the relationships between data breaches and long-term market value of the breached firm. The authors find evidence that the stock market, in the short-term responds negatively to announcements of breaches of confidential data at publicly traded firms. Specifically, the day of the event's announcement, the abnormal return to the event company is -0,23%. The results of the long-term estimations, indicate that the average abnormal return of the company in the 12 months after the event is -10,21%, while in the 24 months and 36 months windows after the event, there are significant abnormal returns of -32,68% and -34,36%, respectively. The result may indicate that the impact of the incident is not one-off but continuous. With the innovation of attack techniques, a security breach may not only silently persist in a firm's IT systems, but also expand further.

In 2017, Abshishta et al. build upon Hovav and D'Arcy's study of 2003 on Denial-of-Service attacks. The authors conduct a web search based on keywords regarding DDoS instances and select a sample of 35 announcements that happened between 2010 and 2015. The companies on which the impact of the announcements is tested are headquartered in multiple nations: Denmark. Finland and the Netherlands are included in addition to the USA. In most cases no significant negative effect is found on the victim stock prices. In particular in the cases where the announcements state that the availability of the infrastructure under attack did not affect the customers, no significant impact is noticed. Nevertheless, there is a noticeable negative impact on the stock prices of the victim firm whenever the attack causes interruptions to the services provided by the firm to its customers. However, Abshishta and the other researchers involved in the study declare themselves unable to comment on the intensity of the impact, because it is firm dependent.

The last part of this section is dedicated to a final paper that aims to help resolve conflicting evidence from previous studies concerning the effect of information security breaches on market returns of firms (Gordon, et al., 2011). This central conflict in the evidence can be guessed from the results of the previously mentioned papers, and it can be summarized as follows: while a part of the first studies of this strand of literature finds significant negative abnormal returns associated with cyber breaches (Garg, et al., 2003; Cavasoglu, et al., 2004), the other part, roughly equal in size, finds negative but overwhelmingly unsignificant abnormal returns (Campbell, et al., 2003; Kannan, et al., 2007). Interestingly, Gordon et. al notice that there is a general tendency for more recent studies to find non-significant results, even if some outliers do exist (Campbell, et al., 2003; Hovav & D'Arcy, 2003; Hovav & D'Arcy, 2004). In order to understand this conflict in results Gordon et al. start from the creation of a sample of events. They do so thanks to a full text search of the major US papers[16] for the period of 1995–2007: the keywords they search are all related to cybersecurity incidents. As a result of the above sample selection criteria the study includes 121 security incidents affecting 85 firms. Furthermore, the authors divide this sample of events into two sub-samples based on a separation date coinciding with the 11th of September 2001: 60 incidents end up in the pre-9/11 sub-period, 61 are in the second sub-period.

After the estimations of the abnormal returns Gordon et al. make an interesting discovery: while the events of the first sub-period mostly yield negative and significant abnormal returns, the events pertaining to the second period yield a total of zero significant abnormal returns. Regarding this result the authors propose the following explanation. Consumers and investors familiarity with information security breaches has grown over time, based on indirect experience if not from direct experience. This increased familiarity with information security breaches may have led investors to revise their assessments of the effect of breaches on the value of the firm. Specifically, investors may suppose that the impact on future sales and profits

[16] The Financial Times, The New York Times, USA Today, The Wall Street Journal and The Washington Post.

of a breach occurring in later years has diminished in comparison to the impact of a similar breach in earlier years. In other words, if increased familiarity with breaches diminishes the negative impact of a breach on customers' confidence in the breached firm, information security breaches could have a smaller effect on sales and profits. Moreover, the authors note that, in fact, by the time of the 9/11 attacks in 2001, announcements of security breaches started to be common even among the best run companies. As a result, it seems to them logical to consider the possibility that consumers developed a much greater tolerance for news on announcements of such breaches. Another explanation, not exclusive with the first one, put forward by the researchers, consists in the fact that firms, over time, have strengthened their remediation and disaster recovery plans and therefore have substantially reduced the cost of an average information security breach.

In addition to the mentioned findings, Gordon et al. discover that security breaches involving information availability have a significant negative effect on stocks. This significant effect is coherently only found in the first sub-period. A security breach is said to affect information availability if it prevents authorized users of information from having access to such resource on a timely basis, think for example of a Denial-of-Service. Conversely, attacks that involve information confidentiality and information integrity do not have a significant negative effect on the shares of the targeted companies in either of the two sub-periods. Attacks that breach information confidentiality are defined as attacks that allow unauthorized users to access confidential information (Campbell, et al., 2003). Attacks that compromise information integrity are breaches that compromise the reliability and validity of a database, such as website defacements.

3.3 Specialized event study literature on cybersecurity and the financial sector

In the existing event study literature, there is a clear gap when it comes to the interaction between financial institutions and cyberattacks. Although multiple papers have analyzed this relationship through the use of the event study methodology, no researchers have yet dedicated an entire study to this relationship (Arcuri, et al., 2018): every time that financial institutions' stocks are measured in view of a cyberevents, this measurement is part of a larger study that also takes into account other types of companies. In synthesis there doesn't exist an exact precedent to our study, which not only undertakes to analyze the relationship between financial companies and cyberattacks, but also restricts the companies to ones that are headquartered in the Eurozone. Thus, our study aims to cover this distinct gap that is present in the literature. For the above reasons, this section is concerned with specific parts of event studies concerned with security breaches of financial institutions.

The first relevant study in this field that we are discussing is the one by Colivicchi & Vignaroli (2019). The authors select a sample from the LexisNexis database, searching for newspaper reports of global cyber-attacks between 1995-2018, using different keywords. They end up with 277 cyber-attacks announcements affecting 149 firms: in particular 96 of these cyber-attacks have financial companies as a target, equal to 34,6% of the total sample. The daily stock market prices are retrieved, adjusted for dividends and splits, from the Thomson Reuters DataStream database. As a result of their estimations, Colivicchi & Vignaroli find evidence of an overall negative stock market reaction to public announcements of information security breaches. Not all results are significant. In particular when the returns are not estimated before the announcement of the event, meaning only in the days after the announcement, they are negative but not significant. In the financial sector, the authors find more negative market returns than other sectors when they also consider abnormal returns in the first few days before cyber risk announcements. Thus, the researchers conclude that it could be possible that cybercriminals are involved in insider trading. Moreover, it is observed that financial entities show greater negative effects on market returns than companies belonging to other economic sectors: for this reason, the researchers suggest that financial companies in particular should make a bigger investment in IT improving their security. The authors propose, as an explanation to the higher losses in which financial entities incur, the fact that banks have a dual challenge when it comes to cybersecurity. Banks and other financial institutions not only have the task of protecting confidential data about their customers, but also have the challenge of safeguarding their systems and networks as well as the financial assets they hold. On the other hand, in light of the abnormal negative returns that they observe even before the announcements are made public, the authors suggest that cyberattacks in the financial sector may be linked to insider trading. Colivicchi & Vignaroli suggest that financial authorities strengthen cybersecurity measures.

Tweneboah-Kodua, et al. provide another important contribution to this field (2018). The study uses the information of the announcements of data breaches on firms listed on the S&P500 between January 2013 and December 2017. Specifically, 96 firms that experienced cyberattacks were chosen. The event dates are considered as the first public announcement of the attacks. Interestingly, the authors perform the empirical analysis in two ways: as a cross-section and at the industry level. They divide the 96 firms into five sub-groups, each corresponding to a specific industry: industrial, information technology, health, retail and financial. The test statistics of the cross-section analysis show that markets do not significantly react to cyberattacks for all the event windows, except when measuring the cumulative abnormal returns starting form 30 days before the announcement and ending 30 days after it. For the industry level, the analysis of Tweneboah-Kodua et al. offers three main results. First, there is no evidence of a cumulative firm reaction to cyberattacks for all the estimation windows for the industrial, information technology and health sectors. Second, for the retail sector, only the generalized Z test shows that the firms marginally reacted when considering the cumulative returns from 20 days before the announcement to 20 days after it. Most importantly, for the financial sector, there is strong evidence of cumulative reaction to cyberattacks for a relatively small estimation period: financial companies show significant negative abnormal returns, when they are measured cumulatively between the first day before the event and the first day after it. The reactions disappear for relative longer event windows. According to the authors, the outcome of this analysis implies the following conclusion: studying the cumulative effects of cyberattacks on prices of listed firms using event study methodology without grouping the firms into various sectors may not be informative. For our purpose it is instead important to note how financial companies seem to react in a significant way in the few days close to the announcement.

Arcuri et al. (2018) also contribute to this topic, it is thus worth briefly going through their methods and results. They select their sample of events from the Factiva[17] database, searching for newspaper reports of global cyberattacks between 1995 and 2015 with the use of specific keywords. The daily stock market prices are obtained from the Thomson Reuters DataStream database, which as already seen (Colivicchi & Vignaroli, 2019) provides adjusted for dividends and splits. The final sample of events includes 226 cyber-attacks affecting 110 firms. Of these 226 security breaches, 67 affected 34 financial entities. The Finance and Insurance sector announced 67 cyber-attacks, equal to 29,6% of the total sample. In particular financial companies registered over 41% of these events in the period between 2013 and 2015: the authors note that cybersecurity is becoming an increasingly important issue in recent years, even more so when considering the financial field. Focusing on the whole sample of cyber-attacks Arcuri et al. find that the average cumulative abnormal returns are negative in all event windows, showing that cyberattack announcements nearly always lead to negative market returns for a company. Furthermore, the extent of these negative market returns and their statistical significance varies according to the event windows. In particular, results in the

[17] Factiva is a comprehensive global news and business information database. It is a product of Dow Jones & Company, a subsidiary of News Corp. Factiva provides access to a vast collection of news articles and business information from around the world by aggregating content from thousands of newspapers, magazines, journals, newswires, and other publications.

symmetric event windows after the announcement show a high statistical significance, at the 90% confidence level or above. The event windows (-5,5) and (-3,3) show mean Cumulative Abnormal Returns of -1,26% and -1,19% respectively. This means that significant negative market returns occur on days both preceding and following the announcement of the information security breaches. These results imply that cybercriminals could be implicated in insider trading, in accordance with Colivicchi & Vignaroli (2019). The authors note that insider threats such as fraud, theft of confidential information and intellectual property and the sabotage of computer systems coming from people within the organization, are in fact one of the most prevalent types of cyberthreats. Furthermore, the point out that, in the age of globalization, sometimes, it is hard to pinpoint the first release date of an information security breach. Negative market returns also occur when considering non symmetrical event windows, but at low statistical significance. Most importantly the researchers classify the sample according to the economic sector of the firms. In particular, they analyze the potential differences between the financial sector and the other ones. The reasoning behind this subdivision is that, according to the authors, the financial sector is one of the industries that are most at risk, given the nature of the data that it holds, and for this reason a different behavior in the returns of the shares could be observed. It is found that, in general, financial entities show a greater negative effect in the event windows before the cyber-attack announcements, meaning when only the returns in the days that precede the announcement are considered. Arcuri et. al further apply another important subdivision of the sample: they divide cyber incidents in two categories based on the disclosure of confidential information or the lack of suck a disclosure. These categories of security breaches are called confidential and non-confidential attacks. In the case of confidential attacks announced by financial entities the authors interestingly find no statistically significant results. Conversely, non-confidential attacks announced by financial entities appear to generate greater negative market returns than confidential attacks. The most significant results were found in the symmetric event windows (-10,10), (-5,5) and (-3,3): this could be interpreted as a result in favor of the existence of insider trading, when dealing with cyberattacks to financial firms. In synthesis, non-confidential attacks in the financial system are found to be more dangerous than confidential attacks. As a possible explanation the researchers point out that, in the financial industry, confidential attack announcements are likely to be predicted by investors because unauthorized access to confidential information is a big concern, and word of mouth is likely to spread fast. Another possible explanation that is given refers to a potential inefficiency of stock markets when dealing with cyberattacks: when cyber-attacks do not concern access to confidential information the negative consequences connected with the attack could be easier to determine by the perspective of investors. As a final interpretation for this seemingly paradoxical finding, Arcuri et al. note that it may be the case that investors perceive financial entities damaged by non-confidential attacks as being more vulnerable. In fact, failure by financial companies to safeguard their own systems and networks could be viewed in a more negative light than failure to protect data. We see once more (Colivicchi & Vignaroli, 2019) how companies in the financial industry face a larger number of threats than companies in other industries.

The final paper that we will mention has been developed by Gatzlaff & McCullough (2010). The study analyzes data breaches in particular. The sample of breaches is compiled by combining searches of the LexisNexis database from January 1, 2004 to December 31, 2006 with a list compiled by the Privacy Rights Clearinghouse[18]. In such a way the authors compile a final list of 77 events, 28 of which have as a target a company operating in the financial sector. Overall, Gatzlaff & McCullough find that the impact of a data breach on shareholder wealth is negative and statistically significant at the 1% level. The mean CAR for all 77 data breach events over the event window (0,1) is −0,84%. Results from the Patell Z-test indicate that the effect persists with varying significance out to 40 days, after which market values appear to return to prebreach levels. Most importantly for our research, the authors conduct a cross-sectional analysis of all the cumulative abnormal returns that they estimated. They then regress these CARs on multiple independent variables, two of which are of our interest in particular: one independent variable (FINANCIAL) assumes the value of 1 if the CAR is measured on the stock of a financial company, another independent variable (INSURANCE) behaves in the same way but for insurance companies. The coefficients for both of these regressors are insignificant when considering a t-test at the 1% level. The authors do not go into depth about this finding and the possible explanations for it.

3.3.1 Event studies on systemic events

Given that our study aims to understand the effects of potential systemic event, which could affect the entirety of the financial system, it is worthwhile exploring in detail some of event studies of the existing literature which have dealt with such events. It is very important to note that no existing research has specifically dealt with systemic events pertaining to cybersecurity and their effect on the financial sector: this means that once again our paper has the role of filling a gap in the literature. Even more so no existing research has dealt with globally relevant cybersecurity incidents and their specific effect on European financial institutions. Event

[18] The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer information and advocacy organization based in the United States. The PRC is known for maintaining a comprehensive and accessible database of information related to privacy breaches, identity theft, and other privacy-related issues.

studies of this type have dealt with events such as: wars (Furdui & Șfabu, 2023; Yousaf, et al., 2022) terrorist attacks (Liargovas & Repousis, 2010; Kollias, et al., 2011; Obi, 2007), financial reforms (Hoesli, et al., 2020; Loipersberger, 2018), banking crises (Repousis, 2016) and pandemics (Pandey & Kumari, 2021). Global cyberevents have also been analyzed (Roškot, et al., 2021), but once again not through the specific lens of financial institutions.

Both of the cited studies regarding war study the impact of the outbreak of the Russo-Ukrainian war[19]. Yousaf et. al examine the impact of this event on the stock exchanges of the G20 and other selected stock markets using the event study approach. While this study is not of particular interest for the present dissertation, the other study regarding this event is especially relevant. Furdui & Șfabu conduct an event study on 32 systemically important banks in 12 developed European countries, for the period from the 19th of May 2021, to the 30th of March 2022. The daily closing prices of each bank are extracted from the Yahoo Finance website. The authors show that all of the institutions in the sample manifest significant negative cumulative abnormal returns during the analyzed period. Furthermore, the country-level analysis shows a different reaction of these banks depending on their exposure to Russia, the dependence of their respective countries on Russian gas and oil, and the level of informational efficiency of the markets in which they are traded. The results indicate that investors penalize banks with very high exposure to Russia, followed by those whose countries depend to a significant extent on Russian gas and oil. Interestingly, the study does not suggest that geographic distance has a significant impact on the observed abnormal returns.

Passing onto the studies dealing with terrorist attacks, Liargovas & Repousis investigate the reaction of 14 Greek banks' stocks to three major international terrorist events: the 9/11 attacks in New York, the Madrid train bombing of 2004[20] and the London train bombing of July 2005[21]. The authors find that, of the three terrorist attacks, only September 11th resulted in significant negative abnormal returns in the Greek bank stocks. According to the researchers several reasons may be responsible for these results but September 11th was more catastrophic probably due to the dominant position of US economy worldwide. This result is important to keep in mind as we also study an event that happened in the US.

[19] The Russian invasion of Ukraine began on the morning of 24 February 2022, when Putin announced a "special military operation" to "demilitarize and denazify" Ukraine.

[20] The Madrid bombings of 2004 occurred on March 11 when multiple train explosions targeted commuter trains. The attacks were carried out by Islamist extremists and were a response to Spain's involvement in the Iraq War.

[21] The London train bombings of 2005, occurred on July 7 when suicide bombers targeted three London Underground trains and a bus. The coordinated attacks were carried out by Islamist extremists.

Kollias et al. investigate the effects of two terrorist incidents, the already mentioned bombed attacks of Madrid and London, on equity sectors. For the purpose of this analysis the daily prices of the three major stock exchanges in Spain (Madrid, Valencia, and Barcelona) and the London Stock Exchange are used. The empirical findings point to a similar reaction on the event day but a significantly different recovery in terms of days needed for the markets to rebound: in particular the London stock exchange seemingly recovers in a single trading day. Kollias et al. put forward a series of tentative explanations to explain this difference including the size, structure and liquidity of the markets involved. A further possible explanatory factor, according to the authors, is the fact that the terrorist cell responsible for the bombings in Madrid was neutralized a few days later thus, in a sense, it continued to present a potential security threat for a short period of time. In contrast, this was not the case for the London terrorists since they were suicide bombers Despite these findings, the dominant conclusion of the research is that the overall net impact on the stock markets in both cases was only transitory. The study also presents the specific results for the banking and finance sector of each of the two countries: there seems to be no significant difference in their reaction when compared to other sectors of the economy.

In 2007 Obi analyzes the financial impact of the 9/11 attacks: in particular he does so, among other firms, on 47 financial services companies headquartered in the USA and Europe. The portfolio of financial firms, after the estimation, presents negative cumulative abnormal returns, but these results are not significant.

Two of these event studies dealing with systemic events analyze the impact of financial reforms. Starting with Hoesli et al., their research focuses on three major European reforms: the first is Basel III, which targets banks and thus potentially changes the availability of credit for firms; the second one is the European Market Infrastructure Regulation (EMIR), which is aimed at derivative trading and impacts the cost of debt for European firms; the final one is the Alternative Investment Fund Management Directive (AIFMD), which could increase compliance costs for funds and reduce their potential investor pool. The effects of these three major events in are studied on the daily stock prices of real estate companies sourced from Thomson DataStream. The 15 countries of the sample include France, Germany and the U.K., as they have the largest listed real estate markets. The main point of interest for us in this research is the way the authors decide to study the three events, even if this specific approach is not going to be employed in our discussion. In order to measure the regulatory impacts, they look at announcements associated with regulatory changes. This approach goes in direct contrast with only considering a single event date for each of the three reforms. The authors pursue this path to account for the fact that the majority of the regulatory events do not involve a single well-defined announcement. Large regulations such as Basel III in fact rather involve a series of smaller announcements which can gradually affect listed real estate companies. Hoesli et al. search for the smaller events on the paper edition of the Financial Times (FT) UK and FT Europe: they find 12 relevant news regarding Basel III, 6 relative to AIFMD, and 4 to EMIR. This approach could reveal useful even in the context of worldwide large-scale cyberattacks that involve multiple phases: an example is represented by the theft of funds from the Bangladeshi Central Bank in 2016 (Ferbrache, 2016), that we chose not to analyze as it doesn't involve a clear event date. This attack started at the beginning of February, but the first public announcements were only released in March, meanwhile some informational leaks most likely occurred.

Loipersberger in 2018, investigates how the introduction of the Single Supervisory Mechanism, the European Union's implementation of harmonized banking supervision, has affected the banking sector in Europe. Once again, the event is so complex that the author decides to divide it into four smaller sub-events, which reflect the development and coming into force of the SSM. The event study is performed on the stock returns of 88 banks of the Euro Area. Evidence for small but significant positive effect is found. This study is of our interest because it deals with banks exclusively headquartered in the Euro Area. Furthermore, these banks are studied in the light of four systemic events.

In 2016 Repousis examined the impact of the Cypriot banking on three banks: Bank of Cyprus, Cyprus Popular Bank and Piraeus Bank. Thanks to the conduction of an event study the author estimates the abnormal stock returns during the ten-day period before the event date, corresponding to the announcement of prohibition and put under suspension trading of all movable securities of Bank of Cyprus and Cyprus Popular Bank. The results show that, regarding Piraeus Bank's shares, during the 10 days before the event there were negative but not statistically significant CARs at the 5% confidence level. On the other hand, the shares of Cyprus Popular Bank exhibited positive but not statistically significant CARs at 5% confidence level during the 10 days before the event. The Bank of Cyprus stocks also showed highly positive CARs for all time periods but not statistically significant at the 5% confidence level. This study could be useful even if the results are not significant: in the context of a banking crisis there doesn't seem to be a significant reaction in the days preceding the event, thus the event windows should mostly focus on day that follow the event.

While the event study on Covid-19 by Pandey and Kumari (2019) does not require our specific attention, as it focuses on stock indexes reactions and doesn't go into detail about the financial sector, the one by Roškot et al. (2021) deserves further analysis. The authors estimate the effect of two major cyberattacks on multiple financial markets at the international level. One of the two major cyberevents is the Peya attack[22], which is not part of our paper. On the other hand, the WannaCry attack is one of the three systemic events considered in our study. Roškot et al. evaluate the effect of large scale attacks on the following European indexes: CAC 40 Paris, DAX Frankfurt, OMXC 20 Copenhagen, LSE London, MICEX Moscow and IBEX 35 Madrid. To evaluate the performance of antivirus companies, the NASDAQ index was also included. The estimations yield results that are abnormal when compared to the conclusions of the other studies in the literature: as we have already seen, the prevailing opinion regarding the impact of cyber-attacks is that public announcements of cyber-security breaches lead to negative stock returns. These authors instead find empirical evidence of positive investor reactions to the announcements of cyber-attacks. Specifically, there is an overall slightly positive impact of WannaCry ransomware attack on market returns. The analysis of the impact of the more aggressive Petya attack, aimed at destroying affected data, also provides evidence that the security breach led to increased market returns. As an explanation for these strange findings the authors propose that, when a company announces that it has been successfully breached, investors perceive this acknowledgement as a positive signal and a first step toward preventing future vulnerabilities. In our view the results are partly flawed in the fact that they are too general. Many companies that are direct competitors of the firms that have been more heavily hit by the cyberattacks were necessarily part of the estimations as the authors choose to base their study on stock indexes. Moreover, the authors do not properly divide their results into ones including the NASDAQ index and ones that do not include such index. As previously indicated, the NASDAQ necessarily reflects the reactions of cybersecurity providers, which have been shown to be significantly positive in the literature (El Ghoul, et al., 2022).

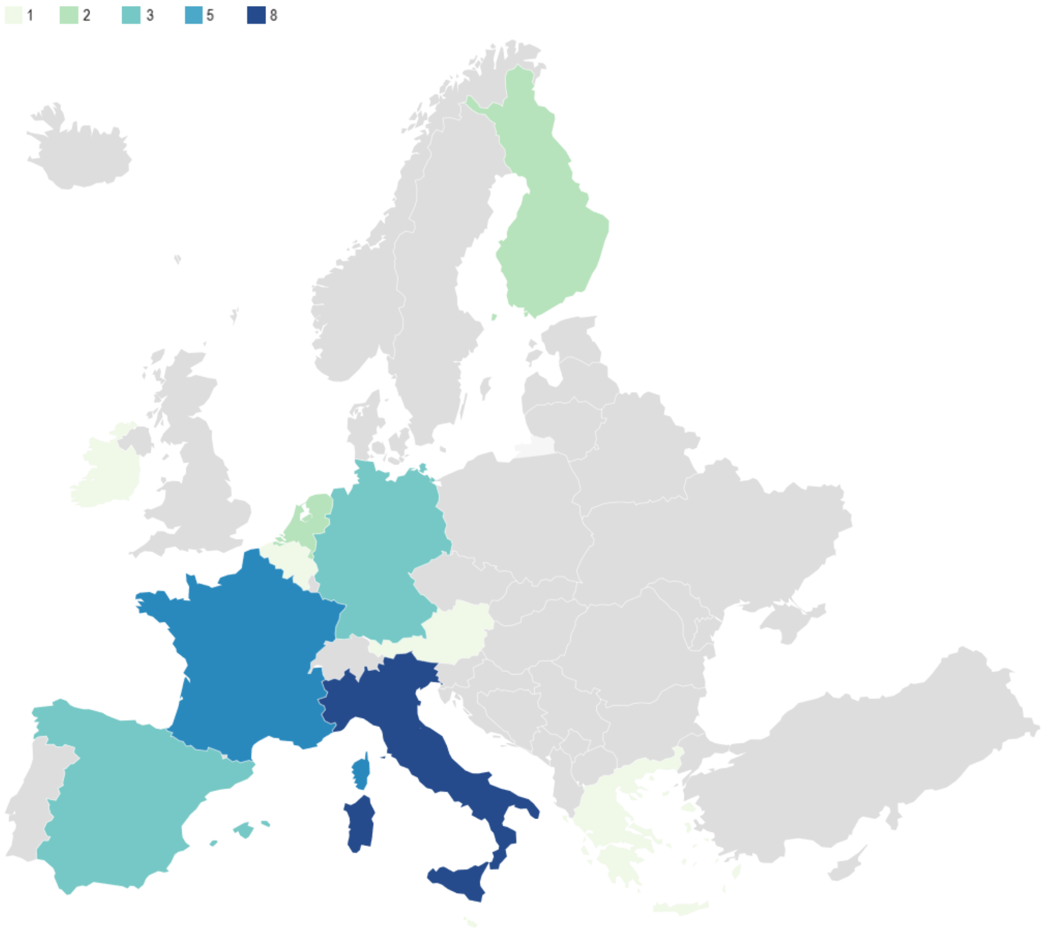
[22] Petya is a ransomware attack that encrypts a computer's master boot record (MBR), rendering the system unusable. Emerging in 2016, it has evolved to encrypt MBR, making it more destructive than traditional ransomware. Attackers demand a cryptocurrency ransom for a decryption key, but payment doesn't guarantee data recovery.

4. DATA

As mentioned, our research focuses on two types of events. The first category of events includes all the cyberattacks that are directly aimed at one or more financial institutions in the Eurozone. A cyberattack is considered as directly aimed to a European financial institution if the news articles reporting on that attack explicitly mention the recipients of said attack. The recipients can be multiple as well as a single one. Given the nature of the event study methodology, naturally only events that explicitly targeted listed companies have been included in the final list. If we consider El Ghoul et al.'s (2022) analysis in section 3.1, this first category comprises both firm-level events and peer-level events. We could also interpret every one of these instances as a firm-level event, some of which happen to occur to their respective targets at the same time. The second category of events refers to those events that could potentially have worldwide repercussions. Consider as an example a cyberattack involving the exploit of a vulnerability of software that is used by banks worldwide. Given this characteristic, such events could have some level of impact on the whole European financial network, even if the specific target of the attack isn't a European financial institution. Once again, when looking at section 3.1, this second category of events corresponds to the peer-level event type. The events part of this second category could also be considered as country-level events, if we allow for the Eurozone being considered as a single political entity.

It is important to point out that the companies studied in systemic events are in part different from the ones hit by direct events. For the systemic events an ad hoc sample has been created to adequately represent the most important economies of the Eurozone, further detail will be given in the two following sections. For now, Figure 5 summarizes the geographical distribution of all the firms involved in the study. The daily stock prices of all the companies have all been extracted from the *Yahoo Finance* website (Yahoo, 2023). This same database provides the daily value of the stock index used in the study: its use will be explained in the following chapter on methodology. On its website, in the Historical Data section for every company, Yahoo not only provides daily closing prices, but also *adjusted closing prices*. These values are adjusted for the following stock events: stock splits, dividends and capital gain distributions. In our estimation we use these adjusted prices to focus on the effect of the events themselves (Arcuri, et al., 2018; Furdui & Șfabu, 2023).

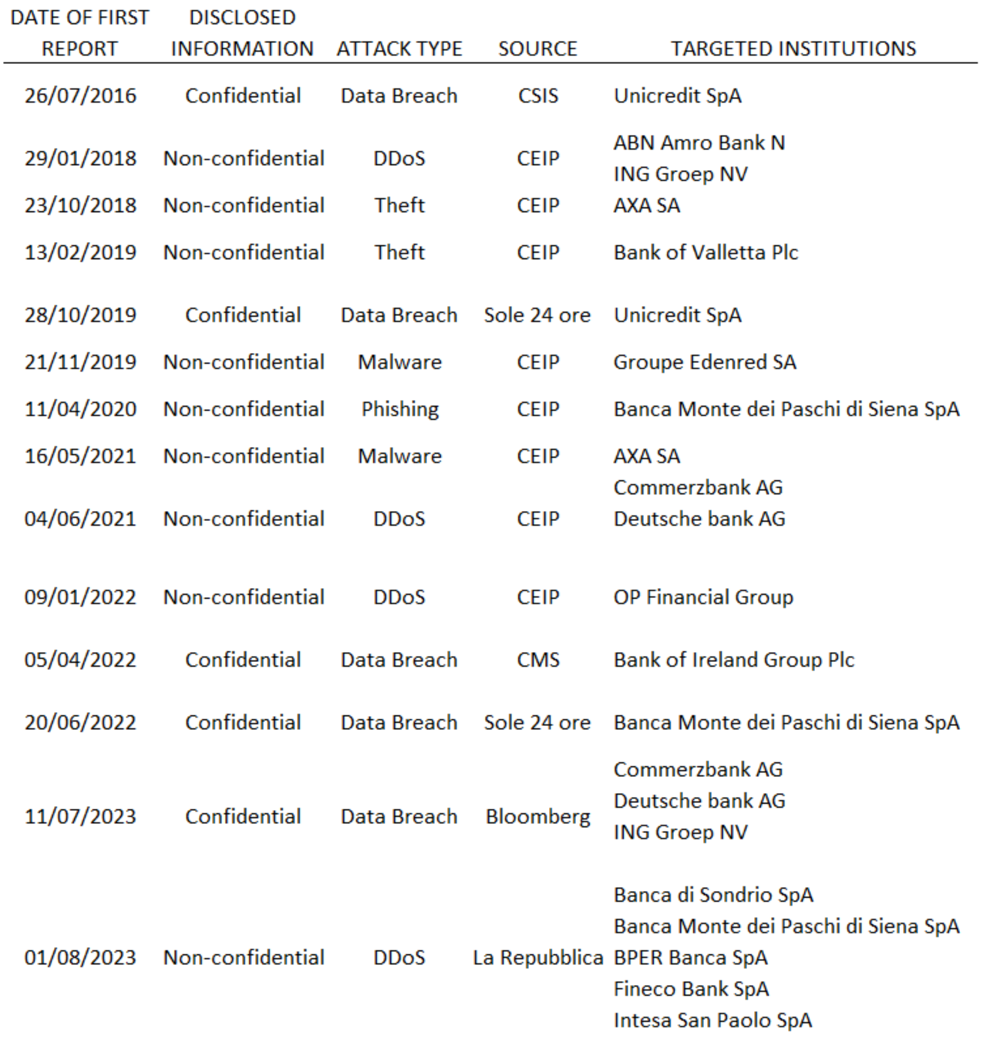
Figure 5: Map of all the financial institutions of the study by country.



4.1 Direct events

Table 2 serves as a summary for the 14 direct cyber events that we selected. The date of first report represents the date in which the first online news article, referring to that specific event, has been published. The attacks are then categorized on the basis of their type and the disclosure of confidential information by the involved hackers. For each cyber incident the targeted financial institutions are listed inside the rightmost column. The greater part of these events has been selected on the website provided by the Carnegie Endowment for International Peace: the website, namely *Timeline of Cyber Incidents Involving Financial Institutions*, chronicles around 200 cyber incidents that have targeted financial institutions worldwide starting from 2007. This database was filtered for cybersecurity incidents which had for a target financial institution of the Eurozone. The remaining part of the 14 events was obtained thanks to the use of a combination of other resources. In particular the Center for Strategic and International Studies regularly updates the *Significant Cyber Incidents* webpage: this timeline records significant cyber incidents since 2006, focusing on cyber-attacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars.

Table 2: Direct cyber events summary.



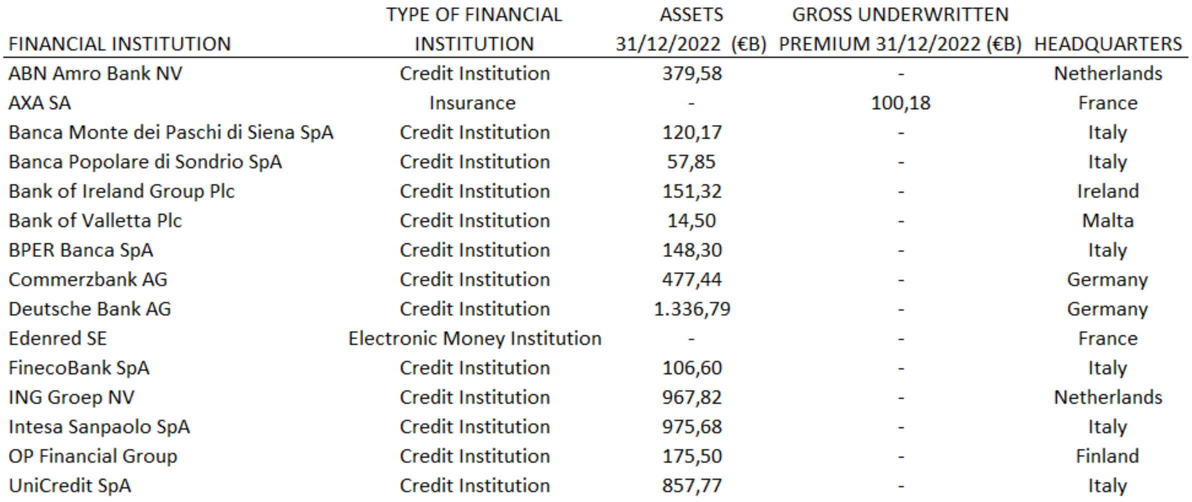
DATE OF FIRST REPORT	DISCLOSED INFORMATION	ATTACK TYPE	SOURCE	TARGETED INSTITUTIONS
26/07/2016	Confidential	Data Breach	CSIS	Unicredit SpA
29/01/2018	Non-confidential	DDoS	CEIP	ABN Amro Bank N ING Groep NV
23/10/2018	Non-confidential	Theft	CEIP	AXA SA
13/02/2019	Non-confidential	Theft	CEIP	Bank of Valletta Plc
28/10/2019	Confidential	Data Breach	Sole 24 ore	Unicredit SpA
21/11/2019	Non-confidential	Malware	CEIP	Groupe Edenred SA
11/04/2020	Non-confidential	Phishing	CEIP	Banca Monte dei Paschi di Siena SpA
16/05/2021	Non-confidential	Malware	CEIP	AXA SA
04/06/2021	Non-confidential	DDoS	CEIP	Commerzbank AG Deutsche bank AG
09/01/2022	Non-confidential	DDoS	CEIP	OP Financial Group
05/04/2022	Confidential	Data Breach	CMS	Bank of Ireland Group Plc
20/06/2022	Confidential	Data Breach	Sole 24 ore	Banca Monte dei Paschi di Siena SpA
11/07/2023	Confidential	Data Breach	Bloomberg	Commerzbank AG Deutsche bank AG ING Groep NV
01/08/2023	Non-confidential	DDoS	La Repubblica	Banca di Sondrio SpA Banca Monte dei Paschi di Siena SpA BPER Banca SpA Fineco Bank SpA Intesa San Paolo SpA

The CMS, an international law firm, regularly updated an online database, the *GDPR Enforcement Tracker*: here one relevant event about the Bank of Ireland was found. The last source, for events that specifically targeted European companies, consisted in a web search containing the following keywords: “data breach”, “cyberattack”, “security breach”, “denial of service attack” and “hacker”; in combination with “Europe”, “European bank”, “European financial institutions”. News relevant for the study were found on the websites of Bloomberg, La Repubblica and Il Sole 24 Ore[23].

The details of each targeted institution can be found in Table 3 below. The specifics of each attack and the relevant news articles can be found instead in Appendix A.

[23] A web search was also conducted with the use of the Italian translation of some of the listed keywords.

Table 3: Financial institutions involved in direct attacks.



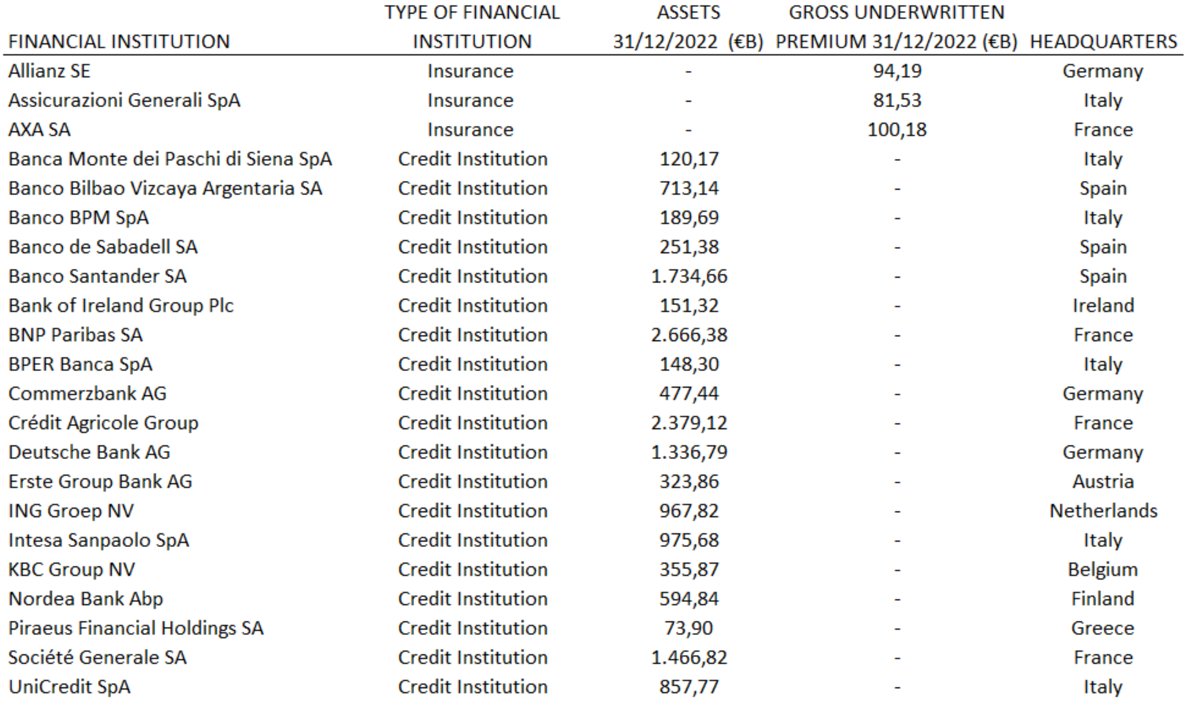
FINANCIAL INSTITUTION	TYPE OF FINANCIAL INSTITUTION	ASSETS 31/12/2022 (€B)	GROSS UNDERWRITTEN PREMIUM 31/12/2022 (€B)	HEADQUARTERS
ABN Amro Bank NV	Credit Institution	379,58	-	Netherlands
AXA SA	Insurance	-	100,18	France
Banca Monte dei Paschi di Siena SpA	Credit Institution	120,17	-	Italy
Banca Popolare di Sondrio SpA	Credit Institution	57,85	-	Italy
Bank of Ireland Group Plc	Credit Institution	151,32	-	Ireland
Bank of Valletta Plc	Credit Institution	14,50	-	Malta
BPER Banca SpA	Credit Institution	148,30	-	Italy
Commerzbank AG	Credit Institution	477,44	-	Germany
Deutsche Bank AG	Credit Institution	1.336,79	-	Germany
Edenred SE	Electronic Money Institution	-	-	France
FinecoBank SpA	Credit Institution	106,60	-	Italy
ING Groep NV	Credit Institution	967,82	-	Netherlands
Intesa Sanpaolo SpA	Credit Institution	975,68	-	Italy
OP Financial Group	Credit Institution	175,50	-	Finland
UniCredit SpA	Credit Institution	857,77	-	Italy

4.2 Systemic events

In the previous section, the financial institutions that are considered in the event study on direct events have already been listed. As anticipated, when dealing with systematic events a particular approach was chosen. Instead of simply evaluating the effects of events with worldwide repercussions on the companies involved in direct events, a new sample was specifically created. This roster only contains two types financial institutions: banks and insurance companies. The former type comprises the majority of the sample, in line with the prevalence of credit institutions in the overall number of European financial institutions (Statista Research Department, 2023).

The banks selected for such a purpose were chosen on the basis of two main criteria. The first criterium consists in the overall economic relevance of the institution. In particular, the amount of assets listed in the banks' balance sheet was identified as a proper indicator for this characteristic. The data regarding the assets marked on the banks' balance sheets was retrieved form S&P Global's Report, which captures a snapshot on the 31st of December 2022 for Europe's 50 largest banks (Mones & Taqi, 2023). The second criterium is that of proper geographical representation of the Eurozone's countries: while two years ago Germany, France and Italy represented 53,26% of the European Union's GDP (McEvoy, 2022), it's nevertheless important to give representation for at least part of the other countries comprising the Eurozone. These two principles resulted in the identification of 19 banks and 3 insurance undertakings . The 3 insurance companies were selected on the basis two similar criteria, although the first of them is partly modified. In order to measure the economic prowess of an insurance company, gross underwritten premium[24], instead of assets in the balance sheet, is chosen as the proper metric.

Table 4: Sample of financial institutions for systemic attacks.



FINANCIAL INSTITUTION	TYPE OF FINANCIAL INSTITUTION	ASSETS 31/12/2022 (€B)	GROSS UNDERWRITTEN PREMIUM 31/12/2022 (€B)	HEADQUARTERS
Allianz SE	Insurance	-	94,19	Germany
Assicurazioni Generali SpA	Insurance	-	81,53	Italy
AXA SA	Insurance	-	100,18	France
Banca Monte dei Paschi di Siena SpA	Credit Institution	120,17	-	Italy
Banco Bilbao Vizcaya Argentaria SA	Credit Institution	713,14	-	Spain
Banco BPM SpA	Credit Institution	189,69	-	Italy
Banco de Sabadell SA	Credit Institution	251,38	-	Spain
Banco Santander SA	Credit Institution	1.734,66	-	Spain
Bank of Ireland Group Plc	Credit Institution	151,32	-	Ireland
BNP Paribas SA	Credit Institution	2.666,38	-	France
BPER Banca SpA	Credit Institution	148,30	-	Italy
Commerzbank AG	Credit Institution	477,44	-	Germany
Crédit Agricole Group	Credit Institution	2.379,12	-	France
Deutsche Bank AG	Credit Institution	1.336,79	-	Germany
Erste Group Bank AG	Credit Institution	323,86	-	Austria
ING Groep NV	Credit Institution	967,82	-	Netherlands
Intesa Sanpaolo SpA	Credit Institution	975,68	-	Italy
KBC Group NV	Credit Institution	355,87	-	Belgium
Nordea Bank Abp	Credit Institution	594,84	-	Finland
Piraeus Financial Holdings SA	Credit Institution	73,90	-	Greece
Société Generale SA	Credit Institution	1.466,82	-	France
UniCredit SpA	Credit Institution	857,77	-	Italy

The selected insurances represent the top three companies of their kind, measured on gross written premium, when considering the European Union (Steve Evans Ltd, 2021). Furthermore, each one of them is headquartered in one of the top three EU's economies cited above. All of the companies part of this sample also respect a third criterium, namely their share must be publicly traded. Country-wise 6 of the institutions of the above sample are headquartered in Italy, 4 in France, 3 in Germany and Spain. The remaining ones are based in Austria, Belgium, Finland, Greece and Ireland. Moreover, some of the institutions of the sample are also considered in direct events, so the two samples are partially overlapping.

The same resources used for the identification of direct events were also used for sourcing three major cybersecurity events with potential worldwide repercussions. In this case the events were not filtered on the basis of their exclusive targetization of European institutions. The three events have instead been selected on the basis of their presence in the majority of established international newspapers. For the specific purposes of this study, these events have been also selected in such a way to account for three completely different types of cyber incidents. The

[24] Gross Underwritten Premium is the total amount of money collected by an insurance company from policyholders for insurance coverage within a specific period. It represents the total premiums before deducting any reinsurance or refunds. Essentially, it's the initial revenue generated from selling insurance policies.

first one is about the breach of information held by a major US bank, the second one deals with a malware epidemic and the third one is about the exploit of a TPP (Third Party Provider) of software solution for governments and companies worldwide. In the following segments we explain in detail the dynamics of each of these cyberattacks.

4.2.1 JP Morgan's 2014 data breach

The 2014 JPMorgan Chase data breach was a cyberattack against the American bank JPMorgan Chase that is believed to have compromised data associated with over 83 million accounts, corresponding to approximately two out of three households in the country, and 7 million small businesses. This data breach is considered one of the most serious intrusions into an American corporation's information system and one of the largest data breaches in history (The Guardian, 2014).

The attack came to the public's attention for the first time the 27th of August 2014. On this date it was first revealed (CNBC, 2014; The New York Times, 2014) that the hackers infiltrated the networks of the JP Morgan, as well as other undisclosed banks, and siphoned off gigabytes of data, including checking and savings account information, in what security experts described as a sophisticated cyber-attack. As the news came out on the 27th of August in the later hours of the day, when all European stock markets were already closed, we conduct our event study for European institutions on the 28th. The details and full extent of the attack were only revealed to the public at a much later date. Newspapers first reported the number of breached accounts and banks on the 2nd of October of the same year (The New York Times, 2014). In particular it was disclosed that the attack was discovered by the JP Morgan's security team in late July 2014, but not completely halted until the middle of August. In the end, as anticipated, the hackers managed to compromise the accounts of 76 million households and 7 million small businesses. Nine other banks were also hit during the attack. As this tally greatly surpassed the previous estimates by the public, we also conduct an event study on the 3rd of October. The delay in the date with respect to the announcement by US paper is due to the same reason as before.

We chose this event as it is prominently reported by both US and European sources (Corriere della Sera, 2014). In addition, there is a consensus that this attack represents one of the most serious information security breaches suffered by an American corporation, even more so a financial one. Our consideration of the two dates, corresponding to the initial announcement of the attack and the reveal of its success, could allow us to assess the breach's effects at a deeper level.

4.2.2 The 2017 WannaCry ransomware epidemic

The WannaCry ransomware attack was a worldwide cyberattack, started in May 2017, by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency (Kasperky, 2017). It propagated by using *EternalBlue*, an exploit developed by the United States National Security Agency (NSA) for Windows systems (Symantec, 2017). EternalBlue was stolen and leaked by a group called *The Shadow Brokers* a month prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. These patches were imperative to cyber security, but many organizations did not duly apply them, in view of the risk of formerly working applications being disrupted, or a lack of personnel or time to install them.

The attack began, and was immediately announced by newspapers, on the morning of the 12th of May 2017 (Forbes, 2017; The Guardian, 2017). The extent of WannaCry's propagation and its damages were not fully known the day in which the spread began. Nevertheless, we conduct an event study on the day of its first announcement. The longer event windows could help us assess whether the impact, if any, of the attack on our sample of stocks had increased with time. A posteriori the attack is recognized as having affected more than 300,000 computers across 150 countries (NPR, 2022). By June 14, 2017, a total of 131 million dollars had been transferred to a publicly available online Bitcoin wallet checker (Roškot, et al., 2021). Beyond the actual ransom paid, the economic costs of WannaCry included business interruptions as well as replacement of infrastructure and repairs. Cyence, a risk-modeling firm, estimated the global economic cost of the attack to be $6 billion (The Independent, 2017).

We include this event in our study as it is also analyzed by Roškot et al. (2021). In addition, it is recognized as the most serious epidemic of a ransomware virus in history.

4.2.3 The 2020 United States federal government data breach

In 2020, a major cyberattack penetrated thousands of organizations globally, including multiple parts of the United States federal government, leading to a series of data breaches. The cyberattack and data breaches were reported to be among the worst cyber-espionage incidents ever suffered by the US, due to the sensitivity and high profile of the targets and the long duration, from eight to nine months, in which the hackers had access to the vulnerable systems (The New York Times, 2020). Within days of its discovery, at least 200 organizations around the world had been reported to be affected by the attack, and some of these may also have suffered data breaches (Bloomberg, 2020).

The cyberattack that led to the breaches began no later than March 2020. The attackers exploited software or credentials from at least three U.S. firms (Huddleston, et al., 2021): Microsoft, SolarWinds, and VMware. A supply chain attack on Microsoft cloud services provided one way for the attackers to breach their victims, depending upon whether the victims had bought those services through a reseller. A supply chain attack on SolarWinds's Orion software, widely used in government and industry, provided the main avenue, if the victim used that software. Flaws in Microsoft and VMware products allowed the attackers to access emails and other documents. The attack, gone undetected for months, was first publicly reported on the 13th of December 2020 (Reuters, 2020) and was initially only known to have affected the U.S. Treasury Department and the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce (The Financial Times, 2020). In the following days, more departments and private organizations reported breaches. We conduct our event study on the 14th of December, given the fact that the 13th was a Sunday. Moreover, the larger event windows which comprise the days after the attack, should give us the ability to assess if the announcement of the exploit and its evolutions had an effect on stock prices. It is relevant to note that in addition to the theft of data, the attack caused costly inconvenience to tens of thousands of SolarWinds customers, who had to invest their resources into checking whether they had been breached or not. In particular at the time of the announcement SolarWinds confirmed that of its 300.000 customers, 33.000 used Orion, with around 18.000 government and private users who actually downloaded compromised versions (The New York Times, 2020).

We selected this event among our three systemic ones as it represents an historical security breach when it comes to governmental bodies. Therefore, we can assess how financial institutions in the Eurozone reacted to this breach suffered by the US government, keeping in mind that the tools used for the breaches were virtually applicable to European firms too.

5. METHODOLOGY

5.1 Development of the hypotheses

It is useful to formalize the hypotheses that we aim to verify with the use of the event study methodology. Furthermore, it is relevant to describe how and why such hypotheses were formulated in the first place. Thes study analyzes both direct and systemic events: for this reason, the first two hypotheses are about direct events, while the other two concern systemic events.

Intuitively, and according to the literature (El Ghoul, et al., 2022; Spanos & Angelis, 2016), the main objective of any study of this type is assessing whether the public announcement of a cyberattack has an effect on the targeted firms. For this reason, the first hypothesis deals with direct events, meaning events that are explicitly directed towards one or multiple financial institutions: the objective is to find if these cyberattacks have any significant negative effect. The second hypothesis deals with the confidentiality of the information that is stolen or leaked as a consequence of a direct cyberattack. In the literature that has been analyzed, we have seen in particular how Arcuri et al. (2018), Campbell et al. (2003) and finally Gordon et al. (2011) have empirically confronted the effects of so called confidential and non-confidential attacks. The sample of the direct events that has been selected for our paper allows for their distinction into confidential and non-confidential breaches: such a division has been possible through the in-depth analysis of each of the news articles associated with each event, detailed in Appendix B. Thus, this third hypothesis aims to add a further empirical conclusion to the previous ones present in the literature. In particular it is useful to remember that according to Campbell et al. confidential attacks have a negative and significant effect on the shares of the breached companies, while non-confidential attacks have negative but non-significant effects. Conversely, the research by Arcuri et al. find that, while confidential attacks have a negative but non-significant effect on stocks, non-confidential events have on average greater negative effects, which are mostly significant. Similarly, Gordon et al. discover that non-confidential security breaches, involving information availability, have a significant negative effect on stocks. On the other hand, attacks that involve information confidentiality are found to have no significant negative effect on the shares of the targeted companies.

The third hypothesis is similar to the first one but deals with systemic events. As we have seen, the effect of a major event has already been studied in the literature on the entirety of a sample

(Furdui & Șfabu, 2023; Pandey & Kumari, 2021; Roškot, et al., 2021). We find it important to highlight once more the fact that this paper, to the best of our knowledge, is the first one in the literature that employs the event study methodology to study the effect of a major cybersecurity event on a sample of European financial institutions. This hypothesis also has the objective of testing the investors' perceived interconnectedness of the European financial system, both internally and externally. In the case of a major cybersecurity event, such as the already mentioned WannaCry attack, that has directly affected a number of European countries, the observation of negative significant abnormal returns for financial companies headquartered in countries that have not been heavily hit would signify that the markets view the European financial system as an highly interconnected one: if, for example, Spain and its major financial corporations were severely hit by a cyberattack, and Italian financial firms showed significant negative returns, it would mean that investors think that the spread of the cyberattack through the interconnected IT systems of such firms is very likely. One of the major cyber events that is analyzed did not target European countries of firms, it was instead directed towards a major US bank: this means that we will be able to assess if the European financial system is perceived by investors as externally connected with the financial system of the USA.

The fourth hypothesis aims to go into more depth about these systemic events. In particular it serves the purpose of assessing if certain countries of the Eurozone react more negatively in the case of a major cyberevent. In the case of the hypothetical scenario presented above about the WannaCry attacks hitting the Spanish economy in particular, this hypothesis would have the role of showing which of the other European countries reacts more negatively to such a cyberattack.

Here are the four hypotheses, formally expressed in their null-forms:

- H_0^I: *the share price of a financial institution is not significantly affected by a direct cyberattack.*
- H_0^{II}: *in case of a direct cyberattack, confidential and non-confidential attacks have the same effect.*
- H_0^{III}: *the share price of a financial institution is not significantly affected by systemic cyberattacks.*
- H_0^{IV}: *in case of systemic attacks, financial institutions do not react differently with respect to the country in which they are based.*

5.2 The ESM in detail

The evet studies in this paper are conducted with the use of the *estudy* command in Stata. We followed the indications given by Pacicco et al. in both their 2018 and 2021 entries in *The Stata Journal*. In particular the second paper deals with an update to the command which allows for the calculation of stocks' reactions for different event dates: this is relevant for the direct events that we will analyze. The commands used for each of our event studies can be found in Appendix A.

The event study methodology has already been discussed on a descriptive level in chapter 3. We now explore the specifics of this method. As anticipated, an event study requires the calculation of Abnormal Returns. An abnormal return, from now on also referred to as AR, is the actual ex post return of the security over the event window, minus the normal return of the firm over the event window. The AR of a generic firm i in the period t is thus defined as:

$$AR_{i,t} = R_{i,t} - E(R_{i,t}|X_t)$$

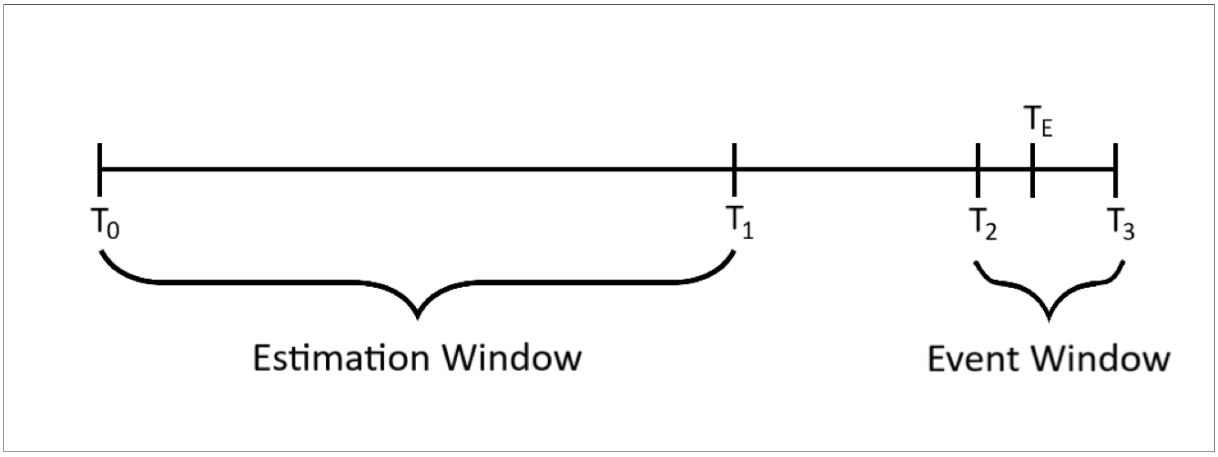
Where $R_{i,t}$is the actual ex post return and $E(R_{i,t}|X_t)$ is the expected return conditioned to the information X of period t, unrelated to the event. In order to estimate these abnormal returns, and the also test their significance, we have to follow the route indicated by MacKinlay (1997). The application of the event study methodology usually follows an established flow divided in these steps:

1) Definition of the event window
2) Computation of the normal returns
    a) Definition of the estimation window
    b) Choice of the estimation model
3) Estimation of the ARs
4) Statistical testing for the significance of the ARs

The event window usually spans one or more days. It can therefore be limited to the event date and also include other dates surrounding it (El Ghoul, et al., 2022; Spanos & Angelis, 2016). It is common to include the days before and after the event in order to allow for the possibility of news leakages preceding the event itself, insider trading (Arcuri, et al., 2018; Colivicchi & Vignaroli, 2019) or delayed reactions of the markets. For our study we chose six event windows. Each of them is defined by two numbers: the first represents the day in which the abnormal return of the security is first measured, the second is the last day in which the abnormal return is measured. The six event windows are: (0,0), (0,1), (-1,1), (-1,2), (0,2), (-2,2). They have been chosen in accordance with the ones used in the relevant event study literature (Arcuri et al., 2018; Campbell et al., 2003; Cavasoglu et al., 2004; Colivicchi & Vignaroli, 2019; Furdui & Șfabu, 2023; Garg et al., 2003; Gatzlaff & McCullough, 2010; Hovav & D'Arcy, 2004; Hovav & D'Arcy, 2003; Kannan et al., 2007; Kuo, et al., 2020). In addition, we have opted not to include time windows longer than four days in accordance with Pastorello's suggestion in *Rischio e rendimento: teoria finanziaria e applicazioni econometriche* (2001): the event window should be as small as possible in order to increase the study's power[25] and also limit the contamination of the returns by other events. Additionally, such small windows are coherent with Tweneboah-Kodua et al.'s findings on financial firms that we previously detailed. Nevertheless, in some windows we include the first day before the event to allow for news leaks that might happen before official sources announce the security breach. Two symmetric event windows are also included, mainly to test Arcuri et al.'s (2018) findings about insider trading, due to the significance of negative abnormal results observed both before and after the event date.

To define the AR, one must proceed to the second step of the analysis and compute the expected performance. This task requires the definition of an estimation window, that is, a sample period prior to the event window, usually leaving a cushion of at least one month to exclude market returns influenced by the event: this avoids the inclusion in this window of anticipation effects or news leaks (Pacicco et al., 2018). Our estimation window takes into account the literature that we have cited in the case of the event winnows. While some estimation windows go as far back as 255 trading days prior to the event (Kuo, et al., 2020), and other go only as far as 141 days (Arcuri, et al., 2018), after considering all of the relevant research we have opted for the (-30,-200) window.

Figure 6: Schematic representation of the time windows of an event study.



[25] Power is the probability of rejecting the null hypothesis when, in fact, it is false.

In order to clarify the time intervals that are involved in an event study, we provide Figure 6. The estimation window, contained within T_0 and T_1, completely pre-dates the event in order to allow for the unaffected estimation of the expected returns. The event window that is represented is an example of a window that contains days both before and after the date of the event. It is delimited by T_2 and T_3: in its time frame the actual returns of the security are measured. Finally, $T_E$bar indicates the date of the event, which in our case is the announcement of a cyber-attack.

The estimation of ARs can be carried out with different models. The most common model, recognized as the standard one (MacKinlay, 1997; Pastorello, 2001; Sorokina, et al., 2013), is based on Sharpe's market model (Sharpe, 1963). This method of estimation is referred to as the Single Index model (SIM) as it only requires one variable for the estimation, namely the daily returns of a market index $R_{m,t}$. The equation for this model is the following.

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

The expected returns of the security depend on the market returns, $R_{m,t}$, that have been observed in the estimation window. The parameters α_i and β_i are estimated with the OLS method. In our study the STOXX 600 index is used as the market index. This benchmark has a fixed number of 600 components representing large, mid and small capitalization companies among 17 European countries and it covers approximately 90% of the free-float market capitalization of the European stock market. Pastorello (2001) notes that different estimation models usually generate results that, when tested, do not contradict each other. For completeness we propose a summary of the other estimation models that have been used in the literature, adapted from the work by Furdui & Șfabu (2023):

- Market Adjusted Model (MAM). This is a special case of the SIM model where a constraint on the parameters α_i and β_i sees them equal to 0 and 1 respectively:

$$AR_{i,t} = R_{i,t} - R_{m,t}$$

- Historical Mean Model (HMM). The ARs are obtained as the actual returns during the event window, minus the average return observed in the estimation window:

$$AR_{i,t} = R_{i,t} - \overline{R}_i$$

- Capital Asset Pricing Model (CAPM) (Fama & French, 2004). It is a more detailed approach as it considers the risk-free rate, $R_{f,t}$, in addition to the market return:

$$R_{i,t} = R_{f,t} + \alpha_i + \beta_i \big(R_{m,t} - R_{f,t} \big) + \varepsilon_{i,t}$$

- Multifactor Model (MFM). In an attempt to improve the variance explained by the SIM, theoretical returns can be estimated by using multiple factors. Fama and French introduced in 1993 a three-factor model: it three variables representing size, value and risk factors to the CAPM.

Once the normal, or expected, returns are computed, it is possible to obtain the ARs. When the event window comprises more than one period, which in this case is one day, it becomes necessary to operate a time-series aggregation of the ARs, thus obtaining the Cumulative Abnormal Returns (CARs). Specifically, they are obtained in the following way:

$$CAR_i(T_2, T_3) = \sum_{t=T_2}^{T_3} AR_{i,t}$$

When the effect of the event is analyzed on a pool of firms, instead of on a single firm, a cross-section aggregation becomes necessary. This means that the average abnormal returns (AARs) have to be calculated in the following way:

$$AAR_t = \frac{1}{N}\sum_{i=1}^{N} AR_{i,t}$$

where $AR_{i,t}$ represents the AR estimated on the ith security and N the securities' population.
Finally, when the focus is on the average effect over multiple days as in our study, it is necessary to perform both of the aggregations just described and compute the CAARs, or Cumulative Average Abnormal Returns, by summing the AARs over time with the following method:

$$CAAR(T_2, T_3) = \sum_{t=T_2}^{T_3} AAR_t$$

Our study, as well as the ones in all the relevant literature that we analyzed, are cross-sectional: this means that the abnormal returns of multiple companies, not just one, are taken in consideration. For this reason, the focus is on CAARs and not on CARs. Only in the case of the (0,0) window, the average reaction of the various stocks is actually an Average Abnormal Return, because it comprises only one day and it is therefore not cumulative.

In the literature there also exists the portfolio approach, which is an alternative method to computing both AARs and CAARs (Kothari & Warner, 2007). By levering on an equally weighted portfolio that groups all securities under scrutiny before computing the abnormal components, researchers can compute the portfolio of ARs and CARs and then consider this portfolio as a single security. This approach is used for longer event windows, in the order of months or even years. In these studies, weekly or monthly returns are often used instead of the daily ones.

The last step in the event study methodology consists in testing the significance of the ARs that were calculated by following the previous steps. The objective is to determine if the results are significantly different form zero, through the use of significance tests. The tests used in this study will be detailed in the following section.

5.3 Significance tests

In the case of cross-sectional studies, such as ours, only the significance of CAARs or AARs is tested. The literature uses two types of tests: parametric test and nonparametric ones (Pacicco, et al., 2018). While the former type assumes a certain distribution of returns, the latter is not anchored to any a priori assumption (Kolari & Pynnönen, 2010; Kothari & Warner, 2007).
With respect to the family of parametric tests, under the assumption of normally distributed securities' returns, ARs follow a normal distribution centered on 0, with variance σ_{AR}^2. Accordingly, AARs, CARs, and CAARs also are normally distributed with mean 0 and variance σ_{AAR}^2, σ_{CAR}^2 and σ_{CAAR}^2 . The first test of this family, which has been used in part of the relevant event study literature (Salotti, 2009), is the t-test. In addition, this kind of test, assumes that returns are Independent and Identically Distributed. The cross-sectional t-test is calculated as follows:

$$t = \sqrt{N}\frac{CAAR}{S_{CAAR}}$$

However, this standard test statistic fails to take the event-induced variance and cross-sectional correlation into account, which is common in the event-study case. Therefore, type I error might still occur (Chee Pung, et al., 2018). For this reason, Patell (1976) suggests a particular Z test. This test is based on scaled, or standardized, ARs. This characteristic brings a twofold benefit: on one hand, the test accounts for the diverse standard deviations between the event window and estimation window residuals, on the other, it prevents securities with large variance to heavily influence the outcome. In particular the ARs are standardized in this fashion:

$$SAR_{i,t} = \frac{AR_{i,t}}{S_{AR_{i,t}}}$$

$S_{AR_{i,t}}$ represents the so-called forecast-error-corrected standard deviation. Specifically:

$$S^2{}_{AR_{i,t}} = S^2{}_{AR_i}\left(1 + \frac{1}{M_i} + \frac{\left(R_{m,0} - \bar{R}_m\right)^2}{\sum_{t=T_0}^{T_1}\left(R_{m,t} - \bar{R}_m\right)^2}\right)$$

Where M_i denotes the number of non-missing ARs during the estimation window, and $\bar{R}_m$ the average market return during this period. The basic intuition is that standardization weights individual observations by the inverse of the standard deviation, which implies that more volatile observations get less weight in the averaging than the less volatile or more reliable observations. While scaled abnormal returns are more difficult to interpret than raw returns, they have been proven to exhibit better statistical properties. Thus, scaled returns should be used only for statistical testing purposes as signal detection devices of the event effect, while raw returns should be used for assessing the economic information that an event carries (Kolari & Pynnönen, 2010). The Z test is then calculated as follows:

$$Z = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} \frac{CSAR_i}{S_{CSAR_i}}$$

Boehmer, Masumeci, and Poulsen (1991) then develop a test that aims to further improve on Patell's one. The BMP test accordingly also accounts for the possible cross-sectional increase in the variance of the returns that may occur within the event window. These authors standardized the CARs in the following way:

$$SCAR_i = \frac{CAR_i}{S_{CAR_i}}$$

Where S_{CAR}denotes the forecast-error-corrected standard deviation. In particular:

$$S^2{}_{CAR_i} = S^2{}_{AR_i} \left(L_2 + \frac{L_2}{M_i} + \frac{\sum_{t=T_2}^{T_3} \left(R_{m,t} - \bar{R}_m\right)^2}{\sum_{t=T_0}^{T_1} \left(R_{m,t} - \bar{R}_m\right)^2} \right)$$

L_2 corresponds to the length of the event window, meaning $L_2 = T_3 - T_2$. The test statistic is:

$$z = \sqrt{N} \frac{\overline{SCAR}}{S_{\overline{SCAR}}}$$

The BMP test, also referred to as the standardized cross-sectional test, is powerful when the null is false and also shows appropriate rejection rates when it is true.

Two decades later Kolari & Pynnönen (2010) challenge this test. Specifically, they demonstrate through a series of event study simulations on real world data that even relatively low cross-sectional correlation in an event study with clustered event days can cause serious over-rejection of the null hypothesis of no event mean effect. This clustering of event days could be a serious issue for our study on systemic events as the event day is shared across all shares. Subsequently, the authors propose a cross-correlation and volatility-adjusted BMP test statistic, namely the ADJ-BMP test. According to the simulations on real returns by Kolari & Pynnönen, their proposed test statistic is robust to both variance changes and cross-correlation. For the above reasons, we opt to use the ADJ-BMP test as our parametric test. It is calculated as:

$$z_{ADJ} = z \times \sqrt{\frac{1-\bar{r}}{1+(N-1)\bar{r}}}$$

Where z stands for the standard BMP test, while $\bar{r}$ denotes the average of the sample cross-correlations of the estimation period normal returns.

Even if the test we use is volatility-adjusted, the most sophisticated approach to account for the heteroskedasticity induced by the event would be its modelling through a GARCH[26] model (Pastorello, 2001). We suggest that other researchers, undertaking a similar study to ours, consider such an expansion route. An example can be found in Colivicchi & Vignaroli's analysis (2019).

Being linked to the normality assumption of the securities' return distributions, the aforementioned tests may underperform when returns are not normal. Given that stock returns are virtually always not normally distributed, Pastorello (2001) strongly suggests the use of a non-parametric test as a way to check and strengthen the results showed by the parametric one. Salotti (2009) underlines this method as especially important for multi-country event studies, such as ours. For these reasons we choose to accompany the ADJ-BMP test with a non-parametric one. According to Nguyen & Wolf (2023), when an event study deals with CAARs calculated on a large number of companies or a large number of days of the event window, the researcher could appeal to the central limit theorem and simply carry out a parametric test. Given that our event study doesn't include either a large number of companies or large event windows, we can't assume a certain distribution of the returns and thus the need for a non-parametric test is strengthened.

The test statistic of this family that we chose for our study was also developed by Kolari & Pynnönen (2011). The authors note that, even if the power of nonparametric rank tests dominates parametric tests in event study analyses of abnormal returns on a single day, problems can arise in the application of nonparametric tests to multiple day analyses of cumulative abnormal returns: this has caused researchers in the past to only rely upon parametric tests. In an effort to overcome this shortfall, they propose a generalized rank testing procedure, referred to as GRANK, that can be used on both single day and cumulative abnormal returns. This is especially relevant for our five multi day event windows. In particular Kolari & Pynnönen show, once again through simulations, that the GRANK procedure outperforms previous rank tests of CARs, such as the Wilcoxon test, and is robust to abnormal return serial

[26] Generalized AutoRegressive Conditional Heteroskedasticity.

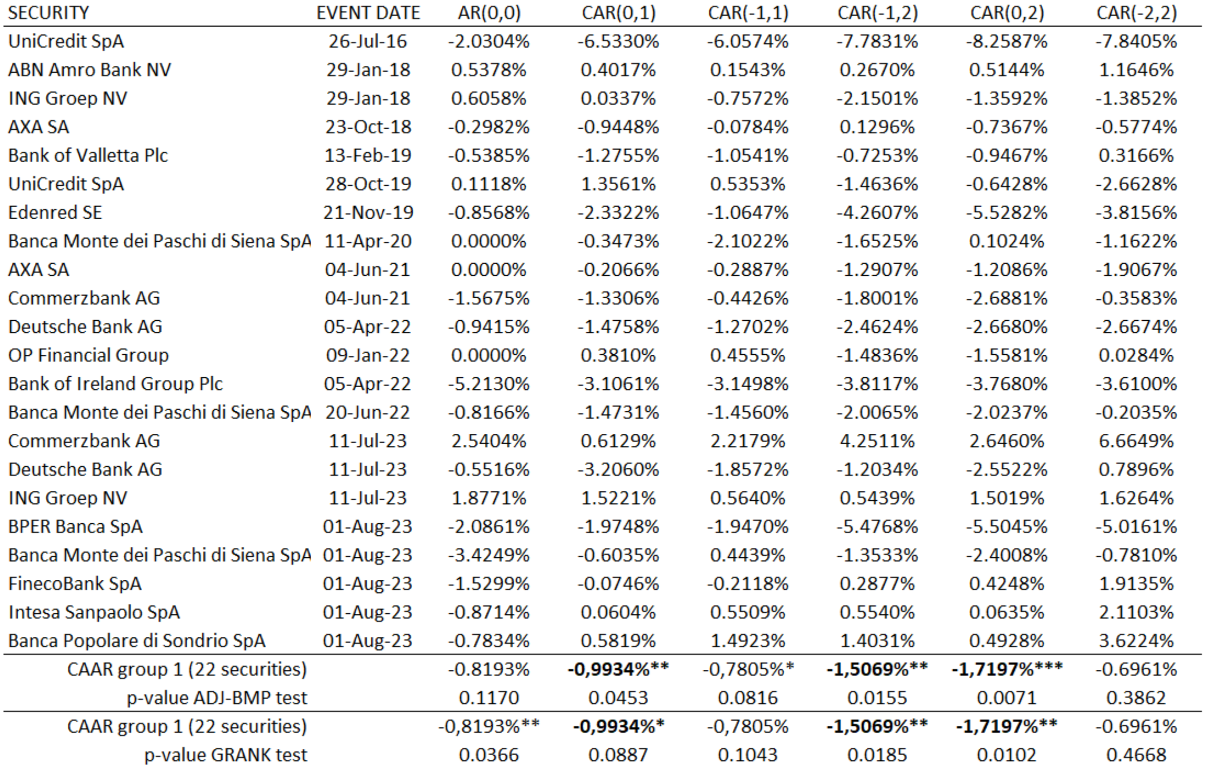
correlation and event-induced volatility. Moreover, the GRANK procedure generally exhibits superior empirical power relative to the popular parametric tests of the literature.

6. RESULTS AND DISCUSSION

6.1 Direct events results

Table 5 contains all of the Cumulative Abnormal Returns associated with the stock of each company involved in a direct event. In the case of the (0,0) window we have proper Abnormal Returns instead of CARs, as the event window comprises only one trading day. For the same reason, when we take the average of the ARs in this window, we observe the Average Abnormal Return and not the CAAR. As is usual in the relevant literature we make observations on the basis of the significance of AARs and CAARs, forgoing the significance of the individual ARs of each company on each trading day of the event window.

Table 5: Results of the event study on all direct events.

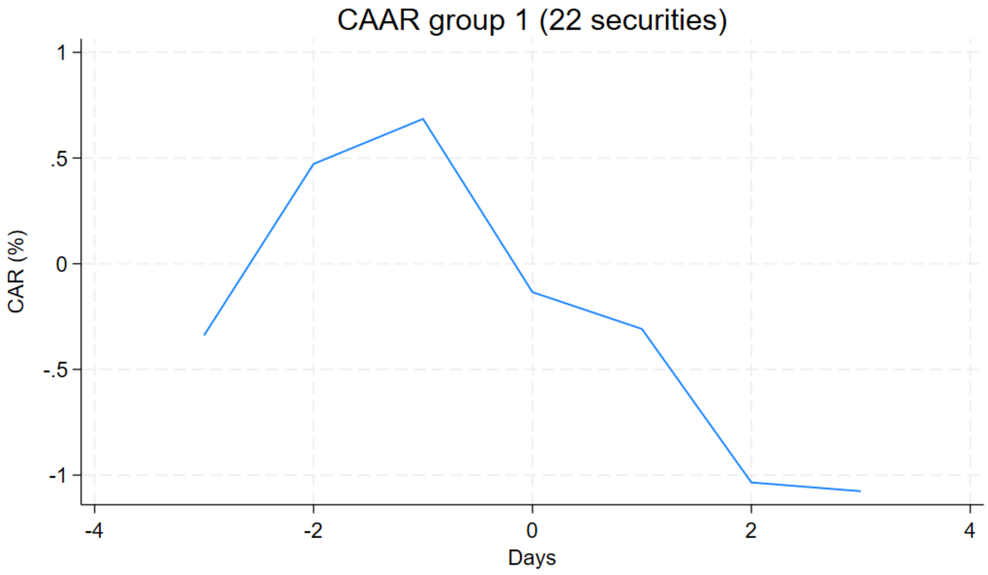


SECURITY	EVENT DATE	AR(0,0)	CAR(0,1)	CAR(-1,1)	CAR(-1,2)	CAR(0,2)	CAR(-2,2)
UniCredit SpA	26-Jul-16	-2.0304%	-6.5330%	-6.0574%	-7.7831%	-8.2587%	-7.8405%
ABN Amro Bank NV	29-Jan-18	0.5378%	0.4017%	0.1543%	0.2670%	0.5144%	1.1646%
ING Groep NV	29-Jan-18	0.6058%	0.0337%	-0.7572%	-2.1501%	-1.3592%	-1.3852%
AXA SA	23-Oct-18	-0.2982%	-0.9448%	-0.0784%	0.1296%	-0.7367%	-0.5774%
Bank of Valletta Plc	13-Feb-19	-0.5385%	-1.2755%	-1.0541%	-0.7253%	-0.9467%	0.3166%
UniCredit SpA	28-Oct-19	0.1118%	1.3561%	0.5353%	-1.4636%	-0.6428%	-2.6628%
Edenred SE	21-Nov-19	-0.8568%	-2.3322%	-1.0647%	-4.2607%	-5.5282%	-3.8156%
Banca Monte dei Paschi di Siena SpA	11-Apr-20	0.0000%	-0.3473%	-2.1022%	-1.6525%	0.1024%	-1.1622%
AXA SA	04-Jun-21	0.0000%	-0.2066%	-0.2887%	-1.2907%	-1.2086%	-1.9067%
Commerzbank AG	04-Jun-21	-1.5675%	-1.3306%	-0.4426%	-1.8001%	-2.6881%	-0.3583%
Deutsche Bank AG	05-Apr-22	-0.9415%	-1.4758%	-1.2702%	-2.4624%	-2.6680%	-2.6674%
OP Financial Group	09-Jan-22	0.0000%	0.3810%	0.4555%	-1.4836%	-1.5581%	0.0284%
Bank of Ireland Group Plc	05-Apr-22	-5.2130%	-3.1061%	-3.1498%	-3.8117%	-3.7680%	-3.6100%
Banca Monte dei Paschi di Siena SpA	20-Jun-22	-0.8166%	-1.4731%	-1.4560%	-2.0065%	-2.0237%	-0.2035%
Commerzbank AG	11-Jul-23	2.5404%	0.6129%	2.2179%	4.2511%	2.6460%	6.6649%
Deutsche Bank AG	11-Jul-23	-0.5516%	-3.2060%	-1.8572%	-1.2034%	-2.5522%	0.7896%
ING Groep NV	11-Jul-23	1.8771%	1.5221%	0.5640%	0.5439%	1.5019%	1.6264%
BPER Banca SpA	01-Aug-23	-2.0861%	-1.9748%	-1.9470%	-5.4768%	-5.5045%	-5.0161%
Banca Monte dei Paschi di Siena SpA	01-Aug-23	-3.4249%	-0.6035%	0.4439%	-1.3533%	-2.4008%	-0.7810%
FinecoBank SpA	01-Aug-23	-1.5299%	-0.0746%	-0.2118%	0.2877%	0.4248%	1.9135%
Intesa Sanpaolo SpA	01-Aug-23	-0.8714%	0.0604%	0.5509%	0.5540%	0.0635%	2.1103%
Banca Popolare di Sondrio SpA	01-Aug-23	-0.7834%	0.5819%	1.4923%	1.4031%	0.4928%	3.6224%
CAAR group 1 (22 securities)		-0.8193%	**-0,9934%****	-0,7805%*	**-1,5069%****	**-1,7197%*****	-0.6961%
p-value ADJ-BMP test		0.1170	0.0453	0.0816	0.0155	0.0071	0.3862
CAAR group 1 (22 securities)		-0,8193%**	**-0,9934%***	-0,7805%	**-1,5069%****	**-1,7197%****	-0.6961%
p-value GRANK test		0.0366	0.0887	0.1043	0.0185	0.0102	0.4668

All event windows show negative, even if not always significant, abnormal stock returns, this is consistent with virtually all of the relevant literature about the financial sector and the wider economy. For clarity of interpretation, we have put in bold characters the CAARs, or AARs, that are significant according to both the parametric ADJ-BMP test and the non-parametric GRANK test. We notice that only the (0,1), (-1,2) and (0,2) event windows show significant stock returns for both tests. In particular the (0,1) window shows results significant at the 10% level for both tests: only the parametric test is significant even at the 5% level. The (-1,2) and (0,2) windows are significant, for both tests, at the 5% level. Furthermore, the ADJ-BMP test for the latter of the two windows is significant at the 1% level. The difference observed in the p-values by the two tests in not extreme. As we have seen the Boehmer, Masumeci and Poulsen test (1991) is a version of Patell's test that is adjusted in order to be robust against the way in which ARs are distributed across the event window. Moreover, Kolari and Pynnönen adjust this BMP test and make it less sensible to the cross-sectional correlation of the ARs. The slight difference between this test and the noon-parametric test, also formulated by Kolari and Pynnönen, could mean that some of the assumptions of the parametric test are not met by our data. In addition, our sample of event is small when compared to the average sample of the literature: in this case the results on significance showed by a non-parametric test are generally more reliable than the ones indicated by its parametric counterpart (Pastorello, 2001).

Figure 7 contains the graph of the CAAR of all securities in the event window (-3,3). Even if this window is not used in our study, it can be useful as it gives a graphical overview of the evolution of the CAAR for each day of the window.

Figure 7: CAAR graph for all events in the (-3,3) window.



In other words, the graph shows how the value of the CAAR changes from the initial AAR observed in (-3,-3) until the window expands to also encompass the other days of the (-3,3) period (Pacicco, et al., 2021). Accordingly, if we chose the same event window for the graph as the (-1,2) window we use in the study, the last point of the graph would correspond to the value of the CAAR reported in the output table for the (-1,2) period, meaning -1,50%. Another way to explain how the graph can be read is that, if we consider the (0,0) AAR we measured at -0,81%, we can see it reflected in the fact that, from T(-1) to T(0), the CAAR measured on (-3,-1) goes from an approximate +0,60% to a – 0,20% when we include one more day, namely with the (-3,0) window. For this reason, we can see which days in the (-3,3) period implied a negative AAR for the surveyed stocks, and to which extent this return was negative.

Focusing on the significant event windows, when we consider our (0,1) window we find that, on average, a financial institution that is directly targeted by a cyberattack, observes a loss in its share price of -0,99%. This loss increases in the longer windows of (-1,2) and (0,2) respectively to -1,55% and -1,71%. Our results are consistent with the ones by Cavasoglu et al. (2004). Cavasoglu et al. found that announcement of a security breach is significantly and negatively associated with the market value of the targeted firm. In this study, breached firms lost an average of 2,1% percent of their market value within the two days after the events. Our results are also consistent with the ones by Garg et al. (2003) regarding the fact that the average loss gets more relevant in the two days after the event when compared to the day of the event in itself. These authors found that, in case of security breaches, the average loss in share price the day of an event's occurrence is around -2,7%, while it increases to -4,5% over a three-day period. The fact that Garg et al. found average losses that are larger than the ones we found can be attributed to two factors. Firstly, their sample of companies, as the one used by Cavasoglu et al., comprises all sectors of the US economy, not being restricted to the financial sector. Secondly the study was conducted more than 20 years ago. As even the study by Cavasoglu, published a year after, showed losses that are slightly higher than the ones we observe, this second reason seems the more likely. This is supported by the findings of Gordon, et al. in 2011. As already seen, these researchers found that security breaches that happened after 9/11 have a less significant, although still negative, effect on stock prices. Their explanation is twofold. In the first place, there is the possibility that consumers developed a much greater tolerance for news on announcements of such breaches. Secondly, and not exclusively with respect to the first reason, firms over time may have strengthened their remediation and disaster recovery plans and therefore may have substantially reduced the cost of an average information security breach. This could be especially true in the case of our European financial institutions, the security measures of which have likely been strengthened as a result of the EU's recent regulations for cybersecurity. If an event study were to be conducted on security breaches predating 9/11, on a similar sample to ours, this explanation could be tested. If similar results were found to the ones by Gordon et. al about US companies, it would mean that the recent legislation by the European Union has had a positive effect on both the actual and perceived security of its financial institutions.

In this sense our results are also consistent with the ones by Gatzlaff & McCullough (2010). 36% of their sample of 77 companies consists in financial institutions. The mean CAR for all the 77 data breach events over the event window (0,1) is -0,84%. This result is much more similar to our one of -0,99%, for the same event window. In addition, the recent study by Kuo, et al. (2020), with an economy-wide sample of US companies, finds that the average loss in share price the day of a cyber incident is -0,23%. This could mean that financial institutions are more sensible than companies of other economic sectors when dealing with security breaches, as suggested by Arcuri et al. (2018) and Colivicchi & Vignaroli (2019).

Our findings are also consistent with the ones by Tweneboah-Kodua et al. (2018), who find that financial companies show significant negative abnormal returns when they are measured cumulatively between the first day before the event and the first day after it.

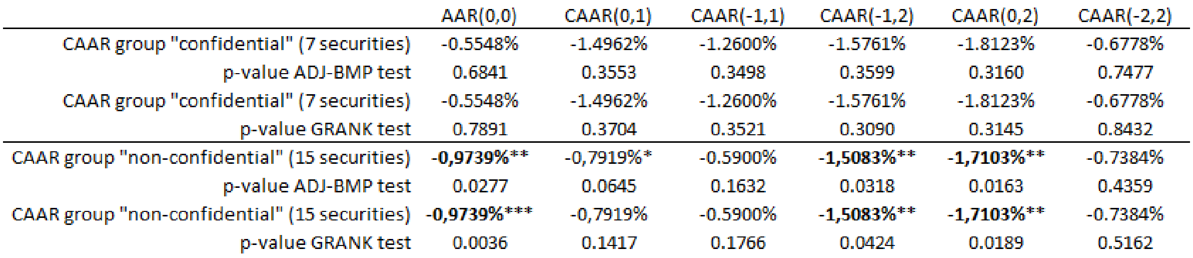
Our results are in stark contrast with the ones by Arcuri et al. (2018) and Colivicchi & Vignaroli (2019) in the fact that these authors found significant negative results, in the case of financial institutions, only for symmetric event windows and event windows that completely precede the event day. The symmetric windows used by these researchers that yield significant results are the (-5,5), (-10,10) and (-20,20) ones. The asymmetric windows that pre-date the event and that also yield significant results are the (-5,-1) and (-3,-1) ones. None of our two symmetric windows, (-1,1) and (2,2) show significant results. The mentioned papers attributed such results to the presence of insider trading in the days prior to the event. In our case we find no evidence in favor of insider trading. In our discussion we opted not to include windows longer than 3 trading days in accordance with the suggestion by Pastorello (2001). Our (-1,2) window, on the other hand, shows significant negative abnormal returns, while including one trading day before the event. This result may be attributed to the presence of leaked news regarding the cyberattacks, before they get publicly announced by the targeted company or newspapers. These considerations on insider trading and information leaks could represent interesting topic for future European legislation: while insider trading apparently does not need specific addressing, informational leaks likely represent an important factor in the market's assessment of the reliability of a financial institution even before official sources have fulfilled their role.

In conclusion we reject H_0^I. In particular the share prices of financial instituitons react in a negative and significant way in the (0,1), (-1,2) and (0,2) event windows. In the first case we reject the hypothesis at the 10% confidence level. In the second and third case we do so at the 5% confidence level.

6.1.1 Results on confidential and non-confidential attacks

When we divide the events in confidential and non-confidential ones, we get the results of Table 6. In particular 7 companies were hit by attacks that involved the disclosure by hackers of some of their confidential information. These attacks all consist in data breaches. The remaining 15 companies were hit by attacks that did not imply such disclosure, such as DDoS attacks, malwares and phishing attacks. We find that only non-confidential attacks are significant: in particular they are so at the 5% confidence level in the (0,0), (-1,2) and (0,2) periods. We recognize that our study, due to its small size, could result in a lower reliability of the significance tests. On the other hand, for small sample sizes, the non-parametric test should still give powerful and reliable results (Kolari & Pynnönen, 2011).

Table 6: Results for confidential and non-confidential events.



	AAR(0,0)	CAAR(0,1)	CAAR(-1,1)	CAAR(-1,2)	CAAR(0,2)	CAAR(-2,2)
CAAR group "confidential" (7 securities)	-0.5548%	-1.4962%	-1.2600%	-1.5761%	-1.8123%	-0.6778%
p-value ADJ-BMP test	0.6841	0.3553	0.3498	0.3599	0.3160	0.7477
CAAR group "confidential" (7 securities)	-0.5548%	-1.4962%	-1.2600%	-1.5761%	-1.8123%	-0.6778%
p-value GRANK test	0.7891	0.3704	0.3521	0.3090	0.3145	0.8432
CAAR group "non-confidential" (15 securities)	**-0,9739%****	-0,7919%*	-0.5900%	**-1,5083%****	**-1,7103%****	-0.7384%
p-value ADJ-BMP test	0.0277	0.0645	0.1632	0.0318	0.0163	0.4359
CAAR group "non-confidential" (15 securities)	**-0,9739%*****	-0,7919%	-0.5900%	**-1,5083%****	**-1,7103%****	-0.7384%
p-value GRANK test	0.0036	0.1417	0.1766	0.0424	0.0189	0.5162

This premise considered, our results are interestingly consistent with the ones observed by Arcuri et al. (2018), who find that confidential attacks in the financial sector do not result in significant negative abnormal returns for the stocks of the attacked companies. Conversely, in a less recent study Campbell et al. (2003) found a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach did not involve confidential information. Arcuri et al. give two explanations to this peculiar finding that we also share. The first explanation is that, in the financial industry, confidential attack announcements are likely to be predicted by investors because unauthorized access to confidential information is a big concern, and for this reason word of mouth is likely to spread fast. In our view the second explanation could be more realistic.: it resides in the fact that the stock markets could be more efficient when cyber-attacks do not concern access to confidential information, as the value of stolen data could be more difficult to assess than the value of lost business during, for instance, a shutdown of the company's systems. According to the authors it may be the case that investors in turn perceive financial entities damaged by non-confidential attacks as being more vulnerable. In fact, as well as protecting confidential and non-confidential data, banks and other financial service organizations have to safeguard their systems and networks. This also means the financial sector faces a larger number of threats than many other industries. We expand on this consideration with the use of the CIA's Triad. Our shared results could indicate that in recent times the availability and integrity of information has become more important for investors than its confidentiality. In the instance of a DDoS attack the utter absence of availability of information could have a relevant impact on the opinion of a financial institution's private and business customers, as well as investors. On the other hand, malware, in the form of ransomware, can compromise the integrity of information: the restoration of this information could represent an even harder challenge for financial firms than the invalidation of leaked confidential information. In the case of a leaked credit card number, pin or password, nowadays it can be relatively easy for the bank itself, or the customer, to notify the other part of the event and duly agree on new credentials, while the previous ones get suspended or invalidated. This reasoning is consistent with the results by Abshishta et al. (2017). In their study, comprising firms from multiple economic sector and countries, these authors found that there is a noticeable negative impact on the stock prices of the victim firm whenever the attack causes interruptions to the services provided by the firm to its customers. This is especially true for DDoS attacks, which in our study represent 45% of the non-confidential cyber events. The relevance of the continuity of operations is also acknowledged by the newer legislation we have explored in Chapter 2. In particular the Essential Entities of the financial sector identified by the NIS2 directive will be required to have contingency plans in place to ensure business continuity in the event of a cyber incident.

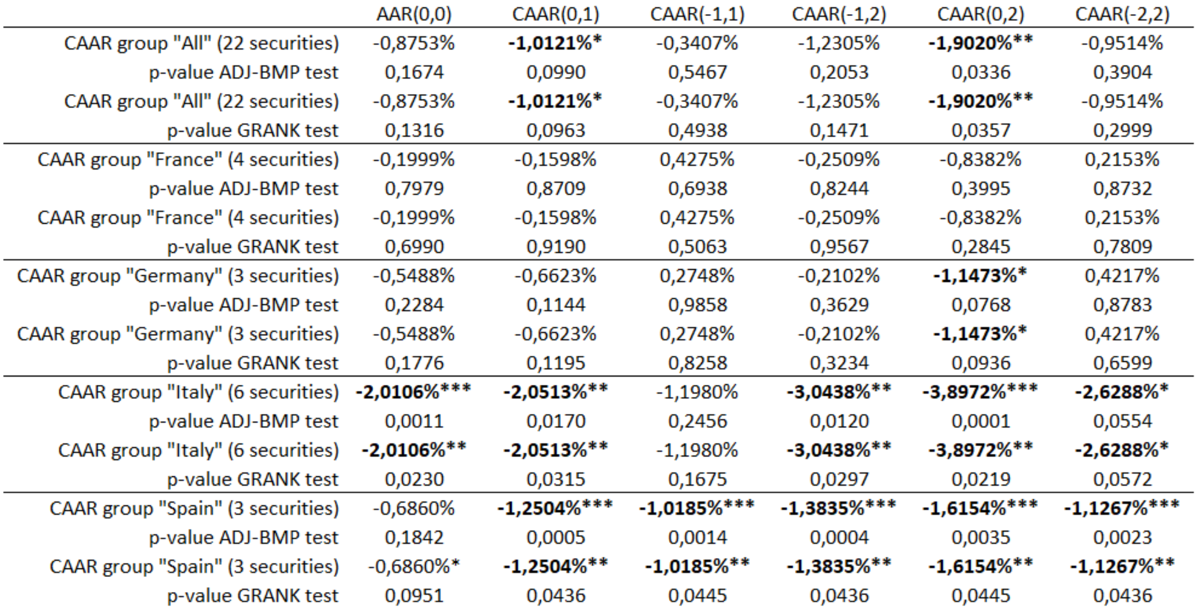
In conclusion we reject H_0^{II}, which stated that, in case of a direct cyberattack, confidential and non-confidential attacks have the same effect. In fact, we find that only confidential attacks have a significant negative effect: in particular in the (0,0), (-1,2) and (0,2) at the 5% confidence level. Nevertheless, it must be considered that the small size of our sample of events may be a partially detrimental factor with respect to the reliability of our results.

6.2 Systemic events results

6.2.1 JP Morgan data breach: initial and subsequent announcement

Following the chronological order of the three systemic events, we start our discussion from the 2014 data breach suffered by JP Morgan. In particular the results in Table 7 are calculated on the 28th of August 2014 as the event date, which corresponds to the date in which it was disclosed that JP Morgan was under attack. The eventual success of the attack was announced on the 2nd of October and is discussed later.

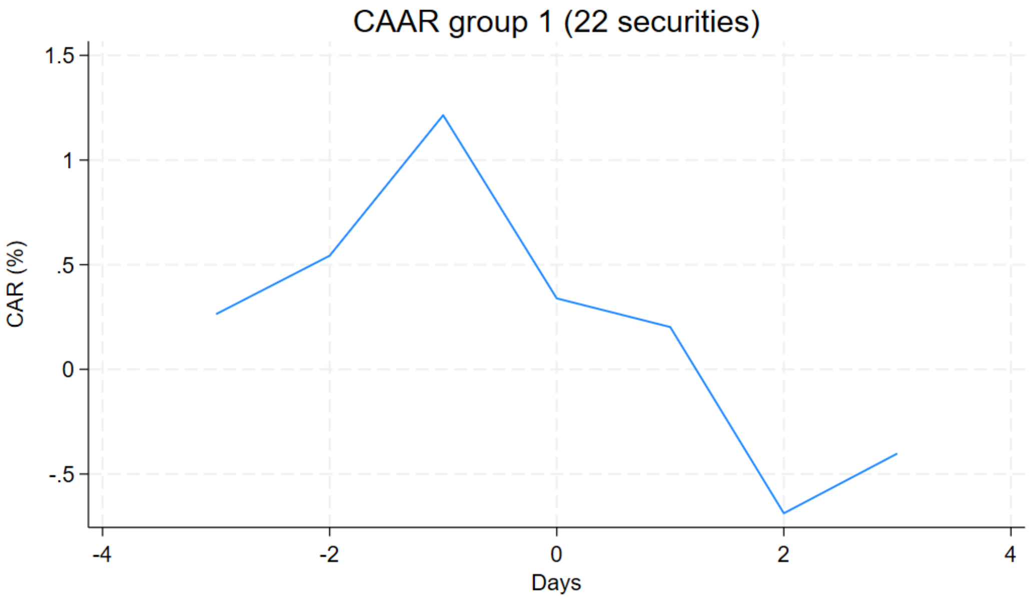
Table 7: Results for the JP Morgan systemic event on 28/08/2014.



	AAR(0,0)	CAAR(0,1)	CAAR(-1,1)	CAAR(-1,2)	CAAR(0,2)	CAAR(-2,2)
CAAR group "All" (22 securities)	-0,8753%	**-1,0121%***	-0,3407%	-1,2305%	**-1,9020%****	-0,9514%
p-value ADJ-BMP test	0,1674	0,0990	0,5467	0,2053	0,0336	0,3904
CAAR group "All" (22 securities)	-0,8753%	**-1,0121%***	-0,3407%	-1,2305%	**-1,9020%****	-0,9514%
p-value GRANK test	0,1316	0,0963	0,4938	0,1471	0,0357	0,2999
CAAR group "France" (4 securities)	-0,1999%	-0,1598%	0,4275%	-0,2509%	-0,8382%	0,2153%
p-value ADJ-BMP test	0,7979	0,8709	0,6938	0,8244	0,3995	0,8732
CAAR group "France" (4 securities)	-0,1999%	-0,1598%	0,4275%	-0,2509%	-0,8382%	0,2153%
p-value GRANK test	0,6990	0,9190	0,5063	0,9567	0,2845	0,7809
CAAR group "Germany" (3 securities)	-0,5488%	-0,6623%	0,2748%	-0,2102%	**-1,1473%***	0,4217%
p-value ADJ-BMP test	0,2284	0,1144	0,9858	0,3629	0,0768	0,8783
CAAR group "Germany" (3 securities)	-0,5488%	-0,6623%	0,2748%	-0,2102%	**-1,1473%***	0,4217%
p-value GRANK test	0,1776	0,1195	0,8258	0,3234	0,0936	0,6599
CAAR group "Italy" (6 securities)	**-2,0106%*****	**-2,0513%****	-1,1980%	**-3,0438%****	**-3,8972%*****	**-2,6288%***
p-value ADJ-BMP test	0,0011	0,0170	0,2456	0,0120	0,0001	0,0554
CAAR group "Italy" (6 securities)	**-2,0106%****	**-2,0513%****	-1,1980%	**-3,0438%****	**-3,8972%****	**-2,6288%***
p-value GRANK test	0,0230	0,0315	0,1675	0,0297	0,0219	0,0572
CAAR group "Spain" (3 securities)	-0,6860%	**-1,2504%*****	**-1,0185%*****	**-1,3835%*****	**-1,6154%*****	**-1,1267%*****
p-value ADJ-BMP test	0,1842	0,0005	0,0014	0,0004	0,0035	0,0023
CAAR group "Spain" (3 securities)	-0,6860%*	**-1,2504%****	**-1,0185%****	**-1,3835%****	**-1,6154%****	**-1,1267%****
p-value GRANK test	0,0951	0,0436	0,0445	0,0436	0,0445	0,0436

The CAARs are measured for the entire sample of institutions as well as the following groups: French firms, German firms, Italian firms and Spanish ones. Firstly, the abnormal returns are, for the most part, negative. As usual CAARs that are significant according to the parametric and non-parametric tests are in bold characters. Only the French and German groups of securities show slightly positive, but not significant, CAARs in two of the six event windows. Regarding the overall group we notice a significant negative reaction in the windows that only comprise the trading days after the event, namely the (0,1) and (0,2) periods. This can be seen graphically in Figure 8 which is constructed with the same logic of the previous graph in Figure 7. As an example, we can graphically see that the first negative AAR is associated with T(0) and not T(1). Namely in the day of the event itself, as shown in the Table above, the AAR for all stocks is of -0,87%, even if not significant for both tests. This could imply that information leaks did not play such a relevant role as the one observed in direct events.

Figure 8: CAAR graph in the (-3,3) window for the JP Morgan systemic event on 28/08/2014.



The overall CAAR for the (0,1) period is significant at the 10% confidence level, while the one for the (0,2) window is significant at the 5% level. On average the financial institutions of the sample incur in a -1,01% cumulative abnormal loss in the day of the event and the one after it. When we add a third trading day the cumulative loss amounts to -1,90%.

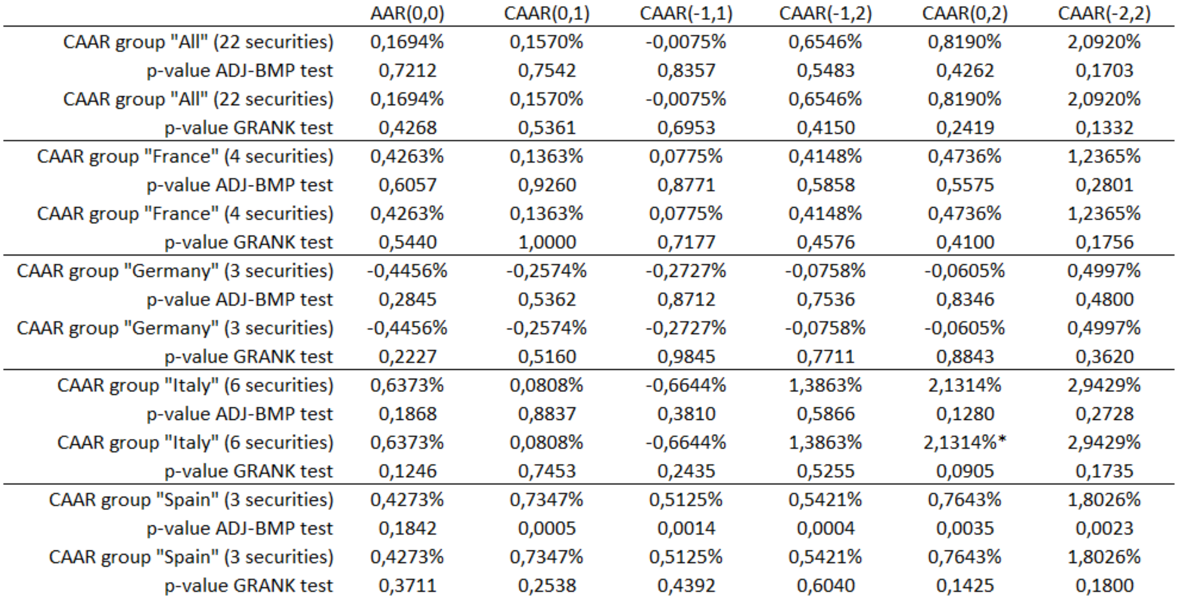
It is important to remember that such an event study has no precedent in literature. Namely no researchers in the past have analyzed the reaction of stock prices of European financial firms in view of a US financial firm being breached. For this reason, we have no significant results with which to compare ours. The significant negative CAARs of the total sample could imply that the markets view an attack on a major US bank as a negative factor for the performance of its European counterparts. This interpretation can be explained in two ways. In the first place, global economies have never been as interconnected as they are today, especially when we consider the so-called Western economies (Seong, et al., 2022). The breach of one of the most globally relevant US financial institutions, such as JP Morgan Chase which at the 31st of December 2023 was the largest US banks by total assets (Federal Reserve, 2024), can be interpreted by investors worldwide as having a negative impact on the economic performance of other firms. In our particular case it possible that investors interpreted such an attack as detrimental to the activities of European financial firms. In the second place, there could be a component of technological interconnectedness on top of the economic one. As we have seen banks can share third party suppliers, such as SolarWinds, as well as conduct their operations thanks to a shared network such as the SWIFT system. Moreover, banks can be interpreted as technologically connected in the sense that they employ similar cybersecurity strategies and measures, in accordance with country-wide or international regulations (Kopp, et al., 2017).

Investors could perceive such an important bank being attacked, along with nine others, as an increase in the vulnerability, from a cybersecurity standpoint, of other banks worldwide. In other words, there is a perceived risk of propagation of the attack and cascade effect across financial firms. As only the event windows that do not contain trading days before that of the event display significant abnormal returns, our results once again are in contrast with the ones observed by Arcuri et al. (2018) and Colivicchi & Vignaroli (2019). Specifically, we do not find significant evidence of insider trading in the days preceding the attack, nor even significant evidence for leaks of news before the event.

If we shift our attention to the country specific CAARs, we notice that five of the six event windows display significant and highly negative stock returns for Italian and Spanish firms. On the other hand, German firms exhibit a significant abnormal reaction only in the (0,2) period, while French companies do not show any significant abnormal return. While the markets could interpret Italian and Spanish firms as being more connected with the American financial sector, a more plausible explanation for this observation could be represented by an exogenous factor to our study. In particular the Italian and Spanish firms could have been seen in a more negative light by investors with respect to their German and French counterparts, in the second part of August 2014, as news about deflation in Italy (Il Sole 24 Ore, 2014) and Spain (BBC, 2014) started to gain traction. From the perspective of European lawmakers, while the US banks' effect on EU firms is not easily addressable, the fact that financial companies in more economically unstable EU countries are more vulnerable to cyberattacks, at least according to investors, should be a topic of interest.

As anticipated, we repeated the test for the date in which the full extent of JP Morgan's data breach was revealed. On the 2rd of October of the same year, after the European markets had closed, it was confirmed that 76 million households had their accounts breached, as well as 7 million small businesses. The results can be found in Table 8. No CAARs, for any event window or any security group, show results that are significant according to both tests. Moreover, the non-significant CAARs are mostly slightly positive. In our view this interesting result could be explained by two main reasons. The first one resides in the fact that, as Arcuri et al. (2018) note, it is possible that in the case of financial institutions being subject to data breaches of confidential information, informational leaks are so prominent that the markets internalize the negative returns days before any official announcement. In this particular case it would mean that investors worldwide already factored-in the repercussions of JP Morgan's breach on the day of the attack: thus, the day in which the number of compromised accounts was revealed to the public, no significant reaction in the stock prices of other financial firms is observed.

Table 8: Results for the JP Morgan systemic event on 03/10/2014.



	AAR(0,0)	CAAR(0,1)	CAAR(-1,1)	CAAR(-1,2)	CAAR(0,2)	CAAR(-2,2)
CAAR group "All" (22 securities)	0,1694%	0,1570%	-0,0075%	0,6546%	0,8190%	2,0920%
p-value ADJ-BMP test	0,7212	0,7542	0,8357	0,5483	0,4262	0,1703
CAAR group "All" (22 securities)	0,1694%	0,1570%	-0,0075%	0,6546%	0,8190%	2,0920%
p-value GRANK test	0,4268	0,5361	0,6953	0,4150	0,2419	0,1332
CAAR group "France" (4 securities)	0,4263%	0,1363%	0,0775%	0,4148%	0,4736%	1,2365%
p-value ADJ-BMP test	0,6057	0,9260	0,8771	0,5858	0,5575	0,2801
CAAR group "France" (4 securities)	0,4263%	0,1363%	0,0775%	0,4148%	0,4736%	1,2365%
p-value GRANK test	0,5440	1,0000	0,7177	0,4576	0,4100	0,1756
CAAR group "Germany" (3 securities)	-0,4456%	-0,2574%	-0,2727%	-0,0758%	-0,0605%	0,4997%
p-value ADJ-BMP test	0,2845	0,5362	0,8712	0,7536	0,8346	0,4800
CAAR group "Germany" (3 securities)	-0,4456%	-0,2574%	-0,2727%	-0,0758%	-0,0605%	0,4997%
p-value GRANK test	0,2227	0,5160	0,9845	0,7711	0,8843	0,3620
CAAR group "Italy" (6 securities)	0,6373%	0,0808%	-0,6644%	1,3863%	2,1314%	2,9429%
p-value ADJ-BMP test	0,1868	0,8837	0,3810	0,5866	0,1280	0,2728
CAAR group "Italy" (6 securities)	0,6373%	0,0808%	-0,6644%	1,3863%	2,1314%*	2,9429%
p-value GRANK test	0,1246	0,7453	0,2435	0,5255	0,0905	0,1735
CAAR group "Spain" (3 securities)	0,4273%	0,7347%	0,5125%	0,5421%	0,7643%	1,8026%
p-value ADJ-BMP test	0,1842	0,0005	0,0014	0,0004	0,0035	0,0023
CAAR group "Spain" (3 securities)	0,4273%	0,7347%	0,5125%	0,5421%	0,7643%	1,8026%
p-value GRANK test	0,3711	0,2538	0,4392	0,6040	0,1425	0,1800

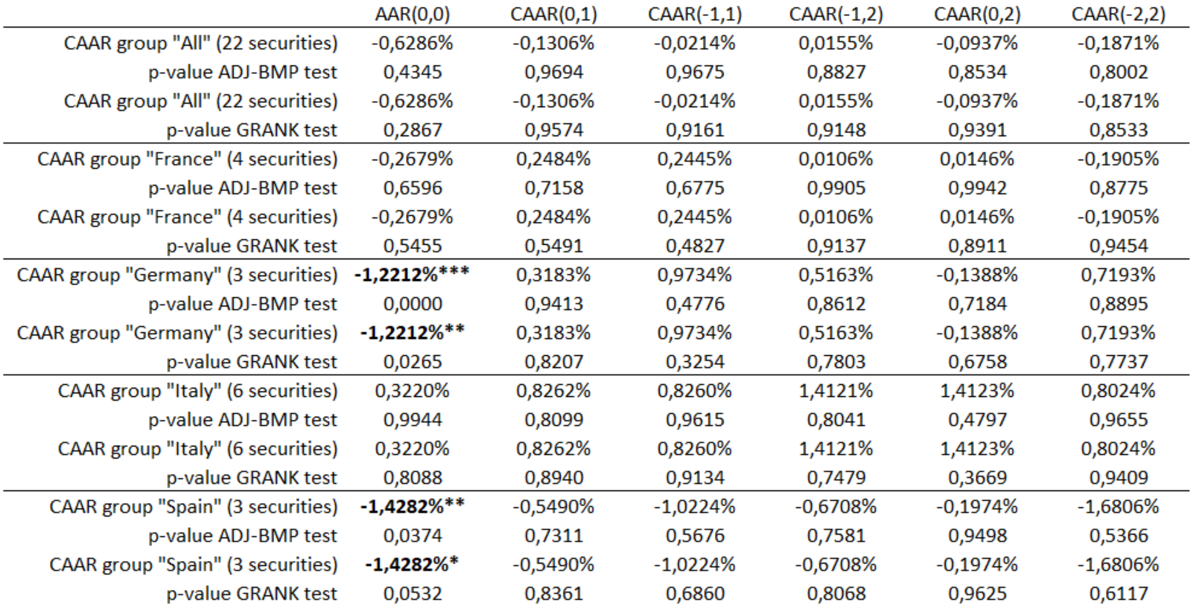
A second explanation could reside in the fact that investors actually do not interpret European financial firms as having performance ties to major US banks. Contrarily, the overall positive even if insignificant CAARs, could point out at the competitive aspect between financial companies across the world.

Overall, when we only consider significant results, it can be assessed that on the day that JP Morgan and the other nine undisclosed US banks came under a serious security threat, the stocks of European firms operating in the financial sector reacted in a negative and significant way in the (0,1) and (0,2) windows, respectively at the 10% and 5% confidence levels. Italy and Spain were the countries whose financial institutions showed the largest and most significant negative returns, possibly in light of their increased vulnerability due to the Eurozone's crisis which heavily impacted the economies of Southern Europe.

6.2.2 WannaCry ransomware outbreak

The second systemic event of our study consists in the WannaCry ransomware epidemic that started on the 12th of May 2017. The CAARs, for the same time windows and groups of securities as before, can be found in Table 9. In the case of the group of all securities no event period presents significant results. On the other hand, the German and Spanish groups both show significant negative returns in the (0,0) window, corresponding to the Abnormal Returns the day of the event itself.

Table 9: Results for the WannaCry systemic event on 12/05/2017.

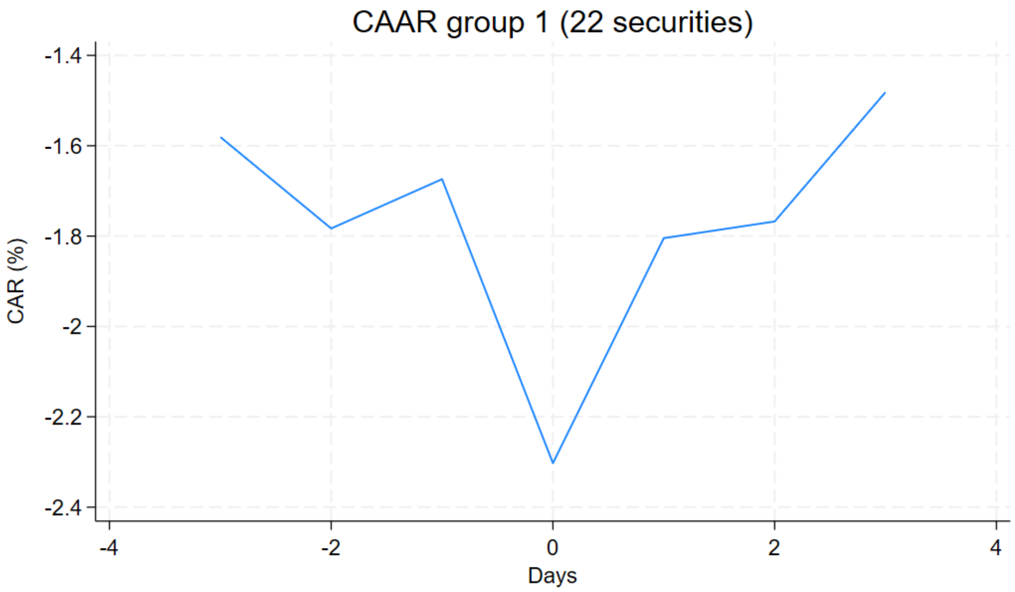


	AAR(0,0)	CAAR(0,1)	CAAR(-1,1)	CAAR(-1,2)	CAAR(0,2)	CAAR(-2,2)
CAAR group "All" (22 securities)	-0,6286%	-0,1306%	-0,0214%	0,0155%	-0,0937%	-0,1871%
p-value ADJ-BMP test	0,4345	0,9694	0,9675	0,8827	0,8534	0,8002
CAAR group "All" (22 securities)	-0,6286%	-0,1306%	-0,0214%	0,0155%	-0,0937%	-0,1871%
p-value GRANK test	0,2867	0,9574	0,9161	0,9148	0,9391	0,8533
CAAR group "France" (4 securities)	-0,2679%	0,2484%	0,2445%	0,0106%	0,0146%	-0,1905%
p-value ADJ-BMP test	0,6596	0,7158	0,6775	0,9905	0,9942	0,8775
CAAR group "France" (4 securities)	-0,2679%	0,2484%	0,2445%	0,0106%	0,0146%	-0,1905%
p-value GRANK test	0,5455	0,5491	0,4827	0,9137	0,8911	0,9454
CAAR group "Germany" (3 securities)	**-1,2212%*****	0,3183%	0,9734%	0,5163%	-0,1388%	0,7193%
p-value ADJ-BMP test	0,0000	0,9413	0,4776	0,8612	0,7184	0,8895
CAAR group "Germany" (3 securities)	**-1,2212%****	0,3183%	0,9734%	0,5163%	-0,1388%	0,7193%
p-value GRANK test	0,0265	0,8207	0,3254	0,7803	0,6758	0,7737
CAAR group "Italy" (6 securities)	0,3220%	0,8262%	0,8260%	1,4121%	1,4123%	0,8024%
p-value ADJ-BMP test	0,9944	0,8099	0,9615	0,8041	0,4797	0,9655
CAAR group "Italy" (6 securities)	0,3220%	0,8262%	0,8260%	1,4121%	1,4123%	0,8024%
p-value GRANK test	0,8088	0,8940	0,9134	0,7479	0,3669	0,9409
CAAR group "Spain" (3 securities)	**-1,4282%****	-0,5490%	-1,0224%	-0,6708%	-0,1974%	-1,6806%
p-value ADJ-BMP test	0,0374	0,7311	0,5676	0,7581	0,9498	0,5366
CAAR group "Spain" (3 securities)	**-1,4282%***	-0,5490%	-1,0224%	-0,6708%	-0,1974%	-1,6806%
p-value GRANK test	0,0532	0,8361	0,6860	0,8068	0,9625	0,6117

Specifically, the three German financial institutions display an abnormal loss of -1,22% which is significant at least at the 5% confidence level for both kinds of test. The three Spanish firms show a -1,42% loss, which is significant according to both tests at the 10% confidence level at least.

By looking at Figure 9, that shows the evolution of the CAAR for the overall group in the (-3,3) period, we can see how the average negative reaction by the stocks of the sample is more relevant in the (0,0) window.

Figure 9: CAAR graph in the (-3,3) window for the WannaCry systemic event on 12/05/2017.



Once again, to the best of our knowledge, there are no researches in the literature that can be directly compared to ours. The only papers in the literature that analyzed the WannaCry epidemic with the event study methodology are the ones by Roškot et al. (2021) and (Castillo & Falzon, 2018). Both of the studies focused mainly on cybersecurity suppliers and found significant evidence for positive abnormal returns. While the former do not specify the significant event windows the latter observe the significant results in the (1,1) period. Our results show two interesting aspects. The first is that significant results are only observed in the (0,0) window and that they are negative. The second one is that these observations only happen for German and Spanish firms. As an explanation to the first consideration, we suggest the fact that the day of the attack itself, which began at 07:44 UTC[27], the kill switch[28] was accidentally discovered by Marcus Hutchins at 15:03 UTC: this solution was duly announced by newspapers with the caveat that individuals and firms would still need to employ other security measures in order to prevent their systems being infected and compromised (The Independent, 2017). A posteriori, as we have seen in the section dedicated the event itself, we know that in the following weeks a large number of companies was infected regardless of this kill switch. Nevertheless, the markets could have overreacted to this positive news, thus explaining our results, graphically shown by the CAAR graph in Figure 9. An event study on intraday returns, for example hourly ones, could verify if this explanation of the investors' reaction is actually true to the reality of the facts. This explanation is similar to the one that Kollias et al. (2011) use for the speedy recovery of Spanish Exchanges after the 2004 Madrid bombings: in this case the terrorist cell responsible for the bombings was neutralized a few days after the event, this reduction in potential threat caused Spanish exchanges to show a negative, but short-timed, negative reaction. As for the second observation about the large negative returns incurred by shares of German and Spanish companies, we propose the following reasoning. In the day of the attack and the first two days after it, news sources have highlighted the seriousness of the epidemic in a select number of countries. This, in turn, reflects the different ways in which WannaCry hit the various countries of the EU. Regarding Spain, newspapers focused on the dire situations of Telefónica, a multinational telecommunications company, as well as other firms including the power supplier Iberdrola and utility provider Gas Natural (BBC, 2017; El País, 2017; Reuters, 2017). In the latter company, employees were reportedly told to "turn off their computers". In the case of Germany, various sources pointed out at the breach suffered by the Deutsche Ban (International Business Times, 2017; Reuters, 2017; The Telegraph, 2017): even travelers tweeted pictures of the hijacked departure boards showing the ransom demand instead of the train times. Furthermore, Telefonica was the parent company of the German

[27] Universal Coordinated Time, which corresponds to the Greenwich Mean Time (GMT)

[28] A ransomware's kill switch is a code that halts and deletes all programs, documents and log files created by the hackers to eliminate their digital footprint. This component of ransomware is part of what makes malware such a difficult threat to contain and control.

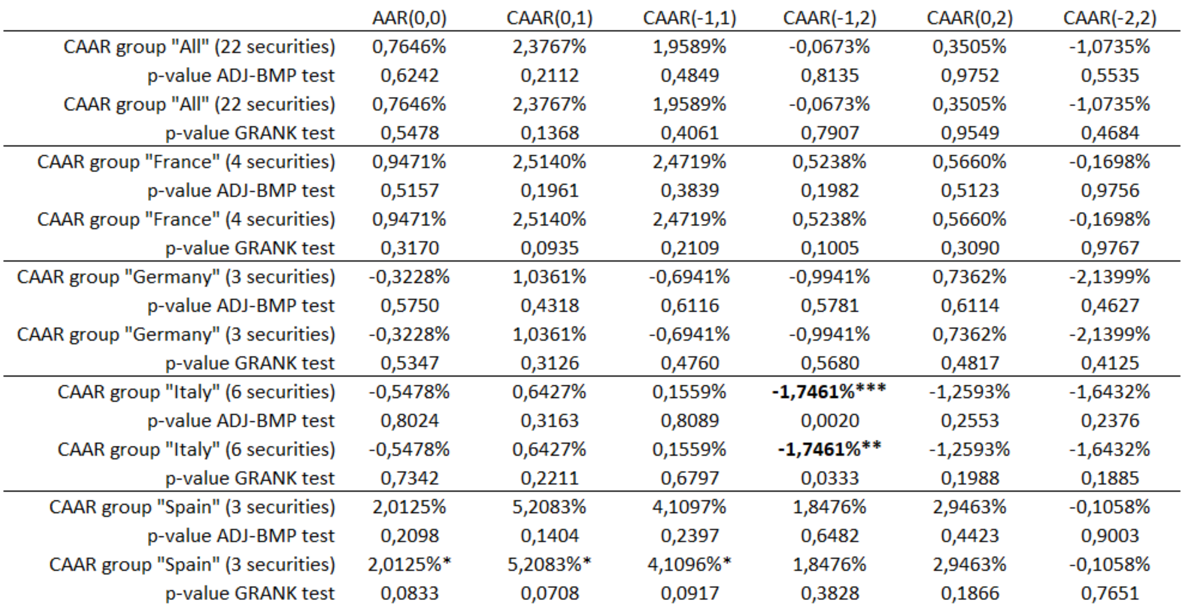
mobile network providers O2 and E-Plus. Because of such reports Spanish and German financial firms could have seen their stock suffer losses together with the rest of these countries' firms. Importantly, no specific breaches were reported in the case of Italian companies. In the instance of France, only Renault is specifically cited as being partially breached. In order to properly verify this explanation another event study would need to be conducted on WannaCry. In particular the study should calculate the abnormal returns for companies of the wider economy in France, Italy, Germany and Spain. As for our results, they could point out at the relevance of the vulnerability of the wider economy when the security of financial institutions is considered. Likely due to this reason, EU lawmakers have provided guidance on security measures for the wider economy and not only for the financial sector, this process being furthered by the NIS2 directive.

In summary we observe significant results for just one time window, the (0,0) one, and for securities of only two of the surveyed EU countries. The fact that Spanish financial companies were also highly sensitive to the announcement of the JP Morgan data breach could point out at the fact that investors perceive those institutions as more vulnerable in situations of heightened cybercrime.

6.2.3 Data breaches following the exploit of SolarWinds, Microsoft and VMware

The third and last systemic event that this dissertation considers is the discovery of the SolarWinds, Microsoft and VMware exploits used to breach US governmental bodies and private companies across the world. Table 10 details the results.

Table 10: Results for the SolarWinds systemic event on 14/12/2020.



	AAR(0,0)	CAAR(0,1)	CAAR(-1,1)	CAAR(-1,2)	CAAR(0,2)	CAAR(-2,2)
CAAR group "All" (22 securities)	0,7646%	2,3767%	1,9589%	-0,0673%	0,3505%	-1,0735%
p-value ADJ-BMP test	0,6242	0,2112	0,4849	0,8135	0,9752	0,5535
CAAR group "All" (22 securities)	0,7646%	2,3767%	1,9589%	-0,0673%	0,3505%	-1,0735%
p-value GRANK test	0,5478	0,1368	0,4061	0,7907	0,9549	0,4684
CAAR group "France" (4 securities)	0,9471%	2,5140%	2,4719%	0,5238%	0,5660%	-0,1698%
p-value ADJ-BMP test	0,5157	0,1961	0,3839	0,1982	0,5123	0,9756
CAAR group "France" (4 securities)	0,9471%	2,5140%	2,4719%	0,5238%	0,5660%	-0,1698%
p-value GRANK test	0,3170	0,0935	0,2109	0,1005	0,3090	0,9767
CAAR group "Germany" (3 securities)	-0,3228%	1,0361%	-0,6941%	-0,9941%	0,7362%	-2,1399%
p-value ADJ-BMP test	0,5750	0,4318	0,6116	0,5781	0,6114	0,4627
CAAR group "Germany" (3 securities)	-0,3228%	1,0361%	-0,6941%	-0,9941%	0,7362%	-2,1399%
p-value GRANK test	0,5347	0,3126	0,4760	0,5680	0,4817	0,4125
CAAR group "Italy" (6 securities)	-0,5478%	0,6427%	0,1559%	**-1,7461%*** **	-1,2593%	-1,6432%
p-value ADJ-BMP test	0,8024	0,3163	0,8089	0,0020	0,2553	0,2376
CAAR group "Italy" (6 securities)	-0,5478%	0,6427%	0,1559%	**-1,7461%****	-1,2593%	-1,6432%
p-value GRANK test	0,7342	0,2211	0,6797	0,0333	0,1988	0,1885
CAAR group "Spain" (3 securities)	2,0125%	5,2083%	4,1097%	1,8476%	2,9463%	-0,1058%
p-value ADJ-BMP test	0,2098	0,1404	0,2397	0,6482	0,4423	0,9003
CAAR group "Spain" (3 securities)	2,0125%*	5,2083%*	4,1096%*	1,8476%	2,9463%	-0,1058%
p-value GRANK test	0,0833	0,0708	0,0917	0,3828	0,1866	0,7651

The first announcements happened on Sunday the 13th in December of 2020, for this reason the study is conducted on the 14th. We observe no CAARs that are significant according to both the ADJ-BMP and GRANK tests for any event window or group of securities, with the exception of Italian securities in the (-1,2) window. As no other significant result is found we attribute the significance of this particular period to exogenous factors. Furthermore, the graph for this systemic event is not presented as no reliable inference can be made.

In summary the results for this last event are interestingly not statistically relevant. There could be many explanations to this outcome. In the instance of the data breach suffered by JP Morgan, we proposed as a possible reason for the negative returns observed in our sample of companies the fear of contagion and cascade effects between financial institutions. Moreover, since this major US bank represents a globally relevant credit institution, the economic consequences of its security breach could have been relevant for the world economy in its entirety. In the case of the present systemic event, no news pointed out at specific financial institutions of any country being directly breached, even if some made use of the Orion software (Business Insider, 2020). For this reason, investors could have forgone the fear of a contagious attack or of important economic downturns. In the case of the WannaCry ransomware outbreak, we have attributed the negative abnormal returns suffered by Spanish and German financial firms to the fact that this cybercrime epidemic heavily hit, or at least seemed to have heavily hit, important companies of other sectors of these two economies. Moreover, a fear of cross-sector contagion could also have been at play in the eyes of investors.

The news for the SolarWinds systemic event initially focused on the breach suffered by American governmental entities: this fact removes from this systemic event all of the factors that we have proposed for the previous two events as possible catalysts for negative effects on European financial institutions. Another relevant aspect of the SolarWinds exploit is that no news reported any serious interruptions in US governmental activities, or even business operations of US companies. It seems as this cybercrime surge was interpreted by newspapers, and subsequently investors worldwide, as an act of espionage financed by a nation state, presumably Russia, without any aim of economic disruption (Reuters, 2020; The Financial Times, 2020). The costs caused by this attack were estimated years after the initial announcement of Dember 2020. The Congressional Quarterly estimates that the overall costs associated with the attack could amount to 10s of billions of US dollars (CQ Roll Call, 2021). All those costs however are due to cleanup efforts regarding the compromised software and not due to other factors such as the loss of confidential data or business operations downtime.

In sum the absence of relevant results for this systemic event can be attributed to multiple reasons. All of them point to the fact that the attack was probably an espionage effort directed against the US government, and thus it didn't entail, according to investors, any negative effect for European financial institutions.

6.2.4 A discussion on the second and third hypotheses

Now that we have discussed in detail the results of each systemic event it is possible to comprehensively address the two hypotheses that we developed for them.

The first null hypothesis H_0^{III} states that the share price of a financial institution is not significantly affected by systematic cyberattacks. While this statement could not be rejected in view of the results on the SolarWinds exploit, the outputs of the JP Morgan Data Breach and the WannaCry ransomware outbreak go in the opposite direction. As we haven't observed significant abnormal returns in every one of the three systematic events, we cannot safely reject this hypothesis. However, we reach some interesting conclusions in regard to the first and second events. As a result of the attack on JP Morgan on the 27th of August 2014, we observed significant negative CAARs for the overall group of securities as well as certain country wide groups, namely the Italian and Spanish ones. We attribute the overall results to the possible fear by investors of a propagation of the cyberattack between financial institutions. In regards to the WannaCry epidemic, first announced on the 12th of May 2017, we observed significant negative CAARs not for the overall sample, but just for the German and Spanish security groups. The third event, that consisted in the breach of US governmental authorities on the 13th of December 2020, although not having any significant effect with respect to European financial firms, still solicited some peculiar observations. In particular we attribute this absence of reaction to the fact that the attacks did not compromise the data availability of any financial institution. Thus, investors were not concerned by a cybercrime wave presumably only focused on espionage against the US government. By considering the three events as a whole we can also put forward Gordon et al.'s (2011) reasoning, in order to explain the decreasingly significant negative abnormal returns that we observe in 2014, 2017 and 2020. According to Gordon et al., as time goes on, investors get more and more used to the announcement of serious data breaches and cyberattacks, thus with each repeated announcement they become less sensitive to the negative news. Instead as time and technology progress, markets become more confident in the ability of companies to successfully meet the cybersecurity challenges that hackers pose them.

The second null hypothesis that we aimed to disprove, H_0^{IV}, states that in the case of systemic attacks, financial institutions based in different EU countries do not react differently with respect to the country in which they are based. As in the case of H_0^{III}, we cannot safely reject this hypothesis because only in two instances out of three we observed significant reactions that varied across the EU countries present in the sample. Once again, some interesting conclusions still emerged. For the JP Morgan systemic event we observe significant and negative reactions by Spain and Italy's financial firms, which are in contrast with France and Germany's firms negative but not significant reactions. We attribute these observations to the increased vulnerability of European institutions based in the Southern countries, caused by the Eurozone's crisis and subsequent deflation observed in the month of August in both Italy and Spain. As per the WannaCry systemic event, we only find significant negative abnormal returns in the stocks of German and Spanish financial companies. We attribute these results to WannaCry's more relevant and marked disruptions of the economies of these two countries. In contrast the news didn't focus as much on Italian or French companies being breached and affected by the ransomware epidemic in the first days after the outbreak.

CONCLUSIONS

Thanks to our study of direct cyberattacks, we found that the involved European Institutions showed a negative and significant reaction in their share prices after their announcement. The Cumulative Average Abnormal Returns, measured on the whole sample, were significant for the (0,1), (-1,2) and (0,2) event windows. The results were significant according to both the parametric ADJ-BMP test and the non-parametric GRANK test. In particular a European financial institution that is directly targeted by a cyberattack, observes a loss in its share price of -0,99% in the day of the attack. This loss increases in the longer windows of (-1,2) and (0,2) respectively to -1,55% and -1,71%. These abnormal losses are consistent with most of the literature, although they are more in line with more recent research, as older research shows greater negative effects. By building on the consideration of Gordon et. (2011) we suggested that this implication could be due to the decreased sensitivity of investors with respect to security breach announcements. On another note, none of our two symmetric windows, (-1,1) and (2,2), showed significant results. Some papers attributed such results to the presence of insider trading in the days prior to the event. In our case we found no such evidence in favor of insider trading. At most our results allowed for the presence of leaks of the news on cyberattacks in the day preceding the attack.

When we divided the sample of direct cyberattacks into confidential and non-confidential attacks, we had some interesting implications: we found that only non-confidential attacks are significant. In particular they are so at in the (0,0), (-1,2) and (0,2) periods. Once again none of our two symmetric windows, (-1,1) and (2,2), showed significant results. We attributed our results on the non-significant impact of confidential attacks to the fact that availability and integrity of information may have become more important for investors than their confidentiality in recent times. This explanation is in line with the ones by Abshishta et al. (2017) and Arcuri et al. (2018). Notably, both the DORA and the NIS2 newer legislative acts take important steps towards to assurance of continuity in daily operations, when it comes to the EU's financial firms.

The outputs of our studies on systemic events were overall less significant, but not less interesting. Unfortunately, no previous relevant literature exists for this part of our research, so no comparisons with exact counterparts by other authors were possible. As a result of the attack on JP Morgan in 2014, we observed significant negative CAARs for the overall group of securities in the (0,1) and (0,2) windows. We attributed these results to a possible perceived fear by investors, when it comes to the propagation of the cyberattacks through contagion or cascading effects between financial institutions. We also observed that certain CAAR groups, namely the Italian and Spanish ones, revealed significant losses unlike their German and French counterparts. We explained this peculiarity in light of the Eurozone's crisis which heavily impacted the economies of Southern Europe in 2014. When the JP Morgan event was studied with respect to the event date in which the ultimate outcome of the attack was revealed by newspapers, no significant effects were registered. In our opinion, the fear of propagation that we mentioned for the first day, did not play a relevant role in this second instance. In regards to the WannaCry epidemic of 2017 we observed significant negative CAARs not for the overall sample, but just for the German and Spanish security groups in the (0,0) period. We explained this asymmetry with WannaCry's different degree of intrusion in the economies of the EU: while news highlighted the fact that multiple important German and Spanish organizations were breached in this surge of cybercrime, no major Italian or French company was hit by such attacks, with the notable exception of Renault. In addition, the discovery of a kill-switch on the same day of the event, could explain the limitation of significant effects to the (0,0) window. The third event, that consisted in the breach of US governmental authorities in 2020, resulted in no significant abnormal returns for any CAAR group in any of the event windows. We presumed that European investors were not preoccupied with a cybercrime wave reportedly merely focused on espionage against the US government. By considering the three events we once again made use of Gordon et al.'s (2011) reasoning, in order to explain the decreasingly significant negative abnormal returns that we observed in 2014, 2017 and 2020.

During the dissertation we have recognized the possible limitations of our study. The most important one is that our analysis employed a sample of events that is small when compared to the literature. Even if our non-parametric tests should have taken care of such a characteristic, in the case of another similar study we suggest dedicating the necessary effort for the creation of a wider sample of events. A sample of this kind could also allow for a second step, namely the regression of the abnormal returns of firms' stocks on a series of variables, as seen in Gatzlaff & McCullough (2010). For instance, dummies associated with the country in which the firm is headquartered could give a clearer insight into the perceived vulnerability of each country's financial sectors. Moreover, our study, except for its inclusion in significance tests, forgoes the analysis of the variance of returns during the event window. Other analyses, such as the one by Colivicchi & Vignaroli (2019), go as far as modeling the heteroskedasticity associated with security breaches. As an expansion to our study, we suggest the use of a similar sample of companies and events for the study of the variance of returns. In this way, in addition to the direction of the stocks' reaction, researchers could get insight on the amount of volatility that each event induces. A high level of volatility without significant abnormal returns in either direction could suggest that investors are unsure on how to react to news of security breaches. Lastly, the peculiar results that we observed for the WannaCry incident suggest the employment of hourly, instead of daily returns. Such a study could provide a better understanding of the intraday reactions of financial institutions to such a systemic event. We also suggest an event study of WannaCry's effect on firms of other sectors: this way it can be understood if the effect on financial institutions shares is correlated with the effect on other companies of the same country.

In sum our study demonstrated that European financial institutions were perceived by markets as vulnerable to direct and systemic attacks. In particular European institutions seemed more vulnerable with respect to attacks that compromise the availability of information, instead of their integrity. In addition, our analysis on systemic events showed that reactions varied depending on the specific nature of each event. Moreover, depending on the event, the financial sectors the four surveyed EU countries presented different reactions in terms of market capitalization losses. Interestingly, fear of contagion and cascade effects could have explained investors' reactions resulting from the attack on JP Morgan. On the other hand, when only US governmental agencies were breached in the SolarWinds event, no such fear of contagion was shown by the markets.

REFERENCES

Bibliography

Abshishta, A., Nieuwenhuis, B. & Joosten, R., 2017. Analysing the Impact of a DDoS Attack Announcement on Victim Stock Prices. *25th Euromicro International Conference on Parallel, Distributed and Network-based Processing,* pp. 354-362.

Akyazi, U., Van Eeten, M. & Gañán, C. H., 2021. Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum. *20th Workshop on the Economics of Information Security.*

Alam, S., 2022. *Cybersecurity: Past, Present and Future.* Adana: Adana Alparsalan Turkes Science and Technology University.

Algarni, A. M. & Malaiya, Y. K., 2016. A consolidated approach for estimation of data security breach costs. *2nd International Conference on Information Management,* pp. 26-39.

Arcuri, M. C., Brogi, M. & Gandolfi, G., 2018. The effects of cyberattacks on stock returns. *Corporate Ownership & Control,* 15(2), pp. 70-83.

Bendovschi, A., 2015. Cyber-Attacks - Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance,* 28(1), pp. 24-31.

Biju, J. M., Gopal, N. & Prakash, A. J., 2019. Cyberattacks and their different types. *International Research Journal of Engineering and Technology,* 6(3).

Boehmer, E., Masumeci, J. & Poulsen, A. B., 1991. Event-study methodology under conditions of event-induced variance. *Journal of Financial Economics,* 30(2), pp. 253-272.

Buzan, B., Waever, O. & de Wilde, J., 1998. *Security: A New Framework fo Analysis.* I ed. London: Lynne Rienner Publishers .

Caldewll, T., 2014. The true cost of being hacked. *Computer Fraud & Security,* Issue 6, pp. 8-13.

Campbell, J. Y., W. Lo, A. & MacKinlay, A., 1997. *The Econometrics of Financial Markets.* II ed. Princeton: Princeton University Press.

Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer security,* pp. 431-448.

Cashell, B., Jackson, W. D., Jickling, M. & Webel, B., 2004. *The Economic Impact of Cyber-Attacks,* s.l.: US Congressional Research Service.

Castillo, D. & Falzon, J., 2018. An analysis of the impact of Wannacry cyberattack on cybersecurity stock returns. *Review of Economics and Finance,* 3(13), pp. 93-100.

Cavasoglu, 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), pp. 70-104.

Chee Pung, N. et al., 2018. Contemporary Event Study Test: Event-Induced Variance and Cross Correlation Among Abnormal Returns in Dividend. *International Journal of Economics and Management,* 12(2), pp. 327-337.

Chen, T. M. & Robert, J., 2004. The evolution of viruses and worms. *Computer Science.*

Chng, S., Yu Lu, H., Kumar, A. & Yau, D., 2022. Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports,* Issue 5.

Cipriani, M., Goldberg, L. S. & La Spada, G., 2023. Financial Sanctions, SWIFT, and the Architecture of the International Payment System. *Journal of Economic Perspectives,* 37(1), p. 31–52.

CLUSIT - Associazione Italiana per la Sicurezza Informatica, 2023. *Rapporto CLUSIT 2023 sulla sicurezza ICT in Italia,* Milano.

Colivicchi, I. & Vignaroli, R., 2019. Forecasting the Impact of Information Security Breaches on Stock Market Returns and VaR Backtest. *Journal of Mathematical Finance,,* Issue 9, pp. 402-454.

Craigen, D., Diakun-Thibault, N. & Purse, R., 2014. Defining Cybersecurity. *Technology Innovation Management Review,* 10(4), pp. 13-21.

De Bandt, O. & Hartmann, P., 2000. Systemic Risk: a Survey. *European central bank Working Paper Series,* Issue Working Paper No. 35.

Depository Trust & Clearing Corporation, 2023. *Systemic risk barometer survey - 2023 risk forecast.*

Dilek, S., Çakır, H. & Aydın, M., 2015. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications,* 6(1), pp. 68-02.

Ekenberg, L., Oberoi, S. & Orci, I., 1995. A Cost Model for Managing Information Security Hazards. *Computers and Security,* 14(8).

El Ghoul, S., Guedhami, O., Mansi, S. A. & Sy, O., 2022. Event studies in international finance research. *Journal of International Business Studies,* Volume 54, pp. 344-364.

European Commission, 2015. Directive 2015/2366 On payment services in the internal market. *Official Journal of the European Union,* Issue L 337/35.

European Commission, 2016. Directive 2016/1148 Concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union,* Issue L 194/1.

European Commission, 2022. Directive 2022/2555 On measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union,* Issue L 333/80.

European Parliament, 2009. Directive 2009/110/EC On the taking up, pursuit and prudential supervision of the business of electronic money institutions. *Official Journal of the European Union,* Issue L 267/7.

European Parliament, 2009. Directive 2009/138/EC On the taking-up and pursuit of the business of Insurance and Reinsurance. *Official Journal of the European Union,* Issue L 335/1.

European Parliament, 2013. Regulation 575/2013 On prudential requirements for credit institutions and investment firms. *Official Journal of the European Union,* Issue L 176/1.

European Parliament, 2016. Regulation 2016/679 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union,* 4 May.Issue L 119.

European Parliament, 2022. Regulation 2022/2554 On digital operational resilience for the financial sector. *Official Journal of the European Union,* Issue L 333/1.

European Systemic Risk Board, 2021. ESRB/2021/17 On a pan-European systemic cyber incident coordination framework for relevant authorities. *Official Journal of the European Union,* Issue C 134/1.

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

Fama, E. F., Fisher, L. J. M. C. & Roll, R., 1969. The adjustment of stock prices to new information. *International Economic Review,* Issue 10, pp. 1-21.

Fama, E. F. & French, K. R., 1993. Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics,* Volume 33, pp. 3-56.

Fama, E. F. & French, K. R., 2004. The Capital Asset Pricing Model: Theory and Evidence. *Journal of Economic Perspectives,* 18(3), pp. 25-46.

Fedele, A. & Roner, C., 2022. Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys,* 36(1), pp. 157-187.

Ferbrache, D., 2016. *Bangladesh hack illustrates rising sophistication of attacks,* London: KPMG.

Fung, C. C., Roumani, M. A. & Wong, K. P., 2013. A proposed study on economic impacts due to cyber attacks in Smart Grid: A risk based assessment. *2013 IEEE Power & Energy Society General Meeting,* pp. 1-5.

Furdui, C. & Șfabu, D. T., 2023. The European banks after the shock of the Russian invasion of 2022: an event study approach. *Sciendo,* Volume 68, pp. 62-77.

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

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

Geer, D., Jardine, E. & Leverett, E., 2020. On market concentration and cybersecurity risk. *Journal of Cyber Policy,* 5(1), p. 9–29.

Gordon, L. A., Loeb, M. P. & Zhou, L., 2011. The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security,* 1(19), pp. 33-56.

Guembe, B. et al., 2022. The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence,* 36(1).

Hoesli, M., Milcheva, S. & Moss, A., 2020. Is Financial Regulation Good or Bad for Real Estate Companies? – An Event Study. *The Journal of Real Estate Finance and Economics,* Issue 61, p. 369–407.

Horn, P., 2006. It's Time to Arrest Cyber Crime. *Bloomberg*, 2 Febbraio.

Hovav, A. & D'Arcy, J., 2003. The impact of Denial-of-Service attack announcements on the market value of firms. *Risk Management and Insurance Review,* 6(2), pp. 97-121.

Hovav, A. & D'Arcy, J., 2004. The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security,* 13(3), pp. 31-40.

Huddleston, J., Ji, P., Bhunia, S. & Cogan, J., 2021. How VMware Exploits Contributed to SolarWinds Supply-chain Attack. *International Conference on Computational Science and Computational Intelligence (CSCI).*

Kannan, K., R. J. & Sridhar, S., 2007. Market reactions to information security breach announcements: an empirical analysis. *International Journal of Electronic Commerce,* Issue 12, p. 69–91.

Kolari, J. W. & Pynnönen, S., 2010. Event Study Testing with Cross-sectional Correlation of Abnormal Returns. *The Review of Financial Studies,* 23(11), p. 3996–4025.

Kolari, J. W. & Pynnönen, S., 2011. Nonparametric rank tests for event studies. *Journal of Empirical Finance,* Volume 18, p. 953–971.

Kollias, C., Papadamou, S. & Stagiannis, A., 2011. Terrorism and capital markets: The effects of the Madrid and London bomb attacks. *International Review of Economics and Finance,* Issue 20, pp. 532-541.

Kopp, E., Kaffenberger, L. & Wilson, C., 2017. Cyber Risk, Market Failures, and Financial Stability. *IMF Working paper,* Issue WP/17/185.

Kothari, S. P. & Warner, J. B., 2007. Econometrics of Event Studies. *Handbook of Corporate Finance: Empirical Corporate Finance,* Volume 1, pp. 3-36.

Krüger, P. S. & Brauchle, J.-P., 2021. The European Union, Cybersecurity, and the Financial Sector: A Primer. *Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System",* Issue 9.

Kruschwitz, L. & Löffler, A., 2006. *Discounted Cash Flow: a theory of the valuation of firms.* West Sussex: John Wiley & Sons Ltd.

Kuo, C. C., Yu-Kai, G. & Shih-Cheng, L., 2020. The Effect of Data Theft on a Firm's Short-Term and Long-Term Market Value. *MPDI Journals - Mathematics,* 8(208).

Liargovas, P. & Repousis, S., 2010. The Impact of Terrorism on Greek Banks'Stocks: An Event Study. *International Research Journal of Finance and Economics,* Issue 51.

Loipersberger, F., 2018. The effect of supranational banking supervision on the financial sector: Event study evidence from Europe. *Journal of Banking and Finance,* Issue 91, p. 34–48.

Lukasik, S., 2010. Why the Arpanet Was Built. *IEEE Annals of the History of Computing,* 33(3), pp. 4-21.

Lyon, J. D., Barber, B. M. & Tsai, C.-L., 1999. Improved Methods for Tests of Long-Run Abnormal Stock Returns. *The Journal of Financa,* Volume 54, pp. 165-201.

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

Manky, D., 2013. Cybercrime as a service: a very modern business. *Computer Fraud & Security,* Issue 6, pp. 9-13.

Marotta, A. et al., 2017. Cyber-insurance survey. *Computer Science Review,* Volume 24, pp. 35-61.

Mones, D. & Taqi, M., 2023. *Europe's 50 largest banks by assets*: S&P Global.

Montanari, F., 2012. *GI Vocabolario della lingua greca.* II ed. Milano: Hoepli.

Nachenberg, C., 1997. Computer virus-antivirus coevolution. *Communications of the ACM,* 40(1), pp. 46-51.

Nguyen, P. A. & Wolf, M., 2023. A note on testing AR and CAR for event studies. *University of Zurich - Department of Economics,* Issue Working Paper No. 425.

Obi, P. C., 2007. Market sector reactions to 9-11: an event study. *Electronic copy available at: http://ssrn.com/abstract=1543360,* 1(1).

Orman, H., 2003. The Morris worm: a fifteen-year perspective. *IEEE Security & Privacy ,* 1(5), pp. 35-43.

Pacicco, F., Vena, L. & Venegoni, A., 2018. Event study estimations using Stata: The estudy command. *The Stata Journal,* 18(2), p. 461_476.

Pacicco, F., Vena, L. & Venegoni, A., 2021. From common to firm-specific event dates: A new version of the estudy command. *The Stata Journal,* 21(1), pp. 141-151.

Pandey, D. K. & Kumari, V., 2021. Event study on the reaction of the developed and emerging stock markets to the 2019-nCoV outbreak. *International Review of Economics and Finance,* Issue 7, pp. 467-483.

Park, W. H., 2010. A Study on Risk Analysis and Assessment of Damages to Cyber Attack. *2010 International Conference on Information Science and Applications.*

Pastorello, S., 2001. *Rischio e rendimento: teoria finanziaria e applicazioni econometriche.* I ed. Bologna: il Mulino.

Patell, J. M., 1976. Corporate Forecasts of Earnings Per Share and Stock Price Behavior: Empirical Test. *Journal of Accounting Research,* 14(2), pp. 246-276.

Ramkumar, J., Joon Ho, L. & JRishika, R., 2018. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing,* Issue 82, p. 85–105.

Repousis, S., 2016. Abnormal stock returns in Greece during the Cypriot banking crisis. *Journal of Money Laundering Control,* 19(2), pp. 122-129.

Roškot, M., Wanasika, I. & Kroupova, Z. K., 2021. Cybercrime in Europe: surprising results of an expensive lapse. *Journal of Business Strategy,* 42(2), pp. 91-98.

Ruthberg, Z. G. & McKenzie, R. G., 1977. *Audit and evaluation of computer security,* Washington D.C.: National Bureau of Standards.

Salotti, V., 2009. Multi-country event study methods. *PhD Theis - Università di Bologna.*

Saravia, F., 2020. *Banking in Europe: EBF Facts & Figures 2021,* Brussels: European baning Federation.

Sharpe, W. F., 1963. A Simplified Model for Portfolio Analysis. *Management Science,* 9(2), pp. 277-293.

Simmons, C. et al., 2009. *AVOIDIT: A Cyber Attack Taxonomy,* Memphis: Department of Computer Science - University of Memphis.

Sorokina, n., Booth, D. E. & Thornton, J. H. J., 2013. Robust Methods in Event Studies: Empirical Evidence and Theoretical Implications. *Journal of data science,* Volume 11, pp. 575-606.

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

Tweneboah-Kodua, S., Atsu, Francis & Buchanan, W., 2018. Impact of cyberattacks on stock performance: a comparative study. *Information & Computer Security,* 26(5), pp. 637-652.

Uma, M. & Padmavathi, G., 2013. A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security,* 15(5), pp. 390-396.

Wang, P., D'Cruze, H. & Wood, D., 2019. Economic costs and impacts of business data breaches. *Issues in Information Systems,* 20(2), pp. 162-71.

Ware, W. H., 1970. *Security Controls for Computer Systems,* Santa Monica: RAND Corporation.

Welburn, J. W. & Strong, A. M., 2022. Systemic Cyber Risk and Aggregate Impacts. *Risk Analysis,* 42(8).

Wiener, N., 1961. *Cybernetics: Or Control and Communication in the Animal and the Machine.* II ed. Cambridge: MIT Press.

Williams, J. B., 1938. *The Theory of Investment Value.* 2014 ed. Hawthorne: BN Publishing.

Wolff, J. & Lehr, W., 2017. Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data. *SSRN Electronic Journal.*

Yousaf, I., Patel, R. & Yarovaya, L., 2022. The reaction of G20+ stock markets to the Russia–Ukraine conflict''black-swan'' event: Evidence from event study approach. *Journal of Behavioral and Experimental Finance,* Issue 35.

Webliography

BBC, 2014. *Eurozone crisis: The grim economic reality.*
Available at: https://www.bbc.com/news/world-europe-28785700

BBC, 2017. *Ransomware cyber-attack: Who has been hardest hit?.*
Available at: https://www.bbc.com/news/world-39919249

Bloomberg, 2020. *At Least 200 Victims Identified in Suspected Russian Hacking.*
Available at: https://www.bloomberg.com/news/articles/2020-12-19/at-least-200-victims-identified-in-suspected-russian-hacking

Business Insider, 2020. *These big firms and US agencies all use software from the company breached in a massive hack being blamed on Russia.*
Available at: https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12?r=US&IR=T

Carnegie Endowment for International Peace, 2023. *Timeline of Cyber Incidents Involving Financial Institutions.*
Available att
https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

CBS News, 2021. *Jerome Powell: Full 2021 60 Minutes interview transcript.*
Available at: https://www.cbsnews.com/news/jerome-powell-full-2021-60-minutes-interview-transcript/

Center for Strategic and International Studies, 2023. *Significant Cyber Incidents.*
Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

CMS, 2023. *GDPR Enforcement Tracker.*
Available at: https://www.enforcementtracker.com/

CNBC, 2014. *JPMorgan and other banks struck by cyberattack.*
Available at: https://www.cnbc.com/2014/08/27/fbi-probes-possible-hack-at-jpmorgan-report.html

Corriere della Sera, 2014. *JpMorgan attaccata dagli hacker violati 80 milioni di conti correnti.*
Available at: https://www.corriere.it/economia/14_ottobre_03/jpmorgan-conti-correnti-80milioni-clienti-attaccati-hacker-a7bf9b56-4acb-11e4-9829-df2f785edc20.shtml

CQ Roll Call, 2021. *Cleaning up SolarWinds hack may cost as much as $100 billion.*
Available at: https://rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/

ECB Banking Supervision, 2022. *SSM supervisiory priorities fo 2023-2025.*
Available at:
https://www.bankingsupervision.europa.eu/banking/priorities/html/ssm.supervisory_priorities202212~3a1e609cf8.en.html

El País, 2017. *Major Spanish firms among victims of massive global cyber attack.*
Available at:
https://english.elpais.com/elpais/2017/05/12/inenglish/1494588595_636306.html#

European Commission, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

EUROPOL, 2022. *EU Policy Cicle - EMPACT.*
Available at: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

Federal Reserve, 2024. *Federal Reserve Statistical Release - Large Commercial Banks.*
Available at: https://www.federalreserve.gov/releases/lbr/current/default.htm

Forbes, 2017. *An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak.*
Available at: https://www.forbes.com/sites/leemathews/2019/05/09/russian-hackers-breach-antivirus-makers/?sh=707176a31db2

Forbes, 2023. *Cybersecurity Trends & Statistics For 2023: What You Need To Know.*
Available at: https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=40e2a0f019db

Fortinet, 2023. *Cyberglossary - CIA Triad.*
Available at: https://www.fortinet.com/resources/cyberglossary/cia-triad

IBM, 2023. *Cost of a Data Breach Report 2023.*
Available at: https://www.ibm.com/reports/data-breach

Il Sole 24 Ore, 2014. *Il ministro Padoan: «L'economia italiana peggiora, la velocità delle riforme è tutto».*
Available at: https://st.ilsole24ore.com/art/notizie/2014-08-06/l-economia-italiana-peggiora-velocita-riforme-e-tutto-063558.shtml?uuid=ABVZ1lhB

International Business Times, 2017. *WannaCry: List of major companies and networks hit by ransomware around the globe.*
Available at: https://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587

Kasperky, 2017. *What is WannaCry ransomware?.*
Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

McEvoy, O., 2022. *Percentage share of the European Union's Gross Domestic Product (GDP) in 2022, by member state.*
Available at: https://www.statista.com/statistics/1373419/eu-gdp-percentage-share-member-state-2022/

Mueller, G. B. et al., 2023. *Cyber Operations during the Russo-Ukrainian War.*
Available at: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

National Institute of Standards and Technology, 2023. *Computer Security Resource Center.*
Available at: https://csrc.nist.gov/glossary/term/cyberspace

NPR, 2022. *U.S. Says North Korea 'Directly Responsible' For WannaCry Ransomware Attack.*
Available at: https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

Oxford University Press, 2023. *Oxford English Dictionary.*
Available at: https://www.oed.com/dictionary/cybersecurity_n?tab=etymology

Privacy Rights Clearinghouse, 2023. *Data Breach Chronology.*
Available at: https://privacyrights.org/data-breaches

Reuters, 2017. *German rail operator affected by global cyber attack.*
Available at: https://www.reuters.com/article/idUSKBN1890DM/

Reuters, 2017. *Telefonica, other Spanish firms hit in "ransomware" attack.*
Available at: https://www.reuters.com/article/idUSKBN1881US/

Reuters, 2020. *Suspected Russian hackers spied on U.S. Treasury emails - sources.*
Available at: https://www.reuters.com/world/us/suspected-russian-hackers-spied-us-treasury-emails-sources-2020-12-13/

Reuters, 2020. *Suspected Russian hackers spied on U.S. Treasury emails – sources.*
Available at: https://www.reuters.com/article/idUSKBN28N0PH/

Seong, J. et al., 2022. *Global flows: The ties that bind in an interconnected world.*
Available at: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/global-flows-the-ties-that-bind-in-an-interconnected-world

Société Générale, 2023. *Newsroom.*
Available at: https://www.societegenerale.com/en/news/newsroom/kerviel-case

Statista Research Department, 2023. *Number of monetary financial institutions (MFIs) in the Europe Union as of October 2023, by type.*
Available at: https://www.statista.com/statistics/1111010/european-union-number-monetary-financial-institutions-by-type/

Steve Evans Ltd, 2021. *Europe's 30 largest insurance companies.*
Available at: https://www.reinsurancene.ws/largest-30-european-insurers/

Symantec, 2017. *What you need to know about the WannaCry Ransomware.*
Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack

The Financial Times, 2020. *US orders emergency action after huge cyber security breach.*
Available at: https://www.ft.com/content/3a635e09-221c-49af-a582-97bc4e803747

The Financial Times, 2020. *What do we know about the SolarWinds hack?.*
Available at: https://www.ft.com/content/3558b9b6-465f-4338-9d66-70b2fbe8f900

The Guardian, 2014. *JP Morgan Chase reveals massive data breach affecting 76m households.*

Available at: https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach

The Guardian, 2017. *What is WannaCry ransomware and why is it attacking global computers?.*
Available at: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20

The Independent, 2017. *Global cyber attacks could trigger economic losses on par with catastrophic natural disasters.*
Available at: https://www.independent.co.uk/news/business/news/global-cyber-attacks-economic-losses-natural-disasters-catastrophic-petya-wannacry-cyence-a7844586.html

The Independent, 2017. *NHS cyber attack: Analyst, 22, discovers WannaCry ransomware's hidden kill switch 'completely by accident'.*
Available at: https://www.independent.co.uk/tech/nhs-cyber-attack-ransomware-wannacry-accidentally-discovers-kill-switch-domain-name-gwea-a7733866.html

The independent, 2020. *Cyber attacks could cause financial crisis, says ECB chief Christine Lagarde.*
Available at: https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html

The New York Times, 2014. *JPMorgan and Other Banks Struck by Hackers.*
Available at: https://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html

The New York Times, 2014. *JPMorgan Chase Hacking Affects 76 Million Households.*
Available at: https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0

The New York Times, 2020. *Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit.*
Available at: https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

The Telegraph, 2017. *Cyber attack hits German train stations as hackers target Deutsche Bahn.*
Available at: https://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/

The Wall Street Journal, 2014. *Target Breach Began With Contractor's Electronic Billing Link.*
Available at: https://www.wsj.com/articles/target-breach-began-with-contractor8217s-electronic-billing-link-1391731112

UBS, 2022. *The History of Digital Banking.*
Available at: https://www.ubs.com/ch/en/wealth-management/womens-wealth/magazine/articles/history-of-digital-banking.html

Yahoo, 2023. *Yahoo Finance.*
Available at: https://finance.yahoo.com/

Appendix A: Stata commands

Commands employ tickers for the identification of stocks. In the study of direct events some companies have been the subject of multiple events, for this reason their tickers are accompanied by numbers in such cases.

- Command for direct events with parametric test: “estudy UCG ABN INGA CS BOV UCG1 EDEN BMPS CS1 CBK DB OPBK BIRG BMPS1 CBK1 DB1 INGA1 BPE BMPS2 FBK ISP BPSO, datevar(date) evdate(Security Event) dateformat(DMY) modtype(SIM) indexlist(MKT) diagnosticsstat(KP) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) decimal(4) price graph(-3 3)”

- Command for direct events with non-parametric test: “estudy UCG ABN INGA CS BOV UCG1 EDEN BMPS CS1 CBK DB OPBK BIRG BMPS1 CBK1 DB1 INGA1 BPE BMPS2 FBK ISP BPSO, datevar(date) evdate(Security Event) dateformat(DMY) modtype(SIM) indexlist(MKT) diagnosticsstat(GRANK) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) decimal(4) price”

- Command for direct events with parametric test and confidential and non-confidential groups: “estudy UCG ABN INGA CS BOV UCG1 EDEN BMPS CS1 CBK DB OPBK BIRG BMPS1 CBK1 DB1 INGA1 BPE BMPS2 FBK ISP BPSO (UCG UCG1 BIRG BMPS1 DB1 CBK1 INGA1) (ABN INGA CS BOV EDEN BMPS CS1 DB CBK OPBK BPE BMPS2 FBK ISP BPSO), datevar(date) evdate(Security Event) dateformat(DMY) modtype(SIM) indexlist(MKT) diagnosticsstat(KP) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) decimal(4) price”

- Command for direct events with parametric test and confidential and non-confidential groups: “estudy UCG ABN INGA CS BOV UCG1 EDEN BMPS CS1 CBK DB OPBK BIRG BMPS1 CBK1 DB1 INGA1 BPE BMPS2 FBK ISP BPSO (UCG UCG1 BIRG BMPS1 DB1 CBK1 INGA1) (ABN INGA CS BOV EDEN BMPS CS1 DB CBK OPBK BPE BMPS2 FBK ISP BPSO), datevar(date) evdate(Security Event) dateformat(DMY) modtype(SIM) indexlist(MKT) diagnosticsstat(GRANK) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) decimal(4) price”

- Command for JP Morgan systemic event on 28/08/2014 with parametric test: “estudy ACA ALV BAMI BBVA BIRG BMPS BNC BNP BPE CBK CS DBK EBS G GLE INGA ISP KBC NDA SAB TPEIR UCG (ACA BNP CS GLE) (ALV CBK DBK) (BAMI BMPS BPE G ISP UCG) (BBVA BNC SAB), datevar(date) evdate(28082014) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) dateformat(DMY) indexlist(MKT) price diagn(KP) graph(-3 3) decimal(4) suppress(ind)”

- Command for JP Morgan systemic event on 28/08/2014 with non-parametric test: “estudy ACA ALV BAMI BBVA BIRG BMPS BNC BNP BPE CBK CS DBK EBS G GLE INGA ISP KBC NDA SAB TPEIR UCG (ACA BNP CS GLE) (ALV CBK DBK) (BAMI BMPS BPE G ISP UCG) (BBVA BNC SAB), datevar(date) evdate(28082014) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) dateformat(DMY) indexlist(MKT) price diagn(GRANK) decimal(4) suppress(ind)”

- Command for JP Morgan systemic event on 03/10/2014 with parametric test: “estudy ACA ALV BAMI BBVA BIRG BMPS BNC BNP BPE CBK CS DBK EBS G GLE INGA ISP KBC NDA SAB TPEIR UCG (ACA BNP CS GLE) (ALV CBK DBK) (BAMI BMPS BPE G ISP UCG) (BBVA BNC SAB), datevar(date) evdate(28082014) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) dateformat(DMY) indexlist(MKT) price diagn(KP) decimal(4) suppress(ind)”

- Command for JP Morgan systemic event on 03/10/2014 with non-parametric test: “estudy ACA ALV BAMI BBVA BIRG BMPS BNC BNP BPE CBK CS DBK EBS G GLE INGA ISP KBC NDA SAB TPEIR UCG (ACA BNP CS GLE) (ALV CBK DBK) (BAMI BMPS BPE G ISP UCG) (BBVA BNC SAB), datevar(date) evdate(28082014) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) dateformat(DMY) indexlist(MKT) price diagn(GRANK) decimal(4) suppress(ind)”

- Command for WannaCry systemic event with parametric test: “estudy ACA ALV BAMI BBVA BIRG BMPS BNC BNP BPE CBK CS DBK EBS G GLE INGA ISP KBC NDA SAB TPEIR UCG (ACA BNP CS GLE) (ALV CBK DBK) (BAMI BMPS BPE G ISP UCG) (BBVA BNC SAB), datevar(date) evdate(12052017) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) dateformat(DMY) indexlist(MKT) price diagn(KP) graph (-3 3) decimal(4) suppress(ind)”

- Command for WannaCry systemic event with non-parametric test: “estudy ACA ALV BAMI BBVA BIRG BMPS BNC BNP BPE CBK CS DBK EBS G GLE INGA ISP KBC NDA SAB TPEIR UCG (ACA BNP CS GLE) (ALV CBK DBK) (BAMI BMPS BPE G ISP UCG) (BBVA BNC SAB), datevar(date) evdate(12052017) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) dateformat(DMY) indexlist(MKT) price diagn(KP) decimal(4) suppress(ind)”

- Command for Solarwinds systemic event with parametric test: “estudy ACA ALV BAMI BBVA BIRG BMPS BNC BNP BPE CBK CS DBK EBS G GLE INGA ISP KBC NDA SAB TPEIR UCG (ACA BNP CS GLE) (ALV CBK DBK) (BAMI BMPS BPE G ISP UCG) (BBVA BNC SAB), datevar(date) evdate(14122020) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) dateformat(DMY) indexlist(MKT) price diagn(KP) graph (-3 3) decimal(4) suppress(ind)”

- Command for SolarWinds systemic event with non-parametric test: “estudy ACA ALV BAMI BBVA BIRG BMPS BNC BNP BPE CBK CS DBK EBS G GLE INGA ISP KBC NDA SAB TPEIR UCG (ACA BNP CS GLE) (ALV CBK DBK) (BAMI BMPS BPE G ISP UCG) (BBVA BNC SAB), datevar(date) evdate(14122020) lb1(0) ub1(0) lb2(0) ub2(1) lb3(-1) ub3(1) lb4(-1) ub4(2) lb5(0) ub5(2) lb6(-2) ub6(2) eswlb(-200) eswub(-30) dateformat(DMY) indexlist(MKT) price diagn(GRANK) decimal(4) suppress(ind)”

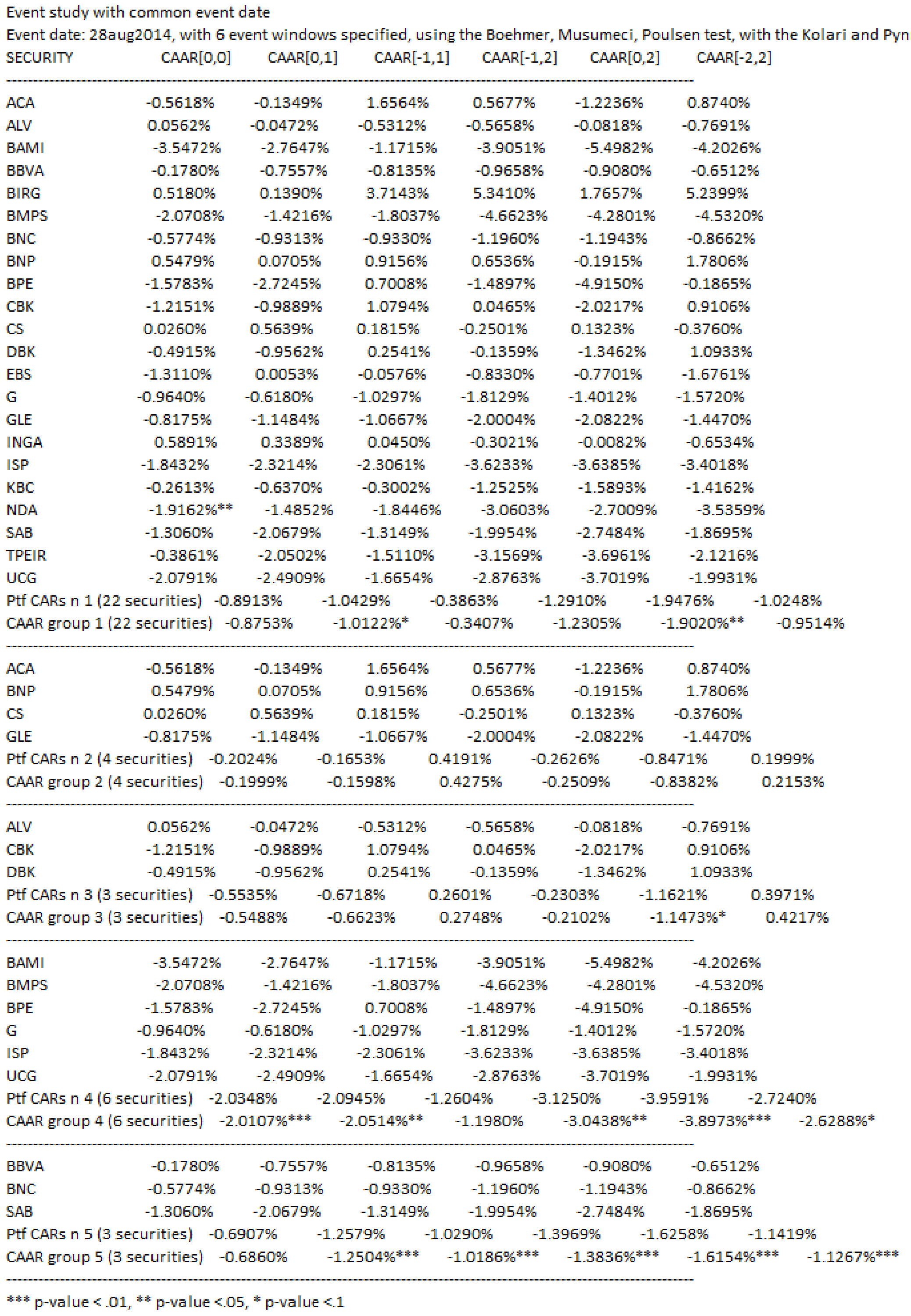
Appendix B: Direct events details

Event Date	Brief description	Newspaper article
26/07/2016	Hackers breach 400,000 UniCredit bank accounts for data	https://www.bloomberg.com/news/articles/2017-07-26/unicredit-says-400-000-clients-affected-by-security-breach#xj4y7vzkg
29/01/2018	Dutch tax office and banks hit by DDoS cyber attacks	https://www.reuters.com/article/us-netherlands-cyber/dutch-tax-office-banks-hit-by-ddos-cyber-attacks-idUSKBN1FI1LM/
23/10/2018	AXA is targeted in Mexico	https://www.reuters.com/article/mexico-centralbank-incident-idUSL2N1X403Z/
13/02/2019	Hacker try to transfer Bank of Valletta's funds abroad	https://www.reuters.com/article/us-bank-valetta-cyber/cyber-attack-on-malta-bank-tried-to-transfer-cash-abroad-idUSKCN1Q21KZ/
28/10/2019	Over 3 million unicredit accounts are violated	https://www.ilsole24ore.com/art/unicredit-violati-dati-3-milioni-clienti-non-erano-sensibili-ACoTY0u
21/11/2019	Edenred is subject to a malware injection	https://www.edenred.com/system/files/documents/predenred22112019eng.pdf
11/04/2020	Staff mailboxes at Monte dei Paschi suffer compromise by hacker	https://www.reuters.com/article/us-monte-dei-paschi-italy-bank-hacker-idUSKCN21T0H6/
16/05/2021	AXA is hit by a ransomware	https://www.reuters.com/article/us-axa-cyber-idUSKCN2CX0B0/
04/06/2021	German banks are hit by DDoS attack on IT provider	https://www.reuters.com/technology/german-it-company-that-serves-banks-experiences-ddos-hack-attack-2021-06-04/
09/01/2022	OP Financial Group online services are suspended due to a cyberattack	https://www.dailyfinland.fi/business/25316/OP-online-banking-comes-under-cyber-attack
05/04/2022	Bank of Ireland fined for corruption in the data feed to the Central Credit Register	https://www.rte.ie/news/business/2022/0405/1290503-bank-of-ireland-fined-by-dpc/
20/06/2022	Monte dei Paschi notifies authorities of a data breach resulting from a cyberattack	https://www.ilsole24ore.com/art/attacco-informatico-danni-mps-trafugati-indirizzi-email-AE2XmAhB
11/07/2023	Deutsche Bank, Commerzbank, ING data are breached as third party supplier is hacked	https://www.bloomberg.com/news/articles/2023-07-11/deutsche-bank-commerzbank-ing-data-breached-in-moveit-hack
01/08/2023	Five Italian banks are targeted with DDoS attacks by Russian hackers	https://www.repubblica.it/economia/2023/08/01/news/hacker_russi_attaccano_5_banche_italiane_lagenzia_cybersicurezza_massima_allerta_sistemi_integri-409730144/

Appendix C: Detailed Stata results for systemic events

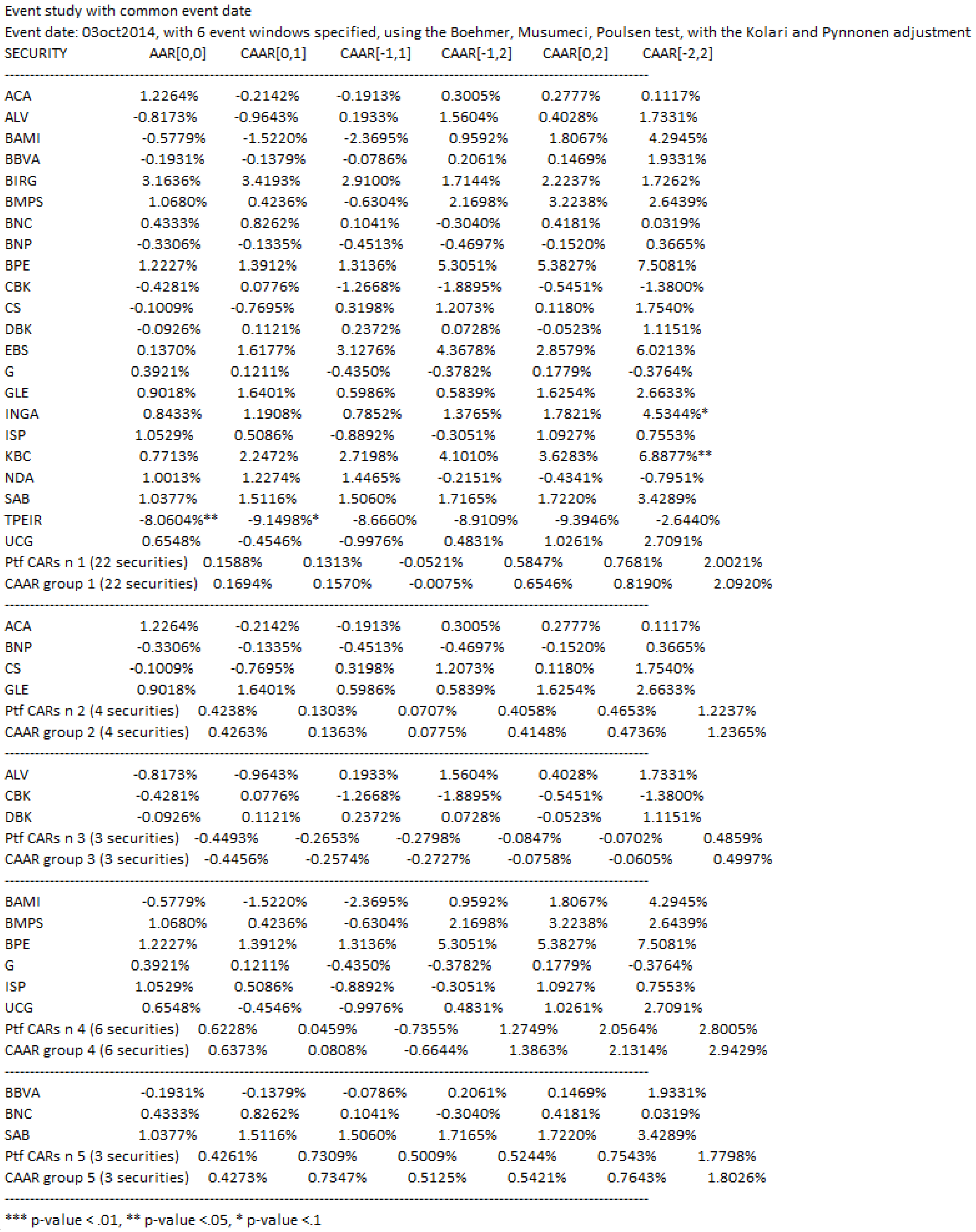
Below are the tables of the results obtained in Stata for systemic events with the detailed AARs and CAARs for each financial institution. For simplicity, only the significance results of the ADJ-BMP test are shown.

JP Morgan 28/08/2014



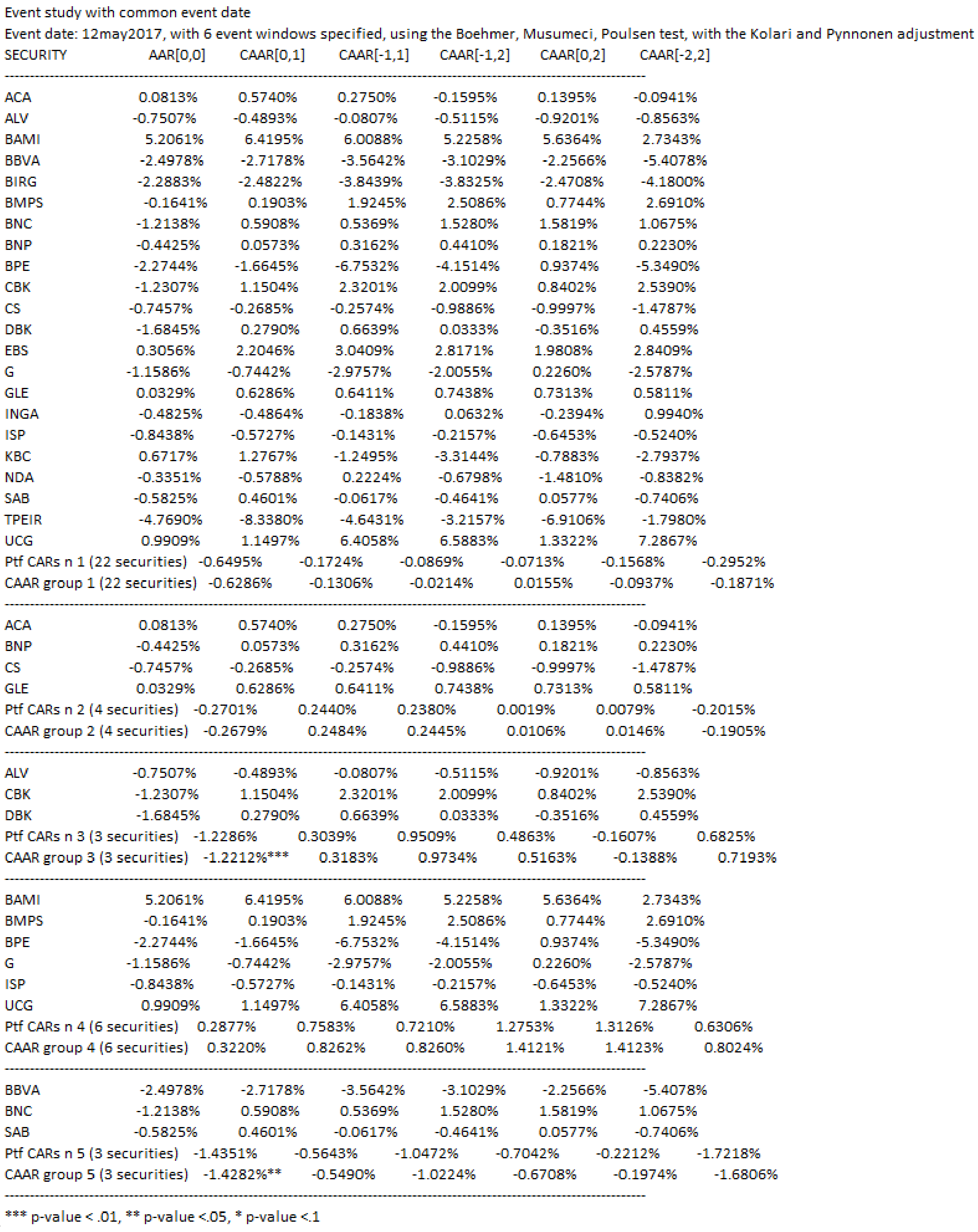
```
Event study with common event date
Event date: 28aug2014, with 6 event windows specified, using the Boehmer, Musumeci, Poulsen test, with the Kolari and Pynnonen adjustment
SECURITY                CAAR[0,0]      CAAR[0,1]      CAAR[-1,1]     CAAR[-1,2]     CAAR[0,2]      CAAR[-2,2]
-----------------------------------------------------------------------------------------------------------------

ACA                     -0.5618%       -0.1349%       1.6564%        0.5677%        -1.2236%       0.8740%
ALV                     0.0562%        -0.0472%       -0.5312%       -0.5658%       -0.0818%       -0.7691%
BAMI                    -3.5472%       -2.7647%       -1.1715%       -3.9051%       -5.4982%       -4.2026%
BBVA                    -0.1780%       -0.7557%       -0.8135%       -0.9658%       -0.9080%       -0.6512%
BIRG                    0.5180%        0.1390%        3.7143%        5.3410%        1.7657%        5.2399%
BMPS                    -2.0708%       -1.4216%       -1.8037%       -4.6623%       -4.2801%       -4.5320%
BNC                     -0.5774%       -0.9313%       -0.9330%       -1.1960%       -1.1943%       -0.8662%
BNP                     0.5479%        0.0705%        0.9156%        0.6536%        -0.1915%       1.7806%
BPE                     -1.5783%       -2.7245%       0.7008%        -1.4897%       -4.9150%       -0.1865%
CBK                     -1.2151%       -0.9889%       1.0794%        0.0465%        -2.0217%       0.9106%
CS                      0.0260%        0.5639%        0.1815%        -0.2501%       0.1323%        -0.3760%
DBK                     -0.4915%       -0.9562%       0.2541%        -0.1359%       -1.3462%       1.0933%
EBS                     -1.3110%       0.0053%        -0.0576%       -0.8330%       -0.7701%       -1.6761%
G                       -0.9640%       -0.6180%       -1.0297%       -1.8129%       -1.4012%       -1.5720%
GLE                     -0.8175%       -1.1484%       -1.0667%       -2.0004%       -2.0822%       -1.4470%
INGA                    0.5891%        0.3389%        0.0450%        -0.3021%       -0.0082%       -0.6534%
ISP                     -1.8432%       -2.3214%       -2.3061%       -3.6233%       -3.6385%       -3.4018%
KBC                     -0.2613%       -0.6370%       -0.3002%       -1.2525%       -1.5893%       -1.4162%
NDA                     -1.9162%**     -1.4852%       -1.8446%       -3.0603%       -2.7009%       -3.5359%
SAB                     -1.3060%       -2.0679%       -1.3149%       -1.9954%       -2.7484%       -1.8695%
TPEIR                   -0.3861%       -2.0502%       -1.5110%       -3.1569%       -3.6961%       -2.1216%
UCG                     -2.0791%       -2.4909%       -1.6654%       -2.8763%       -3.7019%       -1.9931%
Ptf CARs n 1 (22 securities)  -0.8913%   -1.0429%     -0.3863%       -1.2910%       -1.9476%       -1.0248%
CAAR group 1 (22 securities)  -0.8753%   -1.0122%*    -0.3407%       -1.2305%       -1.9020%**     -0.9514%
-----------------------------------------------------------------------------------------------------------------
ACA                     -0.5618%       -0.1349%       1.6564%        0.5677%        -1.2236%       0.8740%
BNP                     0.5479%        0.0705%        0.9156%        0.6536%        -0.1915%       1.7806%
CS                      0.0260%        0.5639%        0.1815%        -0.2501%       0.1323%        -0.3760%
GLE                     -0.8175%       -1.1484%       -1.0667%       -2.0004%       -2.0822%       -1.4470%
Ptf CARs n 2 (4 securities)   -0.2024%   -0.1653%     0.4191%        -0.2626%       -0.8471%       0.1999%
CAAR group 2 (4 securities)   -0.1999%   -0.1598%     0.4275%        -0.2509%       -0.8382%       0.2153%
-----------------------------------------------------------------------------------------------------------------
ALV                     0.0562%        -0.0472%       -0.5312%       -0.5658%       -0.0818%       -0.7691%
CBK                     -1.2151%       -0.9889%       1.0794%        0.0465%        -2.0217%       0.9106%
DBK                     -0.4915%       -0.9562%       0.2541%        -0.1359%       -1.3462%       1.0933%
Ptf CARs n 3 (3 securities)   -0.5535%   -0.6718%     0.2601%        -0.2303%       -1.1621%       0.3971%
CAAR group 3 (3 securities)   -0.5488%   -0.6623%     0.2748%        -0.2102%       -1.1473%*      0.4217%
-----------------------------------------------------------------------------------------------------------------
BAMI                    -3.5472%       -2.7647%       -1.1715%       -3.9051%       -5.4982%       -4.2026%
BMPS                    -2.0708%       -1.4216%       -1.8037%       -4.6623%       -4.2801%       -4.5320%
BPE                     -1.5783%       -2.7245%       0.7008%        -1.4897%       -4.9150%       -0.1865%
G                       -0.9640%       -0.6180%       -1.0297%       -1.8129%       -1.4012%       -1.5720%
ISP                     -1.8432%       -2.3214%       -2.3061%       -3.6233%       -3.6385%       -3.4018%
UCG                     -2.0791%       -2.4909%       -1.6654%       -2.8763%       -3.7019%       -1.9931%
Ptf CARs n 4 (6 securities)   -2.0348%   -2.0945%     -1.2604%       -3.1250%       -3.9591%       -2.7240%
CAAR group 4 (6 securities)   -2.0107%***  -2.0514%**  -1.1980%      -3.0438%**     -3.8973%***    -2.6288%*
-----------------------------------------------------------------------------------------------------------------
BBVA                    -0.1780%       -0.7557%       -0.8135%       -0.9658%       -0.9080%       -0.6512%
BNC                     -0.5774%       -0.9313%       -0.9330%       -1.1960%       -1.1943%       -0.8662%
SAB                     -1.3060%       -2.0679%       -1.3149%       -1.9954%       -2.7484%       -1.8695%
Ptf CARs n 5 (3 securities)   -0.6907%   -1.2579%     -1.0290%       -1.3969%       -1.6258%       -1.1419%
CAAR group 5 (3 securities)   -0.6860%   -1.2504%***  -1.0186%***    -1.3836%***    -1.6154%***    -1.1267%***
-----------------------------------------------------------------------------------------------------------------
*** p-value < .01, ** p-value <.05, * p-value <.1
```

JP Morgan 03/10/2014



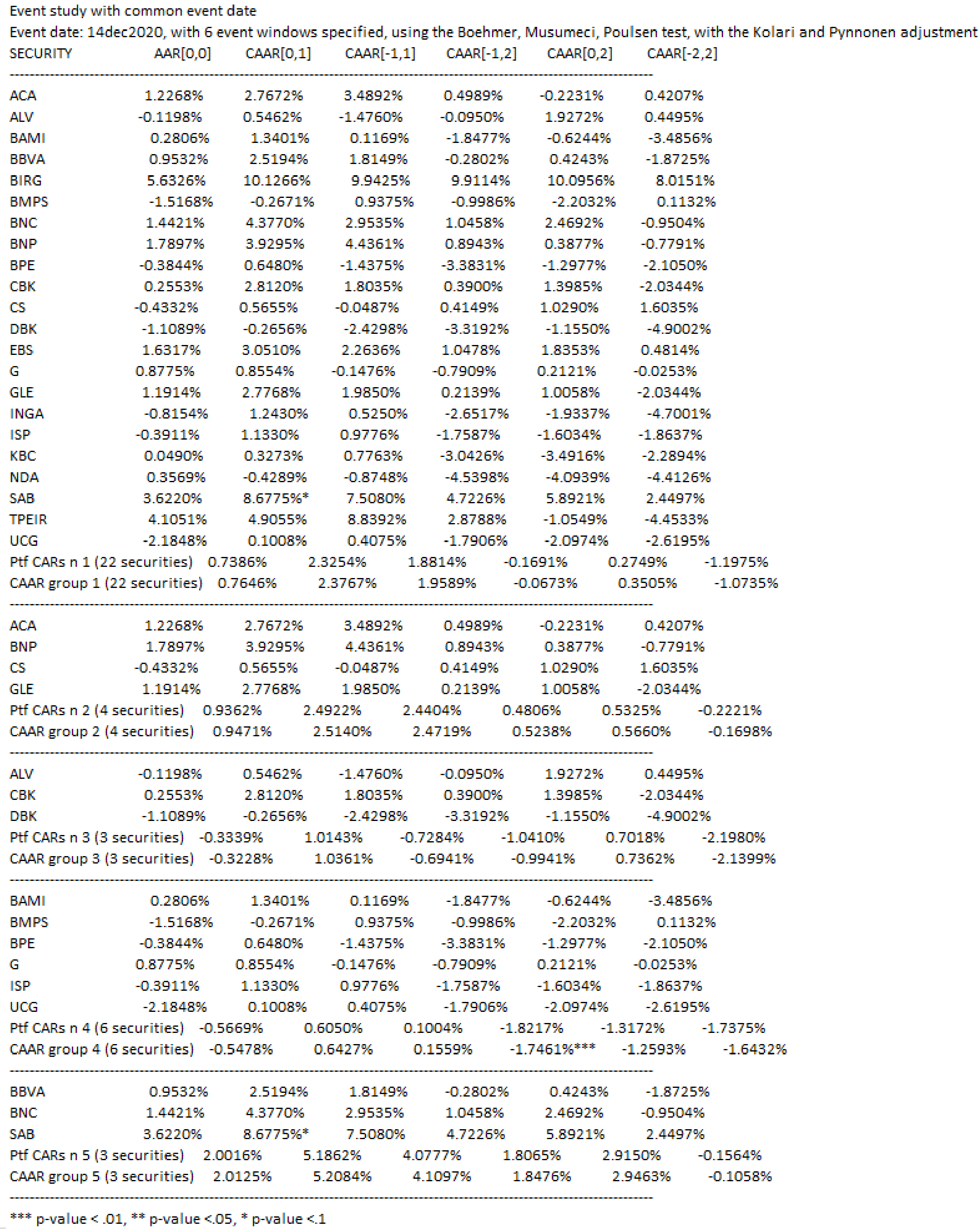
```
Event study with common event date
Event date: 03oct2014, with 6 event windows specified, using the Boehmer, Musumeci, Poulsen test, with the Kolari and Pynnonen adjustment
SECURITY                 AAR[0,0]     CAAR[0,1]     CAAR[-1,1]    CAAR[-1,2]    CAAR[0,2]     CAAR[-2,2]
-------------------------------------------------------------------------------------------------------
ACA                      1.2264%      -0.2142%      -0.1913%      0.3005%       0.2777%       0.1117%
ALV                     -0.8173%      -0.9643%       0.1933%      1.5604%       0.4028%       1.7331%
BAMI                    -0.5779%      -1.5220%      -2.3695%      0.9592%       1.8067%       4.2945%
BBVA                    -0.1931%      -0.1379%      -0.0786%      0.2061%       0.1469%       1.9331%
BIRG                     3.1636%       3.4193%       2.9100%      1.7144%       2.2237%       1.7262%
BMPS                     1.0680%       0.4236%      -0.6304%      2.1698%       3.2238%       2.6439%
BNC                      0.4333%       0.8262%       0.1041%     -0.3040%       0.4181%       0.0319%
BNP                     -0.3306%      -0.1335%      -0.4513%     -0.4697%      -0.1520%       0.3665%
BPE                      1.2227%       1.3912%       1.3136%      5.3051%       5.3827%       7.5081%
CBK                     -0.4281%       0.0776%      -1.2668%     -1.8895%      -0.5451%      -1.3800%
CS                      -0.1009%      -0.7695%       0.3198%      1.2073%       0.1180%       1.7540%
DBK                     -0.0926%       0.1121%       0.2372%      0.0728%      -0.0523%       1.1151%
EBS                      0.1370%       1.6177%       3.1276%      4.3678%       2.8579%       6.0213%
G                        0.3921%       0.1211%      -0.4350%     -0.3782%       0.1779%      -0.3764%
GLE                      0.9018%       1.6401%       0.5986%      0.5839%       1.6254%       2.6633%
INGA                     0.8433%       1.1908%       0.7852%      1.3765%       1.7821%       4.5344%*
ISP                      1.0529%       0.5086%      -0.8892%     -0.3051%       1.0927%       0.7553%
KBC                      0.7713%       2.2472%       2.7198%      4.1010%       3.6283%       6.8877%**
NDA                      1.0013%       1.2274%       1.4465%     -0.2151%      -0.4341%      -0.7951%
SAB                      1.0377%       1.5116%       1.5060%      1.7165%       1.7220%       3.4289%
TPEIR                   -8.0604%**    -9.1498%*     -8.6660%     -8.9109%      -9.3946%      -2.6440%
UCG                      0.6548%      -0.4546%      -0.9976%      0.4831%       1.0261%       2.7091%
Ptf CARs n 1 (22 securities)  0.1588%   0.1313%   -0.0521%   0.5847%   0.7681%   2.0021%
CAAR group 1 (22 securities)  0.1694%   0.1570%   -0.0075%   0.6546%   0.8190%   2.0920%
-------------------------------------------------------------------------------------------------------
ACA                      1.2264%      -0.2142%      -0.1913%      0.3005%       0.2777%       0.1117%
BNP                     -0.3306%      -0.1335%      -0.4513%     -0.4697%      -0.1520%       0.3665%
CS                      -0.1009%      -0.7695%       0.3198%      1.2073%       0.1180%       1.7540%
GLE                      0.9018%       1.6401%       0.5986%      0.5839%       1.6254%       2.6633%
Ptf CARs n 2 (4 securities)  0.4238%   0.1303%   0.0707%   0.4058%   0.4653%   1.2237%
CAAR group 2 (4 securities)  0.4263%   0.1363%   0.0775%   0.4148%   0.4736%   1.2365%
-------------------------------------------------------------------------------------------------------
ALV                     -0.8173%      -0.9643%       0.1933%      1.5604%       0.4028%       1.7331%
CBK                     -0.4281%       0.0776%      -1.2668%     -1.8895%      -0.5451%      -1.3800%
DBK                     -0.0926%       0.1121%       0.2372%      0.0728%      -0.0523%       1.1151%
Ptf CARs n 3 (3 securities)  -0.4493%   -0.2653%   -0.2798%   -0.0847%   -0.0702%   0.4859%
CAAR group 3 (3 securities)  -0.4456%   -0.2574%   -0.2727%   -0.0758%   -0.0605%   0.4997%
-------------------------------------------------------------------------------------------------------
BAMI                    -0.5779%      -1.5220%      -2.3695%      0.9592%       1.8067%       4.2945%
BMPS                     1.0680%       0.4236%      -0.6304%      2.1698%       3.2238%       2.6439%
BPE                      1.2227%       1.3912%       1.3136%      5.3051%       5.3827%       7.5081%
G                        0.3921%       0.1211%      -0.4350%     -0.3782%       0.1779%      -0.3764%
ISP                      1.0529%       0.5086%      -0.8892%     -0.3051%       1.0927%       0.7553%
UCG                      0.6548%      -0.4546%      -0.9976%      0.4831%       1.0261%       2.7091%
Ptf CARs n 4 (6 securities)  0.6228%   0.0459%   -0.7355%   1.2749%   2.0564%   2.8005%
CAAR group 4 (6 securities)  0.6373%   0.0808%   -0.6644%   1.3863%   2.1314%   2.9429%
-------------------------------------------------------------------------------------------------------
BBVA                    -0.1931%      -0.1379%      -0.0786%      0.2061%       0.1469%       1.9331%
BNC                      0.4333%       0.8262%       0.1041%     -0.3040%       0.4181%       0.0319%
SAB                      1.0377%       1.5116%       1.5060%      1.7165%       1.7220%       3.4289%
Ptf CARs n 5 (3 securities)  0.4261%   0.7309%   0.5009%   0.5244%   0.7543%   1.7798%
CAAR group 5 (3 securities)  0.4273%   0.7347%   0.5125%   0.5421%   0.7643%   1.8026%
-------------------------------------------------------------------------------------------------------
*** p-value < .01, ** p-value <.05, * p-value <.1
```

WannaCry 12/05/2017



```
Event study with common event date
Event date: 12may2017, with 6 event windows specified, using the Boehmer, Musumeci, Poulsen test, with the Kolari and Pynnonen adjustment
SECURITY                AAR[0,0]      CAAR[0,1]    CAAR[-1,1]   CAAR[-1,2]   CAAR[0,2]    CAAR[-2,2]
--------------------------------------------------------------------------------------------------
ACA                     0.0813%       0.5740%      0.2750%      -0.1595%     0.1395%      -0.0941%
ALV                     -0.7507%      -0.4893%     -0.0807%     -0.5115%     -0.9201%     -0.8563%
BAMI                    5.2061%       6.4195%      6.0088%      5.2258%      5.6364%      2.7343%
BBVA                    -2.4978%      -2.7178%     -3.5642%     -3.1029%     -2.2566%     -5.4078%
BIRG                    -2.2883%      -2.4822%     -3.8439%     -3.8325%     -2.4708%     -4.1800%
BMPS                    -0.1641%      0.1903%      1.9245%      2.5086%      0.7744%      2.6910%
BNC                     -1.2138%      0.5908%      0.5369%      1.5280%      1.5819%      1.0675%
BNP                     -0.4425%      0.0573%      0.3162%      0.4410%      0.1821%      0.2230%
BPE                     -2.2744%      -1.6645%     -6.7532%     -4.1514%     0.9374%      -5.3490%
CBK                     -1.2307%      1.1504%      2.3201%      2.0099%      0.8402%      2.5390%
CS                      -0.7457%      -0.2685%     -0.2574%     -0.9886%     -0.9997%     -1.4787%
DBK                     -1.6845%      0.2790%      0.6639%      0.0333%      -0.3516%     0.4559%
EBS                     0.3056%       2.2046%      3.0409%      2.8171%      1.9808%      2.8409%
G                       -1.1586%      -0.7442%     -2.9757%     -2.0055%     0.2260%      -2.5787%
GLE                     0.0329%       0.6286%      0.6411%      0.7438%      0.7313%      0.5811%
INGA                    -0.4825%      -0.4864%     -0.1838%     0.0632%      -0.2394%     0.9940%
ISP                     -0.8438%      -0.5727%     -0.1431%     -0.2157%     -0.6453%     -0.5240%
KBC                     0.6717%       1.2767%      -1.2495%     -3.3144%     -0.7883%     -2.7937%
NDA                     -0.3351%      -0.5788%     0.2224%      -0.6798%     -1.4810%     -0.8382%
SAB                     -0.5825%      0.4601%      -0.0617%     -0.4641%     0.0577%      -0.7406%
TPEIR                   -4.7690%      -8.3380%     -4.6431%     -3.2157%     -6.9106%     -1.7980%
UCG                     0.9909%       1.1497%      6.4058%      6.5883%      1.3322%      7.2867%
Ptf CARs n 1 (22 securities)  -0.6495%     -0.1724%     -0.0869%     -0.0713%     -0.1568%     -0.2952%
CAAR group 1 (22 securities)  -0.6286%     -0.1306%     -0.0214%     0.0155%      -0.0937%     -0.1871%
--------------------------------------------------------------------------------------------------
ACA                     0.0813%       0.5740%      0.2750%      -0.1595%     0.1395%      -0.0941%
BNP                     -0.4425%      0.0573%      0.3162%      0.4410%      0.1821%      0.2230%
CS                      -0.7457%      -0.2685%     -0.2574%     -0.9886%     -0.9997%     -1.4787%
GLE                     0.0329%       0.6286%      0.6411%      0.7438%      0.7313%      0.5811%
Ptf CARs n 2 (4 securities)   -0.2701%     0.2440%      0.2380%      0.0019%      0.0079%      -0.2015%
CAAR group 2 (4 securities)   -0.2679%     0.2484%      0.2445%      0.0106%      0.0146%      -0.1905%
--------------------------------------------------------------------------------------------------
ALV                     -0.7507%      -0.4893%     -0.0807%     -0.5115%     -0.9201%     -0.8563%
CBK                     -1.2307%      1.1504%      2.3201%      2.0099%      0.8402%      2.5390%
DBK                     -1.6845%      0.2790%      0.6639%      0.0333%      -0.3516%     0.4559%
Ptf CARs n 3 (3 securities)   -1.2286%     0.3039%      0.9509%      0.4863%      -0.1607%     0.6825%
CAAR group 3 (3 securities)   -1.2212%***  0.3183%      0.9734%      0.5163%      -0.1388%     0.7193%
--------------------------------------------------------------------------------------------------
BAMI                    5.2061%       6.4195%      6.0088%      5.2258%      5.6364%      2.7343%
BMPS                    -0.1641%      0.1903%      1.9245%      2.5086%      0.7744%      2.6910%
BPE                     -2.2744%      -1.6645%     -6.7532%     -4.1514%     0.9374%      -5.3490%
G                       -1.1586%      -0.7442%     -2.9757%     -2.0055%     0.2260%      -2.5787%
ISP                     -0.8438%      -0.5727%     -0.1431%     -0.2157%     -0.6453%     -0.5240%
UCG                     0.9909%       1.1497%      6.4058%      6.5883%      1.3322%      7.2867%
Ptf CARs n 4 (6 securities)   0.2877%      0.7583%      0.7210%      1.2753%      1.3126%      0.6306%
CAAR group 4 (6 securities)   0.3220%      0.8262%      0.8260%      1.4121%      1.4123%      0.8024%
--------------------------------------------------------------------------------------------------
BBVA                    -2.4978%      -2.7178%     -3.5642%     -3.1029%     -2.2566%     -5.4078%
BNC                     -1.2138%      0.5908%      0.5369%      1.5280%      1.5819%      1.0675%
SAB                     -0.5825%      0.4601%      -0.0617%     -0.4641%     0.0577%      -0.7406%
Ptf CARs n 5 (3 securities)   -1.4351%     -0.5643%     -1.0472%     -0.7042%     -0.2212%     -1.7218%
CAAR group 5 (3 securities)   -1.4282%**   -0.5490%     -1.0224%     -0.6708%     -0.1974%     -1.6806%
--------------------------------------------------------------------------------------------------
*** p-value < .01, ** p-value <.05, * p-value <.1
```

SolarWinds 03/10/2014



```
Event study with common event date
Event date: 14dec2020, with 6 event windows specified, using the Boehmer, Musumeci, Poulsen test, with the Kolari and Pynnonen adjustment
SECURITY              AAR[0,0]      CAAR[0,1]     CAAR[-1,1]     CAAR[-1,2]     CAAR[0,2]     CAAR[-2,2]
-------------------------------------------------------------------------------------------------------

ACA                    1.2268%      2.7672%      3.4892%      0.4989%      -0.2231%      0.4207%
ALV                   -0.1198%      0.5462%     -1.4760%     -0.0950%       1.9272%      0.4495%
BAMI                   0.2806%      1.3401%      0.1169%     -1.8477%      -0.6244%     -3.4856%
BBVA                   0.9532%      2.5194%      1.8149%     -0.2802%       0.4243%     -1.8725%
BIRG                   5.6326%     10.1266%      9.9425%      9.9114%      10.0956%      8.0151%
BMPS                  -1.5168%     -0.2671%      0.9375%     -0.9986%      -2.2032%      0.1132%
BNC                    1.4421%      4.3770%      2.9535%      1.0458%       2.4692%     -0.9504%
BNP                    1.7897%      3.9295%      4.4361%      0.8943%       0.3877%     -0.7791%
BPE                   -0.3844%      0.6480%     -1.4375%     -3.3831%      -1.2977%     -2.1050%
CBK                    0.2553%      2.8120%      1.8035%      0.3900%       1.3985%     -2.0344%
CS                    -0.4332%      0.5655%     -0.0487%      0.4149%       1.0290%      1.6035%
DBK                   -1.1089%     -0.2656%     -2.4298%     -3.3192%      -1.1550%     -4.9002%
EBS                    1.6317%      3.0510%      2.2636%      1.0478%       1.8353%      0.4814%
G                      0.8775%      0.8554%     -0.1476%     -0.7909%       0.2121%     -0.0253%
GLE                    1.1914%      2.7768%      1.9850%      0.2139%       1.0058%     -2.0344%
INGA                  -0.8154%      1.2430%      0.5250%     -2.6517%      -1.9337%     -4.7001%
ISP                   -0.3911%      1.1330%      0.9776%     -1.7587%      -1.6034%     -1.8637%
KBC                    0.0490%      0.3273%      0.7763%     -3.0426%      -3.4916%     -2.2894%
NDA                    0.3569%     -0.4289%     -0.8748%     -4.5398%      -4.0939%     -4.4126%
SAB                    3.6220%      8.6775%*     7.5080%      4.7226%       5.8921%      2.4497%
TPEIR                  4.1051%      4.9055%      8.8392%      2.8788%      -1.0549%     -4.4533%
UCG                   -2.1848%      0.1008%      0.4075%     -1.7906%      -2.0974%     -2.6195%
Ptf CARs n 1 (22 securities)  0.7386%      2.3254%      1.8814%      -0.1691%      0.2749%      -1.1975%
CAAR group 1 (22 securities)  0.7646%      2.3767%      1.9589%      -0.0673%      0.3505%      -1.0735%
-------------------------------------------------------------------------------------------------------

ACA                    1.2268%      2.7672%      3.4892%      0.4989%      -0.2231%      0.4207%
BNP                    1.7897%      3.9295%      4.4361%      0.8943%       0.3877%     -0.7791%
CS                    -0.4332%      0.5655%     -0.0487%      0.4149%       1.0290%      1.6035%
GLE                    1.1914%      2.7768%      1.9850%      0.2139%       1.0058%     -2.0344%
Ptf CARs n 2 (4 securities)  0.9362%      2.4922%      2.4404%      0.4806%      0.5325%      -0.2221%
CAAR group 2 (4 securities)  0.9471%      2.5140%      2.4719%      0.5238%      0.5660%      -0.1698%
-------------------------------------------------------------------------------------------------------

ALV                   -0.1198%      0.5462%     -1.4760%     -0.0950%       1.9272%      0.4495%
CBK                    0.2553%      2.8120%      1.8035%      0.3900%       1.3985%     -2.0344%
DBK                   -1.1089%     -0.2656%     -2.4298%     -3.3192%      -1.1550%     -4.9002%
Ptf CARs n 3 (3 securities)  -0.3339%      1.0143%      -0.7284%      -1.0410%      0.7018%      -2.1980%
CAAR group 3 (3 securities)  -0.3228%      1.0361%      -0.6941%      -0.9941%      0.7362%      -2.1399%
-------------------------------------------------------------------------------------------------------

BAMI                   0.2806%      1.3401%      0.1169%     -1.8477%      -0.6244%     -3.4856%
BMPS                  -1.5168%     -0.2671%      0.9375%     -0.9986%      -2.2032%      0.1132%
BPE                   -0.3844%      0.6480%     -1.4375%     -3.3831%      -1.2977%     -2.1050%
G                      0.8775%      0.8554%     -0.1476%     -0.7909%       0.2121%     -0.0253%
ISP                   -0.3911%      1.1330%      0.9776%     -1.7587%      -1.6034%     -1.8637%
UCG                   -2.1848%      0.1008%      0.4075%     -1.7906%      -2.0974%     -2.6195%
Ptf CARs n 4 (6 securities)  -0.5669%      0.6050%      0.1004%      -1.8217%      -1.3172%      -1.7375%
CAAR group 4 (6 securities)  -0.5478%      0.6427%      0.1559%      -1.7461%***   -1.2593%      -1.6432%
-------------------------------------------------------------------------------------------------------

BBVA                   0.9532%      2.5194%      1.8149%     -0.2802%       0.4243%     -1.8725%
BNC                    1.4421%      4.3770%      2.9535%      1.0458%       2.4692%     -0.9504%
SAB                    3.6220%      8.6775%*     7.5080%      4.7226%       5.8921%      2.4497%
Ptf CARs n 5 (3 securities)  2.0016%      5.1862%      4.0777%      1.8065%      2.9150%      -0.1564%
CAAR group 5 (3 securities)  2.0125%      5.2084%      4.1097%      1.8476%      2.9463%      -0.1058%
-------------------------------------------------------------------------------------------------------
*** p-value < .01, ** p-value <.05, * p-value <.1
```