No protection, no business:

An event study on stock volatility reactions to cyberattacks between 2010 and 2015 for firms listed in the USA.

Authors: Erik Collin
Gustav Juntti

Supervisor: Catherine Lions
Abstract

With the surge of Internet-based corporate communication, organization, and information management, financial markets have undergone radical transformation. In the interconnected economy of today, market participants are forced to accept cyberattacks, data breaches, system failures, or security flaws as any other (varying) cost of doing business. While cyberspace encompasses practically any firm in developed economies and a large portion in developing ones, combatting such risks is deemed a question of firm-specific responsibility: the situation resembles an ‘every man for himself’ scenario. Consulting standard financial theory, rational utility-maximizing investors assume firm-specific (idiosyncratic) risk under expectations of additional compensation for shouldering such risk – they are economically incentivized.

The omnipresence of cyberattacks challenges fundamental assumptions of the Capital Asset Pricing Model, Optimal Portfolio Theory, and the concept of diversifiability. The thesis problematizes underlying rationality notions by investigating the effect of a cyberattack on stock volatility. Explicitly, the use of stock volatility as a proxy for risk allows for linking increased volatility to higher risk premiums and increased cost of capital. In essence, we investigate the following research question: What is the effect of a disclosed cyberattack on stock volatility for firms listed in the USA?

Using event study methodology, we compile a cyberattack database for events between 2010 and 2015 involving 115 firms listed on US stock exchanges. The specified time period cover prevailing research gaps; due to literature paucity the focus on volatility fits well. For a finalized sample of 189 events, stock return data is matched to S&P500 index return data within a pre-event estimation window and a post-event window to calculate abnormal returns using the market model. The outputs are used to estimate abnormal return volatility before and after each event; testing pre and post volatility against each other in significance tests then approximates the event-induced volatility. Identical procedures are performed for all subsamples based on time horizon, industry belonging, attack type, firm size, and perpetrator motivation.

The principal hypothesis, that stock volatility is significantly higher after a cyberattack, is found to hold within both event windows. Evidence on firm-specific characteristics is more inconclusive. In the long run, inaccessibility and attacks on smaller firms seem to render significantly larger increases in volatility compared to intrusion and attacks on larger firms; supporting preexisting literature. Contrasting, perpetrator motive appears irrelevant. Generally, stocks are more volatile immediately after an attack, attributable to information asymmetry. For most subsamples volatility seem to diminish with time, following the Efficient Market Hypothesis. Summing up, disparate results raise questions of the relative importance of contingency factors, and also about future developments within and outside academic research.

Keywords: cyberattacks; abnormal returns; volatility; event study; information technology; US stock market; cybersecurity; reactions; financial impact; market efficiency.
Acknowledgements

We extend our deepest and warmest appreciation to our supervisor, Catherine Lions, for all the valuable help, guidance and encouragement. We additionally would like to thank Priyantha Wijayatunga for his constructive and reassuring statistical assistance. Finally, we feel that our respective families deserve a big thank you for their heartening presence during the whole writing process.

Umeå, 23rd of May 2016

Erik Collin Gustav Juntti
Table of contents

1 Introduction .................................................................................................................. 1
  1.1 Problem background .............................................................................................. 1
  1.2 Research question ................................................................................................. 3
  1.3 Knowledge gap ........................................................................................................ 4
  1.4 Research purpose .................................................................................................... 4
  1.5 Delimitations ........................................................................................................... 5
  1.6 Contribution and target Audience ......................................................................... 7
  1.7 Disposition ............................................................................................................... 8
  1.8 Definitions ............................................................................................................. 9

2 Methodology .................................................................................................................. 11
  2.1 Choice of topic and preconceptions ....................................................................... 11
  2.2 Our perspective ...................................................................................................... 12
  2.3 Research philosophy ............................................................................................. 12
    2.3.1 Epistemology .................................................................................................. 13
    2.3.2 Ontology ........................................................................................................ 14
  2.4 Research approach ................................................................................................ 15
  2.5 Research design ..................................................................................................... 17
  2.6 Research strategy .................................................................................................. 18
  2.7 Research perspective ............................................................................................. 20
  2.8 Research method .................................................................................................... 21
  2.9 Literature, data and source critique ...................................................................... 22
  2.10 Ethics ...................................................................................................................... 24
  2.11 Summary of methodology .................................................................................... 26

3 Theoretical framework .................................................................................................. 27
  3.1 Traditional financial theories ................................................................................. 27
    3.1.1 Market efficiency ............................................................................................ 27
    3.1.2 Information asymmetry .................................................................................. 29
    3.1.3 CAPM, risk premium and beta ...................................................................... 30
    3.1.4 Cost of capital ................................................................................................ 34
    3.1.5 Risk-reward tradeoff ...................................................................................... 34
  3.2 Theories of behavioral finance .............................................................................. 35
    3.2.1 Challenging the rationality within finance .................................................... 35
    3.2.2 Regret theory .................................................................................................. 36
    3.2.3 Herding behavior in financial markets ............................................................ 37
  3.3 Volatility .................................................................................................................. 38
    3.3.1 Volatility: a definition ...................................................................................... 38
    3.3.2 Volatility and its relation to information, attention and uncertainty .......... 38
    3.3.3 Idiosyncratic volatility and risk premiums .................................................... 40
  3.4 Discussion of financial IT literature ........................................................................ 41
  3.5 Summarizing model ............................................................................................... 45
4 Practical method and empirical study ................................................................. 46
  4.1 The event study .............................................................................................. 46
    4.1.1 The method............................................................................................. 46
    4.1.2 Data collection ....................................................................................... 48
    4.1.3 The Market model, Abnormal Returns, and Cumulative Abnormal Returns
       .................................................................................................................. 51
    4.1.4 Abnormal volatility ................................................................................. 54
  4.2 Statistical analysis .......................................................................................... 56
    4.2.1 A first inspection ................................................................................... 56
    4.2.2 Outliers .................................................................................................. 56
    4.2.3 Testing for normality ............................................................................. 57
    4.2.4 Type I and Type II errors ..................................................................... 57
    4.2.5 A paired-samples t-test (first moment of hypotheses) ......................... 58
    4.2.6 A two-sample t-test (second moment of hypotheses) ......................... 58
    4.2.7 Heteroscedasticity and Levene’s test ................................................... 59
    4.2.8 Generalized Sign Test ......................................................................... 60
  4.3 Hypotheses ..................................................................................................... 61
5 Empirical findings and analysis ......................................................................... 65
  5.1 Descriptive, summary and visual statistics ...................................................... 65
    5.1.1 Volatility plots – looking for a pattern .................................................. 65
    5.1.2 Descriptive statistics for both event windows – unprocessed data ......... 67
    5.1.3 Outliers .................................................................................................. 68
    5.1.4 Descriptive statistics for both event windows – processed data .......... 69
    5.1.5 Results of normality tests (after outlier removal)................................. 70
  5.2 Results of hypotheses tests ............................................................................. 71
    5.2.1 Results for Hypothesis 1 (H1) ............................................................... 71
    5.2.2 Results for Hypothesis 2 (H2) ............................................................... 72
    5.2.3 Results for Hypothesis 3 (H3) ............................................................... 73
    5.2.4 Results for Hypothesis 4 (H4) ............................................................... 74
    5.2.5 Results for Hypothesis 5 (H5) ............................................................... 75
    5.2.6 Results for Hypothesis 6 (H6) ............................................................... 76
  5.3 Mean plots ..................................................................................................... 77
  5.4 Analysis ......................................................................................................... 77
    5.4.1 Theoretical analysis ............................................................................. 78
    5.4.2 Analysis of individual hypotheses ......................................................... 80
  5.5 Practical implications of results ...................................................................... 84
  5.6 Summary of results ....................................................................................... 86
6 Conclusions ........................................................................................................ 87
  6.1 Truth criteria .................................................................................................. 87
    6.1.1 Reliability ............................................................................................... 87
    6.1.2 Validity .................................................................................................. 88
    6.1.3 Generalizability ..................................................................................... 89
  6.2 Concluding remarks ...................................................................................... 89
6.3 Contributions................................................................. 90
6.4 Ethical considerations..................................................... 91
6.5 Suggestions and recommendations for future research ............... 92
7 Reference list................................................................... 94
8 Appendices ..................................................................... 104
Figure 1: Summary of our methodological outline. 26
Figure 2: Summarizing model of theoretical framework. 45
Figure 3: Volatility plots. 66
Figure 4: 5-day mean volatility increase per subsample. 77
Figure 5: 30-day mean volatility increase per subsample. 77

Table 1: Explanations of subsample categories. 51
Table 2: Descriptives 5-day event window before outlier removal 68
Table 3: Descriptives 30-day event window before outlier removal. 68
Table 4: Descriptives 5-day event window after outlier removal. 70
Table 5: Descriptives 30-day event window after outlier removal. 70
Table 6: Results of significance test for Hypothesis 1. 71
Table 7: Results of significance tests for Hypothesis 2. 72
Table 8: Levene's Test of Homogeneity of Variances for H2. 72
Table 9: Results of significance tests for Hypothesis 3. 73
Table 10: Levene’s Test of Homogeneity of Variances for H3. 73
Table 11: Results of significance tests for Hypothesis 4. 74
Table 12: Levene’s Test of Homogeneity of Variances for H4. 74
Table 13: Results of significance tests for Hypothesis 5. 75
Table 14: Levene’s Test of Homogeneity of Variances for H5. 75
Table 15: Results of significance tests for hypothesis 6. 76
Table 16: Levene’s Test of Homogeneity of Variances for H6. 76
Table 17: Summary of hypotheses and results. 86
1 Introduction

In the following chapter, we seek to enhance readers’ insight into the chosen field of study and theoretical explications within it. Explicitly, the layout of the study, its motivation and background is introduced. Next, we present the background of the topic and problematize it, followed by the connected research question and the knowledge gap we locate the question within. Thereafter, the purpose and limitations are explained. In addition, the proposed contributions and possible target audience(s) of the study are communicated, followed by a disposition of subsequent chapters. We end with a list of definitions to ease continued reading.

1.1 Problem background

Cybercrime is surging. Different types of cyberattacks are not only extremely costly for the global economy but also increasingly severe and frequent. Already in the beginning of 2009, President Barack Obama addressed the American people and declared that cyber threats are “…one of the most serious economic and national security challenges we face as a nation” (Obama, 2009). The annual cost for the global economy is however hard to circle in on. The world’s largest cybersecurity software company, Intel Security Group (formerly McAfee), presents three approaches for approximating the annual monetary figure in a report seeking to estimate the global costs of cybercrime. Between $375 and $575 billion is lost yearly, depending on the group of countries and regions included in the measurement approach (Intel Security, 2014, p. 6). The company itself however declares that “none of these approaches are satisfactory” due to inferior or inadequate “reporting and data collection” (Intel Security, 2014, p. 6).

Herein lie difficulties which academic research has struggled to resolve. Cavusoglu et al. emphasizes that uncertainty stems from the problem “of measuring the costs of security breaches” (2004, p. 69), especially intangible costs such as customer trust and investor confidence (2004, p. 74). Despite this conundrum, sampled firms’ market value on average decreased with 2.1 percent or $1.65 billion within two days of announcing a breach (Cavusoglu et al., 2004, p. 86). Firms tend to focus on tangible costs and underestimate intangible breach-related costs, translating into underinvestment of IT security (Cavusoglu et al., 2004, p. 95). The problem is further complicated by the fact that firms are either “unwilling or unable to quantify their losses” (Campbell et al., 2003, p. 432).

Adding to the issue is the little ability and even less practical knowledge of how to estimate, let alone motivate, a specific cybersecurity investment. When it comes to incorporating cybersecurity, actors stand alarmingly incapable. As tersely put in a white paper by KPMG, “100 percent security is neither feasible nor the appropriate goal” (KPMG, 2014, p. 5). For companies and investors of today, this is the grim reality of business. In a Harvard Business Review article, Elena Kvochko and Rajiv Pant articulate that shareholders of today “neither [have] enough information about security incidents nor sufficient tools to measure their impact” (HBR, 2015). This deficiency of knowledge could entail a lack of shareholder pressure for increased security investments, further decreasing managers’ incentive to engage in such investments. Still, expenditures across the globe on information security technology reached $77 billion in 2014, a number expected to grow to $108 billion in 2019 (Fortune, 2015).
However, even these rather extreme numbers are likely well below required investment levels, reflecting the lack of cost-benefit knowledge when it comes to cybersecurity investments.

The first step in order to acquire such knowledge is to find a way to measure and monetize the costs related to a cyberattack. Previous research tried to accomplish this by scrutinizing effects on stock returns in junction with different types of cyberattack announcements. The results confirm that such announcements are followed by a slight decrease in returns. The negative effect these decreases meant for the market capitalization of the company were considered a proxy for the cost of being attacked (Arcuri et al., 2012; Cavusoglu et al., 2004). Following the event study methodology, others reviewed firms’ abnormal returns following breach announcements and determined the “mean announcement effect” (Campbell et al., 2003, p. 442). Drawing upon that work, Kannan et al. (2007) employed a long-term perspective for estimating the impact of announced cyberattacks on abnormal returns.

Moreover, from a strictly technological viewpoint, academics and researchers have closely followed cybersecurity and cybercrime. Yet, the link to business, and particularly finance, remains weak. However, some relevant work on the subject has previously been conducted. In 2002, shortly after the IT bubble burst in March 2000 (Griffin et al., 2011, p. 1252), economists Lawrence Gordon and Martin Loeb (2002, p. 439) put forth a model for optimal levels of investment into information security. The model laid the theoretical foundation for research aiming to transform abstract and complex IT investments into tangible cost-benefit figures.

In more recent years, Aissa et al (2012; 2010) developed a quantitative model to estimate the “Mean Failure Cost”, a model approximating the dollar amount of loss per hour of interrupted operation. A similar model was proposed by Bojanc and Jerman-Blazič (2008) to quantify a “Single Loss Exposure”. Patel et al. (2008) extends such initiatives by suggesting a new method for quantifying risks into numerical values in order to create a scale for degrees of cybersecurity. What these studies have in common is the intent to link IT security investments to expected loss levels. Research explicitly concentrating on the pure financial side of the matter is rarer.

Considering everything mentioned above, previous research demonstrates a clear lack of investigation into how cyberattacks affect specific financial metrics. One important such metric is the volatility of a particular stock. In financial terms, volatility is considered a proxy for risk, implying that, through the risk-reward tradeoff, an increase in stock and/or market volatility in turn raises investors’ demand for risk premiums (Yoon, S-J., & Byun, S.J., 2012, p. 59). The risk premiums are concretized through, among others, the CAPM model in which the variable beta is used to measure a firm’s relative risk (Brealey et al., 2010, p. 221). Essentially, beta is a measure of firm volatility in relation to the market, representing a stock's sensitivity to systematic risk. Higher relative volatility can be translated into a higher beta, which according to the CAPM model increases a company’s cost of capital (Brealey et al., 2010, p. 204 & 220-221). Additionally, too much volatility can mean risk-averse investors abstain from investing into a company altogether.

While beta incorporates and explains a firm’s sensitivity to market movements, and thereby its exposure to systematic risk, it misses to include a large part of the total risk.
The risk that exists beyond the systemic level is called idiosyncratic or diversifiable risk and covers risks specific to a certain firm. A traditional opinion amongst scholars is that investors will not get compensated for shouldering this type of risk since it can be diversified away (Arnold, 2008, p. 293). Empirical evidence on this matter is however inconclusive; in 2001 two scholars named Amit Goyal and Pedro Santa-Clara (2003) wrote an article in opposition to classical theory, concluding that, not only systematic, but total risk matters to investors and is therefore priced in market returns. This opens up for an interesting discussion beyond the scope of this study, but if found true, a cyberattack’s effect on idiosyncratic risk would be of interest, not only for the attacked companies, but for investors also. Therefore, even though beta, in connection with the CAPM model, vividly decomposes the risk-reward reasoning, total risk will be the focus of investigation throughout this study. That being said, investigating a stock’s reaction to the announcement of a cyberattack in terms of volatility, presents a new and interesting technique for measuring the financial costs related to such attacks.

Summing it all up, the problem lies in the actual measurement of the financial and monetary costs related to cyberattacks, both explicitly and implicitly. While other studies have chosen to address the problem by considering an attack’s effect on the market capitalization of a firm, another interesting angle would be to instead observe how the volatility of a stock behaves before and after an attack. By treating increased stock volatility as one proxy for the costs induced by a cyberattack, it would make sense to explore if such an attack causes increased volatility, if it is a temporary change or if the riskiness persists.

1.2 Research question

While the ultimate goal of measuring the financial cost of cybercrime was established already in the beginning, a feasible research question for accomplishing that goal has to be formulated. The final question originated from thorough discussions about which proxies for financial costs exist and can be utilized to accomplish the abovementioned goal in an efficient way. After much reasoning back and forth, stock volatility was chosen, mainly since it is previously unexplored and since it reflects the riskiness of a stock; increased stock volatility equals increased investor risk which finally ends up as increased cost of capital for the attacked firm. Based on this reasoning, the following research question will be examined:

What is the effect of a disclosed cyberattack on stock volatility for firms listed in the USA?

From the above presented material, it is clear that financial impacts of cybercrime are currently unpredictable. To formulate a research question that captures all nuances is difficult. Therefore, the main enquiry revolves around a single variable, volatility, to narrow the focus and increase the precision of the investigation. The wide scope of the rest of the question is intentional. As the concept of volatility in itself holds many dimensions, primarily those that can be categorized into short or long term, the question raises the need for more specific demarcation. In order to provide a comprehensive answer to the major question, the matter is preferably divided into several ones. Therefore, the study will break down and examine the question from the perspective of two time intervals: ‘short-term’ and ‘long-term’ effect on volatility. A more precise definition of these time intervals will be provided later.
1.3 Knowledge gap

Cybercrime is a highly actual issue, yet the academic attention paid to it is disproportionate to the large risks it possesses. Moreover, the complexity has partially restricted research to focus on mathematical and technical aspects with little integration of elements related to business administration. The tendency is that research focuses on improvements of IT security and infrastructure, forgetting that within corporations it is not an isolated division left to its own devices but instead a vital building block of a larger construct; in other words, there is a gap to abridge between the IT and business perspectives.

Given the information resources available, no similar research has previously been conducted either at Umeå University or elsewhere. In fact, as far as we are aware, no studies attempting to explore the cost relation between volatility and cyberattacks from a quantitative, financial perspective have ever been published. This qualifies the topic itself as both unique and innovative. That being said, the academic landscape solicits a completely new vantage point to study risks and costs from, as research preceding this typically has presumed a less-than-perfect understanding of the financial consequences from cyberattacks. One such vantage point from which the problem can be addressed is the abovementioned, linking the concept of stock volatility and cyberattacks. The logical reasoning behind choosing to examine stock volatility as a proxy for financial cost might need some elaboration, which therefore will be provided under the next headline.

Furthermore, the existing but limited research covering cyberattacks, and financial costs connected to such events, are either outdated or in need of revision as it has not kept pace with developments within the cybercrime area. The retrieved research is by scientific standards insufficient in scope and scale, but must be understood against the background of shifts and evolvement within IT just the recent 10-year period. In relation to the dynamic and constantly evolving nature of the subject, previous research is deemed quite old. Taking into consideration the aspect of time, today’s interconnected contemporary world bears little resemblance with the IT landscape of the early 2000’s, making it essential to carry out research given current premises. Purely based on concerns voiced by businesses, regulators, lawmakers, and experts, there exists a void of information to be filled. There is much reporting and presenting of facts which companies cannot interpret or use, complicating a transition from theory to practical action. In addition, the matter is so multifaceted that companies struggle in systemizing which information or action is relevant.

1.4 Research purpose

The fundamental purpose of this study is to investigate what effect a cyberattack has on the volatility of stock returns for a historical sample of attacked firms. To accomplish this goal, the study seeks to develop, and test, a new approach for measuring the financial cost imposed on a company as a result of a cyberattack. The study treats volatility as a proxy for costs and extrapolates increases in volatility to increases in risk for investors and increases in cost of capital for firms.

Breaking down the overall purpose, the study looks at the impact on cost of capital and risk premiums from a cyberattack. A highly volatile stock is considered a risky investment and, in order to compensate for that risk, investors demand higher risk
premiums than they would if investing in a relatively less volatile stock (Cavusoglu et al., 2004, p. 72). These premiums denote what price is set for shouldering the burden of uncertainty, essentially representing investors’ expected extra compensation from the company as compared to a risk-free investment. This hypothetical causal chain starts with an increase in stock volatility and culminates as an increase in corporate cost of capital, which fundamentally is what this research aims to examine.

On the way toward the overall purpose, the investigation fulfills several corollaries. One is to explore the general idea of cyberattacks within today’s interconnected economy. Another is to investigate the variable ‘cyberattack’ as an economic risk factor for companies, and how it interacts with and affects other variables. Other subpurposes include the gathering of literature and construction of a database for further research. Also, updating the status of previous research to present-day premises has emerged as an additional motive for the study.

Elaborating on the problem at hand, it is interesting to break down the research question and investigate what effect a cyberattack has on the stock volatility for two different time intervals: short-term and long-term. Examining short-term effects has the purpose of capturing the initial and immediate reaction to a cyberattack. A short time window restricts the possibility that factors besides cyberattacks are integrated into volatility swings. Short-term movements also offer a benchmark for market perception of an attack’s severity, when informational asymmetry is more prominent.

The long-term effect stands in firmer connection to the central part of the thesis, namely that a cyberattack is detrimental, not only temporary, but that the event raises the level of uncertainty and risk on a perpetual basis. An increase in the long-term volatility will by definition signify that a cyberattack has the potential to entail heightened average volatility, implying that the two perspectives are interchangeable. A detailed definition of the word ‘cyberattack’ is provided in Section 1.8. Arguments for what is considered ‘short-term’ and ‘long-term’ in the context of this study will follow in chapter 4.

Finally, a more self-evident yet important purpose of this study is to decompose the complex matter of impact of cybercrime on businesses into a comprehensible and isolated element of it. By only committing to examining a small part of the subject, the study in a feasible manner strives to provide insight, thus fulfilling the ultimate purpose of unique knowledge contribution. Although a cyberattack in this study is overly stylized and all events are treated as equals, such simplifications must be employed to operationalize the investigation’s main purpose. The mere vastness of the subject necessitates this sort of downscaling to grasp at the problem’s core. In addition, all attempts to explain each potentially influential variable empty themselves of purpose and use. Therefore, we disregard much of contemporary literature on IT risks and costs to better accentuate the financial effects of a cyberattack.

1.5 Delimitations

As is the case for most research, this too is subject to various delimitations to make the results as sound as possible. However, as long as these delimitations are explained, discussed and constantly kept in mind, they should not pose a threat to the validity and generalizability of the research. To begin with, the research explicitly aims its attention at disclosed cyberattacks. Thus, events that have taken place but never reached attention external of the affected firm cannot be included into the sample and the effects remain
uninvestigated. From a theoretical perspective, setting this limit skew the sample distribution in the sense that only disclosed attacks which “the market” can react to are included in the sample. While critics may argue that arranging the sample this way will impose a non-representativeness bias to the study, it is unavoidable due to prevailing information asymmetry.

In order to gain access to stock data, which is a fundamental prerequisite for this study, the research concentrates on attacks aimed at listed corporations. A problem with publicly listed corporations is that they almost always avoid disclosing negative information if they do not have to. In itself, such circumstances have the potential to create a negative spiral; the study is limited to examining listed companies, but listed companies often restrain completely from reporting cyberattacks. A CNBC article points to this fact by stating that, if a cyberattack, or the risk of such an attack, is not “material to investors”, corporations have no legal obligation to disclose information. They also often refrain from doing so due to “…concerns about possibly scaring off potential or existing customers, damaging their stock value, or incurring potential legal liabilities” (Javers, 2013).

The abovementioned reasoning implies that many cases probably never reach the public eye, in turn narrowing down the population size and making a convenience sample the only possible sampling procedure for this study. Examining the whole (available) population however tackles this problem. Furthermore, even though unfeasible to test due to data limitations, examining what financial impact cyberattacks have on SMEs may bear more practical relevance, especially since professionals state that “…small and middle-market companies may be more vulnerable to attacks because criminals know these businesses do not take substantial preventative measures” (Proppe, 2015). This study however only considers listed companies.

Another relevant delimitation worth discussing is the financial metric studied and utilized throughout the research process. This study makes use of volatility to express which above-the-market level of compensation firms are expected to pay to investors for the uncertainty caused by a cyberattack. No ratios or other performance indicators found in firms’ balance sheets are taken into consideration to review what effects arise from a cyberattack. Hence, industry or firm-specific conditions are disregarded in order to map out the general behavior of stock volatility attributable to a cyberattack.

Physical and industry delimitations are specifically important to denote here, simply since this research has but one. The thesis’ single restriction is to events involving firms listed and traded on U.S. stock exchanges. Framing the sample this way is a completely intentional decision, taken both in order to improve the generalizability and to facilitate statistical and academic comparisons. We acknowledge that these limits will impact the generalizability of the study’s results to other regions, something that must be brought to attention. There is little point in trying to explain the advantageousness of a representative sample when the objective is to draw conclusions about correlation and/or causality. In our case, the form, extent, and frequency of disclosed cyberattacks require us to narrow the perspective to attain a manageable level of observations, whereby we lose out on possibilities to apply the results to certain settings, circumstances, and contexts. However, the intention with this study is not to explain financial costs of cyberattacks while controlling for country or region. To control for geography, an event must be categorized by either country of origin or execution,
requiring extremely detailed information about every cyberattack. Even if the information is available, the time cost per event is not defensible. Focusing on U.S. stock exchanges has one great methodological advantage: settling for a single market bypasses such complexities.

Studying a phenomenon must have bearing on knowledge and research “outside” the particular study if the study is to earn status as generalizable. The intuition is that “unless we can make some generalizations, we are not really pushing knowledge forward” (Adams et al., 2007, p. 239). No research perfectly depicts reality, and can only go so far in attempting to. Research balances between lack of precision and lack of applicability. Creswell (2002) portrays this tradeoff through the metaphoric pyramid, where precise and narrow questions, i.e. “substantive theories”, make out the bottom of the research triangle while “grand theories” reside at the top where general applicability is highest (Creswell, 2002, cited in Saunders et al., 2009, p. 40).

Finally, existing literature can be described as either divergent from the purpose of this thesis, of age, or a combination of the two. Therefore, support from solid theorization is difficult to find, or concerning some issues not possible. In terms of theoretical broadness, the study lacks in scope. This stems both from the choice of proxy for costs and the subject in general. With few exceptions, found literature dates back a decade or more making it practically inept for this study. Also, there is scarce evidence on the cyberattack-volatility relationship, suggesting that the thesis embarks on a narrow and specific path, which in turn must be held up as a delimitation. Lastly, the study only reviews a span of five years between 2010 and 2015. Including, for example, events from the years of financial turmoil in the previous decade would pose the risk of producing explanations for circumstances or effects apart from the objective of the study. The occurrence of cyberattacks has steadily increased since the spawn of Internet, so by delimiting the time range to the last five years a number of incidents are left out, implying a reduction in explanatory capabilities which must be incorporated into the results.

1.6 Contribution and target Audience

Foremost, the study will contribute to the academic community. As the arena on which cyberattacks are carried out expands, empirical research must take new steps in order to understand what is happening, why and when it happens, and how to interpret an event. With more knowledge, scholars can recognize circumstances, examine and criticize assumptions, draw new conclusions, update existing theory or formulate new concepts. The thesis’ primary contribution is thus that of generating original knowledge by simultaneously covering a research gap and a knowledge gap. The claim is both ambitious and demanding, though reflecting the overarching objective with which all research should be undertaken.

Adjacent to this more general contribution, the thesis specifically purports to add to the extensive literature on market efficiency, volatility and risk, as well as cost of capital. Firstly, the concept of market efficiency is neither complete nor finite. The more information, the more room for interpretation of its relative worth, and in turn more situations concerning the effectiveness of markets to study and understand. The general stance among today’s researchers is that corporations do not fully comprehend the severity of a cyberattack and investors imperfectly absorb news of a cyberattack.
Understandably, there is room for additions to the body of market efficiency literature. Secondly, since the thesis concentrates on stock volatility, it will participate in the construction of broader knowledge bases within that area, but also financial risk overall. Concerning volatility, this study can dually enhance the theoretical development of the concept and the practical use of the concept within investing. The degree of contribution may here be modest but not insignificant since it emphasizes a field of scarce earlier work. Third and last, the investigation will improve existing literature about cost of capital. By exploring cyberattacks’ influence on stock volatility, insights into the nature of heightened risk premiums and cost/return of equity can be offered, at disposal for future research discussions about cost of capital.

The thesis also strives to complement its theoretical dimension with practical advice. As companies today struggle with the issue of (enough) protection against cyberattacks, supplying evidence on the potential costs and their permanence can hopefully instill action. Specifically, the study attempts to explain short and long term effects on volatility, key metrics for any company using equity funding. From investors’ perspective, the findings may not be pivotal but could contribute to a deepened understanding of stock and market reactions to announcements of breaches. The results’ usefulness is contingent on individual investing and trading strategy, suggesting the explanatory power is of limited use for some types of investors while of better use for others.

Furthermore, the findings from this research should be of interest for any company that is a potential target for cyberattacks, which includes practically all businesses. Knowing how a cyberattack generally affects stock volatility and company performance could for example aid relevant corporate decision-makers in their efforts of deciding how much to invest in cyber security. Making accurate and informed decisions of this sort, in time, also offers the potential to ease future transitions demanded by legislators.

The thesis ultimately intends to improve the overall knowledge about the costs of a cyberattack. An increased understanding of companies’ situations and the financial turmoil following an attack could be a step toward more harmonized regulation for reporting, an area rich of discussion and policy documents but with little common ground.

1.7 Disposition

The thesis is divided into six chapters for a more intuitive approach to the topic. The first chapter introduces and problematizes cyberattacks. The second chapter elaborates methodological issues. In the third chapter, all relevant theoretical concepts are explained to create a comprehensive framework. The fourth chapter explicates assumptions, calculations, and other practical elements. Statistical results and analysis follow in the fifth chapter. Finally, reflections regarding the process and contributions conclude the thesis.
1.8 Definitions

**Abnormal returns**: above expected returns of a stock in relation to a benchmark index (e.g. S&P500) using a pricing model.

**Abnormal volatility**: average standard deviation of abnormal returns.

**Cyberattack**: Today, a cyberattack happens so often that it is near to impossible to agree on a definition that is 1) general enough to include all forms of breaches, intrusions, attacks and attempts and 2) specific enough to denote a targeted, intentional attack, while 3) not accidentally counting glitches, internal system failures, or other accidental events. In light of such intricate and tricky defining, we will attempt to offer a realistic and relevant interpretation of the term, which pertains both to the nature of the studied attacks and the reviewed literature.

On its global website, electronics corporation NEC, a leading provider of internet, broadband network and enterprise business solutions, has defined a cyberattack as “socially or politically motivated attacks carried out primarily through the Internet. Attacks target the general public or national and corporate organizations and are carried out through the spread of malicious programs (viruses), unauthorized web access, fake websites, and other means of stealing personal or institutional information from targets of attacks” (NEC, 2016).

Kim et al. (2014) in a report for the Korean Ministry of Science, ICT & Future Planning state the following: “A cyber attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.” Cavusoglu et al. (2004, p. 71) explain it simply as “a malicious attempt to interfere with a company’s business and its information.”

In all three, synonyms to the noun ‘firm’ appear: “corporate organizations”; “enterprises”; and “company”. Thus, a proposed fusion of the three examples that this thesis could employ for the remaining text could be: a cyberattack is a deliberate attack, motivated by social and/or political reasons targeting nations or corporations through the use of malicious code, unauthorized web access and other means, orchestrated to steal personal or institutional information or interfere with such information to disrupt operations.

**Cyber crime**: online offences seeking to intentionally harm or damage the reputation, financial situation, physical and/or mental privacy, as well as nations’ security and financial health.

**Cyber espionage** and **cyber warfare**: primarily related to government-sanctioned cyber intelligence activities, attacking systemically sensitive institutions or corporations to retrieve information of national importance or destabilize nations. For example, major international airlines and a travels reservation company they employ were simultaneously attacked, as was a government agency and insurance company, to match flight records and reservations with personal records of high level officers to track movements.
**Data breach**: “a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so” (U.S. Department of Health and Human Services, 2015).

**Denial of Service** or **Distributed Denial of Service** (DoS/DDoS): an attack where large quantities of information requests are sent to the targeted company’s servers. The attack aims at flooding or overloading the servers to the point of shutdown, so the company’s website is inaccessible. Commonly, no data or information is lost, but businesses whose website is the main channel of revenue are impacted to a higher degree than firms with intangible internal assets and capital. Losses also include lowered customer trust about security and privacy.

**E-commerce**: online retailers or trade sites, for example Amazon, Ebay and Alibaba, relying solely on web-based shops and trade to generate revenue, together with advertisement revenue in connection to such online market places.

**Hacktivism**: a word fusion of activism and hacking, with objectives to promote a political agenda pertaining to freedom of speech, information, and conscience, or as online protest movements against companies, agencies, or individuals.

**Internet-specific firms**: companies operating on digital platforms, often driven by user content and advertising channels, which create a digital ecosystem to retain users/customers. Examples include Facebook, Google, Alibaba, Baidu, Tencent and Twitter.

**Malware/malvertising**: malicious software, abbreviated malware, is a specifically constructed software with the built-in purpose of sabotaging or disrupting computer operations, collect sensitive information, oversee computer users’ patterns. Can also mean displaying harmful/detrimental advertisements, hence the portmanteau malvertising.

**Unauthorized access**: breaches into internal databases, records, e-mail or other communication. For example, key client contracts, unique product schemes, sensitive information from negotiations, internal economic communication and reporting, and much more. Example: attack on JPMorgan Chase in 2014, resulting in 84 million stolen customer records.

**Virus attacks**: infects “host” systems by reproducing itself within file systems or operative systems to damage data, erase or modify stored information, or assume control (often disguised). Incurs high maintenance or proactive protection costs as well as costly system failures.

**Volatility**: see chapter 3, page 38.

**Website defacement**: a well-known method of protesting or disavowing a company, agency, government or individual by remotely accessing the object’s web server and replace the original website with personal or political statements, or other pernicious modifications of visual appearance. Commonly used in hacktivism to demonstrate know-how while serving as a protesting gesture.
2 Methodology

In this chapter, the objective is to introduce and develop the philosophical bedrock of the study. Such deliberation concerns preconceptions, the stance on knowledge and reality, as well as the research approach, design, strategy, perspective and method. A discussion about approaches to literature, data and sources ensues, together with an extensive ethical review. Lastly, a figure is given to clarify how the various parts interplay and influence the thesis.

2.1 Choice of topic and preconceptions

Choosing this topic came natural to us for several reasons. Over the course of our education within finance, we repeatedly encountered a core set of financial principles. Of those, the Efficient Market Hypothesis drew the most attention. Consequently, we obtained a good deal of knowledge about market efficiency, the various forms it theoretically takes, and influences on each form. That also strengthened our general understanding of markets, their reactions and how expectations shape stock market behavior. Departing from that knowledge, the view on cyberattacks is ambivalent: they must affect stocks in some way, but how seems more diffuse than the Efficient Market Hypothesis portrays it.

The first, and probably most important, reason for entering this research is our shared interest in both financial and IT-related issues. Already from the start, we knew we wanted to write our thesis on a subject in the borderland between finance and technology. The idea for this specific subject started to crystalize in 2014, after the severe cyberattack on JPMorgan Chase. In that particular attack, data associated with approximately 84 million accounts were breached in what was later described as the largest corporate data breach in history. In the press turmoil surrounding the attack, the research topic materialized. We simply began to wonder, and reason, about the abundance of information and the fact that sources contradicted each other. It seemed unthinkable that information asymmetries did not arise, the question rather being how market participants put the stream of information to use. We perceived a discrepancy between information availability and information utilization, meaning that the foundational financial principle of market efficiency appeared suspended. Did the market fully recognize the magnitude of the announced information? How efficiently did markets incorporate the disclosed attack?

The JPMorgan attack is, however, not unique: every time information about a similar incident reaches the media, news coverage is huge. In response to such events, voices are raised from cybersecurity companies, the president of the United States and many more in between, worryingly warning us about the enormous costs cybercrime impose on the global economy. The question is: does anyone really know, or even know how to approximate, the true financial cost of cybercrime? Scrutinizing articles, books and previous academic work on the subject, it seems not. Herein lies the natural knowledge gap that this research aims to contribute in filling.

Our general preconceptions are rather mapped out. First of all, we expect to find important evidence on the relationship between cyberattacks and stock volatility, with expectations of an existing correlation between cyberattacks and increases in stock
volatility. The preconceptions mainly stem from the prevailing public ignorance and uncertainty related to cyberattacks, and historic financial impact on companies. There are numerous theories, more thoroughly discussed below, relating uncertainty to erratic investor behavior. Our main preconception, briefly explained, is that we anticipate announcements of cyberattacks to cause erratic behavior amongst uninformed investors, in turn leading to increased stock volatility for the attacked corporation. While we do not expect it, were we to find the opposite, that cyberattacks do not inflict stock volatility, it would make for even more interesting evidence. Regardless of our preconceptions about findings, they do not direct the research process in any way. Maintaining an objective and value-free research process is vital for attaining unbiased results.

Summing it up, we, the authors, have a strong interest in the research area, the subject itself is highly current and previously unexplored, and we both expect that our findings can aid companies in their task of estimating financial costs related to cyberattacks.

2.2 Our perspective

We seek to improve existing knowledge about costs for companies’ risks and especially those stemming from cyberattacks. It is therefore, above all, through an investor’s eyes this study examines the issue. Assessing volatility, with extensions into risk premiums and other investor-related components of financial theory, stresses an outside-in posture. First and foremost, the thesis sets out from the investor side. However, as the topic subsumes volatility and cost of capital into a one-dimensional notion, there are additional perspectives to mention.

The focus on risks and risk premiums means the topic becomes a two-sided coin: what is true for investors in terms of higher premiums is equally but negatively true for companies, and an individual investor’s demand of a certain level of premium corresponds to a company facing higher cost of capital given its level of risk. Rephrased, looking at the problem through the lenses of an investor actually is better described as looking through a double-sided mirror because all actions of investors are reflected in the company, and vice versa. The two are mirror images of each other and so is risk premium and cost of capital. Thus, the interchangeability of perspectives inevitably means the study follows parallel narratives.

Shifting over to a corporate perspective, through the investigation of financial costs of being attacked, companies can attain new insights into the effects of suboptimal cybersecurity on their volatility and in extension their cost of capital/cost of equity. The two sometimes-competing views within corporations, IT and finance, become integrated into a new construct: an aggregated cost of an attack. Hopefully, the study provokes self-critique and opens corporations’ eyes for a more holistic approach to cybersecurity. To a lesser extent, academics, researchers, and legislators can profit from the contemplations raised in this thesis, though the perspective is not selected to directly address these.

2.3 Research philosophy

Thorough clarifications of the perspective on how one produces knowledge is the foundation of any research aspiring to legitimacy. In its simplest form, an explanation along the lines of Saunders et al. (2009, p. 107) suffices: the term “relates to the development of knowledge and the nature of that knowledge.” Furthermore, research
philosophy tells reviewers and readers how the researcher(s) regard the world around them and which assumptions they base their research on. By explaining what we know and how we know it, we are in a better position to understand reasons as to why research is conducted with certain approaches or arrive at certain conclusions (Adams et al., 2007, p. 25). For simplicity, only the two chief ingredients, epistemology and ontology, within research philosophy will be considered. The two denote “how we know [knowledge]” and “what knowledge [is]” (Creswell, 2002, p. 6). Below follows a demonstration of these positions.

2.3.1 Epistemology

For most investigations, three distinct schools of thought present themselves toward which researchers need to define their relationship. Principally, research either departs from a background of positivism or interpretivism, with realism as a negotiated blend of the two stances. Primarily, this subdivision of knowledge creation specifies if a researcher regards the world as scientifically determinable or contextually interpretable, i.e. if one adheres to a positivist or interpretivist philosophy. The former holds that research purports to study “an observable social reality” which ultimately will produce “law-like generalizations similar to those produced by the physical and natural scientists”’ (Remenyi et al., 1998, cited in Saunders et al., 2003, p. 83); contrastingly, the latter variant declares that “the social world […] is far too complex to lend itself to theorizing by definite ‘laws’” found in the natural sciences (Saunders et al., 2003, p. 84).

Any research undertaken has its motivation, its process and its objective. These elements are naturally influenced by myriad of circumstances, ranging from resource constraints to imprecise measurement instruments. But above all, scientific exploration seeks to emanate verifiable theories in order to construct laws, just as within natural sciences (Bryman & Bell, 2011, p. 15). Adopting this viewpoint onto the study of social sciences facilitates objective quantifications of the social world, but should not be mistaken for given truths. As laconically phrased by G.E. Box, “All models are wrong, but some are useful” (1979, cited in Adams et al., 2007, p. 34). Positivism simply applies the same approach for examining social relationships as for testing those in nature. Reformulated, the position recognizes the existence of an “external reality” (Bryman & Bell, 2011, p. 17). Therefore, any positivist researcher “is independent, taking the role of an objective analyst” (Blumberg et al. 2011, p. 17), hence making it value-free and installing a straightforwardness unheard of in interpretivist camps.

Upon the deliberation about positivism follows the question of what its alternative consists of. If one for example does not acknowledge that research through its objectiveness is reliable, an explanation for how to assemble, verify or falsify knowledge must be offered in place of positivism. Alas, the epistemological counterpart to positivist research can be described as interpretivist; alternations of the term are constructionism or social constructionism, implying reality is “constructed” as opposed to the independent reality propelled by positivists (Saunders et al., 2003, p. 84). In essence, the premise that the world operates autonomously and is unattached to people within it is disqualified by interpretivists. Rather, all researchers are “part of what is observed” (Blumberg et al., 2011, p. 17), bundling together personal interests and research in a way necessitating an exploration of “the subjective meanings motivating people’s actions in order to be able to understand these” (Saunders et al., 2003, p. 84).
The key descriptor of interpretivism is subjectivity, warranting a meticulous mapping of the actual context(s) to comprehend processes and actions.

Realism deserves a brief account, as it amalgamates the neutrality of positivism with the assertion of interpretivism that socially generated entities shape researchers’ preconceptions and references. This third and often overlooked epistemological branch is best denoted as a middle-of-the-road alternative to the aforementioned theories lining collective knowledge. Generally, confessing to realism postulates a belief that “through the use of appropriate methods, reality can be understood” (Bryman & Bell, 2011, p. 17). Realism is further divided into two strands: empirical and critical realism. The merit to such separation lies in its ability to capture the element of change which new knowledge often precedes. Critical realism thus “recognizes the existence of a gap between the researcher’s concept of reality and the ‘true’ but unknown reality” (Blumberg et al., 2011, p. 18), contending that the gap induces change. By incorporating the role of behavior into explanations of a certain reality, critical realism manages to balance positivism’s emphasis on explaining and interpretivism’s focus on understanding (Bryman & Bell, 2011, p. 16).

In its most distilled form, the purpose of the thesis is to investigate the relationship between a disclosed cyberattack and the attacked company’s stock volatility. The presence, or absence, of direct relationships between variables in a statistically significant correlation allows for drawing conclusions about cause and effect within a selected sample/population. Doing so presupposes value-free, independent researchers examining objective, quantifiable facts in a continuous process of isolating elements to derive laws or “law-like generalizations” (Remenyi et al., 1998, cited in Saunders et al., 2003, p. 83). It therefore naturally follows that the positivist epistemology concurs with the thesis’ fundamental idea and purpose, which is to explain, not understand, behavior of stock volatility. A more behaviorally oriented investigation would have to consider the benisons of critical realism to fully describe factors influencing and driving actions, a compromise this thesis’ cause-effect layout eliminates. Interpretivism’s inherent subjectiveness renders it irrelevant for this thesis.

2.3.2 Ontology

Another important philosophical aspect to consider before advancing in any academic process is ontology. Ontology is an old philosophical discipline that ponders upon the suppositions held about the nature of social reality (Long et al., 2000, p. 190). Bryman & Bell describes the central ontological matter as a question of whether or not social entities are objective and external from the influence of social actors (2011, p. 20). In other words, ontology raises the philosophical question of how to interpret reality; should it be considered a given constant, independent from human interaction? Or should it be considered a subjective social construction, dependent on human perception? A vivid and widely employed aphorism, summarizing the question at hand in one sentence, goes as follows: “does a tree falling in a forest make a noise, even if there is no one there to hear it?” (Lee & Lings, 2008, p. 112).

Ontology is often divided into two different main schools: objectivism and constructionism. As the name suggests, supporters of the objectivistic camp view social reality as objective, whereas followers of the constructionist view consider it subjective and dependent on individual interpretation (Long et al., 2000, p. 190). More precisely, researchers taking an objectivist approach disqualify humans’ ability to, in any way,
alter the social reality on which society is built. Lee & Ling shed light on this by arguing that “objective truth is contingent on a philosophy that suggests that our beliefs, whatever they are, have no bearing on the facts of the world around us”, so what is true is always true, even if we stop existing at all (2008, p. 112). Bearing this in mind, conducting research based on strict objectivistic values disregard the very notion of human influence on society and focuses only on observable and measurable facts of nature.

In direct contrast to objectivism stands constructionism. Researchers taking this philosophical stance believe that, rather than being an independent, constant phenomenon, reality is constructed in the mind of the knower. They suggest that humans create their own reality, or at least interpret it, based on their individual perceptions (Jonassen, 1991, p. 10). An extreme and purely subjective version of constructionism is known as metaphysical idealism. Supporters of that school hold that reality is entirely dependent on people’s perceptions of it, arguing that everything that exists, exist as a product of the human mind and mental experiences (Lee & Lings, 2008, p. 112). Despite it being a philosophical extreme, the aforementioned ‘ism’ rather vividly illustrates the reasoning of constructionists. This boils down to the fact that, as opposed to objectivists, constructionists very much emphasize the individual’s subjective perception as foundation of the society. Thereby, scholars taking the constructionist stance center their research on interaction between individuals and its impact on reality.

This research is conducted based upon objectivist values. While the correctness of taking this stance could be argued back and forth, the main goal of the study is to, objectively, examine a hypothetical phenomenon, not the reasons behind that phenomenon. In other words, the central philosophical perspective of the objectivist stance allows us to examine “what happens”, not “why or how it happens”, which we would be forced to consider if taking a constructionist stance. That being said, it is still very important to realize that the core aspects of our research, cyberattacks and stock volatility, essentially are phenomenons created by humans. This is dangerous and could potentially set the pure objectivity of the research at risk, mainly since the very notion of human influence on the central variables of the study insinuates subjectivity. While it is something we are forced to keep in mind throughout the whole research process, the objective of the study, to establish, not explain a supposed relationship, persists. Therefore, even though a study within the social sciences, its methodology shares many similarities with studies from natural science; the most important characteristic being the reduction of human behavior down to quantifiable variables.

Summing up our reasoning, even though humans and their individual perceptions are the fundamental perpetrators, both behind fluctuations in stock prices and cyberattacks, we will disregard that and, in order to be as objective as possible, consider those two factors forces of nature.

2.4 Research approach

Clarifying how research is influenced or guided by a researcher’s values and perceptions is crucial to gain insight into tests and results. Apart from ventilating epistemological and ontological considerations, researchers must make clear to any reader their approach to research. In other words: a research approach states “the place where you introduce theory” into the proposed research (Blumberg et al., 2011, p. 20).
The categorization specifies whether a study employs a deductive approach, adjacent to epistemological positivism and ontological objectivism, or an inductive approach which is linked to interpretivism and constructionism. Saunders et al. however hesitate about the practical value of “such labelling” (2003, p. 85).

Nevertheless, the deductive approach is invariably connected to the term “scientific research” as it develops a theory “that is subjected to a rigorous test” (Saunders et al., 2003, p. 86). Deduction is described by Blumberg et al. as “a form of inference that purports to be conclusive” (2011, p. 21). Essentially, the approach searches for explanations of “causal relationships” (Saunders et al., 2003, p. 21) and “operates from the general to the specific” by testing universal laws which “are essentially only hypotheses which continue to require testing against the predictions of the laws themselves” (Adams et al., 2007, p. 29). Deductive research presents reasons upon which a conclusion should base itself and “therefore represent proof” (Blumberg et al., 2011, p. 21). The use of logical, rational principles is a hallmark of deduction (Lee & Lings, 2008, p. 6). Important characteristics of the deductive approach are controls, highly structured methodology, observer independence, possibility to operationalize concepts, and generalization (Saunders et al., 2003, p. 86).

Inductive research is antithetical of deductivism. Whereas deduction tests theory, induction builds it. Theory produced in an inductive manner implies “theory would follow data” (Saunders et al., 2003, p. 87) and thus operate “from the specific to the general” (Adams et al., 2007, p. 29; Lee & Lings, 2008, p. 7). The purpose of observations is to expose the behavior of a certain variable to “formulate a general theory” (Adams et al., 2007, p. 29). Because of inductivism’s focus on behavior, it is of equal concern to investigate the nature of circumstances surrounding particular behavior to capture enough evidence for making claims. Yet, in the inductive world a “conclusion is only a hypothesis” and “an inferential jump beyond the evidence presented” (Blumberg et al., 2011, p. 22), so collecting data in order to generate theory is an innately limited process.

Traditionally, quantitative studies predominantly assume a deductive logic where data is checked against pre-existing theories. Conversely, inductive studies are principally of qualitative, theory-generating style within new fields and with modest degree of previous literature. The division is however not categorical. The crux of generating new knowledge means the two approaches are practically inseparable from one another, and as Eriksson & Kovalainen (2016, p. 24) claim, “[t]hese two ‘ideal types’ of research … seldom exist as clear-cut alternatives” so “many researchers use both”. This research however sets out from a vast array of literature on topics such as uncertainty, volatility, risk and risk premium; from thereon, these concepts are applied in a novel setting with differing conditions than that of research found now. In other words, the methodological aim of this study is to fill a knowledge gap by deducing unique hypotheses from already existing theories; these hypotheses will then be operationalized, statistically tested and confirmed or rejected. Based on the outcome, theory will either be revised or modified. In any case, new knowledge will be created. Given these premises, a deductive approach is best suited for this study.
2.5 Research design

Having declared the fundamental philosophies adhered to in this study, it is time to explain the different research designs and their implications. Conducting academic research can very much be compared to constructing a building; before ordering material and turning the first sod, the builders need to have a sketch of the design, a blueprint to follow. The same is true for any properly conducted research. Cooper & Schindler refers to research design as the part that draws up the “blueprint for the collection, measurement, and analysis of data” (2014, p. 124-125). They further state that the three most important design types are: exploratory, descriptive, and causal/explanatory (2014, p. 124-125). Below follows a short introduction to these three designs, followed by an argumentation supporting the choice of design for this study.

Exploratory research aims to explore a perceived problem that has yet to be clearly defined. It often departs from an indistinct intuition saying that something is happening, and aims to explore and more clearly define what that something is (Saunders et al., 2003, p. 96). Both Cooper & Schindler (2014, p. 129) and Saunders et al. (2003, p. 97) emphasize that conducting exploratory research potentially could save researchers both time and money by indicating early that a more formal study is not worth pursuing. Exploratory research could be considered a good technique when the goal is to acquire knowledge about a hypothetical problem of which previous knowledge is scarce. It is also presents a good start to the process of paving the way for more formal studies.

In contrast to the more informal exploratory design stands descriptive research design. The goal of a descriptive study varies but the most common one is to describe a phenomenon associated with a predetermined population. This is often accomplished by the discovery of association among different variables. Such association does not, however, automatically establish a cause and effect scenario (Cooper & Schindler, 2014, p. 136). Furthermore, Saunders et al. state that using a descriptive design is very common in business and management research. They also emphasize that it is vital to have a clear picture of the phenomenon up for scrutinizing before collecting data about it. (2003, p. 97). Considering this, conducting a descriptive study is a good choice when the goal is to describe a phenomenon that is clear and previously known. That it has the potential to provoke the ‘why’ question of explanatory research is of course only a plus (de Vaus, 2001, p. 2).

Explanatory, or causal, research could arguably be considered the last instance in the research cycle. It often builds upon previous exploratory or descriptive studies and, instead of exploring or describing a phenomenon, it aims to establish a causal association between variables (Saunders et al., 2003, pp. 97-98). de Vaus argues that an explanatory study focuses on the ‘why’ question of a phenomenon (2001, p. 2). Cooper & Schindler elaborates on that and states that in order to answer the ‘why’ question, the goal is to establish a cause and effect relationship between an independent and a dependent variable. They further emphasize that control is of the essence and that all factors (as many as realistically possible) except the independent variable need to be held constant in order to establish such a relationship (2014, pp. 136-137). Finally, de Vaus distinguishes between ‘correlation’ and ‘causation’ and argues that, while correlation can be observed, causation cannot; it has to be inferred (2001, p. 4). This strikingly separates a descriptive study from an explanatory: while the former aims to observe and describe a correlation, the latter aims to explain that correlation by inferring causation.
Considering the abovementioned information, this study will be designed in a descripto-explanatory manner. The reasoning behind this is rather clear: since no similar studies have been conducted previously, the first part of the research design aims at finding and describing a hypothetical pattern between cyberattacks and stock volatility. If any pattern is found, the design’s second part will focus on explaining that by inferring statistical causation. This means that the research will start up in a descriptive fashion and finish in an explanatory manner. Designing the research this way is both necessary and academically preferable. To first find and describe a pattern is necessary due to the lack of previous studies. To explain a conceivable pattern is preferable due to the increased meaningfulness of the study’s academic contribution. Constructing the study by way of combining the two designs allows for a more thorough account of the initial research question. The appropriateness of such a selection is confirmed, too, in consideration of the scholarly situation at hand. The research question strives to fill a academic blank by exploring the relationship between a cyberattack and volatility, hence justifying, or rather requiring, the engagement of two separate designs.

2.6 Research strategy

After defining philosophy and approach, researchers must settle on an appropriate strategy for answering the research question. Though a clear-cut answer is called for, among others the objectives with the research, the research question itself, existing literature and resource constraint, all will influence the choice of strategy in various directions (Saunders et al., 2009, p. 141). In the endless field of research, multiple variations of specific strategies have emerged, not to mention the combined use of several. The dynamic domain makes specifications a complicated task, and researchers have no uniform grouping of the strategies. Thus, Saunders et al. (2009, p. 141) list eight subdivisions in contrast to Bryman and Bell’s (2011, p. 45) pentagonal version. To streamline this section, the chosen strategies are explained and argued for, leaving out thorough examining of those that do not apply to this thesis.

Based on Saunders et al., an experiment is the “‘gold standard’” (2009, p. 141) for evaluating all other strategies. The strategy’s function is to establish a causal relationship “between two variables” (Saunders et al., 2009, p. 142) and enjoys strong standing as a mean of deriving answers to questions in both explanatory and exploratory studies. Research-wise, experiments go furthest in eliminating obfuscating factors so that “possible effects of an alternative explanation” are removed (Saunders et al., 2009, p. 142). By controlling for eventual impacts of other variables, the experiment supplies unparalleled “confidence in the robustness and trustworthiness of causal findings” (Bryman & Bell, 2011, p. 45). This study will not make use of a control group, or manipulate the independent variable, insisting upon alternate strategies.

The two alternatives left are quasi-experiments or cross-sectional design: the first-mentioned owning “certain characteristics of experimental designs” in contrast to the second’s focus on data collection and relationship detection (Bryman & Bell, 2011, p. 50-52). Saunders et al. (2003, p. 142-144) simply maintain the experiment-survey dichotomy to infer that any research lacking control groups automatically transmutes itself to a survey strategy. Whether labelled cross-sectional (Bryman & Bell, 2011) or survey (Saunders et al., 2009), the strategy allows for “collect[ing] quantitative data which you can analyze quantitatively using descriptive and inferential statistics” (Saunders et al., 2009, p. 144), data which then can indicate “possible reasons for particular relationships between variables” (Saunders et al., 2009, p. 144). Bryman &
Bell (2011, p. 56) succinctly sum up that “most quantitative business research employs a cross-sectional research design rather than an experimental one” and attribute it to the fact that the “vast majority of independent variables with which business researchers are concerned cannot be manipulated” (Bryman & Bell, 2011, p. 45). Subsequently, the thesis is therefore of “ex post facto” format (Blumberg et al., 2011, p. 149).

In complement to the cross-sectional design, there is need to involve a form that covers the temporal aspect. Bryman & Bell denote such designs as “longitudinal” (2011, p. 57), somewhat differing from Saunders et al.’s terminology of “archival” (2009, p. 150). In any situation, making use of secondary data not originally collected for research implies that the research by nature is archival, or in the words of Saunders et al.: “part of the reality being studied” (2009, p. 150).

Continuing, some research strategies are of little use for this study but still have direct and practical use in other situations. For example, in qualitative research, the employed strategy should help in answering ‘Why?’ and ‘How?’ questions” (Blumberg et al., 2011, p. 256). Utilizing case studies is especially suitable in situations where researchers aim to “gain a rich understanding of the context” (Saunders et al., 2009, p. 145). As the case study strategy has issues regarding separation of the object of study and “the context within which it is being studied” (Saunders et al., 2009, p. 146), and the type of research question put forward in this study is of ‘What?’ character, the strategy is irrelevant.

A combined note on the remaining strategies can expedite the discussion about strategies that do not apply in this case and why. Blumberg et al. (2011) group the following four strategies together under one chapter dealing with ‘other qualitative approaches’: narrative analysis, ethnographic studies, action research, and grounded theory. All therefore disapply in one way or the other for this thesis.

Narrative analysis “allow[s] for in-depth investigations” (Blumberg et al., 2011, p. 297) by reviewing wording, sequence of elements in stories and anecdotal information, entailing the strategy is subjective and of limited use. Ethnography revolves around the notion of description: it relies heavily on portraying “the world it studies” (Blumberg et al., 2011, p. 299). Notwithstanding the need to understand settings and forces fanning cybercrime, it is beyond this thesis’ scope to study these.

Action research engenders a sense of trial-and-error solely through its naming, and the iterative strategy continuously weaves back and forth between resolving issues through action and evaluating such actions to instigate organizational change (Blumberg et al., 2011, p. 300; Saunders et al., 2009, 147). Lastly, grounded theory is highly symbolic in its perspective, focusing almost exclusively on interpreting the interrelational man-world duo (Blumberg et al., 2011, p. 300). All preconceptions on the researcher’s behalf should be, to the extent possible, eliminated by abstaining from reading “existing previous literature on the topic” (Blumberg et al., 2011, p. 300-301) and avoid all other sources of interference. Saunders et al. elucidate by explaining that “data collection starts without the formation of an initial theoretical framework” (2009, p. 149), and that observations feed into data that subsequently formulate a theory, whereupon the data feeds newer predictions that are tested and ultimately confirmed or rejected. Thus, theory is “grounded” in data (Saunders et al, 2009, p. 149). None of the two support the pursuance of an answer to the research question and can hence be discarded in this setting.
In summary, the strategy for a thesis depends in large on the included variables, the possibility (and intention) to manipulate and control these, and the type of question (why or what) asked by the researcher. Because no feasible experimental setting is achievable, this study relaxes such conditions to instead assume a survey strategy (sometimes referred to as a cross-sectional strategy). Due to the non-experimental setup, the study additionally is retrospective in its dealings with variables (also called ex post facto), translating into a position “after” the establishment of facts, in this case historic stock behavior. Moreover, retrieving that sort of data demands access to and exploitation of various archives, thus insisting on an archival research strategy. Settling for a case study would trade this thesis’ what-question for a why-question, so that alternative is rejected, together with the four strategies (narrative, ethnography, grounded theory, action research) primarily reserved for qualitative studies. Emanating from the broadness of cyberattacks and cybersecurity, the research question demands a wider perspective than case studies offer, while at the same time ridding itself of the controlled treatment needed for a truly experimental strategy. Therefore, it can from the question be derived that flexibility and compromise drive the choice of strategies.

2.7 Research perspective

No research enjoys infinite time spans. Besides stating the obvious, there is need to delimit and restrict any study in order for it to bear any relevance, ours being no exception. Thus, a certain period of time, or a time window, applies for retrieval of individual events as well as measuring the presumed impact of a cyberattack on volatility.

Another aspect of time worth mentioning is that which attends to a study’s purpose: either a single point in time or multiple occasions are to be investigated. Saunders et al. (2003, p. 95) advance two options for any researcher’s time horizon. The choice stands between an exact recounter, a “snapshot”, and a sequential development over the course of time, illustrated as a “diary”. Choosing is not categorically rule-based but instead dependent on the posed research question, although independent with respect to research strategy. The snapshot methods correspond to a cross-sectional time frame, meaning that the diary-styled approach covering “more” time represents longitudinal research.

Cross-sectional analysis “[seek] to describe the incidence of a phenomenon” (Saunders et al., 2003, p. 96) with data collected at a particular time, as opposed to longitudinal studies’ “capacity [...] to study change and development” (Saunders et al., 2003, p. 96). Seeing as this study mixes elements of the two methods, there is no decisive answer as to which approach is appropriate. On one hand, the short-term effect of a cyberattack on stock volatility is analyzed at time of occurrence; on the other, the time perspective must be prolonged to illuminate long-term/average volatility levels.

Adjacent to the question of time limitations is the aspect of a time frame to capture an event. Event studies are widely used within research in economics, finance and accounting, since the method “measures the impact of a specific event on the value of a firm”, thus enabling an estimation of the economic impact of an event based on the logic that “given rationality in the marketplace, the effects of an event will be reflected immediately in security prices” (MacKinlay, 1997, p. 13). Hence, this study relies on an event study to approximate the impact of a cyberattack (the event) on firms’ stock volatility (a proxy for value). An event study focuses on abnormal returns “at and
around the time of some event” (Armitage, 1995, p. 25) to compare with returns prior to an event to infer effects produced by a specific event. At best, an event study offers understanding of “sources and causes of the effects (or lack of effects) of the event under study” (MacKinlay, 1997, p. 16).

All this however assumes perfect conditions for identifying the date of an event, something which is easier said than done. MacKinlay holds up the sluggishness of newspapers as a distorting factor when concentrating on announcement dates (1997, p. 35). Financial (and other) press may very well have received the information one or several days before disseminating it, meaning that market actors too could have accessed and acted upon it, so the event could already be incorporated into a security’s price pre-announcement.

2.8 Research method

In discussions of method, parties convey the impression that the choice more often than not stands between a qualitative and quantitative one. As a matter of fact, the third and sometimes omitted alternative, a mixed method, is of equal interest for research. Understanding the three methods is critical to attain legitimacy, validity and credibility for one’s study. The inclination to divide explicitly business research into an either-or field is somewhat detrimental to the examination of different methods, as the purpose is not to arrive at a definite answer. Rather, the fortes and drawbacks must be illuminated to allow for fruitful business research.

Predominant traits of a quantitative method include a deductive approach to theory and research, based on positivism and objectivism (Bryman & Bell, 2011, p. 27). On the other hand, qualitative research highlights “words rather than quantification” (Bryman & Bell, 2011, p. 27) and assumes an inductive, theory-generating approach with interpretivist and constructionist connotations. Saunders et al. (2009, p. 151) describe the quantitative method as one dealing with or generating numerical data. Blumberg et al. echo this, stating that quantitative methods “rely on” numbers and figures, all the while emphasizing the impossibility in deciding which method is “better or more useful” (2011, p. 144). Clear is, however, that the quantitative method corresponds to the epistemological assertion that reality is measurable, although “the line between positivism and interpretivism” (Blumberg, 2011, p. 144) isn’t as accentuated as that between quantitative and qualitative methods.

The purpose of research will subsequently determine in which direction the methodological path goes. If the objective is to deduce hypotheses and explanations through statistical (or other testing) it requires research based on quantitative material, weighed against the qualitative orientation pursuing deeper understanding of phenomena through extensive investigation and analysis of such phenomena (Blumberg et al., 2011, p. 144). In cases where such distinctions do not serve the objectives, integrating the two separates is arguably a smart compromise. Much critique has been directed at the combination due to underlying philosophical controversies and inherent irreconcilability in general (Bryman & Bell, 2011, p. 629). However, “mixed methods research has become an increasingly used and accepted approach to conducting business research” (Bryman & Bell, 2011, p. 630). Saunders et al. (2009, p. 151) juxtapose “multiple methods” and “mono method” to explain how multiple methods constitute a full and worthy option but still internally demand a quantitative-or-qualitative disposition.
Considering the thesis’ aim, namely to describe and measure the effect on and change in volatility in connection with a cyberattack, the only viable alternative for choosing a method is the quantitative technique. By formulating hypotheses to test statistically, the epistemology, ontology and research approach all corroborate the use of a quantitative method. This choice of method is further endorsed by the quantitative archival data utilized in the statistical measurement and hypothesis testing process.

2.9 Literature, data and source critique

Having access to literature, relevant data and other sources of information is a crucial part of every research process. Without the inspiration from previous knowledge to build upon, it would be very hard to create new knowledge. Luckily, with access to modern libraries and the incalculable abundance of information the World Wide Web provides, sources of knowledge are not scarce. In their book on research methodology, Saunders et al. divide such sources into three categories: ‘primary sources’, ‘secondary sources’, and ‘tertiary sources’ (2009, p. 68). Primary sources are described as the first knowledge instance and the original pieces of work. They include published reports, government publications, letters etc. Secondary sources constitute the second instance in the knowledge flow and consist of material such as books and journals, secondary sources are often also easier to locate than primary ones. The last category is assigned to tertiary sources, also called ‘search tools’, such sources often function simply as an instrument, utilized to introduce or find the former mentioned categories of sources. Examples of tertiary sources are indexes, abstracts encyclopedias (Saunders et al. 2009, p. 69).

This research avails itself almost exclusively of secondary data to compile the sample, retrieve data and perform tests. Adams et al. define secondary data as data “which are made available or have been collected for other research purposes” (2007, p. 85). Exploring such data, Adams et al. continue, requires that the researcher “should start first with an organization’s own data archives” (Adams et al., 2007, p. 85). The thesis meets such demands to a moderate extent, as it utilizes press releases, communiqués and other corporate announcements to locate and specify dates of cyberattacks subsequently matched with stock movements. The same is true for the collection of data on stock returns, which will be collected solely from the Thomson Data Stream database.

Secondary data offers advantages that primary or tertiary data do not. Blumberg et al. reason along the lines of frugality, pressing on the fact that using secondary data “saves time and money” (2011, p. 236) which reproduces the idea of Saunders et al., that secondary data saves “enormous” quantities of resources (2009, p. 268). Finding secondary data is naturally time consuming, but the strain can be alleviated by using databases and archives. For the purpose of data collection, this study is largely dependent on secondary data, as it is neither feasible nor desirable to collect primary data on for example stock volatility or company information about announced cyberattacks. The consequence of high dependency is that access is vital, and if the data is spread over numerous sources, compilation may be impaired (Blumberg et al., 2011, p. 236).

It should however be mentioned that sources other than secondary have been relied upon during the research process. Primary sources played a somewhat important role, especially during the initial monitoring process and as a part of the foundation for the theoretical structure. Most of the sources, both primary and secondary, have been
collected using electronic and physical resources from the university library. Databases such as EBSCO, JStor, Elsevier, and Business Source Premier have functioned as the principal tools for general information gathering. The Media Archive and Retriever Business have provided the needed access to initial press mentions surrounding announced cyberattacks. Adding to the list of sources, reports from national and global IT security agencies and authorities were collected and used, together with various research papers and annual surveys from large multinational consulting bureaus and other market research firms.

When searching the databases for material, keywords have been applied, some more frequent than others. The most commonly used ones are ‘cyberattack’, ‘volatility’ and ‘stock volatility’, often in conjunction with each other. Other regularly used words are: ‘cyberrisk’, ‘cyber intrusion’, ‘market capitalization’, ‘hacking’, ‘corporate hacking’, ‘financial effects of cyberattack’, ‘stock return’, ‘financial cyberrisk’, ‘cyberattack disclosure’, ‘risk disclosure policy’.

An extremely important aspect to consider when gathering all abovementioned information is source critique. In order to conduct as unbiased research as possible, authors constantly need to evaluate and consider the authenticity and the underlying motive behind all sources of knowledge. In the process of evaluation, a number of different principles should be considered and adhered to. In his book discussing aspects of source critique, Torsten Thurén describes four important principles: ‘authenticity’, ‘temporal association’, ‘independency’, and ‘freedom of tendency’ (2005, p. 13).

Simply explained, the principle of authenticity revolves around whether or not the author speaks the truth. Findings could for example potentially be altered in the way the author sees fit. In a worst case scenario, information and its associated research could be completely falsified (Thurén, 2005, p. 29). The second principle, temporal association, deals with the concept of time and oblivion. Thurén states that a contemporary source is more reliable than one of age, especially down to the small details (2005, p. 30). The principle of independency distinguished between primary and secondary information and establishes that, in general, primary sources are more reliable than secondary. This stems from the concept of “handing down”, or “altering of information in several stages”. Thurén argues that information from a secondary source never should be used to authenticate and confirm information from a primary source (2005, p. 53). The fourth and last principle, freedom of tendency, deals with bias. When collecting information from sources such as official messages, political propaganda, interest groups etc., the author should be extremely vigilant since the risk of biased knowledge is imminent (Thurén, 2005, p. 68).

Going through sources, be they primary or secondary, requires an understanding and use of the four mentioned principles. To improve the interpretational routines, departing from these criterions, can be done with the aid of five additional factors. These are, in turn: purpose; scope; authority; audience; and format (Blumberg et al., 2011, p. 239). Pertinent to each of the five evaluative factors are a number of questions that researchers should strive to answer continuously.

The first factor, purpose, fundamentally sets out to uncover what the source “is trying to accomplish” (Blumberg, 2011, p. 239). Most importantly, asking about purposes behind any information can reveal biases affecting the balance of the conveyed message, so as to promote certain values or withhold other perspectives. Moreover, the purpose is
intimately connected to the scope. Reflecting upon, for instance, the age of the information, the frequency with which it is updated, its geographical scope, and proximity to other research fields, will help evaluate the usefulness and credibility of utilized sources (Blumberg, 2011, p. 238). The current study primarily include academic, peer-reviewed sources presumed adequately objective; yet, some material is produced by IT security firms, IT security consulting agencies, and other institutions benefiting from increased awareness and knowledge about cybercrime on pure self-serving grounds.

In complement, the authority, audience, and format of a source affects the receiver of the information, making it vital to recognize whom the information actually addresses (Blumberg et al., 2011, p. 238). Generally, the packaging of information holds many subtle facts about a source’s appropriateness. The majority of sources used in this study are of academic journal format, with the respective journals’ bibliographical standards ensuring reliability. The remainder follow the particular companies’ or other institutions own format, though in no way suggesting reasons to mistrust these solely because of the format.

2.10 Ethics

At its core, ethics is the term encapsulating collectively determined or accepted principles of behavior, morally permissible actions, and interaction with others. The scope of such principles is subject to complex and abstract philosophical reasoning, thus not of relevance for the sake of this thesis. Even so, ethical dilemmas within business or other research materialize frequently. Researchers aspire to many objectives with their research, which can conflict with some indisputable personal, social or legal values. The linchpin of credible and constructive research is its ability to make use of material to independently formulate new theories and not just replicate or repeat preexisting knowledge. This requires a rigorous review of source credibility, correct reproduction of the original material so as to avoid plagiarism, and foremost strong integrity by the researcher to acknowledge and respect the principle of objectiveness. Wherever possible, biases must be identified and eliminated to render support for arguments, results and conclusions of one’s own research.

Principally, business researchers alternate between two philosophical stances: a teleological and a deontological view (Saunders et al., 2009, p. 184). Teleologically permissive studies build upon a utilitarian notion of ends justifying the means irrespective of relative costs, in contrast to the deontological abstention from research whose methods are not fully ethical, a sort of scientific version of the Kantian categorical imperative (Saunders et al., 2009, p. 184).

Research is by nature something upsetting: it can turn conventions, norms, laws, theories and concepts upside down by disproving or falsifying previously established assumptions. That characteristic stipulates a clear view of the ethical implications of any study, an anticipation required beforehand to supply the research with legitimacy and the results with applicability. As Creswell formulates it, discussing such issues is quintessential in order to establish justifications for the studying of something (2002, p. 62). Major features of ethical issues within research largely follow the structure of the study itself, and can be divided in following subsections: ethical issues in the research problem statement; ethical issues in the purpose statement and research questions; ethical issues in data collection; ethical issues in the data analysis and interpretation;
and ethics in writing and disseminating the research (Creswell, 2002, p. 63-66). To combat these, several instances have been installed to “tame” research: independent ethical committees, research protocols to increase transparency, participation agreements and clarifications about withdrawal, and overseeing the disposing of data, to name a few (Gorard, 2013, p. 188).

To begin with, a researcher which in its problem statement declares where a problem has been identified simultaneously criticizes prevailing theories and research. While the critique can be a reason for conducting new research, it can also be a unintentional side effect of seeking new knowledge. Either way, the problem identified should not damage participants or researchers, or conversely should “benefit individuals being studied” (Creswell, 2002, p. 63), which is problematic to fully foresee in advance but nevertheless remains a principle to be upheld. Intimately linked with this ethical predicament are those ethical issues arising from the development of a research purpose and research question. As it is here that researchers indicate what their “central intent” (Creswell, 2002, p. 63), the potential to mislead participants and other external subjects is pronounced. But as Gorard (2013, p. 187) reasons, most “writing about ethical issues in research” accommodates the target to not harm participants, but often neglects those not partaking directly in the research. Based upon the thesis’ objectives, and in extension its neutrality vis-à-vis individuals, the ethical implications of these two sections are of limited type.

Most ethical dilemmas emerge in the data collection stage (Creswell, 2002, p. 64). As a result, serious research must offer an “informed consent form” specifying which rights regarding participants that apply, such as the right to participate voluntarily and withdraw, the study’s purpose and procedures, and individual privacy (Creswell, 2002, p. 64-65). Beside the potential complications of accessing participants and data, the need to “respect research sites” is prevalent, translating into an awareness of one’s impact on the setting studied and a minimization of such impacts (Creswell, 2002, p. 65).

Additionally, Creswell mentions the need for “good ethical decisions” (2002, p. 66) coupled with data analysis. No form of coercion, convincing, abuse or misuse of data or individuals appear as the thesis deals only with non-personal, secondary data from databases and archives, increasing the ethicality of this study. Lastly, all compiled material has the potential to satisfy individual preferences or purposes rather than scientific ones, although these mostly are aligned within proper research environments. Writing, presenting and distributing the study at hand is of course of more interest for some groups than others, but is not undertaken with any other purpose than that of academic contribution and does not entail elements of exclusion to advance certain groups. The inquiry only seeks to shed light upon costs for companies finding themselves in the midst of a cyberattack to better estimate what comprises adequate IT security. If there is any one group at disadvantage due to this, it is cybercriminals which themselves display a total indifference to harming others.
Lengthy discussion about the matter is superfluous. It suffices to say that sensible use of methodology, conscientious planning, rigorous review instances, capacity to adapt and adjust, and unequivocal informing go a long way toward ensuring ethically defensible research. In combination with open dialogue between authors and supervisors (and participants, to the extent possible), dubiouness can be reduced or even eliminated. No ethical obstacles present themselves beforehand, based upon given conditions and the thesis’ ambitions. Market data and news archives are presumably unaffected by exploitation, and no other parties can be classified as directly and detrimentally affected by the thesis. A reservation for unforeseen complications is nevertheless called for.

2.11 Summary of methodology

![Diagram of methodological outline]

*Figure 1: Summary of our methodological outline.*
3 Theoretical framework

For a better overview of the topic, it is crucial to elaborate on some of the foundational financial theories underpinning our reasoning. We present and discuss: the Capital Asset Pricing Model and its implications for costs of a cyberattack; the concept of market efficiency and the Efficient Market Hypothesis (EMH); and information asymmetry and how a cyberattack induces information-related costs. Then, a connection is drawn to the thesis’ core concept: stock volatility. It is defined and contextualized thoroughly. We thereafter expand on theories originating in behavioral finance and relate those to volatility. A detailed and extensive section regarding existing literature on cyberattacks and financial metrics is provided to attach financial theory with IT, to form a comprehensive framework engulfing important aspects of cyberattacks. A summarizing figure displaying the theoretical process concludes the chapter.

3.1 Traditional financial theories

3.1.1 Market efficiency

A market is efficient where the prices of stocks and securities “...always “fully reflect” available information” (Fama, 1970, p. 383). No discussion about market efficiency escapes this rudimentary assumption. Research has constantly to measure and evaluate itself in relation to this financial principle. But since there are multiple markets, there must be more than one way of being efficient. Indeed, market efficiency is categorized into three forms: weak; semi-strong; and strong (Fama, 1970, p. 383). The first form only assesses efficiency in terms of how past returns can help predict future ones. The second form moves a step further by reviewing the pace with which announcements of public information become incorporated into security prices by the market. Lastly, the third form goes beyond all public information to factor in if some investors hold information not reflected in prices (Fama, 1991, p. 1576).

Interestingly, Fama came to opt for a name change from semi-strong to event studies, as event study methods developed substantially in the time period between his two papers and furthermore “give the most direct evidence on efficiency” (Fama, 1991, p. 1577). Notwithstanding Fama’s expertise on the matter of market efficiency, the idea is to quantify and concretize the costs of a cyberattack by proxying stock volatility for higher company cost of capital. Only indirectly is the question of market efficiency actualized, suggesting that the study of market reactions to announcements of cyberattacks itself typifies a proxy for “the adjustment of prices to various kinds of information” (Fama, 1991, p. 1575).

Prices of securities are thus subject to change only through attainment of new information. The efficient market hypothesis (EMH) then postulates that security prices, reflecting all available information but not all information needed to properly price a security, can be erroneous as a product of random deviations and not systematic inefficiency (Arnold, 2008, p. 563). EMH credits such randomness for ruling out the possibility of skilled investors outperforming market returns on own merits, albeit not completely discarding the possibility of above-market returns for certain stocks (Arnold, 2008, p. 565). Based on EMH and its restrictions, the research question can push theory
in two chief directions. Either a stock fluctuates more in junction with an attack than it would without, indicating ambiguity and uncertainty precipitate incorrect security pricing where some undervalue and some overvalue new information and produce volatility; or investors act on announcements in a pattern largely reiterating EMH, so that divergences fall within the range of randomness expected by the hypothesis.

Like all popular theories, EMH has endured much scholarly antagonism. DeBondt & Thaler (1985, p. 795) advanced an overreaction hypothesis, which, in light of their empirical results, violated the weak form of market efficiency. The authors propose the following: extreme stock price movements render similar movements in the opposite direction, where the magnitude of the first movement defines the subsequent reversion. If overreactions appear permanent, this “[systematic] overshoot” implies past return data houses predictability of reversals (DeBondt & Thaler, 1985, p. 795). However, any overreaction must be defined in relation to a suitable reaction to decide if investors overreact.

Grossman & Stiglitz (1980) leveraged a row of theoretical paradoxes against the EMH, suggesting it being not merely impractical but impossible to posit markets as efficient. Stigler (1961, p. 213) problematized the costliness involved in retrieving price information, or what he named “the ascertainment of market prices”. On the grounds that information is costly to retrieve, engaging in information-retrieving activities must render a return which “uninformed” investors cannot achieve, and this will be reflected in security prices (Grossman & Stiglitz, 1980, p. 404). Clearly, market efficiency becomes an impossibility if prices should compensate informational advantages while carrying all information. Furthermore, if stock prices are exposed to systematic investor overreactions to unexpected news, one will be hard pressed to claim prices convey the information at hand accurately.

Efficiency presupposes a set of information to be efficient about. One part of market efficiency concerns the availability or incompleteness of information. Another, much less discussed aspect, refers to investors’ capacity to deploy an unexpected piece or stream of information in security valuation. Brown et al. (1988, p. 355-356) forward an uncertain information hypothesis (UIH), arguing that EMH cannot oversee “the full extent” of the “eventual impact on stock prices” from “major informational surprises”. The fundamental assumption for the UIH is that “investors often set stock prices before the full ramifications of a dramatic financial event are known” (Brown et al., 1988, p. 356). Hence, good and bad news “increase risk, and therefore the expected returns on securities” (Brown et al., 1988, p. 357), although “prices react more strongly to bad news than good” (Brown et al., 1988, p. 355). The results of the study showed that, “in the aftermath of an unanticipated informational shock”, levels of risk and expected returns increase for the stock in question; this is true “regardless” of which way (positive or negative) the price initially reacted (Brown et al., 1988, p. 376).

With reference to this, the UIH certainly applies in cases of cyberattacks, considered in this thesis as ‘bad news’ that investors sub-optimally weigh in when pricing securities. It can come across as counterintuitive to declare EMH relevant in view of the abovementioned theories. Yet, market efficiency can be said to take place whenever new information enters the investor beehive: reactions need not be rational or irrational; they only need to take place. Firm valuations are continuously revised, without ever being scrutinized for “appropriateness”. Thus, all that matters is if investors perceive new information as negative, implying that it is “only logical to expect” a downward
revision (Yayla & Hu, 2011, p. 63). True to form, the thesis concerns itself with exactly this logic. The scope includes the size of investors’ actions, not their proportionality to new information. We therefore operate in the vicinity of traditional EMH literature.

3.1.2 Information asymmetry

Closely connected to concepts like market efficiency, uncertainty, overreactions, and stock prices is the asymmetry of information pervading modern-day financial markets. A transaction inherently consists of an exchange between parties with varying perspectives. Theoretically, any completed transaction means the price a seller is willing to sell for is harmonized with the amount a buyer is willing to expend. First to point out possible discrepancies between sellers and buyers was Akerlof (1970), who in his seminal paper exposed the “lemons” problem: due to asymmetric information (in Akerlof’s example regarding product quality), product valuation becomes ever-so complicated until the point of market cessation. Despite Akerlof's logical reducto ad absurdum, he cuts to the core of information asymmetry: with informational (dis)advantages, prices are driven away from the “true” value, ultimately dissuading consumption.

One can think of the distance between observed and theoretical price as the cost of information. It is exactly this distance which investors must quantify if they are to make correct and rational decisions about a stock’s value. The extent of most cyberattacks are unfathomable to the public, something partly true for investors. This should come as no surprise: in businesses, “making… the case for cybersecurity remains a major challenge” because management has little knowledge of “the scale of the threat” (Baker et al., 2009, p. 14). Holding this myopic statement for true, one imminent implication is that investors can’t be expected to know what management does not know, making cyberattacks an abstract distortion of typical information asymmetry. Moreover, an attack will thus superimpose investors’ additional informational costs on the attacked company’s losses/costs, exacerbating the asymmetry of information surrounding cyberattacks.

At its basic, information asymmetry arises when one part is superior in knowledge to another in a transaction (Healy & Palepu, 2001, p. 407). This applies to any company or individual investor consistently. Then, as a consequence, the part with inferior knowledge is relatively less well-endowed to accurately value the product in transaction, in this case a company’s stock. Under the settings laid forth in this study, where a company possesses no prior knowledge of imminent attacks, investors are placed in a “second line” of asymmetry behind unknowing or non-disclosing companies. It is reasonable to assume, we argue, that such additional distance to the information frontier inflicts additional dissonance in pricing. The consequences of a cyberattack are thus self-reinforcing: because corporations have grave trouble adjudging severity, reports about a cyberattack are often delayed, inferior, or inconsistent, setting investors further back from the information frontier; this fuels uncertainty and irrationality about accessible disclosures, converging into extrainformational guesstimates about a cyberattack’s acuteness.

Myers & Majluf (1984, 189-190) point out that in cases of external financing, firms hold more knowledge about the worth of planned investments than do outsider investors, and reducing this informational asymmetry will be costly. Rational investors
will interpret the state of a firm and its investment opportunities based on its decision to take on debt or issue equity, and modify their view on stock prices of the firm thereafter. But corporate finance is a two-way street: investor sentiment, driven by information asymmetry, affects firms’ decisions (Myers & Majluf, 1984, p. 188). Considering the nature of a cyberattack, the reasoning of Myers & Majluf can be adopted to conditions present around events studied in this thesis. The incentives for a firm to disclose a cyberattack must be weighed against costs from both informational and operational loss, and shareholders’ loss of confidence. Preceding such quandaries is however the more pressing issue of cybersecurity investments: racking up protection demands a substantial input of resources. Do firms attempt to communicate plans about cybersecurity investments, and if so, how is such communication interpreted by shareholders? Is it desirable, or even favorable, to do so? Conflicting interests loom large.

Meckling & Jensen (1976) described these kinds of interest conflicts in their path-breaking concept of agency costs. Essentially, numerous interests of disperse entities coexist within an economic organization, so it would be unreasonable to collapse these into a single and unitary preference. When one party (a principal) engages another party (an agent) to carry out one or more tasks in the principal’s position, and the agent receives autonomy to execute decision-making in capacity of the principal’s agent, Meckling & Jensen (1976, p. 308) claim an agency relationship is formed. Assuming the two parties are utility maximizers, “there will be some divergence between the agent’s decisions and those decisions which would maximize the welfare of the principal” (Meckling & Jensen, 1976, p. 308). In standard financial literature, shareholders are considered principals and corporate employees or managers their agents (Arnold, 2008, p. 849).

With recourse to this foundational principle of businesses, the incident of a cyberattack distinctly epitomizes the “agency costs” connected to these relationships (Meckling & Jensen, 1976, p. 308). The more principals, the larger variety of interests to align, making agency costs a function of shareholders (Meckling & Jensen, 1976, p. 313). The seniority of debt and equity issues will, too, incur higher agency costs (Healy & Palepu, 2001, p. 409). One intriguing aspect of cyberattacks and security rarely discussed is intraorganizational agency costs. The part managing and overseeing IT security is customarily not responsible for resource allocation, but is presumably subordinated to a financial department’s budgeting (Anderson, 2006; Walker, 2012, p. 11). Firms face internal information asymmetry, and investors’ exogenous information asymmetry is conditioned with firms’ endogenous equivalent, driving up total agency costs. Information asymmetry is understandably located at the puzzling nexus of cyberattacks, making the issue extra prominent in this thesis.

### 3.1.3 CAPM, risk premium and beta

Theoretical financial literature, and indeed much practical financial conduct, spring from Harry Markowitz’s (1952) seminal optimal portfolio theory work and, subsequent but independent, economy-wide applications of it by William Sharpe (1964), John Lintner (1965), and Jan Mossin (1966); best known as the Capital Asset Pricing Model (hereafter CAPM). The model is today regarded as a “centerpiece of modern financial economics” (Bodie et al., 2011, p. 308) and “a conceptual cornerstone of modern capital market theory” (Pratt & Grabowski, 2010, p. 105). But as with any model, theory,
concept, or idea, the CAPM has attracted much critique and stirred up equally much debate about its usefulness and accuracy. Most reservations against the model center on its adjunct notion of unrealistic idealization and oversimplification regarding conditions in financial markets (Mullins, 1982). Discussion about shortcomings and limitations pervade the coming sections.

Naturally, one asks why finance relies so heavily on such a rudimental model. Without dismissing the many assumptions and simplifications included into the model, it still offers a genuine and practical way of predicting the return any single investor is correct in expecting from an asset given the same asset’s observed risk; in a wider sense, the CAPM allows for generalizations about any set or combination of stocks, their relative risk and the return corresponding to that risk (Bodie et al., 2011, p. 309). Moreover, the model is the standard bearer when it comes to estimating equity cost of capital, especially so for larger corporations (Graham & Harvey, 2001, p. 201; Pratt & Grabowski, 2010, p. 104). These assumptions, and uses, of the model are at the heart of this study’s reasoning around investors’ behavior and corporations’ cost of capital.

But the CAPM is not the well of financial theory, only a part of the mass. It must be understood in a broader context to be fully compatible with the surrounding literature, and the assumptions and simplifications existing within that context require explanations in order for the CAPM to derive its value. Despite the model’s prominence among financial scholars and the highly developed literature encircling it, it finds itself embedded in the voluminous capital market theory (CMT) (Pratt & Grabowski, 2010, p. 104). Markowitz (1952) drew up the outline of investor behavior and subsequent portfolio optimization, implying that there are a slew of assumptions dictating how an investor rationally should act given the desire to maximize wealth and utility. This precedes explanations from the CAPM. Within CMT, the CAPM has attained positive standing because it portrays what happens on markets in case investors follow Markowitz’s prognosis, itself an assertion practically unchallenged (Pratt & Grabowski, 2010, p. 105).

Setting aside the general discussion about the imperfections of all models, the CAPM requires certain assumptions fulfilled if it is to explain anything. Only investors’ initial levels of wealth and risk aversion are allowed to vary (Bodie et al., 2011, p. 309). The following assumptions are posited for the CAPM model (Arnold, 2008, p. 295; Bodie et al., 2011, p. 309; Pratt & Grabowski, 2010, p. 113):

- Investors act rationally to attain efficient portfolios, putting to use Markowitz’s Portfolio Selection Model (1952).
- The holding period or time horizon of an investment is equal for all investors.
- Economically, investors view the world identically, generating homogeneous expectations about risk-free rates, expected rates of returns, security prices et cetera.
- There exist no transaction costs or investment-related taxes (for example on returns, be they capital gains, interest or dividend income).
- Investors can borrow and/or lend whichever amount preferred at equal, risk-free rates.
The model, or rather equation, arrived at thus looks as follows (Bodie et al., 2011, p. 321):

\[ E\left(r_i\right) = r_f + \beta_i \left[E(r_M) - r_f\right] \]

where:

- \( E\left(r_i\right) \) is the expected rate of return (cost of capital) for asset \( i \);
- \( r_f \) is the risk-free rate of return;
- \( \beta_i \) is the beta (systematic risk) coefficient of asset \( i \);
- \( [E(r_M) - r_f] \) is the equity risk premium (ERP) over the market portfolio; and
- \( \beta \) is asset \( i \)'s covariance with the market portfolio over the market portfolio’s variance so that \( \beta_i = \frac{cov(r_i, r_m)}{var(r_m)} \)

Theoretically speaking, the implication is that any and all investors can and will compose a portfolio of assets/stocks to reduce the riskiness of the investment to the degree where they simply achieve a replication of the market portfolio (Bodie et al., 2011, p. 309). This risk-reducing process is commonly referred to as diversification, empowering an investor with the hypothetical possibility to decrease a portfolio’s level of risk (total risk) by adding more assets to the pool of held securities. These individual securities’ unsystematic (idiosyncratic) risk contributes in varying fashion to the portfolio’s risk, thus in aggregate cancelling out each other’s variability. The investor ends up with a bundle of systematic (market) risk which is treated as a given, constant variable for any market participant (Arnold, 2008, p. 285).

The classic adage not to put all eggs in one basket is often used to illustrate this spreading of risk, though the metaphor isn’t completely apt: it assumes that a rational investor allocates all its resources for purchasing eggs, incorrectly drawing on the thinking that the more eggs (assets) collected and placed in a basket (portfolio), the more the owner stands to lose if the parcel is dropped; yet according to the CAPM an investor should lose relatively less the more pieces held, an assumption arising from the theoretical benefit of diversification. Even more troubling is the presupposition that the eggs/assets contribute equally to the overall risk level, whereas in reality they display varying amounts of risk and have countering, neutralizing effects on overall risk, which is where the concept of diversification draws its strength. Borch (1978) succinctly articulated that “[p]ortfolio theory is for risk lovers”.

From this reasoning follows that there is a more realistic description of the concept ‘diversification’ than the conventional eggs-in-a-basket explanation; the CAPM is incompatible with the (false) idea of risk pooling as detrimental to investors’ overall wealth. Semantics aside, the relationship between the level of total risk and unsystematic risk is generally graphed as a convex curve which decreases, though in diminishing pace, with an increasing number of securities in a portfolio. For an intuitive exhibit of diversification, see Arnold (2008, p. 285).

Systematic risk is an elusive risk factor. Within the CAPM model, systematic risk is denoted by a security’s beta, which embodies how closely the return of a stock co-varies with the market portfolio’s return (Arnold, 2008, p. 286; Bodie et al., 2011, p. 315; Pratt & Grabowski, 2010, p. 104; Mullins, 1982, p. 108). Note here that the term ‘market portfolio’ refers to a proxy, for example market indices such as S&P500, and not meant in the figurative sense of Arnold’s (2008, p. 285) theoretical definition, i.e. “a portion of
all the potential assets in the world weighted in proportion to their respective market values.” Beta should theoretically be the only variable of concern for investors since “[they] can eliminate company-specific risk simply by properly diversifying portfolios” (Mullins, 1982, p. 107). This precondition then suggests that an investor cannot expect to be compensated for bearing unsystematic risk (Arnold, 2008, p. 293; Mullins, 1982, p. 107), and so only the level of systematic risk for a security will impact the expected returns (Pratt & Grabowski, 2010, p. 105).

Thus, beta has the following basic features (Arnold, 2008, p. 287; Mullins, 1982, p. 108; Pratt & Grabowski, 2010, p. 107-108):

- Beta = 1.0; meaning that a one per cent change in the market portfolio’s returns induces an equal percentage change of a stock’s returns with such beta coefficient;
- 0 < Beta < 1; meaning that a one per cent change in the market portfolio’s returns induces a less-than one per cent change of a stock’s returns with such beta coefficient; and
- Beta > 1; meaning that a one per cent change in the market portfolio’s returns induces a higher-than one per cent change of a stock’s returns with such beta coefficient.

Hence, the risk-return relationship is, in view of CAPM, simply the amount of systematic risk taken on by an investor, and it is for bearing this systematic risk an investor will be compensated (Mullins, 1982, p. 107). Contrary to this belief, but in line with the position of this thesis, are the Douglas-Lintner results. In the first direct tests of CAPM (performed by Douglas, 1967), some irregularities appear, the most conflicting of which run counter to the model: asset returns’ covariance with index returns did not display any significantly positive relation (Jensen, 1972, p. 364). The evidence, referred to as the Douglas-Lintner results, “seem to indicate that an asset’s own variance is as important as (or perhaps even more important than) the asset’s covariance or portfolio risk in determining its equilibrium price and expected return” (Jensen, 1972, p. 365). Such inconsistencies support the intuition behind this thesis, namely that the riskiness from cyberattacks translates into more volatility, creating costs in form of demands of higher risk premiums. For an exhaustive review of the CAPM and capital market theory, see Jensen (1972) in its entirety.

CAPM has faced, and continues to face, criticism: Roll (1977) inveighed against its untestability due to inferior proxies for the market portfolio, and Fama & French (1992) and Black (1993) have separately proved that correspondence between betas and returns is questionable to the point of it not even existing. Chan & Lakonishok (1993) did identify a weak relationship between betas and returns under the condition that testing stopped short of using return data from 1982 and onward, coincidentally the same year Mullins (1982, p. 110) declared that “beta appears to be related to past returns.” Although not directly intruding on the reasoning of this thesis, the objections by such prominent authorities raise a set of questions to entertain while investigating the possibility to use volatility as a proxy for the cost of a cyberattack. Firstly, is beta the only feasible estimate of riskiness for a stock? The criticizers a few rows up, among others, would unequivocally dispute the claim. Secondly, are cyberattacks to be regarded as systematic or unsystematic risk? This is crucial to answer, as it comes with implications for risk premiums/cost of capital. Thirdly, are investors rewarded for shouldering the uncertainty of cyberattacks? According to the CAPM, if cyberattacks
are considered firm-specific, they should not be, as compensation only comes from bearing systematic risk; though, in reality, no investor will choose to invest in risky assets without prospects of returns above the risk-free assets.

Why it all matters in the context of cyberattacks and costs has to do with the logic underpinning CAPM. For an investor to choose a stock, which is riskier than a risk-free asset, the investor will demand a premium for incurring risk. Risk premiums are functions of market risk premium and stock betas (Bodie et al., 2011, p. 317). If a cyberattack causes higher volatility for a company’s stock, it must be reflected in higher risk premiums for the same stock, implying one of two things: investors treat the attack as a systematic risk factor since the risk premium is a function of beta; or, the CAPM fails to incorporate volatility into the estimation of cost of equity. To halt confusion in its tracks, the CAPM is for now put aside. Nevertheless, as a final note, the model is not refuted, only employed as a point of departure without direct application to the sample.

3.1.4 Cost of capital

In its most distilled form, cost of capital symbolizes the price, in per cent, that investors deem appropriate in relation to the additional risk they accept by choosing to invest in a company’s stock rather than other risk-free, lower-return assets. Cost of capital is the mainstream expression for investors’ opportunity cost (Welch, 2009, p. 389). Why capital “costs” is because shareholders could put to use their resources elsewhere for similar risk, and so a company must “pay” the investor for it to devote resources to the company. Such investments of money require a return “greater than shareholders could obtain elsewhere” (Arnold, 2008, p. 717). Cost of capital is however not something decided upon by a firm beforehand, but instead a percentage of returns of initial investments which market participants expect to realize, thus being subject to market forces (Pratt & Grabowski, 2010, p. 3). Capital in the context of investors is referred to as cost of equity capital, since public firms often have several alternative channels of funding apart from equity capital (Baker et al., 2010, p. 139).

But cost of equity is a product of expectations, making it subjective and arbitrary and in extension difficult to correctly quantify. Indeed, Pratt & Grabowski maintain that quantification “is arguably one of the most difficult analyses in the field of corporate finance” (2010, p. 46). Cost of capital for investments is, as shown above, often computed with the help of CAPM, in spite of the model’s looseness. The output of the model is thus based on subjective reasoning, because, according to Welch (2009, p. 250), one gets the right output if you supply the correct input about investment risk.

In addition to judging risks before investing, investors will revise and update their beliefs over time as new information reaches them (Welch, 2009, p. 307); this is the thesis’ central tenet. All risk premiums above the risk-free rate adhere to uncertainty. Investing in equity reduces the predictability of realizable returns and drives up uncertainty, which is why equity cost of capital is greater than all other capital sources (Pratt & Grabowski, 2010, p. 47)

3.1.5 Risk-reward tradeoff

In light of the proposed relationship between risk and expected return, financial economists have with much effort investigated what sort of discernible relation between the two variables actually exists. French et al. (1987) explored relations between stock returns and market volatility, concluding that risk premiums are positively linked with
stock return volatility. Similarly, Campbell & Hentschel (1992) investigated the belief that increased market volatility puts upward pressure on the required rate of returns, and did find support for their hypothesization. Moreover, the authors improved substantially on the ‘volatility feedback’ concept, evidencing the correlation of stock price fluctuations and future or expected volatility.

Merton (1980) conducted an exploratory study about market risk premium and volatility, analyzing three different models for estimating expected returns while also accounting for the level of market risk. The results were formulated as the “Reward-to-Risk Ratio” for investors with dissimilar risk aversion (Merton, 1980, p. 328) under the assumption that “the expected return must be higher[]” in order to “induce risk-averse investors to bear more risk” (Merton, 1980, p. 328). Ghysels et al. (2005, p. 509) proved the “[significant] positive relationship between risk and return in the stock market” using daily and monthly return data from the period 1928-2000. In addition, they, in line with French et al. (1987), found an “insignificant (and sometimes negative) coefficient” when utilizing a “rolling window estimator… of variance” (Ghysels, 2005, p. 511) but notice deviations among the study’s results when the time window duration is increased. Thus, the risk-reward tradeoff is sensitive to investment time horizons, in turn corroborating findings by Campbell & Viceira (2005, p. 34) who claim that risk “may be significantly different for different investment horizons, thus creating a “term structure” of the risk-return trade-off.” This was repeated more recently by Albargli’s (2015) work covering time horizons’ effect on risk aversion. Lastly, Lundblad (2007) reviewed the risk-return trade-off over an expanded time period (1836-2003) and estimates a positively correlated, statistically significant risk-return trade-off.

The academic discussion is however not as uniform as the recent paragraph gives impression of. Disagreement is widespread and opponents abundant, touching many aspects: some the reliability and validity of data, tests and models (see for example Nelson (1991); Roll (1977); and Engle & Ng (1993)); others the form of the relationship or even the direction of it (see for example Bollerslev et al. (2006); Harvey (2001); Scruggs (1998); and Turner et al (1989)); and yet others the underlying statistical assumptions (Borch, 1969; Feldstein, 1969) or the choices made when factoring in risk (Kahneman & Tversky, 1979).

3.2 Theories of behavioral finance

3.2.1 Challenging the rationality within finance

Up until now, the framework has exclusively handled classical financial theories. While these theories seek to understand the financial market through models relying on investor rationality, alternative explanations exist. In recent years, researchers in the field of behavioral finance have questioned generally accepted notions from the traditional financial paradigm (e.g. Fama’s (1970) Efficient Market Hypothesis). The goal has been to provide original explanations to market phenomenon by addressing the difficulties and inconsistencies faced by traditional beliefs (Barberes & Thaler, 2003, p. 1053). The greatest leap from conservative theories, and also the most uniform assumption made by advocates of behavioral finance, is the relaxation of investor rationality. Letting irrationality into financial theories and model has opened up for many interesting discoveries; the arguably most important ones being documented in the literature on “limits to arbitrage”. These papers show that irrationality can have both
substantial and long-lived effects on asset prices in an economy where rational and irrational investors interact (Barberies & Thaler, 2003, p. 1053).

The framework will continue to discuss and elaborate on some of the theories in behavioral finance built upon the “limits to arbitrage” papers (Barberis & Thaler, 2003). It will further connect those theories to classic financial notions such as volatility and risk premium; mainly in order to provide an understanding of the reasoning behind the upcoming hypotheses in the next chapter. Nevertheless, it is important to stress that explaining the fundamental reasons behind the financial effects of a cyberattack is beyond the scope of this study. However, explaining theories underlying its essential assumptions is only necessary in order to provide the readers with a full picture.

3.2.2 Regret theory

Sometimes, decisions taken with the information at hand will incur a sense of loss when the outcomes are discovered. Therefore, some people will imitate others to minimize the possibility of a regrettable action. Bell (1982, p. 961) coined the term “decision regret” in an attempt to prove that, under uncertain conditions, a priori consequences of decisions can be dissimilar to actual outcomes, and the “correct” choice proves to be “wrong”. Regret theory places itself on two premises: a capacity to “experience the sensations we call regret and rejoicing” and that people “try to anticipate and take account of those sensations” (Loones & Sugden, 1982, p. 820). A decision maker will, regardless of rationality, strive to avoid prima facie negative consequences and match these with the expected relative doses of “euphoria” and “self-congratulation” involved in every decision-making process (Bell, 1982, p. 961). In that sense, regret theory is iterative as it revisits an investor’s pre-informational position with a post-informational pretense.

Theories about decision regret came as a reaction to classical economic utility theory, especially Von Neumann & Morgenstern’s (2004 [1947]) expected utility theorem, when empirical research noted many deviations and paradoxes for utility maximization under uncertain conditions; the most prominent paradoxes are those of Allais (1953) and Ellsberg (1961). Loones & Sugden (1982, p. 819) explain that regret theory does more than simply predict “systematic violations of conventional expected utility theory” – it disposes of explanations emerging in irrationality altogether and replaces them with a set of axiomatic assumptions far less restrictive than expected utility theory but coherent enough to explain that anticipation of outcomes will influence choices.

Regret theory can serve as the theoretical link between two choices confronting an investor when a cyberattack occurs. Firstly, the investor will attempt to decide whether the event is significant enough to divest from the attacked company. Secondly, observing others’ reactions, the investor must interpret a mixture of signals and convert it to action, passivity being one choice of (in)action. Loones & Sugden (1982, p. 807) start with the assumption that an individual can derive choiceless utility, or utility resulting from an outcome “without having chosen it.” Simplified, the investor is suspended by introspective personal conflict: by not acting, when others are, the investor runs the risk of regretting holding the security, and contrastingly incurs a risk of regretting overreaction provided the new information. Consulting Bell (1982, p. 963), regret represents the distance “between the assets actually received and the highest level
of assets produced by other alternatives.” And this is the tormenting enigma of cyberattacks in its entirety.

Barberis et al. (2006) include regret into their analysis of decisions around market participation by laying forth that regret will, and could, arise with every single choice made by an investor when one equates choice with gamble. Basically, an investor (“an agent”) being “offered a new gamble” will “[evaluate] that gamble in isolation”, and often display reluctance toward such gambles even though outcomes can be “equiprobable” (Barberis et al., 2006, p. 1069). This individual risk evaluation is known as narrow framing. The reasoning makes for unnecessarily extensive applications of regret for this study, but is nonetheless a useful insight: investors can shun passivity in preference for some action, since they view the opposite, e.g. doing nothing, as a gamble they are not willing to take. It is with this in mind we should consider the flock mentality observable in connection to unanticipated events, partly explainable by herding theory but complemented by regret theory.

### 3.2.3 Herding behavior in financial markets

Regret theory is intimately related to herding behavior; one might even stretch as far as considering it the main trigger behind crowd tendencies. Briefly explained, financial herding emerges when an investor intends to make a specific investment, but refrains from doing so when she finds that others have decided not to invest. The opposite is of course also true (Bikhchandani & Sharma, 2000, p. 280).

The supposed reasons behind herding behavior are many. In their survey article on herding in financial markets, Bikhchandani & Sharma (2000) discuss some of them. They argue that information symmetry is an important trigger; investors follow each other simply since they believe others’ actions on the market reveal hidden information, implying sort of a circular behavior. Another reason could be that some investors merely “…have an intrinsic preference for conformity” (Bikhchandani & Sharma, 2000, p. 280). The authors further state that, when influenced by others’ decisions, investors very well might herd on an investment decision that is faulty for all of them. This often by definition means that when new information arrives, “…investors eventually reverse their decisions[,] starting a herd in the opposite direction. This, in turn, increases volatility on the market” (Bikhchandani & Sharma, 2000, p. 281). Moreover, the authors accentuate the potentially powerful effects of herding behavior. For example, even in cases where the grand majority of investors intend not to invest, some of them could be persuaded to change their mind simply as a reaction to the first few who decide to invest. In extension, this behavior has the potential to trigger a snowballing effect, switching a majority of rational nay-sayers to a majority of irrational yea-sayers (Bikhchandani & Sharma, 2000, p. 280).

Herding behavior is closely related to information and uncertainty and, by definition, also to market efficiency. Bikhchandani & Sharma (2000) argue that, given strong market efficiency, a stock price always adjusts to include all publicly available information. Information not publically available will be revealed and reacted upon directly after the investor with private information takes action (Bikhchandani & Sharma, 2000, p. 289). This means that an investor with access to all freely available information will be precisely indifferent between buying and selling. If this were completely true in reality, herding behavior would never be an issue (Bikhchandani & Sharma, 2000, p. 289). In other words, given perfect capital markets, the aggregate of
publically available information will trigger a pricing mechanism, adjusting stock prices to their fair values and, in effect, hinder herding behavior.

Reality is, however, often a bit too complex to perfectly mirror the abovementioned reasoning. In their article on multidimensional ambiguity and herding, Avery & Zemsky (1998) elaborate on reasons behind collective investor behavior by presenting three different dimensions of uncertainty. They argue that, as long as only the first dimension, uncertainty about price, is at play, herding is hindered by the market’s self-adjusting price mechanism (Avery & Zemsky, 1998, p. 724, 740). However, if uncertainty extends to the second dimension, insecurity about the existence of a price shock, herding is possible (Avery & Zemsky, 1998, p. 724). When the third dimension, uncertainty about the meaning and quality of available information, is reached, herd behavior can lead to significant mispricing and “highly volatile price paths” (Avery & Zemsky, 1998, p. 724, 741). That reasoning is well in line with the underlying assumptions of this thesis; possibly providing theories of financial herding with explanatory power over its hypothesized phenomenon.

3.3 Volatility

3.3.1 Volatility: a definition

‘Volatility’, ‘stock volatility’, ‘return volatility’ and ‘market volatility’ are frequently recurring terms in this thesis, and therefore require some explanation and elaboration. First of all, ‘volatility’ and ‘return volatility’ are general terms, incorporating all type of fluctuations, both for specific securities and for the market as a whole and can be used interchangeably. ‘Stock volatility’, on the other hand, refers to the fluctuations of a particular security, and ‘market volatility’ only denotes fluctuations in the market as a whole.

From a purely financial perspective, “a variable’s volatility, $\sigma$, is defined as the standard deviation of the return provided by the variable per unit of time when the return is expressed using continuous compounding” (Hull, 2015, p. 201). Roger Ibbotson, a professor in finance at Yale School of Management, simply defines volatility as the “up-and-down movements of the market,” further stating that it often is measured by “the standard deviation from the expectation” (Ibbotson, 2011). Volatility can naturally also be measured by the variance of returns, which is derived merely by squaring the standard deviation ($\sigma^2$). It can be calculated during any given time frame; depending on the purpose of the calculation, one year and one day are frequently used intervals (Hull, 2015, p. 201). In financial terms, volatility is often used as a proxy for risk, which in extension also means that it has a positive correlation with the, by investors demanded, risk premium. This is for example proven by French et al. (1987) in their article on expected stock return and volatility.

3.3.2 Volatility and its relation to information, attention and uncertainty

The academic debate about potential drawbacks, effects and general implications of stock market volatility has been both protracted and filled with distinct opinions. However, one fact, almost universally established, is that “volatility is a natural consequence of trading” (Gregoriou, 2009, p. 7). Price fluctuations are fundamentally created by trading and speculation; in fact, without any stock market fluctuations, investors would be unable to make any profits and trading would be reduced to a minimum. This highlights the importance of sound market volatility. In a book edited
by Greg N. Gregoriou, designated to explicit discussion of stock market volatility, the author states that even though volatility and risk are closely related, volatility as a concept need not be a bad thing; “in fact, fundamentally justified volatility can form the basis for efficient price discovery” (Gregoriou, 2009, p. 4). Volatility’s prominence in the financial world is further accentuated by the fact that it affects the outcome of almost all asset pricing models, and that derivatives valuation is contingent on reliable forecasts (Gregoriou, 2009, p. 4).

Being such an important financial metric, it is both interesting and important to understand what factors create, accelerate and, in general, affect volatility. While theories on the subject are abundant, this study is focusing on those factors connected to its underlying assumptions: information, attention and uncertainty. In their article on investor attention and stock market volatility, Daniel Andrei and Michael Hasler (2015) establish a relationship between attention to news, return volatility and risk premium. First and foremost, they show that “stock volatility and risk premium increase with attention” (Andrei & Hasler, 2015, p. 34). They argue that high attention to news create volatile returns simply since, with investors being vigilant, learning is fast and news are immediately reacted upon and quickly incorporated in the price. In extension, this attention-induced volatility creates a demand for higher risk premiums. The opposite is true for stocks attracting little or no attention from investors (Andrei & Hasler, 2015, p. 34).

The abovementioned reasoning is relevant for this study for several reasons; most importantly since it, through the learning mechanism, can be extended to uncertainty. Andrei & Hasler (2015, p. 34) settle that “[w]hen attention is low, learning is slow”, and when learning is slow, knowledge is low; which in turn creates high uncertainty and, by definition, also increased volatility and investor demand for risk premium. These discoveries imply a sort of circular investor behavior, meaning both high and low attention to news has the potential to create increased stock volatility. Andrei & Hassler (2015, p. 34) recognize this and conclude that “[a]ttention and uncertainty […] have a joint impact on equilibrium asset prices” The aforementioned relationship is of particular relevance, mainly since this research is conducted based upon the central assumption that news of a cyberattack increase both investor attention and uncertainty.

Other pertinent work, adding to the literature about uncertainty connected to stock market volatility, is Arzu Ozoguz’ (2009) research on dynamics of investors’ beliefs and Bayesian uncertainty about the state of the economy. First, the author concludes that investor uncertainty has negative impact on asset valuation, both at a market and a portfolio level. Second, she settles that uncertainty associated with investor belief, utilized as a risk variable, “…shows remarkable success in explaining the cross-sectional variation of average stock returns” (Ozoguz, 2009, p. 4378). A similar conjunction is argued for in a survey article by Pástor & Veronesi (2009), compiling work on learning in financial markets. The authors connect Bayesian learning of dividend growth to, among other metrics, return volatility. They argue that increased learning about dividend growth levels decreases uncertainty and, in extension, also reduces return volatility (Pástor & Veronesi, 2009). The work shows that, as a result of the learning factor, older firms in general experience milder return volatility than do younger (Pástor & Veronesi, 2009, p. 367). The authors demonstrate a valid relationship not only for uncertainty related to dividend growth, but also for uncertainty related to future earnings (Pástor & Veronesi, 2009, p. 369), which is better in line with the hypotheses set up for this study.
3.3.3 IDIOSYNCRATIC VOLATILITY AND RISK PREMIUMS

The classic and generally accepted opinion among scholars is that investors only are compensated for shouldering systematic risk. This argumentation stems from Harry Markovitz’s (1952) and is supported by his Optimal Portfolio Theory; concluding that unsystematic risk is possible to diversify away using correlation and portfolio optimization techniques (Arnold, 2008, p. 293). This way of reasoning has paved the way for several market models, aiming to measure the fair risk premium or required return for investors. The far most famous and well debated one is however the, by Sharp (1964) and Lintner (1965), created CAPM model (Arnold, 2008, p. 275). Nevertheless, as previously discussed, a storm of deliberation and critique has rained over the famous model over the last decades, most of which regards alleged erroneous estimation of beta and market risk premium (Welch, 2009, p. 274). Some have even questioned the explanatory power of the classic beta measure altogether and pointed out other factors that might be more practically suitable (Welch, 2009, p. 268). Being skeptical to classical asset pricing models, Fama & French (1993) for example, expanded CAPM from a one factor to a three factor model after finding empirical regularities between stock returns, firm size and firm price to book ratio.

Whatever case might be true regarding CAPM’s validity and beta’s explanatory power, one thing is impossible to argue against; the original CAPM model considers beta, and thus systematic risk, the sole risk factor for asset pricing purposes (Welch, 2009, p. 268). While Fama & French (1993) and others have expanded and developed several advanced models, striving to include all relevant asset pricing variables, relatively few have identified idiosyncratic (unsystematic) risk as a possible risk factor. Some researchers have however deviated from the assumptions of modern portfolio theory in order to explore the implications of idiosyncratic risk.

In early studies, one of the CAPM founding fathers, John Lintner (1965), repeated by economist George W. Douglas (1967), challenged the assumptions made by CAPM by showing that the cross-section of returns are related, not only to a stock’s covariance with other securities, but to total stock variance. While the validity of this work was questioned and tested by for example prominent economists Miller & Scholes (1972), they were never able to fully overturn its results (Rubinstein, 2006, p. 220). Douglas’s findings were furthermore reaffirmed by Lehman (1990) after conducting a thorough econometric analysis (Goyal & Santa-Clara, 2003, p. 976).

Both Lintner’s and Douglas’s research has later been built upon by, among others, Amit Goyal and Pedro Santa-Clara (2003). In their paper on idiosyncratic risk and stock market returns, they challenge classic asset pricing models by showing that average stock risk, mostly driven by unsystematic risk (Goyal & Santa-Clara, 2003, p. 976), entail predictive power of market returns. They confirm their results with several robustness checks and, viewing capital structure from an option perspective, explain their findings by discussing how stocks gain in value at the expense of debt holders when average variance increases. (Goyal & Santa-Clara, 2003, p. 998).

More recently, two other scholars, Zhanhui Chen and Ralitsa Petkova explain the unsystematic volatility puzzle of Ang et al. (2006; 2009) by decomposing “…aggregate market variance into an average correlation component and an average variance component” (2012, p. 2745). First they identify a risk factor, supposedly missing from the Fama-French model, and show that the same factor is priced in the market. Second,
they sort stocks with high and low idiosyncratic volatility into two groups and show that they differ from each other relative to the missing factor. Lastly they prove that the spread in idiosyncratic volatility loadings between the two groups is large enough to explain the difference in average returns (Chen & Petkova, 2012, p. 2746).

The risk-reward debate related to idiosyncratic risk is both exhaustive and continuous. Much evidence points to the fact that total variance actually is priced in the market, other, more conservative research, contradict this view. While adding to this debate is not the purpose of this research, it is interesting to discuss from an observational point of view. This is true simply since it affects the applicability of our results; if total, and not only systematic, risk is priced in the market, our findings will be of interest for a much broader range of readers. Therefore, this study will investigate a cyberattack’s impact on both systematic and unsystematic risk.

3.4 Discussion of financial IT literature

Cyberattacks and cybersecurity are relatively new concepts, especially in the field of economic and financial research. For that reason, associated problems and research dedicated to the field is scarce, historically. Despite the large academic gap, some relevant work dating back to the years just after the IT bubble has been conducted (e.g., Campbell et al., 2003; Garg et al., 2003; Ettredge & Richardson, 2003; Hovav & D’Arcy, 2003; Cavusoglu et al., 2004; Hovav & D’Arcy, 2004). Common for most of them has been the pursuit to try and quantify the costs related to different types of cyberattacks and security breaches by assessing stock market reactions to news of such events (Yayla & Hu, 2011, p. 61). Lack of research between then and now has however been remarkably large considering the ever-evolving nature of the subject. Nevertheless, five years ago, two scholars named Ali Alper Yayla and Qing Hu (2011) picked up the torch in order to elaborate on outdated theory. They point out that, even though positive IT announcements bear rather strong empirical support for being associated with optimistic market reactions, results from research relating pessimistic market reactions to negative IT announcements are inconclusive (Yayla & Hu, 2011, p. 63). They also conclude that temporally short event windows along with fairly small sample sizes have left essential questions unanswered; the most important for this study being: “[i]f security events do have negative impacts on firm values, are such impacts temporary or long lasting?” (Yayla & Hu, 2011, p. 61).

Almost a decade earlier, a group of researchers led by Katherine Campbell (2003) conducted one of the first event studies in the area linking negative information security events to finance. Their primary goal was to analyze stock market reactions following cyberattacks against publicly traded US corporations (2003, p. 431). Being a pioneering study in its field, it is only natural that the sample, control variables, and methodology in general are not perfectly refined. The researchers did however manage to discriminate between cyberattacks gaining access to confidential information and those that did not (Campbell et al., 2003, p. 439). While ending up with no significant support for overall adverse stock market reactions, they did find substantial evidence showing that cyberattacks involving unauthorized access to confidential information indeed implicated negative market response (Campbell et al., 2003, p. 445). Also worth noting is that Campbell et al. (2003), in contrast to Yayla & Hu (2011), found no support for so called DoS (Denial of Service) attacks having adverse effects on stock return. All results aside, it would be unwise to ignore the study’s small sample size. The fact that it
consists of merely 43 incidents, out of which only 11 are related to confidential data theft, greatly limits the generalizability of their results (Yayla & Hu, 2011, p. 63).

The same year, two other researchers named Anat Hovav and John D’Arcy (2003) pursued a quest similar to that of Campbell et al. (2003), but with some important differences. More specifically, they filtered out all security breaches except DoS attacks from their sample and investigated what impact such attacks have on firms’ abnormal stock returns. In line with Campbell et al. (2003), their results indicated that the market does not punish companies that experience DoS attacks, at least not in terms of significant negative returns (Hovav & D’arcy, 2003, p. 108). Their findings were however a bit ambiguous in the sense that they did support negative market reactions for a sub-sample of “internet-specific” firms, dependent on their websites for business continuity (Hovav & D’arcy, 2003, p. 111).

Nevertheless, the logic behind these results is easy to comprehend. Consider the case of a pure e-commerce firm, which is entirely dependent on the Internet for its daily business. Such companies should reasonably be more damaged by an attack disabling its only business channel - the website - than a firm keeping both physical stores and a web shop. The same reasoning is stressed by the early DoS attacks against Yahoo and Ebay in 2000, estimated to have cost the firms around $1.2 billion in lost revenues and decreased market capitalization (Niccolai, 2000). Yet, it should be mentioned that the study as well as the exemplified incidents are of age, which means that both investor attitudes and firm protection very well might have evolved during the years. Furthermore, Yayla & Hu once again criticize the small sample of only 20 incidents used in the study (2011, p. 63).

One year later, Hovav & D’Arcy (2004) were at it again, this time using the same event study methodology but with a much larger sample of 186 incidents. Interestingly enough, they switched the independent variable from DoS attacks to virus attacks, keeping abnormal returns as the dependent variable. Nevertheless, the results turned out similar to their last study, showing no empirical evidence for decreased market value following a virus outbreak (2004, p. 38). This research too has however been subject to subsequent critique by Yayla & Hu (2011). They state that the findings might lack validity, arguing that virus outbreaks “...often affect[] a large number of firms simultaneously”, in turn having the potential to “render event analysis less effective.” (Yayla & Hu, 2011, p. 63). The scholars continue their argument by explaining that abnormal return is defined as a specific stock’s excess return in comparison to the market as a whole. Following that logic, if a wide variety of companies simultaneously are affected by a virus outbreak, a large part of the market will be punished; in theory meaning that abnormal return of a single attacked company will stay unaffected (Yayla & Hu, 2011, p. 63). While that reasoning led Yayla & Hu to exclude virus attacks from their sample altogether (2011, p. 63), this study aims to more precisely separate firm specific worms from mass outbreaks of viruses. The qualified attacks will be included in the sample, making expansion of prior work possible.

Other work, contemporaneous to those discussed above, are Garg et al. (2003) and Cavusoglu et al. (2004). These studies are similar and consider samples in the time interval between 1996 and 2002. The big difference is the sample size; while Garg et al. (2003) managed to collect 22 incidents, Cavusoglu et al. (2004) assembled a three times larger sample of 66 incidents. In contrary to the abovementioned, both studies settled support for negative abnormal market return in response to a security breach, using the
full sample (Yayla & Hu, 2011, p. 63). Cavasoglu et al. (2004) measured an average loss in market capitalization of 2.1 percent and just like Hovav & D’Arcy (2004), report that adverse effects were more severe for Internet-specific firms. They also found that smaller firms were more harshly penalized than larger firms in terms of market capitalization loss (Cavasoglu et al., 2004, p. 94). While Garg et al. concluded that investor reactions were different across security breach type (2003, p. 82), Cavusoglu et al. admitted their shortcomings in categorizing the attacks properly, and thus refrained from drawing any far reaching conclusions (2004, p. 96, 97). Aside from the recurring issue with small sample size, the studies are limited by narrow event windows, something this study intends to elaborate on.

A distinct common denominator for almost all studies discussed above is small sample sizes. A central issue, as argued for by Brown & Warner (1985), is high degrees of skewness and kurtosis. Both being important problems for these types of studies with highly non-normal distributions of returns; especially in cases where sample size is smaller than 50 (Yayla & Hu, 2011, p. 63). For early work it is evident that small sample sizes have been an issue hard to tackle, mostly due to the relatively modest amount of recognized and reported attacks. Yayla & Hu (2011, p. 62) confirm this and emphasize that the information-gathering process on security events is all but friction free. First and foremost, they discuss two major issues: “the hazard of even detecting a security breach in the first place” and “the rather small percent of recognized attacks, actually disclosed to the public”. Nevertheless, in comparison to older studies, Yayla & Hu manages to collect a rather sizeable sample of 123 incidents during the period between 1994 and 2006 (2011, p. 67), something that heightens the statistical validity and generalizability of their research. The goal of this study is to pick up where they left off by both testing a larger and more current sample.

Yayla & Hu (2011) furthermore point out drawbacks associated with too narrow event windows, like the popular 1-day window (i.e., [-1,1]), previously used in similar studies. They state that adverse effects, lasting only a couple of days after an attack, are “irrelevant to information system management” (Yayla & Hu, 2011, p. 61). On the other hand, if the event proves to incur abiding effects, shareholder value is threatened and the problem should become highly relevant for IT managers and top executives (Yayla & Hu, 2011, p. 61). The same reasoning is well in line with the methodology of this research, intending to examine 5 and 30-day event windows to better explore event persistence. Yayla & Hu tackled the problem by considering 5 and 10-day windows, however concluding that no event study so far has explored the “long range windows (i.e., >30 days),” further suggesting that “future research could shed significant light” on the subject by doing so (2011, p. 75). It is however important to note that although the nature of longer event windows makes it possible to examine event effect persistency, a much more extensive screening for confounding effects is needed; something that this study has engaged in (see Section 4.1.2).

Two other purported improvements in Yayla and Hu’s research compared to previous work are “enhancement of grouping for different security breach types” and “inclusion of several contingency factors” (i.e. control variables) (2011, p. 61). Both of these enhancements are made possible by the study’s comparably larger sample, and use of variables such as industry classification, business type separation, and type of attack/security breach (2011, p. 61). Monitoring contingency factors has historically been rare, which naturally only makes it more interesting, especially since the authors find significant proof for relationships between some of them (2011, p. 74). Therefore,
with the benefit of an even larger and more current sample, this research will elaborate on previous work, both in terms of classifying attacks and monitoring contingencies.

Finally, as a direct result of methodological improvements and a larger sample, the most significant results in Yayla and Hu’s (2011) study are their findings connected to time horizon and other contingencies. More specifically, they found significant support for negative stock market reactions in connection to firm-specific security breaches, however, settling that the degree of adverse effects is subject to various circumstances (Yayla and Hu, 2011, p. 75). They conclude that “…the magnitude of negative effects of security breaches changes over time and the magnitude and direction of this change vary across sub-samples of various contingencies.” (Yayla and Hu, 2011, p. 75). The researchers further argue that those findings accentuate the grave importance of incorporating time into the analysis, going so far as to state that, without doing so, “the value and validity” of conducting these types of studies would be “significantly limited” (Yayla and Hu, 2011, p. 75). A figurative example of the uniqueness of their results is the findings related to DoS attacks. Yayla and Hu identify that, although the attacks themselves normally are ephemeral, “…their negative impact on firms’ market value escalates with time.” (2011, p. 75). In concrete numbers, investors’ negativity towards DoS attacks is reflected by the average decrease of 7% in market value over the 10-day period following an attack (Yayla and Hu, 2011, p. 75). Moreover, they find that the adverse effect of a security breach intensifies with time for technology firms, regardless of attack type (Yayla and Hu, 2011, p. 75).

Yayla & Hu conclude their study by suggesting interesting routes for future research; among others, these include: examine longer event windows; reexamine results from prior studies; and, first and foremost, to study the “…risk effects of security breach announcements.” (2011, p. 75). They state that including “systematic and unsystematic firm risk into the market model” recently has been “proposed in the [Information Security] literature” (Yayla & Hu, 2011, p. 75). The logic behind doing so naturally follows from the argument that cyberattacks have the potential to harm firms’ current and future cash flow. Considering risk effects can therefore help improving “…the estimation of market valuation” (Yayla & Hu, 2011, p. 75). This study has taken all these suggestions, and more, into consideration, and will therefore contribute with important knowledge to the field of financial IT literature.
3.5 Summarizing model

Figure 2: Summarizing model of theoretical framework.
To convey the process involved in the data collection and the creation of a cyberattack database, we here demonstrate the means by which the sample was collected, screened, coded and tested. Calculations and motivations for abnormal returns are supplied. Moreover, the developed Abnormal Volatility measure, and its background, is deliberated upon. From this, we proceed to the statistical properties of sampled data and the significance tests applied to the various outputs for both event windows. All hypotheses are explained formally and numerically, to concretize how we investigate Abnormal Volatility before and after a cyberattack.

4.1 The event study

4.1.1 The method

The kingpin of financial research is the event study method (Armitage, 1995; Fama, 1991; MacKinlay, 1997; McWilliams & Siegel, 1997; Peterson, 1989; Salinger, 1992). Though initially intended to investigate market efficiency by reviewing the pace with which security prices adapt to new information (Fama et al., 1969), the method proved relevant for all sorts of fields; above all, finance, economics, and accounting researchers took it to their hearts, but the idea was further applied to matters of law and regulation. The common denominator is the desire to “measure the effects of an economic event on the value of a firm” (MacKinlay, 1997, p. 13). Thus, the objective with event studies center on the notion of abnormal deviations traceable to certain unanticipated events or information (Peterson, 1989, p. 36). The method is hence retrospective, making use of confirmed data but with a time lag between observed price fluctuations and full knowledge of economic impact. The method serves best as a precursor to deeper-going studies since it is mainly preoccupied with establishing as direct as possible a link between an event and a monetary figure (Yayla & Hu, 2011, p. 62). It is important to point out that although the method mostly appears in studies of negative economic impacts from an event, it is still relied upon to derive a value for a positive event too: this mercurial feature is embodied in the core ‘abnormal returns’ concept (Peterson, 1989, p. 57).

These events range from mergers and acquisitions to announcements on earnings, dividends, and equity or debt issues to interest-rate policy changes or other economy-wide events, as well as effects of updates in corporate policy (MacKinlay, 1997; McWilliams & Siegel, 1997). In IT, the method is generously operated for assessing how technological development impacts firm value (Yayla & Hu, 2011, p. 62), making the method suitable in the context of cybersecurity investments and cyberattacks. Academic recognition stems from its relatively undemanding manner: assuming market efficiency, an event will be reflected in stock prices (Ball & Torous, 1988, p. 123). Event studies are generally considered better proxies of effects on true economic value since stock prices are relatively less susceptible to manipulation than accounting numbers (McWilliams & Siegel, 1997, p. 626-627).

Seizing the impact of an event on a firm can prove a puzzling task, especially if the objective is to pinpoint some observed change to a specific economic incident. One basic task, which could turn into an obstacle, is to properly identify event date and
period (MacKinlay, 1997, p. 14). The method loses most or all descriptive power without a defined period to study. The period investigated is in event study literature referred to as the ‘event window’, adjustable depending on an event’s magnitude and longevity. Since firms undertake a number of activities simultaneously, not chronologically, event windows can coincidentally include incidents which the research question does not strictly intend to explore. Results can thus be distorted and complicate the isolation of an event and its impact. Inference in event studies hinges on three key assumptions: non-confounding effects in event window; an unanticipated event; and market efficiency (McWilliams & Siegel, 1997, p. 629). For implementation, the following issues are critical: sample size; nonparametric tests to identify outliers; length of, and justification for, event window; confounding effects; and clarification of abnormal returns (McWilliams & Siegel, 1997, p. 629-630). Contingency factors and firm-specific variables must also be identified to bolster conclusions about event effects (MacKinlay, 1997, p. 15; Yayla & Hu, 2011, p. 65).

Deriving evidence for an event’s impact necessitates some sort of deviations from the “normal” state of the firm. Event studies therefore make use of abnormal stock returns to detect amounts attributable to the considered event. MacKinlay defines abnormal returns as “the actual ex post return of the security over the event window minus the normal return of the firm over the event window” (1997, p. 15); McWilliams & Siegel explain the concept as “subtracting the expected return from the actual return” where “any significant difference” between the two is treated as the event’s infliction of abnormality to a firm (1997, p. 628). Leaving calculations to Section 4.3, the equation for obtaining abnormal returns is:

$$AR_{it} = R_{it} - E(R_{it} | X_{t})$$

where $AR_{it}$ and $R_{it}$ are the abnormal and actual ex post returns for firm $i$ respectively; $E(R_{it} | X_{t})$ the expected or normal return; and all in time period $\tau$ as specified by the event window; and $X_{t}$ refers either to the constant mean return model or the market model (MacKinlay, 1997, p. 15). For more detailed calculations, see Section 4.3.

Fama (1991, p. 1607) propagated for the use of event studies as they offer “a clear picture” of markets’ adjustment speeds when new information uncovers. MacKinlay (1997, p. 13, 34) notes that the method has “many applications” within economics and finance, while stressing that issues of sampling, event date uncertainty and statistical robustness, among others, are intrinsic drawbacks of event studies. McWilliams & Siegel (1997, p. 626) contend that the method is a “powerful tool” to gauge unanticipated events’ financial impact. Armitage (1995, p. 25-26) summarizes the method as the go-to term within finance for estimating abnormal returns and testing the EMH. He furthermore presents the various procedural differences and results for estimating abnormal returns, as they are somewhat mutually inconsistent. The separation bases itself on two key parameters in any event study: choice of model and choice of significance tests (Armitage, 1995, p. 26). We deal with such concerns in Section 4.3 and 4.5 respectively.

Peterson (1989) describes the many options a wealth-effect study faces, but only presents the commonest elements of the varying approaches as the methodology practically could be tailored to suit a specific research purpose. She finishes with explicit crediting of “invaluable information” (Peterson, 1989, p. 55) about the assumptions, tests and results to Brown & Warner (1980, 1985). The two authors are perhaps the loudest advocates for event studies, having through numerous deep-delving
papers examined the feats and caveats of the method using monthly and daily return data. The use of daily return data, with potential non-normality characteristics, “presents few difficulties” for the sake of event studies, and autocorrelating abnormal returns have a negligible effect on the results (Brown & Warner, 1985, p. 25-26).

For more extensive and detailed discussion of advantages and disadvantages with event studies, see for example Ball & Torous (1988); Boehmer et al (1991); and Corrado (1989). For questions pertaining to the study at hand, readers are referred to Section 4.3 to gain a better overview of the estimation of abnormal returns.

4.1.2 Data collection

Studying the financial costs of cyberattacks is a multifaceted inquiry. This research focuses on a five-year period immediately superseding the global financial crisis. Already in the time frame delimitation, a number of companies subject to large-scale cyberattacks are excluded. This is however a necessary narrowing in order to form an administrable sample. As IT-related financial literature has become increasingly dispersed and specialized, there is a clear lack of updates for the recent years’ explosive growth in cybercrime and cyberattacks. A thorough compilation based on media coverage and reporting together with attacked companies’ own public communication around these issues is an attempt to synthesize previous literature with contemporary conditions.

The first moment for this thesis concerns the construction of a representative sample. We must deal with two prime obstacles in this process: it is reasonable to assume that a number of attacks have never been publicly disclosed for reasons as diverse as the cyberattacks themselves, and the informational vastness of today does not allow for complete coverage. Sampling is thus reduced to the famous equivalent of localizing the needle in a haystack. Combining the reach of search engines and academic databases, a string of key terms or words (e.g. “cyberattack”; “hack”; “breach”; “intrusion”; “data theft”) were employed in queries to recognized financial press such as The Wall Street Journal, Financial Times, and Bloomberg, together with other international outlets such as NY Times and Washington Post. We motivate the use of these channels by treating their coverage as a criterion for the relative materiality of an attack.

But much of ongoing cybercrime never reaches a wider audience, forcing us to go beyond traditional journalism and corporate press releases to locate more incidents. In plain, this meant scouring websites, blogs, forums, organizations and firms. IT security experts’ professional/personal reporting through company or own research lined the mainstream press reports. As the Internet is littered with conflicting evidence, anecdotes and suggestive speculation, this procedure involved time-consuming source reviews apart from the cumbersome task of obtaining sufficiently significant incidents involving publicly traded corporations. All incidents involving government agencies, private companies, educational institutions, private individuals or other parties unfound on capital markets were eliminated. After combing through long lists of news archives, security reports, and personal cybersecurity intelligence work, the initial sample consisted of 340 separate occasions, placing this study’s sample size far above previous ones.

The second moment was to screen the population for confounding effects, a requirement voiced in practically all notable event studies. The defined event window of this study ([0, 5] and [0, 30] days) imposes restrictions on inclusion of multiple events. Repeated
attacks in rapid succession (i.e. daily in a week or multi-daily in one month) were removed so only initial date of an attack series is used. To secure inferential possibilities between cyberattacks and stock volatility, each event within the sample was screened for interfering announcements that either reinforce or counteract disseminated information around an event. The term “announces” together with each collected company’s name and a string of terms recommended consequently throughout event study literature (“acquisition”; “CEO”; “dividend”; “earnings”; “merger”; “partner”) were used to filter out “contaminated” events to the extent possible. In total, 14 individuals were noted for interfering announcements within one of the event windows. This screening was performed separately, drawing on Cavusoglu et al.’s methodology (2004, p. 80), revealing a high level of intercoder reliability (78%).

This “rough” screening was complemented with a co-performed detailed screening of all separate cases, leaving 9 of the 14 cases in the sample and 5 dropped.

Screening for confounding effects also means that we, as far as possible, trace events to the earliest date of mentioning. Only the first public disclosure about an event is used, and indeed needed, in event studies, meaning multiple reports were removed according to a “date of first mention” principle. Such filtering significantly reduced the amount of individual events. The overhanging drawback of the event study method is its dependence on correct identification of event date. Formerly, drawing dates from press mentions suffered from a one-day time lag, but basing sourcing on modern online editions with instant notification to subscribers removes such potential lags. Furthermore, an event date can be deduced by examining quantities of certain words or terms in news archives around the approximated date.

Entering all remaining companies one by one together with year, month and the term “cyberattack” into Google and Retriever News archive further enhanced the sample as a slew events were dropped due to insufficient or insignificant coverage. Here, we recognize the subjectivity and arbitrariness involved in screening each event. As a final step, all individuals in the sample without sufficient stock data, i.e. spanning from 130 days before an event to 30 days after, were removed from the final sample. Within the studied five-year period, a row of companies suffered numerous attacks. We accommodated such temporal scattering by sampling stock price data for all companies from January 1st 2009 to March 30th 2016. As some events took place early 2010, the estimation window for returns stretched back 130 trading days into mid-2009. At the other end of the spectrum, the sample included events from late 2015, implying the 30-day event window would run well into the first calendar quarter of 2016. This step in the process was extremely tedious as stock data had to be manually compiled within the Thomson Reuters/Eikon (previously Datastream) database, exported and entered into one large data set.

Adjusting the sample for testing involved various steps. 22 events occurred on non-trading days and so were moved to the next trading day following the event date. All firms were then ranked based on market capitalization at the time of attack, where conventional classification served as scale for sorting firms into one of five categories: mega cap (> $200bn); large cap ($10-200bn); mid cap ($2-10bn); and small cap (< $2bn) consisting of two subcategories: micro ($50m-2bn) and nano (< $50m). The process was conducted in two steps. First, using YCharts and in some instances Google Finance,

---

1 Author 1 found 9 confounding events. Author 2 found 14 confounding events. All 9 events of author 1 were also identified by author 2. Inter coder reliability: (9 + 9)/(9 + 14) ≈ 0.78 = 78%
historical market cap figures were retrieved for all firms. Second, the numbers from foreign firms or those denoted in other currencies were converted to U.S. dollars using the prevailing exchange rate at time of conversion. Market caps of foreign firms were sometimes irretrievable or unavailable through YCharts, something we bypassed by matching and cross-referencing each firm’s OTC securities market cap figure with current market cap figures from Google Finance, and subsequently converting the figure to U.S. dollars. This process gave the correct market cap size within a range of 100,000 dollars every time.

To facilitate testing and minimize confusion, each firm was then assigned a separate code based on stock exchange and order in the sample list. Since some firms experienced repeated attacks in the same or different years, every firm received a unique code to expedite further grouping and match firms with event dates and windows during calculations. After company coding, the sample was further categorized into and coded by industry type, type of attack, and motivation behind an attack, inasmuch attacks were traceable or taken responsibility for. The reason is simple: to discover contingencies and potential effects on the cost of an attack, there is need for separation of attack type, the industry/ies these occur in, and if some firms or industries display proneness for certain types of or motives for attacks. Align with previous literature, event classification is preferable, as certain sorts of attacks are presumed worse than others. The academic discrepancy within the field is exemplified by Campbell et al.’s (2003) conclusions about unauthorized access and database breaches as more damaging, at odds with Yayla & Hu’s (2011) evidence that DDoS attacks have higher negative impact than do other sort of attacks. For full coding scheme, readers are referred to Appendix A through D.

For two reasons, an overarching regrouping of the taxonomy was conducted. First, multiple categories contained one or a few observations, impeding statistical analysis. Second, the amount of tests would, from a practical perspective, be nonsensically extensive. All initial coding and classification served to attach an event to a more general label in order to formulate and subsequently test hypotheses. For example, after systematizing all firms into fourteen different industry sectors, the sublevels were in a binary fashion grouped into either a technological or traditional firm. Regarding motivation behind attacks, events were principally categorized as cyber crime, hacktivism, cyber espionage and cyber warfare. Because cyber crime involves theft of assets, the illegal appropriation is deemed motivated by personal gains. In contrast, cyberattacks such as temporary shutdowns (DoS/DDos) or website defacements to demonstrate power or propagate politically are considered primarily undertaken with non-financial interests, hence labeled political. As to the type of attack, previous research has offered contradictory evidence on whether it affects the cost, stock returns and other aspects. We therefore make the following split: inaccessibility attacks where companies’ customers and other parties cannot access the product or service, and intrusions where attackers gain access to company assets. A brief description of each grouping variable is given in Table 1, see next page.

Crafting the sample so thoroughly simplified the data processing within the specialized software specifically constructed for purposes similar to those in this study. It also opened up for wider analyses using several indices, though the S&P500 served as a base-rate case against which all events were matched. Within the software, event window modification and adjustment of estimation window offered simultaneous
measurements of the study’s selected time windows, making for a more comprehensive answer to the initial research question.

4.1.3 The Market model, Abnormal Returns, and Cumulative Abnormal Returns

To see if an event has the hypothesized effect, the observed or realized returns of a stock conditional on an event occurring must be compared to predicted returns unconditional of the event occurring. Reformulated, the returns given the presence of an event should be different from those obtained given its absence as predicted under a “normal” scenario. Producing a benchmark as reference point for assessing abnormality is the first step in event studies, the second being to calculate Abnormal Returns (hereafter referred to as AR) and Cumulative Abnormal Returns (hereafter referred to as CAR). For detailed explications, readers are referred to MacKinlay (1997), Pynnönen (2005) and Serra (2002; 2004).

Producing the needed benchmark is tantamount to selecting an appropriate return model. Commonly, event studies either use a constant mean return model or a market return model, the difference being the former’s assumption about constant security returns over time and the latter’s assumption of a “stable linear relationship” between market and security returns (MacKinlay, 1997, p. 15). Brown & Warner (1980; 1985) demonstrate that more advanced models are only marginally better for most event studies. This study makes use of the market return model based on the following justifications: “[t]he market model represents a potential improvement over the constant

<table>
<thead>
<tr>
<th>Technological</th>
<th>A firm whose content or products are created and/or sold/consumed digitally, or involves technological consumer products. For example: social media platforms, online retailers, or software/hardware producers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional</td>
<td>Firms with mainly physical assets or service elements, e.g. airlines, banks, hotels.</td>
</tr>
<tr>
<td>Inaccessibility</td>
<td>DoS/DDoS attacks, website defacement/alteration, or attacks on other external channels.</td>
</tr>
<tr>
<td>Intrusion</td>
<td>Virus/malware attacks, unauthorized access to databases, servers, records, or other internal data.</td>
</tr>
<tr>
<td>Small/Medium Cap</td>
<td>Small: market cap &lt; $2bn; Medium: $2bn &lt; market cap &lt; $10bn</td>
</tr>
<tr>
<td>Large/Mega Cap</td>
<td>Large: $10bn &lt; market cap &lt; $200bn; Mega: $200bn &lt; market cap</td>
</tr>
<tr>
<td>Personal motivation</td>
<td>Cybercrime such as theft, fraud, and scam of money, intangibles or identities/identificatory information, internal documents.</td>
</tr>
<tr>
<td>Political motivation</td>
<td>Hacktivism, cyber espionage and cyber warfare such as Anonymous operations, government cyberintelligence, non-financially motivated or prestige-driven attacks, communicating ideologies or advancing political agendas.</td>
</tr>
</tbody>
</table>

Table 1: Explanations of subsample categories.
mean return model” (MacKinlay, 1997, p. 18); and Cable & Holland’s findings which “clearly favour choice of the Market Model” (1999, p. 339) in competition with other “frequently used models” (1999, p. 332).

We motivate the use of S&P500 as the market index with several arguments. Firstly, approximately half of the finalized sample includes firms listed on NASDAQ, with the other half being listed on NYSE. Using either the NASDAQ100 index or NYSE Composite in the market model could introduce serious bias in estimations of expected returns and abnormal return calculations, although Bodie et al. (2011, p. 77) maintain that the NYSE Composite is even broader than the S&P500. Notwithstanding such inveighments: to isolate an event, expected returns are calculated under a no-event assumption, and then posited against actual returns given the event to derive event-induced effects on returns. If the attacked firm is included in the same index used in the market model, we can expect a measure of stock-index reaction homogeneity. Additionally, NASDAQ100 bases itself on the “most actively traded non-financial domestic and international securities” (SEC, 2012); since many events involved financial institutions, and the presumed volatility increase after a cyberattack means heightened trading activity, the index could be misrepresentative.

Another determining factor for choice of index concerns sample diversity. A broad market index is better suited to the wide range of industries included in the sample. The DJIA is price-weighted and based on 30 large blue chip stocks, meaning it may not be “representative of the broad market” (Bodie et al., 2011, p. 73). The S&P500 is “an improvement over the [DJIA] in two ways” (Bodie et al., 2011, p. 76): it is broader, and market-value-weighted. Additionally, due to the index’ “significant portion of the total value of the market, it also represents the market” (Nasdaq, 2016). MacKinlay (1997, p. 18) also suggests the S&P500 as a fitting index when using the market model. However, the value weighting can entail movements caused by single stocks’ swings after the public gains knowledge about a cyberattack. The S&P500 is an acceptable but imperfect market index, something borne in mind for the results. However, as we extracted closing prices of each firm and the market index, we recalculate from closing prices to stock return by taking the natural logarithm (ln) of prices so the return calculation looks as follows:

\[ r_{it} = \ln\left(\frac{P_t}{P_{t-1}}\right) \]

where:

- \( P_t \) is the closing price at time \( t \),
- \( P_{t-1} \) is the previous day’s closing price, i.e. at time \( t - 1 \)

The abnormal return equation (MacKinlay, 1997, p. 15) is:

\[ AR_{it} = R_{it} - E(R_{it}|X_t) \]

where: in time period \( \tau \) as specified by the event window,

- \( AR_{it} \) is the abnormal returns of firm \( i \),
- \( R_{it} \) is the actual ex post returns for firm \( i \),
- \( E(R_{it}|X_t) \) the expected or normal return,
• $X_t$ refers either to the constant mean return model or the market model.

Following MacKinlay (1997, p. 18), the **market model** is:

$$\bar{R}_{it} = \alpha_{it} + \beta_{it} R_{mt} + \varepsilon_{it}$$

where:

• $\bar{R}_{it}$ is the expected return of firm $i$ in period $t$,
• $\alpha_{it}$ is the model’s constant for firm $i$ in period $t$,
• $\beta_{it}$ is the model’s coefficient for firm $i$ in period $t$,
• $R_{mt}$ is the market index return $m$ in period $t$,
• $\varepsilon_{it}$ is the estimation error/disturbance term firm $i$ in period $t$.

Pynnönen (2005) provides another, intuitive presentation of the model with only symbolic modifications. Nota bene: the terms “market model” and “market return model” are used interchangeably but refer to the same concept.

The term $E(R_{it} | X_t)$ is thus replaced with a market model estimation ($\bar{R}_{it}$) of expected normal returns assuming no event, and $AR$ for firm $i$ at time $t$ is actual returns $R_{it}$ less $\bar{R}_{it}$.

Abnormal returns are hence defined as the residuals between actual and expected returns predicted by the market return model. Setting correct event dates is complicated and critical: specifying incorrect event dates means the event could be included into the estimation period, distorting $AR$ calculations. To accommodate for this, all event windows are adjusted back two days. For every event, $AR$ event windows $[0, 5]$ and $[0, 30]$ are retrograded to $[-2, 3]$ and $[-2, 28]$.

Estimation and event windows never overlap to prevent contamination of the market model. The estimation window is long because, with time, “the sampling error of the [market model] parameters vanishes,” (MacKinlay, 1997, p. 21) leaving only the variance of the disturbance term left and so “the abnormal return observations will become independent through time” (MacKinlay, 1997, p. 21). By extending our estimation window, we strengthen the data, which hopefully improves the robustness of forthcoming significance tests.

MacKinlay’s method (1997, p. 20) is further employed to estimate market model parameters $\alpha$ and $\beta$ in the 120-day estimation window preceding the event date $\tau = 0$, i.e. $t = -133, -132, \ldots, -3$, and used to compute the reference points against which abnormal returns are calculated. Estimation of $\beta$ is done by dividing firm $i$’s covariance with the market index over the market portfolio’s variance so that

$$
\beta_{it} = \frac{(\sum_{t=T_0+1}^{T_1} (R_{it} - \bar{R}_{it}) (R_{mt} - \bar{R}_{me}))}{\left(\sum_{t=T_0+1}^{T_1} (R_{mt} - \bar{R}_{me})^2\right)}
$$
where:

- $R_{it}$ is the return of firm $i$ in period $t$,
- $\bar{R}_{ie}$ is the average return of firm $i$ in estimation window $e$,
- $R_{me}$ is the market index return $m$ period $t$,
- $\bar{R}_{me}$ is the average market index return $m$ in estimation window $e$.

Estimating $\alpha$ is then simply a reorganization of the original market model equation from MacKinlay (1997, p. 20): $\alpha_{it} = \bar{R}_{ie} - (\beta_{it} \bar{R}_{me})$. Using the above steps in combination, we can thus compile abnormal returns:

$$AR_{it} = R_{it} - \bar{R}_{it}$$

Across the sample, AR’s must be aggregated as they “are rarely per se useful in drawing general inferences about the event effects” (Pynnönen, 2005, p. 332). All AR’s are summed (“cumulated”) into a CAR figure per event period $\tau$ according to the equation

$$CAR_{it} = \sum_{t=1}^{\tau} AR_{it}$$

which seriatim is refined by averaging CAR’s over time and individual firms to receive a Cumulative Average Abnormal Returns (CAAR), because individual companies’ CAR’s are “usually pretty noisy” and so it is better to “deal with averages instead” when testing for significance (Pynnönen, 2005, p. 333), so

$$CAAR_{\tau} = \frac{1}{N} \sum_{t=1}^{\tau} CAR_{it}$$

### 4.1.4 Abnormal volatility

The concept of abnormality, whether referring to returns or volatility, pivots around the assumption of a state of normality prior to a moment of abnormality. Hence, abnormality deals with pre and post temporal dimensions. An event’s impact on volatility can thus be deduced by a ratio of pre-to-post event volatility. Inspiration is drawn from Agrawal et al. (2003, p. 13), yet this study modifies the calculations to fit the products of $AR$ calculations.

Assume $\lambda = abnormal volatility$. So, instead of:

$$\lambda_{pre} = \frac{\sigma^2_i}{\sigma^2_m}$$

and

$$\lambda_{post} = \frac{\sigma^2_i}{\sigma^2_m}$$

as in Agrawal et al. (2003)
where

- $\sigma_i^2$ is the estimated stock return volatility of firm $i$ using its return data sample standard deviation, and
- $\sigma_m^2$ is the market volatility using return data sample standard deviation,

we simplify the calculation by utilizing $AR$ for firm $i$ and their respective sample standard deviation to construct the Abnormal Return Volatility measure ($ARv$).

We motivate this with the following reasoning:

1. When calculating $AR_{it}$, stock return data is already put in relation to market returns as shown, so;

2. $AR_{it}$ substitutes $\frac{\sigma_i^2}{\sigma_m^2}$ which;

3. effectively removes the square root since we directly calculate sample standard deviation of $AR_{it}$, i.e. $\sigma_{pre}$ and $\sigma_{post}$, instead of dealing with variances or $\sigma^2$. Thus;

4. $\lambda_{pre}$ and $\lambda_{post}$ are reduced to $ARv_{\sigma_{pre}}$ and $ARv_{\sigma_{post}}$ for any firm $i$, and;

5. all $AR_{it}$ are calculated for the same window length, where;

6. $ARv_{pre}$ for $n$ firms is estimated in $[-L, 0]$ where $-L$ can take values $-5$ or $-30$, and;

7. $ARv_{post}$ for $n$ firms is estimated in $[L, 0]$ where $L$ can take values $5$ or $30$.

Hence, we should end up with two samples of size $n$: one with pre-event figures and one with post-event figures. These can then be tested against each other for statistically significant changes with “a simple [parametric] t-test” (Agrawal et al., 2003, p. 14). This approach departs from previous work in two ways. First, the assemblage of pre and post-event volatility measures are temporally separated, and tested separately. Agrawal et al. (2003, p. 13-14) use overlapping windows (3, 6, 12 and 24 months), producing four volatility figures which are averaged into “cross-sectional average $\lambda$s”. This is technically incorrect as it risks “serious bias in the standard error estimates” (Pynnönen, 2005, p. 335), from which $\lambda$s are constructed. Second, according to the Central Limit Theorem (CLT), reasonably large samples can be assumed to follow a normal distribution (Encyclopædia Britannica, 2016; Lantz, 2014, p. 81). Performing a parametric t-test, resting on the foundation of distributional normality of data, is thus acceptable considering the sample size.

Calculating and testing the volatility of abnormal returns can seem farfetched, but there is ground for stretching theory to this point. In event studies, all individuals are vetted for confounding effects around the event date and within the event windows to discern event-induced effects only. Likewise, by stepping above and beyond “normal” volatility, we manage to separate market-wide movements and isolate the “true” event induced volatility. Another rationale behind the choice is that investors can be expected to disregard the normal and opt for abnormality. If we assume investors will not care for normal returns, only above-market or abnormal returns, then it is equally fair to focus on the part of volatility which cannot be expected from market movements. Moving
from returns to abnormal returns we thence arrive at abnormal return volatility, which should function as an event-concentrated proxy for volatility. To answer the initial research question about cyberattack effects on stock volatility, it would simply not be sufficient to report a date and a volatility figure: the relative volatility must be placed in an informative context.

4.2 Statistical analysis

4.2.1 A first inspection

In combination with reviews of descriptive statistics, z-scores for skewness and kurtosis are calculated to complement the normality analysis, mainly to support the software-produced statistic tabulations. A standard normal distribution has a skewness of 0 (Lantz, 2014, p. 68) and kurtosis of 3 (DeCarlo, 1997, p. 292). For medium-sized samples ($50 < n < 300$), the z-scores must be $\pm 3.29$ at a significance level of $\alpha = .05$ to reject the null hypothesis, i.e. that the data follows a normal distribution (Kim, 2013, p. 53).

A skewness z-score is the quotient of the normality test’s skewness figure over its own standard error, so that

$$Z_{skewness} = \frac{\text{skewness}}{\text{Std.error}_{skewness}},$$

and the kurtosis z-score is the quotient of the normality test’s kurtosis figure over its own standard error, so that

$$Z_{kurtosis} = \frac{\text{kurtosis}}{\text{Std. error}_{kurtosis}}.$$

To add robustness, histograms, and Normal Q-Q plots are inspected to conclude if the data “looks” normal or non-normal. Only large-enough samples ($n < 50$) offer a fairly reliable graphical exhibition of normality. To strengthen ARv data and tests, boxplots served as a complement to normality tests to eliminate outliers using the $MAD_E$ method from Leys et al. (2013); see next section. Normally, all values situated more than 1.5 quartile distances away from the first and third quartiles in a boxplot are considered outliers (Körner & Wahlgren, 2015, p. 56).

4.2.2 Outliers

Controlling for outliers is a subjective and time-consuming yet important process. The logic is easy to grasp; extremely deviating values sometimes have the power to singlehandedly affect the rest of dataset, in effect distorting the final results of the research. Many procedures, both graphical and mathematical, exists for the purpose of discovering extreme values, the only tricky part is to pick the right one for the data at hand.

After reviewing literature and considering different methods, we chose the $MAD_E$ (Median Absolute Deviation) method over the more conventional Z-score method. The main argumentation behind this choice rests on statistical indicators; as opposed to the Z-score method, which uses the mean and standard deviation to estimate distribution specifics, the $MAD_E$ utilizes the median and the median absolute deviation (Seo, 2002, p. 17). According to Leys et al. (2013), using mean and standard deviation when
screening for outliers defeats its own purpose. They argue that, at the same time as the mean and standard deviation are supposed to guide the outlier detection process, the indicators themselves are “…altered by the presence of outlying values” (2013, p. 765). Furthermore, unlike the Z-score method, which reliability also hinges on normally distributed data, \( MAD_e \) is robust and largely unaffected by the presence of extreme values (Seo, 2002, p. 10, 17); something that our data clearly exhibits through its descriptive statistics.

To calculate \( MAD_e \) we followed the procedure of Leys et al. (2013, p. 765):

\[
MAD_e = b M_i \left( x_i - M(X) \right)
\]

where:

- \( x_i \) is the \( n \) original observations,
- \( M_i \) is the median of the series,
- \( b = 1.4826 \) and is a normalization constant (disregarding the abnormality induced by outliers).

We picked the, by Seo (2002, p. 17) specified, “3 \( MAD_e \) Method”; this basically means that we classified all observations, placed more than \( \pm 3 \) \( MAD_e \) away from the median, as outliers and removed them accordingly. See Section 5.1.3 for results from the outlier removal process.

4.2.3 Testing for normality

The criterion for further significance testing is whether \( CAAR \) and \( ARv \) figures follow a normal or non-normal distribution around the mean in form of a symmetric, bell-shaped curve. Here, the literature offers deviating answers. Kolari & Pynnönen (2010, p. 2) state that “daily stock returns and abnormal returns are not normally distributed”, pointing in the direction of nonparametric tests. On the same note, Corrado (1989) proclaimed the proposed rank test superior to parametric t-tests. Cowan (1992) propagated for a generalized sign test. Much attention within event studies has been designated to parametric tests employing normally distributed stock prices or returns (e.g. Boehmer et al. (1991); Brown & Warner (1980; 1985); Patell (1976)). Further description of the difference in assumptions, limitations and power of parametric and nonparametric tests will be offered throughout the current and forthcoming chapter.

The \( CAAR \) and \( ARv \) data are thus subjected to Shapiro-Wilk (1965) and Kolmogorov-Smirnov tests of normality, though for example Stephens (1974) ventilate objections toward the suitability of normality testing of the latter test. Under the null hypothesis that the data equals a normal distribution, the data will violate assumptions of normality if \( (p < 0.05) \) meaning “there is only a 5 per cent likelihood of the actual data distribution differing from a comparable normal distribution by chance” (Saunders et al., 2016, p. 535).

4.2.4 Type I and Type II errors

Inference can seem straightforward given the relative simplicity of performing statistical tests. Erroneous result interpretation is however not uncommon. In statistical terms, the probability of making such errors hinges on the selected significance level. A
Type I error occurs when a true null hypothesis is falsely rejected; a Type II error, on the other hand, takes place when a false null hypothesis is rejected (Bryman & Bell, 2011, p. 354). The probability of the first sort of error equals the chosen significance level: because we use 0.05 throughout the thesis, the number represents the possibility that our conclusions regarding post-attack volatility are inaccurate. As the missteps are inversely related, a higher significance level (e.g. 0.01 as opposed to 0.05) aiming to reduce Type I error probability is reflected in increased Type II error probability (Saunders et al., 2016, p. 538). Generally, reducing the likelihood of Type I errors is “more important” in research (Saunders et al., 2016, p. 538). Increasing sample sizes is one effective measure to lower chances of rejecting true nulls, as long as one sample is not more than 1.5 times larger than the other. The two-sample t-test is fairly robust against Type I error assuming relatively large sample sizes (Warner, 2012, p. 186-187); more reasoning about size discrepancies is found in Section 4.5.6. Adhering to these principles adds robustness to the significance tests we intend to perform.

4.2.5 A paired-samples t-test (first moment of hypotheses)

The use of paired-samples t-tests comes from the fact that the thesis applies a before/after perspective for abnormal return volatility around cyberattacks. The test is preferable when one has “numerical data for two variables that measure the same feature but under different conditions” (Saunders, 2016, p. 543). Adapting the terminology onto our research question and hypotheses, the “two variables” are ARv, measuring volatility (“the same feature”) before and after an attack (“under different conditions”). The test thus assesses “the likelihood of any difference between your two variables […] occurring by chance alone” (Saunders et al., 2016, p. 543).

The test is also applicable when observations or samples are not independent, as is the case for volatility here: any mean volatility before an attack has bearing on the volatility after an attack, as the two are but separated in time, not nature. Importantly, the p-value of the test statistic will indicate if there is a statistically significant difference in ARv before and after a cyberattack for the various subsamples, or in other words that observed changes in volatility between the periods are not a product of mere chance. The test allows for answering intra-sample differences, i.e. all hypotheses pairs of type:

\[
H_0: \mu_{ARv_A} - \mu_{ARv_B} = 0 \\
H_{a}: \mu_{ARv_A} - \mu_{ARv_B} > 0
\]

where \(\mu_{ARv_A}\) is the mean volatility before an attack, and \(\mu_{ARv_B}\) is the mean volatility after an attack. These include H1 in its entirety and the first moment of H2-H6. As the test is two-sided, the reported p-value must be divided in 2 (Körner & Wahlgren, 2015, p. 150). The significance level is set at 5 % (\(p < 0.05\)) as conventional in business statistics (Bryman & Bell, 2011, p. 354). For more detailed explications of hypotheses, see Section 4.3.

4.2.6 A two-sample t-test (second moment of hypotheses)

Statistically, if it is possible to classify a numerical variable dichotomously, it is also possible to test the means of the two groups against each other for significant differences. The two-sample t-test (also called independent t-test, unpaired t-test or Student’s t-test) uses “a measure of the spread of the scores” (Saunders et al., 2016, p. 543) to answer if the difference in means is likely to have occurred randomly. The test
is useable for assessing the difference in volatility before and after an attack between different and independent subsamples, e.g. if a statistically significant difference exists between the mean volatility for technological or traditional firms (and, of course, for all other subsample specific variables).

For answering H2-H6, this test is necessary to perform as the paired-samples t-test only allows for conclusions regarding differences in mean before and after an attack. The second moment of the hypotheses H2-H6 concerns inter-sample differences, or the “difference between differences” if one wills.

Hence, the test is applied to all hypotheses of type:

\[ H_0: \mu^D AR_{CV1} = \mu^D AR_{CV2} \]
\[ H_a: \mu^D AR_{CV1} > \mu^D AR_{CV2} \]

where \( \mu^D \) is the mean difference in volatility \( AR_{CV1} \) for categorical variable 1, and \( \mu^D \) is the mean difference in volatility \( AR_{CV2} \) for categorical variable 2.

These involve: short and long-term windows (H2); industry classification (H3); type of attack (H4); size (H5); and motivation (H6). A second moment hypothesis will only be applied in those cases where the first moment hull hypothesis is rejected. Note here two things. One: the second moment hypothesis applies to both event windows, and so one result will be presented in connection to each. Two: all p-values are reported as two-sided in this test, and so must be divided by 2 in order to get the correct p-value to assess significance (Körner & Wahlgren, 2015, p. 150). The significance level is set at 5% \( (p < 0.05) \) as conventional in business statistics (Bryman & Bell, 2011, p. 354).

For proper testing, the size of the two samples should be similar. A rule of thumb is that the two-sample t-test is not adequately robust for comparison of two samples when the difference in sample size exceeds 1.5 (Saunders et al., 2016, p. 544). For size differences above this ratio, the chance for making a Type 1 error (falsely rejecting a true null hypothesis) increases. The alternatives are:

- to substitute the independent-sample t-test for a Mann-Whitney U test for hypotheses where sample sizes differ by more than 1.5;
- adjust affected sample sizes by removing observations; or
- draw a random sample of correct size from the population and re-run the independent-sample t-test.

Applying a Mann-Whitney U test, however, requires non-violation of the assumption of homogeneity of variances, i.e. a non-significant Levene’s test (explained in section below). The test is also peculiar in the sense that it tests either a significant distributional difference of two populations or a significant median difference, and neither function fits the hypotheses. For more detailed explications of hypotheses, see Section 4.3.

4.2.7 Heteroscedasticity and Levene’s test

Pertinent to a two-sample t-test is the test of homogeneity of variances (homoscedasticity) most commonly referred to as Levene’s test. Basically, independent samples should display similar (homogeneous) inter-sample variances if one intends to
subject the samples to t-tests (Moser & Stevens, 1992, p. 19). Interpreted numerically, the null hypothesis here is

\[ H_0: \sigma_a^2 = \sigma_b^2 \]

whereby we derive that in cases of violation of homogeneity of variances (heteroscedasticity), i.e. a significant Levene’s test \((p < 0.05)\), the rejection criterion is fulfilled. Outputs from Levene tests are reported underneath each of its corresponding two sample t-test table in the results section.

An alternative approach in cases of prevailing heteroscedasticity is that of Welch (1937), which in SPSS outputs is represented in the row ‘equal variances not assumed’. For statistical correctness, we shall report the alternative Welch-adjusted t-test and its significance value whenever Levene’s test is significant. Since SPSS performs a Welch-adjusted t-test simultaneously to the regular t-test, the adjustment is not a new or separate testing procedure, why we resist from detailed delineation of its statistical modifications.

### 4.2.8 Generalized Sign Test

For clarity: Cumulative Average Abnormal Return (CAAR) calculations are reported together with their corresponding significance levels (produced by the Generalized Sign Test) next to the Average Abnormal Volatility (ARv) tests in the result tables. This is done both to be able to compare our results with those of previous similar studies, by using the same metric; and for internal comparisons with the ARv tests. We formulate no hypotheses for the sake of testing such figures. Traditional event studies start and stop with abnormal returns and the statistical significance of event-related changes. This study partly centers on the abnormal returns concept, but then only as a precursor to the volatility stage of the inquiry. That being so, test results of CAAR calculations will be presented but only in the spirit of adhering to event study methods for business research purposes, not due to their theoretical centrality.

In any case, t-tests are essential. Such tests can be classified into one of two categories: parametric and nonparametric. The key difference underlining this division concerns the data to be tested, as it for some ought to be (approximately) normally distributed while it mustn’t be in the case of other tests (Cowan, 1992, p. 343; Saunders et al., 2016, p. 533). The theme throughout many nonparametric advocates’ papers is that abnormal returns, and return data in itself, are rarely normally distributed, calling for use of nonparametric tests. This can appear confusing when juggling the notion of the central limit theorem and the inclination of financial research for sizeable samples, especially in security and portfolio research. For the purpose of this thesis, a nonparametric alternative suffices.

Cowan (1992) added to the assortment of significance tests a nonparametric generalized sign test; he proposed a measurement “based on the percentage of positive abnormal returns in an estimation period” (Cowan, 1992, p. 343). The test aggregates the proportion of positive CAR before an event and a post-event amount, whereby it sets these in relation to total estimation and event window CAR. Under the null hypothesis of no abnormal returns, the event window ratio should not chronically deviate from the fraction of positive CAR in the estimation window. Compared to the popular Corrado (1989) rank test, we favor the generalized sign test for its power when event windows increase (Cowan, 1992, p. 344). The focus of this study is on longer event windows,
why applying Cowan’s sign test becomes a natural progression from our raw data. Thus, regardless the shape of the distribution, the generalized sign test permits conclusions as to if \( CAAR \) change due to a cyberattack and if the change is statistically significant.

### 4.3 Hypotheses

It should not be ruled out that future academic and professional discussion about the ubiquity and severity of attacks will force a rethink, but for now a cyberattack is declared a firm-specific risk. Investors value firms based on specific prospects or risks, and transmit their opinions through the capital markets. They weigh all cumulated information, although imperfectly, into decisions. Fama’s (1970) Efficient Market Hypothesis dictates that all newly attained information will ultimately be incorporated into security prices. As discussed in Chapter 3 (specifically, Section 3.4) and also throughout Chapter 1, the prevalence, frequency, and severity of cybercrime has steadily increased year by year since the conception of the Internet. This has spawned research on the financial markets’ reaction to knowledge of cyberattacks (Arcuri et al., 2014; Campbell et al., 2003; Cauusoglu et al., 2004; Ettredge & Richardson, 2003; Garg et al., 2003; Gordon et al., 2011; Kannan et al., 2007; Yayla & Hu, 2011) from which one can conclude that: 1) markets penalize the already hurt, and 2) returns and abnormal returns are more negative after markets gain knowledge about an attack. Negative response is commensurate to heightened insecurity and erratic trading. The theoretical leap from there to the assumption that abnormal returns of an attacked firm will fluctuate above “normal” is not immense. Hence, as the first hypothesis, we posit that:

**Hypothesis 1:** A cyberattack will increase the volatility of a firm’s abnormal returns in connection to public disclosure of such an attack.

\[
H_0: \mu_{AR_A} - \mu_{AR_B} = 0
\]

\[
H_a: \mu_{AR_A} - \mu_{AR_B} > 0
\]

The jury is out on whether capital markets are efficient. This study departs from the EMH (Fama, 1970; 1991) while making no attempt to review or develop any version of it. That markets react quickly and negatively to new information was proposed by Brown et al. (1988) and Ball & Torous (1988). The longevity of an attack’s effect on stock prices remains a contested topic. Yayla & Hu attained mixed results in their study of abnormal returns over 1, 5 and 10 days, and suggested “using longer event windows” to “[reexamine] the established conclusions in the […] literature” (2011, p. 75). Arcuri et al. (2014) extend windows to 20 days and find a statistically negative reaction at a confidence level of 90 % (\( \alpha = .10 \)). Hovav and D’arcy (2003) used 25-day windows, concluding returns were negative albeit insignificant, but as they only investigated DoS attacks there is reason to extend not only windows for those attacks but for other attacks as well. Following Yayla & Hu’s conclusions, maybe short-term windows aren’t felicitious for capturing effects from the multitude of attacks taking place today.
With that said, we hopefully add a building block to existing literature by suggesting:

**Hypothesis 2**: A cyberattack will have a larger increase on long-term (i.e. 30 days) volatility of abnormal returns than on short-term (i.e. 5 days) in connection to public disclosure of such an attack.

\[
H_0: \mu_{AR_{longA}} - \mu_{AR_{longB}} = 0 \quad H_0: \mu_{AR_{shortA}} - \mu_{AR_{shortB}} = 0
\]

\[
H_a: \mu_{AR_{longA}} - \mu_{AR_{longB}} > 0 \quad H_a: \mu_{AR_{shortA}} - \mu_{AR_{shortB}} > 0
\]

and

\[
H_0: \mu^D_{AR_{long}} = \mu^D_{AR_{short}} \quad H_a: \mu^D_{AR_{long}} > \mu^D_{AR_{short}}
\]

It is hard to present a definition of a technology firm which any and all can agree on. For our purposes, a technological firm is defined as one whose content or products are created and/or sold/consumed digitally, or involves technological consumer products. For example, this involves social media platforms; smartphone, computer, and software producers (not manufacturers); and online retailers. Airlines, banks, and hotels of course are not technology-free but for classificatory reasons their products are deemed to a higher degree involve physical or service elements. The need for clear separation has however been emphasized more and more in event study literature, as results (e.g. Cavusoglu et al., 2004; Hovav & D’arcy, 2003) point to greater negative abnormal returns for e-commerce firms compared to “conventional” firms in connection to cyberattacks. Agrawal et al. (2003) evidence heightened stock return volatility when shifting to e-commerce business areas. Moreover, e-commerce/online retailers or other firms with highly internet-dependent business models will presumably experience greater disruptions to daily operations and in turn revenues than “conventional” firms with physical sales channels. Thus, we propose that:

**Hypothesis 3**: A cyberattack will have a larger increase on the volatility of abnormal returns of pure technological firms than on traditional firms in connection to public disclosure of such an attack.

\[
H_0: \mu_{AR_{TechA}} - \mu_{AR_{TechB}} = 0 \quad H_0: \mu_{AR_{TradA}} - \mu_{AR_{TradB}} = 0
\]

\[
H_a: \mu_{AR_{TechA}} - \mu_{AR_{TechB}} > 0 \quad H_a: \mu_{AR_{TechA}} - \mu_{AR_{TechB}} > 0
\]

and

\[
H_0: \mu^D_{AR_{Tech}} = \mu^D_{AR_{Trad}} \quad H_a: \mu^D_{AR_{Tech}} > \mu^D_{AR_{Trad}}
\]

A layman’s guess is that studies of this sort must factor in the type or category of attack to provide relevant and meaningful additions to the field. Hovav & D’arcy (2003) only considered DoS attacks. Campell et al. (2003) only investigated virus attacks, as did Hovav & D’arcy (2004). Cavusoglu et al. relax the limitations by widening the scope to “security breaches of all types” (2004, p 71). The results are incompatible: while Campbell et al. (2003) claim a relation between type of attack and CAR, neither Hovav & D’arcy (2004) nor Cavusoglu et al. (2004) find one. Gordon et al. does in fact show that attacks “related to information availability” (2011, p. 54) have significant impact
on firms’ stock returns, as opposed to other categories. Yayla & Hu too provide proof that “market reactions to DoS attacks are considerably stronger than to all other types” (2011, p. 70). Taken together, the material is inconsistent and deserves attention. On that note, we postulate that:

**Hypothesis 4**: A cyberattack will have a larger increase on the volatility of abnormal returns for inaccessibility attacks than for intrusion attacks in connection to public disclosure of such an attack.

\[
H_0: \mu_{AR_{v_{InaccA}}} - \mu_{AR_{v_{InaccB}}} = 0 \quad H_0: \mu_{AR_{v_{IntrA}}} - \mu_{AR_{v_{IntrB}}} = 0
\]

\[
H_{a}: \mu_{AR_{v_{InaccA}}} - \mu_{AR_{v_{InaccB}}} > 0 \quad H_{a}: \mu_{AR_{v_{IntrA}}} - \mu_{AR_{v_{IntrB}}} > 0
\]

and

\[
H_0: \mu_{AR_{v_{smacc}}} = \mu_{AR_{v_{intra}}} \quad H_0: \mu_{AR_{v_{smacc}}} = \mu_{AR_{v_{intra}}}
\]

\[
H_{a}: \mu_{AR_{v_{smacc}}} > \mu_{AR_{v_{intra}}} \quad H_{a}: \mu_{AR_{v_{smacc}}} > \mu_{AR_{v_{intra}}}
\]

The firm “size effect” which Banz (1981) introduced, signals that risk-adjusted returns are higher for small firms than large firms. The sampling and screening process in the current study collected many events involving large or very large companies. In total, the sample consist of 133 corporations in the two largest size classes (LMC’s: large and mega cap) and 50 in the lower half (SMC’s: small and medium cap). Smaller corporations to a higher degree tend to neglect the risks and vulnerabilities of cyberattacks (Proppe, 2015). Such delinquency can prove costly. Furthermore, investments in IT security systems could hypothetically be cheaper per X amount of protected assets for larger corporations due to economies of scale. Size is also a proxy for financial strength in monetary terms, translating into higher purchasing power on the cybersecurity market. Inversely, larger market cap size can increase the target’s attraction. Since many if’s and but’s linger in discussions about size, the uncertainty is instead leveraged into a statistical enquiry, ergo:

**Hypothesis 5**: A cyberattack will have a larger increase on the volatility of abnormal returns for SMC’s than for LMC’s in connection to public disclosure of such an attack.

\[
H_0: \mu_{AR_{v_{SMCA}}} - \mu_{AR_{v_{SMCB}}} = 0 \quad H_0: \mu_{AR_{v_{LMCA}}} - \mu_{AR_{v_{LMCB}}} = 0
\]

\[
H_{a}: \mu_{AR_{v_{SMCA}}} - \mu_{AR_{v_{SMCB}}} > 0 \quad H_{a}: \mu_{AR_{v_{LMCA}}} - \mu_{AR_{v_{LMCB}}} > 0
\]

and

\[
H_0: \mu_{AR_{v_{SMC}}} = \mu_{AR_{v_{LMC}}} \quad H_0: \mu_{AR_{v_{SMC}}} = \mu_{AR_{v_{LMC}}}
\]

\[
H_{a}: \mu_{AR_{v_{SMC}}} > \mu_{AR_{v_{LMC}}} \quad H_{a}: \mu_{AR_{v_{SMC}}} > \mu_{AR_{v_{LMC}}}
\]

Lastly, one original contribution from this thesis concerns the motivation behind an attack. It would be irresponsible for risk executives to view cyberattacks one-dimensionally and ignore the social and political dimensions of an attack. Gupta et al. (2000) did model perpetrator motivation and political/ideological background in experiments on cybersecurity strategies for banks. Motivation behind attacks did for example determine the intensity of an attack, while offering no quantification of costs. Also, behavior did not come from real-life events, only from “genetic algorithms” (Gupta et al., 2000, p. 673), a quixotic attempt to investigate drivers of cyberattacks.
Tellingly, research at the IT/finance intersection is sparse and results meager to say the least. With the rise of hacktivism for political statements, the surge in cybercrime, and cyberspace as the new battlefield for espionage and warfare, the reason behind an attack could influence market reaction to cyberattacks, or investors display insensitivity. Therefore, we expand the literature with a new element, namely motivation behind a cyberattack and consequently advance that:

**Hypothesis 6**: A cyberattack will have a larger increase on the volatility of abnormal returns when the motivation is personal than political in connection to public disclosure of such an attack.

\[ H_0: \mu ARv_{\text{per}A} - \mu ARv_{\text{per}B} = 0 \]

\[ H_0: \mu ARv_{\text{pol}A} - \mu ARv_{\text{pol}B} = 0 \]

\[ H_a: \mu ARv_{\text{per}A} - \mu ARv_{\text{per}B} > 0 \]

\[ H_a: \mu ARv_{\text{pol}A} - \mu ARv_{\text{pol}B} > 0 \]

and

\[ H_0: \mu^D ARv_{\text{per}} = \mu^D ARv_{\text{pol}} \]

\[ H_a: \mu^D ARv_{\text{per}} > \mu^D ARv_{\text{pol}} \]

In the coming chapter, all results are presented and tables accompany all hypotheses. The presentation primarily refers to abnormal volatility. The figures will also report CAAR values with related p-value for significance testing. This is done to not deviate excessively from the standard format of an event study, which conjectures purely upon abnormal returns. We hence retain the original structure and in tandem apply it to a novel dimension.
5 Empirical findings and analysis

Visual and numerical data observations are discussed. Results of the previously introduced normality and significance tests are exhibited. In connection, a brief comment is given to each statistical test and if the hypotheses can or cannot be rejected. The first moment of all hypotheses in both event windows are primarily answered, and the second moments are subject to further exploration and discussion. Statistical tabulations and illustrations are stringently given to complement plain writing. A summarizing table closes the chapter to install in readers the theoretical conclusions discussed in the succeeding chapter.

5.1 Descriptive, summary and visual statistics

In order to provide a quick and comprehensive overview of the data used in forthcoming tests, descriptive and summary statistics precede statistical outputs. Some grouping variables will be handled and discussed separately in cases where they stand out from the rest.

5.1.1 Volatility plots – looking for a pattern

Just as with any properly conducted statistical study, the first analytical procedure conducted in this research was to plot the data. Due to the nature of the research question, the pattern of interest is a change in frequency and strength of up and down movements in abnormal returns, after compared to before an event. In order to establish such a pattern, fifteen random events were picked out. The mean of the corresponding firms’ abnormal returns were then plotted against a time horizon of 30 days before and 30 days after the event in question. As Figure 3 illustrates, all four randomly picked events demonstrate far more volatile post-event abnormal returns than they do during the pre-event period.

The graphs displayed underneath were specially picked out since they represent two commonly reoccurring patterns in the sample. Looking at the first pattern, displayed by Figure 3 on the following page, abnormal returns seem to drop dramatically during the days just after the event, only to rapidly retract to a somewhat normal level again. While a large but transient drop in abnormal returns could be troublesome for a firm, the second reoccurring pattern, displayed by Figure 3 is much more disconcerting.
This is true especially in the sense that it indicates a *persistent* increase in volatility, which potentially could mean that a new and higher “normal level” of volatility has been reached. Worth noting is that persistence of negative effects related to events previously has been argued a factor having potential to pose significant problems for firms, mainly due to consequences like lost shareholder value and confidence (Yayla & Hu, 2011, p. 61). Both these visualized patterns are later confirmed and elaborated on using additional statistical analysis, often in relation to interesting contingency factors that seem to affect their severity.

![Volatility plots](image)

*Figure 3: Volatility plots.*
5.1.2 Descriptive statistics for both event windows – unprocessed data

Following the event study methodology, the goal of the empirical analysis is to establish and isolate a cause and effect scenario by detecting a significant difference in a pre-specified variable, after compared to before an event (Peterson, 1989, p. 36), in our case volatility of abnormal returns. In order to provide a first brief view over their dispositions, these differences are calculated and provided along with their corresponding descriptive statistics in the tables below. It is however important to note that the statistics in these tables are based on crude sub-sample data, not yet controlled for normality, heteroscedasticity or outliers. Two new tables, presenting descriptive statistics of the final samples used in the hypothesis tests, are provided and discussed underneath. The idea behind this layout is to describe the whole analytical process, from beginning to end, in an as informative way as possible.

The tables speak for themselves but some interesting observations can easily be spotted. One can for example settle that the mean increase in post-event volatility (denoted as ‘Mean Statistic’ in the tables) for the grouping variable ‘Intrusion Attack’ is much larger during the 5 day event window compared to the 30 day window; something that is further elaborated on in the next chapter. Another interesting observation, parallel to the previous, would be the high level of negative skewness and positive (excess) kurtosis for the distribution of the same grouping variable during the 5 day window. The skewness statistic of approximately -2 along with the kurtosis statistic of almost 12 indicate that, relative to the normal distribution, this distribution is both skewed to the left as well as distributed with abnormally fat tails (confirmed by its variance); in turn potentially designating an asymmetrical distribution with many extreme observations, or outliers (DeCarlo, 1997, p. 298). In fact, distributions for almost all grouping variables in the 5 day window seem to have more excess kurtosis compared to their corresponding peers in the 30 day window. This circumstance along with their comparably larger variance (Std. Deviation) provides an indication of more extreme observations in the 5 day window compared to the 30 day window (DeCarlo, 1997, p. 298).

Finally, comparing the statistics for the grouping variable ‘Traditional Industry’ over the two event windows, one will notice that both the maximum and mean volatility increase is larger in the short run compared to the long run. Comparing the same statistics to the ones corresponding to ‘Technology Industry’, the difference between the short run and the long run is not nearly as large; potentially flagging for a relatively more persistent volatility increase for firms in the tech sector compared to firms in the traditional sector.

While observations like these provide a hint of what verdicts more specific tests will deliver, one should once again remember that the data in the above table is of the “raw” sort. Distributions need to be checked, potential heteroscedasticity needs to be controlled for and qualified outliers need to be removed; all in order to provide as reliable statistical conclusions as possible when conducting sharp hypothesis tests.
<table>
<thead>
<tr>
<th>Statistic</th>
<th>N</th>
<th>Min.</th>
<th>Max.</th>
<th>Mean</th>
<th>Std. Dev.</th>
<th>Skewness</th>
<th>Kurtosis</th>
<th>Std. Error</th>
<th>Std. Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Firms</td>
<td>183</td>
<td>-0.08467</td>
<td>0.05562</td>
<td>0.0023541</td>
<td>0.01245902</td>
<td>-1.237</td>
<td>0.180</td>
<td>14.591</td>
<td>0.357</td>
</tr>
<tr>
<td>Technology Industry</td>
<td>66</td>
<td>-0.07642</td>
<td>0.05895</td>
<td>0.0032692</td>
<td>0.01600876</td>
<td>-1.237</td>
<td>0.295</td>
<td>10.405</td>
<td>0.582</td>
</tr>
<tr>
<td>Traditional Industry</td>
<td>117</td>
<td>-0.02861</td>
<td>0.04000</td>
<td>0.0018708</td>
<td>0.00847247</td>
<td>0.587</td>
<td>0.224</td>
<td>4.329</td>
<td>0.444</td>
</tr>
<tr>
<td>Large/Mega Mkt. Cap</td>
<td>133</td>
<td>-0.02861</td>
<td>0.03230</td>
<td>0.0021737</td>
<td>0.00916904</td>
<td>-0.032</td>
<td>0.210</td>
<td>1.717</td>
<td>0.417</td>
</tr>
<tr>
<td>Small/medium Mkt. Cap</td>
<td>50</td>
<td>-0.07642</td>
<td>0.05895</td>
<td>0.0029110</td>
<td>0.01687312</td>
<td>-1.148</td>
<td>0.337</td>
<td>11.627</td>
<td>0.662</td>
</tr>
<tr>
<td>Personal Gain</td>
<td>109</td>
<td>-0.07642</td>
<td>0.05895</td>
<td>0.0020833</td>
<td>0.01369511</td>
<td>-0.856</td>
<td>0.231</td>
<td>12.007</td>
<td>0.459</td>
</tr>
<tr>
<td>Political Message</td>
<td>74</td>
<td>-0.02086</td>
<td>0.02780</td>
<td>0.0028050</td>
<td>0.00809917</td>
<td>-0.061</td>
<td>0.279</td>
<td>1.332</td>
<td>0.552</td>
</tr>
<tr>
<td>Inaccessibility Attack</td>
<td>71</td>
<td>-0.01589</td>
<td>0.05895</td>
<td>0.0029610</td>
<td>0.00971619</td>
<td>2.716</td>
<td>0.285</td>
<td>14.989</td>
<td>0.563</td>
</tr>
<tr>
<td>Intrusion Attack</td>
<td>68</td>
<td>-0.07642</td>
<td>0.04000</td>
<td>0.0026354</td>
<td>0.01488527</td>
<td>-1.993</td>
<td>0.291</td>
<td>11.704</td>
<td>0.574</td>
</tr>
</tbody>
</table>

Table 2: Descriptives 5-day event window before outlier removal.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>N</th>
<th>Min.</th>
<th>Max.</th>
<th>Mean</th>
<th>Std. Dev.</th>
<th>Skewness</th>
<th>Kurtosis</th>
<th>Std. Error</th>
<th>Std. Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Firms</td>
<td>183</td>
<td>-0.03386</td>
<td>0.05440</td>
<td>0.0011472</td>
<td>0.00876924</td>
<td>1.317</td>
<td>0.180</td>
<td>10.111</td>
<td>0.357</td>
</tr>
<tr>
<td>Technology Industry</td>
<td>66</td>
<td>-0.03386</td>
<td>0.05440</td>
<td>0.0017312</td>
<td>0.01275949</td>
<td>1.033</td>
<td>0.295</td>
<td>5.087</td>
<td>0.582</td>
</tr>
<tr>
<td>Traditional Industry</td>
<td>117</td>
<td>-0.01386</td>
<td>0.01694</td>
<td>0.0008177</td>
<td>0.00539651</td>
<td>0.520</td>
<td>0.224</td>
<td>1.715</td>
<td>0.444</td>
</tr>
<tr>
<td>Large/Mega Mkt. Cap</td>
<td>133</td>
<td>-0.02107</td>
<td>0.02008</td>
<td>0.0004471</td>
<td>0.00635798</td>
<td>-0.491</td>
<td>0.210</td>
<td>2.888</td>
<td>0.417</td>
</tr>
<tr>
<td>Small/medium Mkt. Cap</td>
<td>50</td>
<td>-0.03386</td>
<td>0.05440</td>
<td>0.0030092</td>
<td>0.01310960</td>
<td>1.322</td>
<td>0.337</td>
<td>5.551</td>
<td>0.662</td>
</tr>
<tr>
<td>Personal Gain</td>
<td>109</td>
<td>-0.03386</td>
<td>0.05440</td>
<td>0.0013921</td>
<td>0.01025221</td>
<td>1.340</td>
<td>0.231</td>
<td>8.351</td>
<td>0.459</td>
</tr>
<tr>
<td>Political Message</td>
<td>74</td>
<td>-0.02107</td>
<td>0.02008</td>
<td>0.0007864</td>
<td>0.00599987</td>
<td>0.080</td>
<td>0.279</td>
<td>4.251</td>
<td>0.552</td>
</tr>
<tr>
<td>Inaccessibility Attack</td>
<td>71</td>
<td>-0.02082</td>
<td>0.01656</td>
<td>0.0013704</td>
<td>0.00562658</td>
<td>-0.614</td>
<td>0.285</td>
<td>4.232</td>
<td>0.563</td>
</tr>
<tr>
<td>Intrusion Attack</td>
<td>68</td>
<td>-0.03386</td>
<td>0.02008</td>
<td>0.0003056</td>
<td>0.00837617</td>
<td>-0.868</td>
<td>0.291</td>
<td>3.833</td>
<td>0.574</td>
</tr>
</tbody>
</table>

Table 3: Descriptives 30-day event window before outlier removal.

5.1.3 Outliers

After conducting a first control of the descriptive statistics for each subsample, all of them were plotted one by one using histograms and boxplots (see appendices G through H for examples) both in order to identify potentially qualified outliers and to study the shape of the distributions. Subsequently, an initial Shapiro-Wilk normality test was conducted, showing non-normality for all distributions. This fact, along with observations made from studying the descriptive statistics above, clearly indicated the need for a more thorough outlier screening process.

It is however important to note that identifying outliers is a very arbitrary process; false positives can accidentally be kept (or removed) no matter what visual or numerical statistical tool used to identify the extreme values. Nevertheless, one can hedge against too extreme errors in the outlier screening process by using tools suitable for the particular sample distribution at hand. As discussed in Section 4.2.2, the $MAD_e$ (Median Absolute Deviation) method was picked and utilized as the main tool when screening for outliers.
Since it would be excessive to describe the outlier removal process for each subsample separately, we refer to the descriptive statistics found above and below in Tables 2-3 and 4-5 where all sample sizes, before and after removing outliers, can be found.

5.1.4 Descriptive statistics for both event windows – processed data

Looking at the new tables, showing descriptive statistics for both event windows, one can see that a couple of things have changed after removing qualified outliers. One of the most obvious differences is the relatively lower kurtosis statistics, especially for the data in the 5-day event window. This basically means that removing outliers has provided distributions that, at least in terms of kurtosis statistics, are closer to 3; which is the kurtosis statistic of the normal distribution² (DeCarlo, 1997, p. 292). To a milder degree, the same is true for the data in 30-day window. Although still not perfect, the skewness statistics for both event windows also have approached the normal level of 0 (Lantz, 2014, p. 68).

Summing it all up, the analytical process of observing the data, both visually and numerically, has made it possible for us to optimize the distributions of our samples in order to furnish for more reliable final tests. However, as the section below explains, the distributions still are not perfect; although, according to ours and our statistical supervisor’s subjective judgment, sufficiently good in order to provide trustworthy results. Nota bene: the number of removed outliers for each subsample can easily be calculated by subtracting the processed data sample sizes from the unprocessed data sample sizes.

---

² In SPSS outputs: the kurtosis statistic of the normal distribution = 0.
³ \((\text{volatility after} - \text{volatility before})/(\text{volatility before})\)
normally distributed data, contingent on sample size discrepancies. Second, with
despite its distribution. First of all, both
depend on the former’s output. All hypothesis tests did however employ the same data, in
Kolmogornov distributed. In some instances, Shapiro
event windows result in a rejection of the null hypothesis that data is normally
The trend is evident: in a majority of cases, both tests applied to all samples in both
ple of normality tests. For H1, four samples (before and after for 5 and 30
days) must be tested. For H2, first moment hypothesis pairs require four tests per
event window, for a total of 12
tests use
results here and refer readers
normality where
- Smirnov tables.
- Smirnov contradicted the result, and we therefore decided to principally
- full Shapiro
H6, first moment hypothesis pairs require four tests per
- Shapiro/Kolmogornov

Table 4: Descriptives 5-day event window after outlier removal.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All Firms</td>
<td>180</td>
<td>-0,01822</td>
<td>0,03861</td>
<td>0,0027606</td>
<td>0,00953045</td>
<td>0,775</td>
<td>0,181</td>
<td>1,731</td>
<td>0,360</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Industry</td>
<td>64</td>
<td>-0,02086</td>
<td>0,03230</td>
<td>0,0036444</td>
<td>0,01068934</td>
<td>0,075</td>
<td>0,299</td>
<td>0,580</td>
<td>0,590</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traditional Industry</td>
<td>113</td>
<td>-0,01589</td>
<td>0,01775</td>
<td>0,0013985</td>
<td>0,00658377</td>
<td>-0,150</td>
<td>0,227</td>
<td>-0,039</td>
<td>0,451</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large/Mega Mkt. Cap</td>
<td>130</td>
<td>-0,02086</td>
<td>0,02166</td>
<td>0,0019691</td>
<td>0,00811441</td>
<td>-0,242</td>
<td>0,212</td>
<td>0,634</td>
<td>0,422</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small/Medium Mkt. Cap</td>
<td>47</td>
<td>-0,01323</td>
<td>0,02780</td>
<td>0,00226174</td>
<td>0,00825804</td>
<td>0,629</td>
<td>0,347</td>
<td>0,673</td>
<td>0,681</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Gain</td>
<td>106</td>
<td>-0,01999</td>
<td>0,04000</td>
<td>0,0025770</td>
<td>0,00970594</td>
<td>0,861</td>
<td>0,235</td>
<td>2,298</td>
<td>0,465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Political Expression</td>
<td>73</td>
<td>-0,02086</td>
<td>0,02166</td>
<td>0,0024626</td>
<td>0,00759682</td>
<td>-0,445</td>
<td>0,281</td>
<td>0,851</td>
<td>0,555</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inaccessability Attack</td>
<td>70</td>
<td>-0,01589</td>
<td>0,01978</td>
<td>0,0021611</td>
<td>0,00704926</td>
<td>0,094</td>
<td>0,287</td>
<td>0,345</td>
<td>0,566</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intruson Attack</td>
<td>66</td>
<td>-0,01999</td>
<td>0,04000</td>
<td>0,0043067</td>
<td>0,01069500</td>
<td>0,773</td>
<td>0,295</td>
<td>2,148</td>
<td>0,582</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Descriptives 30-day event window after outlier removal.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All Firms</td>
<td>179</td>
<td>-0,02107</td>
<td>0,02008</td>
<td>0,0006791</td>
<td>0,00658411</td>
<td>-0,217</td>
<td>0,182</td>
<td>1,967</td>
<td>0,361</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Industry</td>
<td>63</td>
<td>-0,02107</td>
<td>0,02996</td>
<td>0,0008865</td>
<td>0,00914983</td>
<td>0,006</td>
<td>0,302</td>
<td>1,673</td>
<td>0,595</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traditional Industry</td>
<td>117</td>
<td>-0,01386</td>
<td>0,01694</td>
<td>0,0008177</td>
<td>0,00539651</td>
<td>0,520</td>
<td>0,224</td>
<td>1,715</td>
<td>0,444</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large/Mega Mkt. Cap</td>
<td>132</td>
<td>-0,02107</td>
<td>0,01818</td>
<td>0,0002984</td>
<td>0,00614555</td>
<td>-0,727</td>
<td>0,211</td>
<td>2,901</td>
<td>0,419</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small/Medium Mkt. Cap</td>
<td>49</td>
<td>-0,01305</td>
<td>0,05440</td>
<td>0,0037616</td>
<td>0,01210556</td>
<td>2,135</td>
<td>0,340</td>
<td>6,477</td>
<td>0,668</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Gain</td>
<td>106</td>
<td>-0,02082</td>
<td>0,02996</td>
<td>0,0008805</td>
<td>0,00752185</td>
<td>0,195</td>
<td>0,235</td>
<td>2,287</td>
<td>0,465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Political Expression</td>
<td>72</td>
<td>-0,01528</td>
<td>0,01656</td>
<td>0,0008219</td>
<td>0,00500401</td>
<td>0,497</td>
<td>0,283</td>
<td>3,603</td>
<td>0,559</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inaccessability Attack</td>
<td>68</td>
<td>-0,00460</td>
<td>0,01656</td>
<td>0,0021328</td>
<td>0,00430937</td>
<td>1,373</td>
<td>0,291</td>
<td>2,001</td>
<td>0,574</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intruson Attack</td>
<td>67</td>
<td>-0,03386</td>
<td>0,01818</td>
<td>0,0001014</td>
<td>0,00807528</td>
<td>-1,100</td>
<td>0,293</td>
<td>4,287</td>
<td>0,578</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.1.5 Results of normality tests (after outlier removal)

The current study’s strength, a large sample with many grouping variables, brings with it a multiplicity of normality tests. For H1, four samples (before and after for 5 and 30 days) must be tested. For H2-H6, first moment hypothesis pairs require four tests per event window and two tests for each second moment event window, for a total of 12 tests per hypothesis. To report Shapiro-Wilk test outputs for data for one hypothesis is impractical, let alone for six. We therefore summarize the results here and refer readers to appendices E through F for full Shapiro-Wilk/Kolmogornov-Smirnov tables.

The trend is evident: in a majority of cases, both tests applied to all samples in both event windows result in a rejection of the null hypothesis that data is normally distributed. In some instances, Shapiro-Wilk’s indicated non-normality where Kolmogornov-Smirnov contradicted the result, and we therefore decided to principally rely on the former’s output. All hypothesis tests did however employ the same data, in spite of its distribution. First of all, both t-tests used are fairly robust against non-normally distributed data, contingent on sample size discrepancies. Second, with
reference to Lantz (2014, p. 81) all included samples can be assumed normal according to the Central Limit Theorem. Moore et al. (2011, p. 108) rectify use of parametric t-tests despite possible non-normal data for sample size \( N > 40 \).

### 5.2 Results of hypotheses tests

#### 5.2.1 Results for Hypothesis 1 (H1)

The main research question asks what effects a disclosed cyberattack has on stock volatility. Therefore, the entire set of volatilities before an event is tested against post-event volatilities for both event windows. Results from paired-samples t-tests indicate a statistically significant change in volatility after a cyberattack for five days (mean difference \( \approx 0.0027, p < 0.0005 \)) and thirty days (mean difference \( \approx 0.001, p = 0.008 \)).

<table>
<thead>
<tr>
<th>Test</th>
<th>Full Sample</th>
<th>Event window</th>
<th>N</th>
<th>( \Delta ARv )</th>
<th>t-value</th>
<th>Sig.</th>
<th>CAAR</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test of Main Hypothesis</td>
<td>Before/After</td>
<td>[0, 5]</td>
<td>178</td>
<td>0.0026826</td>
<td>3.909</td>
<td>0.000**</td>
<td>-0.0074</td>
<td>0.000**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>172</td>
<td>0.0010291</td>
<td>2.424</td>
<td>0.008**</td>
<td>-0.0251</td>
<td>0.026**</td>
</tr>
</tbody>
</table>

*Table 6: Results of significance test for Hypothesis 1. * \( p < 0.10 \); ** \( p < 0.05 \)

On average, the sample’s stock returns are 23.72\%\(^3\) more volatile five days after a cyberattack and 7.99\% more volatile 30 days after. Translated to statistical lingo, the results are significant at the \( \alpha = .05 \) significance level to conclude that the average volatility actually is higher after a cyberattack, and we thus can reject the H1 null hypothesis \( H_0: \mu ARv_A - \mu ARv_B = 0 \). The conclusion is reinforced by the respective positive mean differences of the two event windows.

\(^3\) \((\text{volatility after} - \text{volatility before})/(\text{volatility before})\)
5.2.2 Results for Hypothesis 2 (H2)

Adjacent to the respective mean volatility difference for both event windows is the second moment of H2, namely that the long-term volatility will be significantly higher than the short-term volatility after a cyberattack. Testing the first moment H2 is identical to the paired-samples t-test answered in H1 (i.e. the full sample) and similarly the first moment H2 null hypothesis pair \( H_0: \mu_{ARv_{longA}} - \mu_{ARv_{longB}} = 0; \) and \( H_0: \mu_{ARv_{shortA}} - \mu_{ARv_{shortB}} = 0 \) is rejected.

\[
\begin{array}{|c|c|c|c|c|c|c|}
\hline
\text{Test} & \text{Time Horizon} & \text{Event window} & \text{N} & \Delta ARv & \text{t-value} & \text{Sig.} & \text{CAAR} & \text{Sig.} \\
\hline
\text{Moment 1 Test} & 5 \text{ days (All firms)} & [0, 5] & 178 & 0,0026826 & 3,909 & 0,000** & -0,0074 & 0,000** \\
\hline
\text{Moment 1 Test} & 30 \text{ days (All firms)} & [0, 30] & 172 & 0,0010291 & 2,424 & 0,008** & -0,0251 & 0,026** \\
\hline
\text{Moment 2 Test} & 30 \text{ days VS 5 days} & [0, 5] & 359 & -0,0020815 & -2,409 & 0,992 & \\
\hline
\end{array}
\]

Table 7: Results of significance tests for Hypothesis 2.

For the second moment, the independent-sample t-test is applied to the two populations of mean volatilities. To begin with, the assumption of homogeneity of variances was violated as assessed by Levene’s test \( (p < 0.0005) \), whereby we reject the null hypothesis \( (H_0: \sigma_i^2 = \sigma_j^2) \) and focus on the alternative Welch-adjusted t-test.

\[
\begin{array}{|c|c|c|}
\hline
\text{Moment 2 test} & \text{Event window} & \text{Levene sig.} \\
\hline
30 \text{ days VS 5 days} & [0, 5] & 0,000** \\
& [0, 30] & \\
\hline
\end{array}
\]

Table 8: Levene's Test of Homogeneity of Variances for H2.

The results display no significantly larger increase at the \( \alpha = .05 \) significance level \( (p = 0.992) \) between the two event windows’ mean volatility. Were the hypothesis reversed, there would be a significantly larger increase for the 5-day. That explains the negative difference of means between them \( (-0.00208145) \), pointing in the “wrong” direction. The increase in long-term volatility is on average 61.64% lower than the short-term increase. Hence, we fail to reject the second moment H2 null hypothesis \( (H_0: \mu^D ARv_{long} = \mu^D ARv_{short}) \) since it is directionally predetermined in favor of the long-term volatility as stated in H2.
5.2.3 Results for Hypothesis 3 (H3)

When testing the two types of industry, we initially proposed that a cyberattack would render significantly higher volatility for both technological and traditional firms. In the 5-day event window, technology firms display a statistically significant 29.70% increase in mean volatility ($p = 0.002$); traditional firms also exhibit a significant increase (16.54%, $p = 0.006$). Testing in the longer event window reiterates findings of the shorter window: longevity of volatility for technology firms is 11.42% higher and significant ($p = 0.02$), and traditional firms’ average volatility is approximately 7.90% higher ($p = 0.003$).

<table>
<thead>
<tr>
<th>Test</th>
<th>Industry</th>
<th>Event window</th>
<th>N</th>
<th>ΔARv</th>
<th>t-value</th>
<th>Sig.</th>
<th>CAAR</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moment 1 Test</td>
<td>Technology</td>
<td>[0, 5]</td>
<td>63</td>
<td>0.0040202</td>
<td>3.086</td>
<td>0.002**</td>
<td>-0.0042</td>
<td>0.160</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>56</td>
<td>0.0017602</td>
<td>2.116</td>
<td>0.020**</td>
<td>-0.0419</td>
<td>0.032**</td>
</tr>
<tr>
<td>Moment 1 Test</td>
<td>Traditional</td>
<td>[0, 5]</td>
<td>112</td>
<td>0.0016365</td>
<td>2.587</td>
<td>0.006**</td>
<td>-0.0091</td>
<td>0.000**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>114</td>
<td>0.0008899</td>
<td>1.903</td>
<td>0.030**</td>
<td>-0.0156</td>
<td>0.237</td>
</tr>
<tr>
<td>Moment 2 Test</td>
<td>Tech VS Trad.</td>
<td>[0, 5]</td>
<td>177</td>
<td>0.0022459</td>
<td>1.525</td>
<td>0.066*</td>
<td>0.478</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>180</td>
<td>0.0000688</td>
<td>0.055</td>
<td>0.177</td>
<td>0.430</td>
<td></td>
</tr>
<tr>
<td>Moment 2 Test (Even Sample Sizes)</td>
<td>Tech VS Trad.</td>
<td>[0, 5]</td>
<td>155</td>
<td>0.0022359</td>
<td>1.454</td>
<td>0.075*</td>
<td>0.430</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>153</td>
<td>0.0002312</td>
<td>0.177</td>
<td>0.430</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 9: Results of significance tests for Hypothesis 3.

The first moment H3 null hypothesis pair ($H_0: |\mu_{AR_{TechA}} - \mu_{AR_{TechB}}| = 0$; and $H_0: |\mu_{AR_{TradA}} - \mu_{AR_{TradB}}| = 0$) is therefore rejected. Tests for homogeneity of variances show a statistically significant result for both event windows ($p = 0.001$).

<table>
<thead>
<tr>
<th>Moment 2 Test</th>
<th>Event window</th>
<th>Levene sig.</th>
<th>Adjusted sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tech VS Trad.</td>
<td>[0, 5]</td>
<td>0.001**</td>
<td>0.011**</td>
</tr>
<tr>
<td></td>
<td>[0, 30]</td>
<td>0.001**</td>
<td>0.005**</td>
</tr>
</tbody>
</table>

Table 10: Levene’s Test of Homogeneity of Variances for H3.

Due to significant Levene’s test results, the second moment H3 null hypothesis is assessed with reported p-values from the Welch t-test, i.e. the row “equal variances not assumed” in SPSS outputs in Appendix. These indicate congruency with the proposed null hypothesis for either event window: the second moment H3 null hypothesis ($H_0: |\mu^{D}_{AR_{Tech}} - \mu^{D}_{AR_{Trad}}| = 0$) cannot be rejected. The average volatility increase is however almost significantly larger in the shorter event window ($p = 0.066$) at $\alpha = .05$, but nowhere close in the extended window regardless of significance level ($p = 0.478$).

However, the sample sizes differ substantially in size. In the 30-day independent-sample t-test, $N_{tech} = 63$, and $N_{trad} = 117$ ($N_{total} = 180$). Therefore, we used SPSS to draw a random sample from the population of traditional firms to even out the sample size differences. The new distribution, $N_{tech} = 63$ and $N_{trad} = 90$, showed a changed significance value ($p = 0.430$ compared to $p = 0.478$) but still not a statistically significantly larger increase in volatility. The same was done in the 5-day window, resulting in $N_{tech} = 64$ and $N_{trad} = 91$, but results remain statistically insignificant ($p = 0.075$). Again, the second moment H3 null hypothesis is not rejected.
5.2.4 Results for Hypothesis 4 (H4)

For inaccessibility cyberattacks, the significance test reveals a significant increase in volatility after an attack for the 5-day event window ($p = 0.003$), and equally a significant increase in the 30-day window ($p = 0.004$) with $\alpha =.05$. Five days after an inaccessibility attack the average volatility is 23.15% higher, and 14.51% higher thirty days after an inaccessibility attack.

For intrusion attacks, the same pattern is discernible: for 5-day and 30-day windows, the increase is significant ($p = 0.007$ and $p = 0.05$ respectively). The increases are 28.20 and 9.37 percent, respectively. The first moment H4 null hypothesis pair ($H_0: \mu_{ARv_{inaccA}} - \mu_{ARv_{inaccB}} = 0$; and $H_0: \mu_{ARv_{IntrA}} - \mu_{ARv_{IntrB}} = 0$) is rejected in similar fashion as H2 and H3.

![Table 11: Results of significance tests for Hypothesis 4.](image)

As for the second moment of H4, the independent-sample $t$-test shows a statistically significantly larger increase in mean volatility between inaccessibility and intrusion attacks for the longer event window ($p = 0.03$). The former has approximately 37% higher volatility than the latter.

![Table 12: Levene’s Test of Homogeneity of Variances for H4.](image)

For the shorter window, we fail to reject the null hypothesis ($H_0: \sigma_{1}^{2} = \sigma_{2}^{2}$) for Levene’s Test of Homogeneity ($p = 0.083$), a window which nonetheless displays an insignificant and smaller increase in volatility for inaccessibility attacks ($p = 0.917$). In consequence, we reject the 30-day second moment H4 null hypothesis ($H_0: \mu^{D}ARv_{inacc} = \mu^{D}ARv_{Intr}$) but fail to reject the corresponding 5-day second moment H4 null hypothesis.
5.2.5 Results for Hypothesis 5 (H5)

This hypothesis investigates a possible size effect. The conclusion is straightforward: SMC’s and LMC’s have a significant increase in volatility after a cyberattack. In the 5-day event window, the mean increase is 20.1% for LMC’s (p = 0.001) and 29.7% for SMC’s (p = 0.005). Within the 30-day event window, mean increases are lower but significant: 8.2% (p = 0.01) and 17% (p = 0.03) for LMC’s and SMC’s respectively. Thus, the first moment H5 null hypothesis pair (H5: μARvSMCA – μARvSMCB = 0; and H5: μARvLMCA – μARvLMCB = 0) is rejected.

<table>
<thead>
<tr>
<th>Test</th>
<th>Market Cap</th>
<th>Event window</th>
<th>N</th>
<th>∆ARv</th>
<th>t-value</th>
<th>Sig.</th>
<th>CAAR</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moment 1 Test</td>
<td>Small/Medium</td>
<td>[0, 5]</td>
<td>47</td>
<td>0.0037511</td>
<td>2.684</td>
<td>0.005**</td>
<td>-0.0194</td>
<td>0.000**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>48</td>
<td>0.0027069</td>
<td>1.935</td>
<td>0.030**</td>
<td>-0.0367</td>
<td>0.935</td>
</tr>
<tr>
<td>Moment 1 Test</td>
<td>Large/Mega</td>
<td>[0, 5]</td>
<td>128</td>
<td>0.0022207</td>
<td>3.186</td>
<td>0.001**</td>
<td>-0.0029</td>
<td>0.026**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>125</td>
<td>0.0009798</td>
<td>2.352</td>
<td>0.010**</td>
<td>-0.0208</td>
<td>0.010**</td>
</tr>
<tr>
<td>Moment 2 Test</td>
<td>SM. VS LM.</td>
<td>[0, 5]</td>
<td>177</td>
<td>0.0006484</td>
<td>0.467</td>
<td>0.630</td>
<td>0.004**</td>
<td>0.004**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>181</td>
<td>0.0034632</td>
<td>0.813</td>
<td>0.321</td>
<td>0.031**</td>
<td></td>
</tr>
<tr>
<td>Moment 2 Test (Even Sample Sizes)</td>
<td>SM. VS LM.</td>
<td>[0, 5]</td>
<td>119</td>
<td>0.0011856</td>
<td>0.551</td>
<td>0.292</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>115</td>
<td>0.0037971</td>
<td>2.013</td>
<td>0.024**</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 13: Results of significance tests for Hypothesis 5.

However, as Levene’s test assesses, the shorter window fails to reject the null hypothesis meaning the populations have significant homogeneity of variances (p = 0.646), in contrast to the 30-day window’s violation of the assumption of homogeneity (p < 0.005).

<table>
<thead>
<tr>
<th>Moment 2 test</th>
<th>Event window</th>
<th>Levene sig.</th>
<th>Adjusted sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM. VS LM.</td>
<td>[0, 5]</td>
<td>0.646</td>
<td>0.630</td>
</tr>
<tr>
<td></td>
<td>[0, 30]</td>
<td>0.000**</td>
<td>0.004**</td>
</tr>
</tbody>
</table>

Table 64: Levene’s Test of Homogeneity of Variances for H5.

The short event window mean volatility increase between SMC’s and LMC’s is also not significant (p = 0.321) so the associated 5-day second moment H5 null hypothesis (H5: μARvSMC = μARvLMC) is not rejected. Conversely, a larger and significant increase in the 30-day SMC mean volatility compared to LMC mean exists (p = 0.031) implying a rejection of the 30-day second moment H5 null hypothesis.

Just as in H3, sample sizes here diverge considerably. In the longer event window, NSMC = 49, and NLMC = 132 (Ntotal = 181), reducing robustness of the independent-sample t-test results. Drawing a new, randomized sample halved observations in the LMC category, so NSMC = 49, and NLMC = 66 (Ntotal = 115), with an even lower significance value (p = 0.024). Repeated in the shorter window, subsamples changed from NSMC = 47, and NLMC = 130 (Ntotal = 177) to NSMC = 49, and NLMC = 70 (Ntotal = 119) though remaining insignificant (p = 0.2915). As before, the 30-day second moment H5 null hypothesis is rejected, while the 5-day second moment H5 null hypothesis is not rejected.
5.2.6 Results for Hypothesis 6 (H6)

In dealing with motivations behind attacks, the initial proposition was that a cyberattack will significantly increase the volatility irrespective of motive. As such, the paired-sample t-tests confirmed the suggestion. Both personally ($p = 0.001$) and politically ($p = 0.001$) motivated attacks affected the 5-day mean volatility, increasing it by 23.8 and 33.8 percent.

The increases were significant in the 30-day span as well, with a 7.7% ($p = 0.032$) average increase after personally motivated attacks and a 13% ($p = 0.007$) average increase after politically motivated ones. This means the first moment H6 null hypothesis pair ($H_0: \mu_{ARv_{per}} - \mu_{ARv_{pol}} = 0$; and $H_0: \mu_{ARv_{polA}} - \mu_{ARv_{polB}} = 0$) is uniformly rejected. From that, we conclude that the empirical evidence demonstrate a significant increase in volatility after a cyberattack.

<table>
<thead>
<tr>
<th>Test</th>
<th>Motivation</th>
<th>Event window</th>
<th>N</th>
<th>ΔARv</th>
<th>t-value</th>
<th>Sig.</th>
<th>CAAR</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moment 1 Test</td>
<td>Personal Gain</td>
<td>[0, 5)</td>
<td>104</td>
<td>0.0029467</td>
<td>3.194</td>
<td>0.001**</td>
<td>-0.0055</td>
<td>0.016**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>98</td>
<td>0.0010760</td>
<td>1.884</td>
<td>0.032**</td>
<td>-0.0215</td>
<td>0.099</td>
</tr>
<tr>
<td>Moment 1 Test</td>
<td>Political Expression</td>
<td>[0, 5)</td>
<td>70</td>
<td>0.0029740</td>
<td>3.506</td>
<td>0.000**</td>
<td>-0.0102</td>
<td>0.004**</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>69</td>
<td>0.0013349</td>
<td>2.564</td>
<td>0.007**</td>
<td>-0.0303</td>
<td>0.131</td>
</tr>
<tr>
<td>Moment 2 Test</td>
<td>Personal VS Political</td>
<td>[0, 5)</td>
<td>179</td>
<td>0.0001144</td>
<td>0.084</td>
<td>0.467</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[0, 30]</td>
<td>178</td>
<td>0.0000585</td>
<td>0.062</td>
<td>0.475</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 15: Results of significance tests for Hypothesis 6.

Pitted against each other, the categories’ increases in volatility offer a unanimous answer: we cannot discriminate among the two, which holds true for the two event windows. The 5-day independent-sample t-test fulfills the assumption of homogeneity of variances ($p = 0.138$), but nevertheless fails to reject the second moment H6 null hypothesis ($H_0: \mu^0_{ARv_{per}} = \mu^0_{ARv_{pol}}$) as ($p = 0.47$) is much above the significance level $\alpha = 0.05$.

<table>
<thead>
<tr>
<th>Moment 2 test</th>
<th>Event window</th>
<th>Levene sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal VS Political</td>
<td>[0, 5]</td>
<td>0.138</td>
</tr>
<tr>
<td></td>
<td>[0, 30]</td>
<td>0.002**</td>
</tr>
</tbody>
</table>

Table 16: Levene’s Test of Homogeneity of Variances for H6.

The populations in the 30-day t-test firstly does not meet the assumptions of homogeneity in Levene’s test ($p = 0.002$), and in turn fails to reject the second moment H6 null hypothesis since ($p = 0.48$). We conclude that none of the second moment H6 null hypotheses can be rejected given the strong empirical evidence supporting them, meaning no larger and significant increase in volatility after personally motivated attacks than after politically motivated. Despite insignificant, 5 and 30-day volatility change is 0.9% and 19.4% lower after a personally motivated attack than one politically motivated.
5.3 Mean plots

In order to furnish for a complement to the very quantitative test tables, we have included two easy-to-comprehend “mean graphs” that provide a visual summary of our results for both event windows. All sub-sample grouping variables are plotted along the x-axis, with their corresponding mean change in volatility plotted along the y-axis. It is easy to compare the two event windows and see that the grouping variable, worst affected in one window is not the same as the grouping variable worst affected in the other. An illustrative example is the large difference in volatility increase for small/medium-sized firms between the two event windows, presented below.

![Figure 4: 5-day mean volatility increase per subsample.](image1)

![Figure 5: 30-day mean volatility increase per subsample.](image2)

5.4 Analysis

For the results to materialize into purposeful information, they must be analyzed in relation to the proposed research question, previous academic work, and the process behind. It is therefore meaningful to reiterate the initial research question from which the research departed:

**What is the effect of a disclosed cyberattack on stock volatility for firms listed in the USA?**

Based on our results, a short and handy answer is that stocks display heightened and statistically significant volatility in the wake of a cyberattack. The combined results of all moment 1 tests unequivocally confirm this picture. While this falls in line with our own beliefs, the results settle in a debate filled with disparate documentation. Before entering discussions linking IT and finance, as well as specific reasoning around individual hypotheses, the results are superimposed on a general sketch of relevant financial principles.
5.4.1 Theoretical analysis

The line of argument from the research question and onwards, leading up to the first hypothesis, proved correct. We do indeed find sufficient and significant support to claim that a cyberattack triggers abnormal stock volatility for the attacked company’s stock. Most notably, the abnormal fluctuations are more prominent in the shorter event window studied here. This clashes with the hypothesized statement that a cyberattack would raise long-term volatility on a perpetual basis, as the decrease in abnormal volatility from the shorter to the longer window signals stock recovery and market adjustment. However, as we proposed in Section 1.4, the fact that an increase in long-term post-event volatility is significant suggests a semi-temporary and gradual incorporation of uncertainty by markets into investment patterns. The two paradigms compete for further theoretical support, but largely trail the semi-strong version of Fama’s (1970; 1991) Efficient Market Hypothesis: over time, market participants factor in all public information into security prices, which move to a new equilibrium.

We can therefore say two things in connection to the temporal decay of abnormal volatility. First, the new information is initially met with ambiguity and hesitancy, provoking a re-pricing period in which investors battle information asymmetry and thus cannot rely on market prices for more than an ad hoc benchmark of attack severity. Such early scrambling reinforces DeBondt & Thaler’s (1985) overreaction hypothesis and Brown et al.’s (1988) uncertain information hypothesis. The observed abnormal volatility suggests that before much is known about an event or the substance behind new information, investors are reluctant to ignore relevant, possibly utility-reducing information, as can be expected assuming rationality.

Ironically, they seem to value the certainty of other stocks over the “victim stock” even though the decision to sell itself is based on incomplete and uncertain information at this preliminary disclosure stage. Such collective overreaction could be the reason why volatility is higher shortly after a cyberattack disclosure than further away from one. Also, the EMH does not aptly capture how security prices instantly “react to major informational surprises” according to Brown et al. (1988, p. 356), suggesting that short-term volatility is the direct result from distorted market efficiency and sluggish pricing mechanisms. One evident objection is that market efficiency is not distorted whenever pricing dissonance occurs, because such readjustment is innately connected to markets’ very endowment of efficiency. In defense of Fama (1970), EMH-irreconcilable results can very well be products of the random element incorporated into the theory, also designated as efficient market anomalies.

Furthermore, the short-term reactions are laden with connotations from behavioral finance. The observed behavior is similar to the regret theory advanced by Bell (1982) and Loones & Sugden (1982). Decision regret (Bell, 1982) arises when actors perceive actions of others as legitimate given informational premises and therefore imitate those actions to minimize regret later on. Regret is the interval “between the assets actually received and the highest level of assets produced by other alternatives” with Bell’s (1982, p. 963) definition. Presumably, the observed volatility just after a cyberattack disclosure is a large-scale version of such regret-minimization. Additionally, because investors are humans and human beings possess the capacity to anticipate outcomes, utility-maximizing actors will try to do so in any given situation (Loones & Sugden, 1982). Therefore, deriving the highest economic utility is transformed into a mixture of economic and personal sensations, which would explain why the results point to a
sharper initial jump in volatility. Shortsighted wealth conservation trumps long-term return prospects.

In an even wider context, decision regret is a microcosm of the anticipated behavior in herding theory, another central tenet within behavioral finance. Basically, attitudes and behavior within larger populations tend to reverberate throughout the collective and install a (sometimes false) narrative of appropriate and inappropriate action. Information asymmetry, especially protruding in junction to cyberattacks, is one important trigger of such flock mentality (Bikhchandani & Sharma, 2000). A reasonable presupposition is that investor actions around a cyberattack are products not of fully informed decisions but of psychological instincts. Avery & Zemsky (1998) forward a multidimensional theory of herding where the third dimension pertains to the uncertainty regarding meaning and quality of information. The abnormal volatility patterns in the short-term event window originate in exactly such uncertainty. The patterns are attributable to Barberis et al.’s (2006) narrow framing notion, namely that investors likely expect higher reward for action than inaction because they consider the event in isolation, equating to a stand-alone gamble. Concluding, short-term volatility is an amalgamation of inferior information, fear of regret, and conformity desires.

That stock volatility over time diminishes is attributable to several financial principles. Firstly, Bikhchandani & Sharma (2000, p. 281) posit that initial herding is often countered with reversed herding, which in turn augments volatility. As seen in Figure 3, abnormal returns continue to vacillate substantially in subsequent trading days, suggesting a relationship between observed volatility and expected volatility, corroborating the volatility feedback concept (e.g. Campbell & Hentschel, 1992). However, thirty days after a cyberattack disclosure, returns in the full sample are on average 7.99% more volatile compared to 23.72% five days afterward. This pattern of temporally contingent corrections follows the EMH (Fama, 1970; 1991). But for investors to reduce the distance to the information frontier, i.e. the theoretical price equilibrium given the newly disclosed cyberattack information, they must undertake information retrieval, something they simultaneously expect compensation for. The EMH however has room for randomness: prices must not be systematically misspecified due to information asymmetry, but can be stochastically explained. It is therefore not straightforward to ascribe decreasing volatility purely to new information.

Nevertheless, security prices are supposed to reflect accessible information (Fama, 1970). The public disclosure of a cyberattack must be treated as one separate piece of information for investors to factor in. The abnormal volatility can be seen as a sign that investors are unsure of the value of current information, provoking the search for more to revise their security valuations. Retrieving information is costly (Stiglitz & Grossman, 1980). If it did not pay off, no one would undertake the task: so simple is the logic. When abnormal volatility reverts toward a steadier state, security prices should converge accordingly since they are formed by the relative informational homogeneity of investors. We can therefore view the lower (30-day) abnormal volatility as a direct result of investors’ superior informational position compared to the 5-day position. Investors have simply gained better knowledge of the extent of the attack.

The implication from that argument, however, is that the cost for improvement must be allocated somewhere. Investors do not only expect compensation for retrieving information, but also a premium for assuming risk (Bodie et al., 2011, p. 317). A volatile stock is a risky stock, hence the connection to the risk premium concept. The
Douglas-Lintner results (Douglas, 1967; Miller & Merton, 1972) indicate that the expected return of an asset is strongly influenced by its own variance, i.e. volatility. The fundamental reasoning of the thesis connects higher volatility to increased financial costs. We are therefore in the position to argue for increased costs as a product of the observed increases in volatility. Furthermore, if the general trend that abnormal volatility decreases with time and information should be contextualized, we further consult the Capital Asset Pricing Model (Lintner, 1965; Mossin, 1966; Sharpe, 1964).

Abnormal volatility is per definition the above-market risk. According to CAPM, no investor would receive additional compensation for bearing unsystematic or firm-specific (idiosyncratic) risk because of the diversification concept. Having already invested in the security, the investor however has incurred risk by desisting from investing in a risk-free asset. Using Merton’s (1980) Risk-to-Reward ratio argument, such investment is presumably undertaken with the prospect of higher expected returns. And as pointed out above, investors engage in costly additional risk-mitigating activities which they in theory should be compensated for. Risk premiums are thus under pressure from two sides to increase after a disclosed cyberattack. This conclusion finds support in French et al.’s (1987) evidence of a positive relationship between risk premiums and stock return volatility.

But if the CAPM is reduced to a beta-comparing equation in light of diversification, theory is once again strained. If investors are only rewarded for systematic risk, capital markets should ignore all cyberattacks as they are firm-specific. Yet we observe negative abnormal returns and increased volatility after disclosures of cyberattacks. Such behavior can only be interpreted as reallocations for reoptimization, suggesting investors rebalance their portfolios according to the first CAPM assumption of rational investors (see Section 3.1.3, page 30). Once more, we seem to have incompatible results. Investors cannot be irrational in their initial reaction (as Bikhchandani & Sharma (2000) and Avery & Zemsky (1998) suggest) and maintain compatibility with CAPM rationality assumptions (foremost that of Markowitz’s (1952)).

Market response to cyberattacks can be argued behaviorally rational and financially irrational. Considering this inconsistency, the results of this study test the limit of Optimal Portfolio Theory and Markowitz’s Portfolio Selection Model (1952). As such, the evidenced theoretical discrepancy in connection to cyberattack disclosures could mean that the Optimal Portfolio Theory only holds for initial portfolio construction. Thereafter, events such as cyberattacks constantly challenge the status quo where only systematic risk counts, to the point of inadmissibility. The argument against Markowitz (1952) finds support in the Douglas-Lintner results (Douglas, 1967; Miller & Merton, 1972) as well as in works of Black (1993) and Fama & French (1992). This conflict between static theory and dynamic information highlights the Gordian knot that is a cyberattack.

5.4.2 Analysis of individual hypotheses

In extension to our main hypothesis, five additional sub-sample specific hypotheses were stated in order to open up for more interesting conclusions. All except one are anchored in verdicts from previous research and included in the analysis for several reasons. The most important reason being that of investigating if the relations between a cyberattack and average abnormal volatility (ARv) are similar to those between a cyberattack and cumulative average abnormal return (CAAR), the latter being the
variable used in all prior studies. Hypothetically one could imagine that even if CAAR proves to remain unchanged subsequent to such an event, the same stock still could have suffered abnormally high volatility during the period. The logic behind such a statement simply rests on econometrical rationality: a period of stock movements that are exactly equally volatile up as down will, at the end of the period, merely average out to a mean change in abnormal return of zero. Even though being a theoretical extreme, the reasoning is valid and makes a comparison between CAAR and ARv interesting.

The other reason behind dividing the full sample into sub-samples is based on the possibility of identifying relationships between firm specific factors and severity in volatility increase. Furthermore, testing all hypotheses for two different event windows, where 5- and 30-day periods proxy for the short and the long run respectively, contributes with a second dimension to the whole analysis. That being said, the outcome of the tests confirms the fruitfulness of the statistical and empirical layout and all findings are discussed below.

First of all, the fact that all moment 1 tests corresponding to our sub-samples turned out positive strengthens our main hypothesis in a rather convincing manner. Fundamentally it means that we, with 95% confidence, have established that stock volatility actually does increase as a result of a cyberattack, for the full sample of firms as well as for all sub-samples separately. This fact alone is quite remarkable, especially in the sense that it both contradicts and confirms findings from several prior studies when comparing ARv to CAAR. The moment 2 tests provide results for an even deeper analysis of the relative volatility effect strength between the grouping variables.

After establishing a significant volatility increase during both event windows for all firms grouped together, we wanted to examine the general persistence of that increase. In order to furnish such conclusions, we tested the two event windows, 5 and 30 days, against each other in a moment 2 test. Our hypothesis, stating that volatility will increase more rigorously in the long run, was mainly anchored in theories of financial herding behavior connected to uncertainty. Bikhchandani & Sharma (2000) points out the powerful implications of collective investor behavior and argues that in cases were great uncertainty is present, herding behavior can potentially trigger a snowballing effect on financial markets (2000, p. 280). That, along with Andrei & Hasler’s (2015, p. 34), argument that uncertainty and stock market volatility are closely connected convinced us of a likely larger increase in long-run than short-run volatility. Nevertheless, the test provided us with a contradictory picture. Volatility increase prior to a cyberattack seems to be statistically more severe in the short run than in the long run; something that, with the benefit of hindsight, would be a natural result adhering to the Efficient Market Hypothesis by Fama (1970), which argues that new information immediately are incorporated into market prices.

Continuing our analytical process, we look to the results produced by Yayla & Hu (2011). They concluded that DoS attacks are among the most financially deterring attack types, both in terms of adverse market response and longevity of that adverse response. They even claim that DoS attacks’ negative impact on stock value escalates with time, even though the attacks themselves often are ephemeral (Yayla & Hu, 2011, p. 75). Our results show a slightly different picture. For the purpose of comparison, we have included an extra column in the result tables, displaying CAAR movements along with their corresponding statistical significance values for all moment 1 tests. Analogous to Yayla and Hu (2011), we find that DoS attacks (denoted as
‘Inaccessibility’ in hypotheses and results) have a statistically significant adverse effect on CAAR, both in the short run and the long run.

When instead considering ‘Intrusion Attacks’, we find that CAAR movements are, although not confirmed by statistical significance, still negative following an attack. Again, these results ratify previous verdicts from Yayla & Hu (2011). The interesting part starts when studying the results from the moment 1 ARv tests which, contradictory to Yayla & Hu’s (2011) findings, show statistically significant support for an increase in stock volatility for both event windows. This confirms the above reasoning: even though intrusion attacks do not seem to significantly affect a firm’s stock return per se, unusually high volatility of stock return still seem to be present during the period. While deviating from Yayla & Hu’s (2011) findings, this conclusion leans towards what Campbell et al. (2003) found regarding attacks gaining access to confidential information, in a way placing our results somewhere in between those studies.

It gets even more interesting when studying the result generated by the moment 2 test, testing for volatility increase caused by inaccessibility attacks against volatility increase caused by intrusion attacks. Our preconceptions of the test result first and foremost rested on Yayla & Hu’s (2011) findings regarding the stark damage inaccessibility attacks previously proved to have on firms’ stock return. In the long run, the test proved us right, suggesting that attacks causing inaccessibility do have a stronger effect on volatility increase than do intrusion attacks. During the 5-day event window, however, the test proved us wrong and demonstrated a strong statistical significance in the opposite direction. In plain writing: intrusion attacks cause a significantly stronger increase in stock volatility in the short run than inaccessibility attacks do. In other words, the test both confirms and extends Yayla & Hu’s (2011) findings; just like inaccessibility attacks seem to cause a persistent decrease in stock return over the long run, they also seem to cause a persistent increase in stock volatility. However, in extension to Yayla & Hu (2011), we also establish evidence for intrusion attacks triggering a short-term volatility peak, stronger than that of inaccessibility attacks.

In our endeavor of building on previous research, we proceeded by dividing the full sample into ‘Small/Medium’ cap and Large/Mega’ cap firms in order to investigate potential differences in volatility response between the two groups. Following prior verdicts from Cavusoglu et al. (2004) and Garg et al. (2003), who both found that smaller firms generally are punished harder in terms of negative stock return following an attack, we hypothesized that the same relation also would be true for volatility increase. Once again, our CAAR tests and ARv tests contradict each other. While the moment 1 ARv tests turned out confirmatory for both groups, showing a significant increase in volatility during both event windows, the corresponding CAAR tests tell a slightly different story. More precisely, they do not show support for a significantly negative short-term return response amongst the small/medium cap group. This is something that, by itself, contradicts prior results from both Cavusoglu et al. (2004) and Garg et al. (2003), but since our focus is on volatility of stock returns and not stock returns per se, we refrain from further elaboration on that point.

For the purpose of this study, testing the two groups against each other are of higher interest. During the 5-day event window, the test showed no significant support for a larger volatility increase among small/medium cap firms compared to large/mega cap firms. For the 30-day window however, the results turned out significantly positive. This means that, while both small/medium and large/mega cap stocks seem to
experience a general volatility increase subsequent to a cyberattack, the increase appears to be significantly more persistent for smaller firms than for larger. Furthermore, since the moment 1 CAAR test shows no significant support for decrease in abnormal return during the same period, this test also provides justification to the abovementioned reasoning; suggesting significant abnormal stock volatility can be present without significant abnormal stock return. It also adds to the findings by Cavusoglu et al. (2004) and Garg et al. (2003), both owing to the fact that we examine stock volatility instead of stock return, and that we consider both short-run and long-run effects.

Following findings from Hovav & D’Arcy (2003) and Cavusoglu et al. (2004), indicating that technology firms are more severely affected in terms of negative market return than are traditional firms, we tested if the same relation also is present in terms of volatility increase. One should however remember a couple of important factors: while Hovav & D’Arcy (2003) considered both short and long run effects, they only included DoS attacks in their sample; and, although Cavusoglu et al. (2004) included both DoS attack and other attacks in their sample, they only measured short run effects. Anyhow, disregarding both of their delimitations, our findings both confirm and contradict their results when comparing stock volatility to stock returns. In contradiction, the moment 2 test provides no significant support for a larger long run volatility increase amongst technology firms compared to traditional firms. In confirmation, the same test does provide weak significant support for larger short run volatility increase amongst firms in the technology sector. Put another way, the relatively larger volatility peak, induced to stocks of technology firms right after a cyberattack, seems to diminish in the long run.

For the purpose of comparison, it is also interesting to add that the CAAR tests once again exhibit opposing results compared to the ARv tests. While, technology firms show a significant decrease in abnormal returns only during the 30-day window, traditional firms show the same significant decrease only during the 5-day window. This is partly in line with what Hovav & D’Arcy (2003) found, and possibly indicates an inverse relationship between abnormal volatility and abnormal returns when considering industry belonging.

Finally, in an effort to discover something original, not at all anchored in previous work, we tested if the motivation behind an attack, by us grouped between ‘Personal Gain’ and ‘Political Expression’, had any bearing on the severity of volatility increase. Even though the results turned out slightly disappointing, a number of conclusions are still possible to draw. First of all, though not statistically significant, the result from the moment 2 test reveal that personally motivated attacks trigger relatively higher abnormal stock volatility than politically motivated ones, which is in line with our reasoning underlying the formulation of the hypothesis. We argued from the perspective that theft is perceived more negative than temporary malfunction or inaccessibility; losing an asset permanently should theoretically reduce utility more than having parts of one’s accumulated assets be damaged. Investors are thus assumed more risk averse toward acts of cybercrime than hacktivism or cyber espionage, inasmuch investors can be expected to differentiate between the categories at all.

On the other hand, it is also possible that investors perceive a politically motivated attack as more acute, owing to the fact that perpetrators exploit a company’s channels to advance own agendas rather than engaging in direct theft of internal assets. Such
impersonal behavior casts light on security flaws and system weakness, conveying the picture of a company being in the hands of extremely skilled and potent groups who essentially want to make a statement rather than a cash withdrawal. One could also speculate about how well the actual values of stolen assets are estimated by investors. As repeated throughout the thesis, many companies cannot assign concrete dollar figures to their intangible assets. Intangibles are, naturally, the only potential target for cybercriminals: they cannot steal buildings. So the question arises yet again: what is the cost of stolen information? With little to go on, investors could potentially experience indifference out of sheer ignorance.

5.5 Practical implications of results

Many conclusions can be drawn from the above analysis, both of the theoretical and practical sort. We have chosen to summarize the most important practical implications here. The most general implication connects back to the answer of our main hypothesis (hypothesis 1); cyberattacks do increase the volatility of stock returns for U.S. listed firms. Having proven that, we have in effect also added another risk dimension to the whole cybersecurity investment dilemma, in turn providing decision makers with a more solid foundation to base investment choices on. We have also established that short-term volatility generally increase more, subsequent to a cyberattack, than do long-term volatility. While some interpretations, resting on the transient nature of effects associated with cyberattacks, could use this fact as an argument not to invest in cyber protection, we can only conclude that there is more to the matter. Even if the general picture shows that short-run volatility increases are more severe, it is still significant in the long run, and on some specific occasions even more significant.

The more explicit implications connect back to the other five sub-sample hypotheses. A highly important one concerns the type of attack directed at a company. As described above, attacks aimed at intruding into companies’ databases, often with the sole purpose of gaining access to confidential information, seem to cause short-term transient volatility peaks after being disclosed to the public. The effect of inaccessibility attacks, on the other hand, seems to be more latent in the short term directly after an attack, only to burst out and increase into full strength in the long run. For financial and IT managers to share this knowledge, could potentially help in their collective effort of deciding what tailor-made measures need to be taken in order to counteract effects, based on attack specifics.

Another essential implication concerns firm size. Our results show that stocks of both small cap and large cap firms seem to react approximately equal in terms of volatility increase in the short run. In the long run however, the story is completely different; relative to large cap, the volatility increase for small cap stocks is considerably larger. This clearly indicates that investors’ skepticism and uneasiness towards cyberattacks are more tenacious when investing in small firms compared to large firms; in turn providing an even bigger incentive for small cap managers to invest in preventive cyber protection measures (even tough large cap managers of course also should consider it).

The last practical implication is aimed at industry belonging. Although with weak statistical significance, our findings specify that firms belonging to the technology sector are more likely to experience a larger short-term volatility peak compared to firms operating in a traditional sector. This fact alone can have many implications, but safe to say is that although the volatility reaction for technology stocks is more extreme in the short run, it is still significantly present in the long run for both industry types.
This means that, even though managers representing both technology and traditional firms should prepare for potential attacks, technology firms’ managers ought to prepare a little extra for the short-term impact.

Considering everything abovementioned, we would like to conclude with two advices - one specific and one more general. The specific advice would be that small cap firms operating in the technology sector should take a closer look at their cyber protection measures, especially those shielding the company from inaccessibility attacks. The more general, and probably also much more important, advice is that all IT and financial managers representing listed firms from all industry sectors, in all size categories should prepare and implement protection for all different types of cyberattacks because cyberattacks actually do increase a firm’s stock volatility.
## 5.6 Summary of results

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Event window</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypothesis 1: A cyberattack will have a increase on the volatility of a firm’s abnormal returns in connection to public disclosure of such an attack.</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Hypothesis 2: A cyberattack will have a larger increase on long-term (i.e. 30 days) volatility of abnormal returns than on short-term (i.e. 5 days) in connection to public disclosure of such an attack</td>
<td>Not Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Hypothesis 3: A cyberattack will have a larger increase on the volatility of abnormal returns of pure technological firms than on traditional firms in connection to public disclosure of such an attack.</td>
<td>Weakly supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Hypothesis 4: A cyberattack will have a larger increase on the volatility of abnormal returns for inaccessibility attacks than for intrusion attacks in connection to public disclosure of such an attack.</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Hypothesis 5: A cyberattack will have a larger increase on the volatility of abnormal returns for SMC’s than for LMC’s in connection to public disclosure of such an attack.</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Hypothesis 6: A cyberattack will have a larger increase on the volatility of abnormal returns when the motivation is personal than political in connection to public disclosure of such an attack.</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

*Table 17: Summary of hypotheses and results.*
6 Conclusions

In capacity of the final chapter, this section entails reflections and discussions about the achieved results. Among others, how well the end product fits the intended purpose, the alignment between initial and actual hypothesization, and whether we manage to contribute to the field, are discussed. The entire process is then summarized. Lastly, suggestions and recommendations for future research are offered.

6.1 Truth criteria

Quality is the central tenet for quantitative research within the social sciences, which transmute into matters of reliability and validity, or using Saunders et al.’s (2016, p. 202) connotation, “the scientific canons of inquiry”. Reliability has to do with the possibility for external researchers to replicate the performed research, and also the level of consistency of results in relation to existing literature. Simplified, replicability and consistency pertain to research design. Validity, on the other hand, deals with: the appropriateness of measures; how accurate the ensuing analysis is; and how relevant results are in terms of applicability to “outside” conditions, or the results’ generalizability (Saunders et al., 2016, p. 202).

6.1.1 Reliability

When assessing research quality, often a separation of internal and external reliability is upheld as beneficial in order to disconnect the question of whether results have bearing on the outside from that of how the methods selected to achieve the results have bearing on the results themselves. Internal reliability concerns itself with the proverbial red thread of any research, so actions of individual researchers do not influence the outcome in an unnaturally biased way. If instructions, purpose, objective etc. are all clearly communicated, this raises the internal reliability as it eliminates chances of individual manipulation or systematic misinterpretations. Seeing to that all elements pull in the same direction ensures high internal reliability.

For this research, it was essential to compile and adhere to a number of criteria in the sampling process. As documented in Section 4.2, the process was guided by a certain (limited) amount of words, i.e. a search engine string, and a set of primary sources to collect events from. These were complemented by many other sources to construct a richer picture of the cybersecurity arena in 2010-2015. As far as possible, both authors have been involved in discussing, reviewing, and justifying each included event, both in the initial sampling and also in the screening process. Scrutinizing all events individually and jointly can be counted as a reliability-improving measure, but is equally susceptible to researcher error (Saunders et al., 2016, p. 203). These interpretations of course build in an amount of arbitrariness and subjectivity, or researcher bias, suggesting the need for future interpretators to replicate ours in order to attain similar results. As it is unthinkable, internal reliability in the form of consistency cannot be optimally established in studies of the kind; we must accept that our findings could differ substantially from previously conducted work due to lack of informational rigorousness, and in turn future findings can deviate from this study depending on personal judgment.
To ensure reliability, as it preoccupies itself with securing consistency, there are two avenues of reasoning to follow. Either, for the sake of external reliability we would need to offer an exhaustive list of consulted web sites, news articles, press releases, corporate reports, etc., so others could follow along step by step; or the final list of events is provided alongside criteria about size, materiality, extent, duration and all other constituents of event interpretation to match against new interpretations. We strengthen the external reliability by providing all events gathered in one database, describing the procedures for calculating abnormal returns and volatility, and clarifying which tests apply to what population and hypothesis. Throughout the thesis, motivation behind techniques and procedures are offered to reinforce external reliability.

Contiguous with consistency is replicability, the other aspect of reliability. As much effort goes into ensuring internal and external reliability, we automatically obtain high replicability. The steps taken within and between metrics/tests are carefully explained and exemplified, keeping in mind that calculations, assumptions, and notations must be intuitive for a novel reader. There is never a perfect reconstruction of a research process, and we have no ambitions of writing a manual for identical results, but the lengthy explications in Chapter 4 should serve the purpose of replication well. We therefore feel confidence in the chosen methods and employed procedures, as for the whole process.

6.1.2 Validity

Research quality also rests on validity, which in turn is underbuilt with high reliability. A study’s validity can never be higher than its reliability (Lantz, 2014, p. 43). Validity is concerned with matching the right tool to the correct task (Körner & Wahlgren, 2015, p. 15). The term problematizes used measures and methods in a self-reflecting manner to ensure that what is intended to be gauged lines up with what the specific measures and methods gauge. To ensure measurement validity (Saunders et al., 2016, p. 202) we have persistently and notoriously followed the basic steps within event study method literature, specifically striving to pursue outlines in studies examining wealth effect of certain events as well as studies investigating event-induced volatility. We surveyed the field for the most prominent significance tests for abnormal returns, discussing advantages and disadvantages among the alternatives. With recourse to purposes of existing studies, the methods from those studies most similar to our purpose were chosen, ensconcing the study in high-validity bounds. We should thus be in a position to claim that the performed tests agree with our measurement intentions, and therefrom conclude high measurement validity. One must, however, always bear in mind that operationalization of measures could confound the fact that they measure something with the fact that they measure what they should.

External validity is, as the term suggests, the transferability of results to the exterior milieu. The results of this study are non-generic and not directly translatable to all incidents taking place daily around the world, but comprise a tile in the mosaic that is financial cybersecurity research. When discussing external validity, much emphasis is placed on sample size. With over 300 events initially, and around 180 in the finalized sample, the findings relate to a broad scope of firms. One drawback comes from the geographical limitations. The Americano-centric perspective detracts from the study’s external validity, yet we perceive the overall level as high.
Internal validity “is established when your research accurately demonstrates a causal relationship between two variables” (Saunders et al., 2016, p. 203). Though we are reluctant to claim a perfect causal relationship between a cyberattack and heightened stock volatility, all significance tests in some way or another suggested higher post-event volatility. Saunders et al. (2016, p. 203) further elaborate that internal validity often is associated with positivist, quantitative research of explanatory design. Seeing as this study is epistemologically positivist, quantitative, and descripto-explanatory, and the results indicate causality, we satisfy the internal validity condition for research quality.

6.1.3 Generalizability

If research enjoys high external validity, the results are (almost always) automatically generalizable in new settings. An exception would be if the research and results observe/confirm a predicated circumstance, but the findings are applicable only to a very confined or controlled setting, and hence lack relations to a more general context. Business administration research is rarely so specific that it seals off connections to the environment it poses to investigate. The thesis at hand offers room for compromise regarding real-world impact of the proposed results and conclusion, notwithstanding the point that all companies physically exist, events have digitally-physically taken place, and stock and market returns are tangible.

The sums (costs) of cyberattacks are monetarily disputable, not materially. Therefore, two competing perspectives emerge in view of the results. One advances the notion of tangibility, that attacks cause extra volatility, so instinctively the results are generalizable. The other maintains a need for reobservation and that real generalizability insists on repeated reaffirmation of preliminary verdicts. With some creativity, these are but two sides of the same coin. A first and humble degree of generalizability can apply to all firms listed or attacked (or both) in the U.S, mostly due to the study’s representative sample for that specific market. Extended, firms on Asian and/or European exchanges could be seen to experience similar volatility, since American results can be a proxy of more general phenomena.

6.2 Concluding remarks

Over the course of this research, many interesting and completely new aspects of business, and particularly finance, presented themselves. Concepts like cybercrime and cyberattacks not only stir up immediate legal, ethical and corporate dilemmas, but run deep into basic ideas about ownership, worth/value, democracy, communication and national sovereignty.

The problem, as we see it, consists of many moveable components. One is today’s extreme dependence on computers and Internet within business operations, paired with a recurring interest misalignment problem between cybersecurity companies, purchasers of protection, and insurers. Another concerns the focus and scope. A prerequisite for performing studies such as this is proper delimitations. The abundance of events hints at clear time period demarcation together with properly specific geographical criteria.

In a world with finite monetary resources, we see a clear need for leadership and cooperation within legislation. Corporations, consortiums, and conglomerates invest extreme amounts of private capital into protection and prevention. Many nation states have completely disregarded this area of legislation, while others are incapable of
upholding the laws they have in place, putting private companies at the crosshairs of highly advanced cybercriminals while also letting them foot the bill for shielding societal values. The issue has reached a critical stage and demands global attention if the international economy is to be alleviated from the anarchistic attitudes to ownership frequently found in cyberspace.

It goes without saying that the results presented in this thesis are preliminary and suggestive. With that reservation, a couple of incontestable points can be emphasized. A cyberattack is a multifaceted incident whereas the responsible elements in most cases remain anonymous. Businesses thrive off transparent institutions and societies, accentuating the need for better-illuminated online platforms for business, trading, and exchange. Gaining physical access to companies often incurs rigorous identification processes, at least in the U.S. In contrast, cyberspace creates a parallel dimension in which anyone, from anywhere, can gain access to extremely sensitive information. Modern businesses’ total dependence on integrated communication chains for value-adding has driven up the tempo of enterprises and commerce to a critical point. Mistakes can often be corrected, but at a certain speed the room for maneuver is practically removed. Firms of today have effectively placed themselves face to face with elements refusing to compete, with only one business model: theft.

In a time of irreversible globalizing forces, it should be in the interest of nation states to ensure citizens and corporations reliable means of conducting personal and professional business services. To do so demands much work. We point out a few tentative areas in Section 6.5.

6.3 Contributions

The contribution of our study is a three-pronged construction. We set out to add to academic literature within market efficiency, volatility and risk, and cost of capital. Another area we wished to build upon is the practical advices concerning the financial consequences of corporations’ IT security investments and management. The third component is that of time, where the matter becomes somewhat more diffuse and disentanglement of factors more complicated.

To begin with, our results have pointed out academic inconsistencies of CAPM and portfolio theory. We maintain a moderate approach as to the implications of our results apropos the well-established financial theories; yet, uncovering the abnormalities of markets pertinent to cyberattacks do stress their applicability. It must not be so that they are discarded, merely bent and experimented with in emerging settings. The digital arena is indisputably a recent phenomenon in economic history, in contrast to the theoretical (but mostly practical) base of financial markets. Digitalization of exchanges and trading has upset or altered the very conditions precipitating classical financial theorization. Just as society at large faces forces of creative destruction, so does the well-embedded academia. The study may not present revolutionizing ideas, but it surely points out where theory collides with reality. It is not unexpected to observe that investors react quickly and distinctly upon receiving negative news. The unexpectedness lies in how financial theory attempts to explain the observations.

Financial actors are prone to repeat what is not challenged. With this study, we confront conventional financial principles with the dynamics of cyberspace. Our prime contribution revolves around notions of market inefficiencies, un navigable informational environments, and detached investors seemingly left at their own devices.
We succeed in establishing increases in stock volatility after a cyberattack. Attaching the results to more behaviorally oriented financial theory deploys them in a way which should provoke reflection. Specifically, by introducing abnormality into the analysis, we go beyond what can be expected to be explained by standard models and theories. The main findings hence operate beyond the classical but shy of the genuinely transformative. We do, nonetheless, provide a current and exhaustive review of modern cybercrime, which hopefully is put to use in the financial IT literature.

In practical terms, the thesis uncovers hidden assumptions surrounding IT investments and cybersecurity. Many companies simply have suboptimal protection, and manifest a troubling ambiguity toward the topic. However conservatively or creatively the results are interpreted, they stress the severity with which markets view cyberattacks. Investors are not willing to bear the imminent stress from cyberattacks. Cybersecurity is not only within the realm of corporate self-interest, since it indirectly becomes another area of competitive advantages. In a broadened sense, that raises questions of moral and psychological nature, for example on corporate responsibility vis-à-vis shareholders. Companies relying on or intending to rely on equity capital should thus take heed of the observed volatility and strategize upon where, protection-wise, investors expect the company to be, and where the company in fact stands. This, we perceive, is a genuine contribution from the study.

Time is of the essence for an attacked company. Restoring systems and operations, resuming business, reorganizing and improving procedures and policies are fervently recommended as crucial instant responses. But with the damage already done, a company must offer credible and balanced longer-term solutions to dampen market insecurity and regain investor (and customer) confidence. The increasingly widespread problem for corporations to do so is one contribution from this study. How hard it is for investors to assess such steps by firms is another, the importance of adequate and reliable information a third. And in combination, the foremost imputation is the worth of cyber investments over time for companies.

In more methodological terms, we have problematized and developed the concept of abnormal returns. As reasoned in Chapter 4, abnormal returns are not per se ideal when seeking to quantify (or theorize on) potential costs. Thus, the investigating of abnormal return volatility adds a new dimension to quantification, and concurrently enhances event study methodology in general. Doing so also fuses IT and financial literature in a progressive manner, all notable contributions. Moreover, constructing a cyberattack database is no negligible addition to business administration and IT research. The undertaken study also introduced motivation as a new factor, unfound in previous literature, in complement to novel juxtaposing of classificatory sets.

6.4 Ethical considerations

The general ethical implications of research are extensively discussed in Section 2.10. This study strives to add academically and benefit professionals, why we do not identify ethical obstacles between the target audiences and us. The complete future ramifications of the thesis are unintelligible. Thus, only concrete ethical issues are raised.

Strictly ethically, the numerical results and conclusions of the study are dislodged from individuals, and will in capacity of independent entities not directly damage any individuals. A cyberattack is however not a product of research, but of conscious and concerted human action against companies (or other parties). Investigating these attacks
- uncovering costs, pointing out risks, examining reasons – can potentially translate into counteractions from companies, agencies and governments, meaning actual implications in the eyes of perpetrators. It is of utmost importance to maintain two parallel trains of thought when eyeing cyberattacks. On one hand, some attacks are outright illegal and break laws, and must face legal process. On the other, some are only 21st century extensions of democratic defense of principles in a territory with outdated societal and legal codes. Hence, we have moved into discussions about legal grey areas, which is a perfectly sensible extension of research in this field. Not that this study will trigger policy updates by lawmakers, but continued exploration most certainly will. Cost estimates for cyberattacks could therefore be used as pretext for dubious countermeasures simply by referring to the economic burden they impose on markets and countries.

The occurrence of cyberattacks raises, by itself, questions about societal consequences. Why do they happen? Which country is responsible for legal processes against perpetrators, that where it took place or where it was conducted from, some middle part or a combination? How should victims be treated? Should victims be punished with higher fines, as proposed in new EU legislation? What about systemically important, high profile targets such as financial institutions and government agencies, should they be prioritized in protective work? Today, most jurisdictions levy financial penalties to incentivize cybersecurity investments. Can smaller, financially weaker firms be exempt of such frameworks? Should cyberattacks be thought of as just another cost of doing business, or reversed: is cybersecurity an area for competitive advantage? It is not certain that shareholders, or if widened, stakeholders, want answers to such controversial issues. Casting light on the area is necessary, together with informed discussion of why, how, and most importantly who. Contributing with knowledge is seldom uncomplicated.

6.5 Suggestions and recommendations for future research

During the research process, many alternative approaches to the subject were discovered. For example, the current study limited itself to one index (S&P500) for the market model. Because of sample heterogeneity, a clear improvement would be to construct a weighted-average market model with the use of several indices, e.g. NASDAQ100, DJIA, NYSE Composite, or Wilshire 5000. By doing so, calculations would be more representative of the actual market movements and fit better to the sample’s industry diversity. Another enhancement would be to go outside of the U.S. market and weigh in attacks in Asia and Europe, but, of course, that would affect the choice of market index/indices. In the sampling process, we noticed an abundance of large-scale cyberattacks in Europe and advanced Asian economies such as Korea, Japan, Singapore and China.

Extending the scope in such a way also means a reworking of the market model to utilize national indices; including several ones would be the ultimate combination. This would hopefully broaden the results of the thesis to other important financial markets. In connection to widening the market focus, we also suggest a specific investigation of cyberattacks in the financial sector, whether in the U.S. or elsewhere. Many events involved financial institutions, and many were repeatedly attacked. Due to their vital national and international economic role, threats to the sector in many ways jeopardize the stability of entire countries and regions. Future branch-specific research can uncover
if the financial sector is more exposed than other, to increase awareness around cyberattacks.

Entering into a company perspective, the question of how companies actually estimate what to protect is a rich extension of this study and a suitable future research topic. More specifically, when does a company consider itself protected, and why, could both be developed into research projects; either, additional quantitative studies can improve quantifications from/for companies’ viewpoint, or qualitative studies refine aspects such as change in cost of capital, investment decisions, cost benefit analysis of attack management, or investor behavior. A business-legal perspective on the topic is also highly relevant for quantitative and qualitative research. Much remains to explore within business and human behavior around a cyberattack.

The human side of stock market reactions to cyberattacks can, and should, be explored further. For example, using prospect theory to investigate how investors perceive and value information after a cyberattack can open up new paths within behavioral (and hopefully traditional) finance. Another theoretical refinement is to involve pure game theory under an experimental design to investigate investor choices.

The specific angle taken within this research makes it pioneering of sorts. The performed significance tests only go so far in explaining relationships between variables used in Hypotheses 2 to 6. With the use of the tests, we establish a degree of interrelatedness, and simultaneously lay the foundation for constructing a simple or multiple regression model. A final recommendation is thus to develop a regression model using the categorical variables of this study. The ability to conclude which factors influence attack severity with higher precision comes from such development, a useful tool in estimating firm-specific cyberattack vulnerability. With even better controlled contingency factors, more can be added to the process initiated with this study. In combination to statistical refinements, a three-factor market model would improve abnormal return calculations, making it a qualified candidate for upcoming research, and so would the use of an ARCH/GARCH volatility model for estimating stock volatility.
7 Reference list


8 Appendices

Appendix A: Company list and coding

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Company Code&lt;sup&gt;4&lt;/sup&gt;</th>
<th>Company Name</th>
<th>Company Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activision/Blizzard Inc.</td>
<td>USNA020</td>
<td>Equifax Inc</td>
<td>USNY048</td>
</tr>
<tr>
<td>Adobe</td>
<td>USNA052</td>
<td>E-trade Financial Corp</td>
<td>USNA016</td>
</tr>
<tr>
<td>Alibaba.com/Alibaba group</td>
<td>USNY022</td>
<td>Facebook</td>
<td>USNA043</td>
</tr>
<tr>
<td>Ally Financial</td>
<td>USNY028</td>
<td>Fifth Third Bancorp</td>
<td>USNA035</td>
</tr>
<tr>
<td>American Airlines</td>
<td>USNA013</td>
<td>First Citizens Bancshares</td>
<td>USNA038</td>
</tr>
<tr>
<td>American Express</td>
<td>USNY058</td>
<td>Fred's Inc.</td>
<td>USNA009</td>
</tr>
<tr>
<td>Ameriprise Financial</td>
<td>USNY056</td>
<td>Global Payments Inc.</td>
<td>USNY080</td>
</tr>
<tr>
<td>AOL</td>
<td>USNY008</td>
<td>Google</td>
<td>USNA054</td>
</tr>
<tr>
<td>Apple</td>
<td>USNA044</td>
<td>Hilton World Wide Holdings</td>
<td>USNY016</td>
</tr>
<tr>
<td>ArcelorMittal</td>
<td>USNY073</td>
<td>Home Depot</td>
<td>USNY019</td>
</tr>
<tr>
<td>ASML</td>
<td>USNA100</td>
<td>HSBC</td>
<td>USNY102</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>USNY014</td>
<td>Huntington Bancorp</td>
<td>USNA037</td>
</tr>
<tr>
<td>Autonation</td>
<td>USNY011</td>
<td>Hyatt Hotels Corp</td>
<td>USNY023</td>
</tr>
<tr>
<td>AVG Technologies</td>
<td>USNY057</td>
<td>ING Bank</td>
<td>USNY060</td>
</tr>
<tr>
<td>B&amp;G Foods Inc.</td>
<td>USNY069</td>
<td>Innodata Inc.</td>
<td>USNA065</td>
</tr>
<tr>
<td>Bank of America</td>
<td>USNY034</td>
<td>Intercontinental Hotel Group</td>
<td>USNY103</td>
</tr>
<tr>
<td>Bank of Montreal</td>
<td>USNY107</td>
<td>Juniper Networks Inc</td>
<td>USNY025</td>
</tr>
<tr>
<td>BB&amp;T</td>
<td>USNY029</td>
<td>KB Financial Group</td>
<td>USNY105</td>
</tr>
<tr>
<td>BBVA</td>
<td>USNY039</td>
<td>KeyBank/KeyCorp</td>
<td>USNY038</td>
</tr>
<tr>
<td>Bebe Stores Inc.</td>
<td>USNA032</td>
<td>Las Vegas Sands Corp.</td>
<td>USNY005</td>
</tr>
<tr>
<td>Bell/BCE Inc.</td>
<td>USNY108</td>
<td>Linkedin</td>
<td>USNY083</td>
</tr>
</tbody>
</table>

<sup>4</sup> “USNA” denotes a US firm listed on the NASDAQ stock exchange. “USNY” denotes a US firm listed on the New York Stock Exchange.
<table>
<thead>
<tr>
<th>Company Name</th>
<th>NASDAQ Symbol</th>
<th>Company Name</th>
<th>NASDAQ Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big Fish Games/Glu Mobile</td>
<td>USNA003</td>
<td>M&amp;T Bank</td>
<td>USNY040</td>
</tr>
<tr>
<td>Booking.com/Priceline Group</td>
<td>USNA025</td>
<td>Mantech international</td>
<td>USNA056</td>
</tr>
<tr>
<td>Booz Allen Hamilton</td>
<td>USNY075</td>
<td>MasterCard</td>
<td>USNY081</td>
</tr>
<tr>
<td>Boston Scientific</td>
<td>USNY003</td>
<td>McDonald's</td>
<td>USNY054</td>
</tr>
<tr>
<td>CafePress Inc./EZprint</td>
<td>USNA027</td>
<td>Medtronic</td>
<td>USNY002</td>
</tr>
<tr>
<td>Capital One Financial Corp</td>
<td>USNY061</td>
<td>Microsoft</td>
<td>USNA064</td>
</tr>
<tr>
<td>Charles Schwab Corp</td>
<td>USNY064</td>
<td>Monsanto</td>
<td>USNY076</td>
</tr>
<tr>
<td>Chase Bank (JP Morgan)</td>
<td>USNY049</td>
<td>Moody's</td>
<td>USNY074</td>
</tr>
<tr>
<td>Chevron</td>
<td>USNY050</td>
<td>Nasdaq Inc</td>
<td>USNA050</td>
</tr>
<tr>
<td>Citigroup</td>
<td>USNY035</td>
<td>Natural Grocers</td>
<td>USNY006</td>
</tr>
<tr>
<td>CNN/Time Warner</td>
<td>USNY001</td>
<td>Neustar Inc.</td>
<td>USNY010</td>
</tr>
<tr>
<td>Coca Cola (enterprises)</td>
<td>USNY077</td>
<td>New York Times Co</td>
<td>USNY042</td>
</tr>
<tr>
<td>Comcast Corporation</td>
<td>USNA023</td>
<td>Nokia</td>
<td>USNY043</td>
</tr>
<tr>
<td>Comerica</td>
<td>USNY037</td>
<td>Northrop Grumman</td>
<td>USNY066</td>
</tr>
<tr>
<td>Ebay</td>
<td>USNA002</td>
<td>Nvidia</td>
<td>USNA033</td>
</tr>
<tr>
<td>Electronic Arts Inc.</td>
<td>USNA017</td>
<td>Oceaneering</td>
<td>USNY051</td>
</tr>
<tr>
<td>Epsilon/Alliance Data</td>
<td>USNY072</td>
<td>Orange SA</td>
<td>USNY100</td>
</tr>
<tr>
<td>People's United Financials</td>
<td>USNA039</td>
<td>Starbucks</td>
<td>USNA007</td>
</tr>
<tr>
<td>PNC Financial Services</td>
<td>USNY031</td>
<td>StarWood Resorts</td>
<td>USNY021</td>
</tr>
<tr>
<td>Rackspace Hosting Inc.</td>
<td>USNY027</td>
<td>SunTrust Banks</td>
<td>USNY055</td>
</tr>
<tr>
<td>Regions Financial</td>
<td>USNY036</td>
<td>Supervalu Inc.</td>
<td>USNY020</td>
</tr>
<tr>
<td>Royal Bank of Scotland</td>
<td>USNY104</td>
<td>Symantec</td>
<td>USNA053</td>
</tr>
<tr>
<td>Sabre Corp</td>
<td>USNA012</td>
<td>Synovus Financial Corp.</td>
<td>USNY041</td>
</tr>
<tr>
<td>Sally Beauty Holdings Inc.</td>
<td>USNY007</td>
<td>Target</td>
<td>USNY070</td>
</tr>
<tr>
<td>Sears Holding Corp.</td>
<td>USNA004</td>
<td>The GEO Group</td>
<td>USNY079</td>
</tr>
<tr>
<td>Company Name</td>
<td>Ticker</td>
<td>Company Name</td>
<td>Ticker</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------</td>
<td>------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Shinhan Financial group</td>
<td>USNY101</td>
<td>T-Mobile</td>
<td>USNA058</td>
</tr>
<tr>
<td>Shutterfly Inc.</td>
<td>USNA030</td>
<td>Toronto-Dominion Bank</td>
<td>USNY109</td>
</tr>
<tr>
<td>Sony</td>
<td>USNY110</td>
<td>Twitter</td>
<td>USNY009</td>
</tr>
<tr>
<td>St. Jude Medical Inc.</td>
<td>USNY004</td>
<td>Ubiquiti Networks Inc</td>
<td>USNA011</td>
</tr>
<tr>
<td>Staples</td>
<td>USNA024</td>
<td>UMB Financial Corp.</td>
<td>USNA040</td>
</tr>
<tr>
<td>Umpqua Holdings Corp</td>
<td>USNA042</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Union Bankshares Corp</td>
<td>USNA041</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UPS</td>
<td>USNY017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>US Bancorp.</td>
<td>USNY026</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Walmart</td>
<td>USNY015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web.com</td>
<td>USNA014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wells Fargo</td>
<td>USNY032</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viator/Tripadvisor</td>
<td>USNA021</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VISA</td>
<td>USNY082</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vodafone Group PLC</td>
<td>USNA101</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo!</td>
<td>USNA001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zappos.com/Amazon</td>
<td>USNA059</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zions Bancorporation</td>
<td>USNA036</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Unique Firms</strong></td>
<td><strong>115</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Appendix B: Specific subsamples

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Code</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>Virus/Malware</td>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
<td>45</td>
</tr>
<tr>
<td>Website alteration/defacement</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>Database</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>DDoS</td>
<td>6</td>
<td>68</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Market Cap (Smillion)</th>
<th>Code</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mega Cap (≥200,000)</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>Large Cap (≥10,000&lt;200,000)</td>
<td>2</td>
<td>121</td>
</tr>
<tr>
<td>Mid Cap (≥2,000&lt;10,000)</td>
<td>3</td>
<td>32</td>
</tr>
<tr>
<td>Small Cap (≥50&lt;2000)</td>
<td>4</td>
<td>18</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Motivation to Attack</th>
<th>Code</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Crime</td>
<td>1</td>
<td>110</td>
</tr>
<tr>
<td>Hacktivism</td>
<td>2</td>
<td>68</td>
</tr>
<tr>
<td>Cyber Espionage</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry</th>
<th>Code</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet &amp; E-commerce</td>
<td>1</td>
<td>23</td>
</tr>
<tr>
<td>Software</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>Retail</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Tourism, Food &amp; Hospitality</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>Technology</td>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>Business services</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Transportation</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Finance</td>
<td>8</td>
<td>67</td>
</tr>
<tr>
<td>Telecom</td>
<td>9</td>
<td>13</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Media</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>News</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>Utility</td>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>Real estate</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>
Appendix C: General subsamples

<table>
<thead>
<tr>
<th>Industry</th>
<th>Code</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technological Firms (1,2,5,11)</td>
<td>1</td>
<td>66</td>
</tr>
<tr>
<td>Traditional Firms (2,3,4,6,7,8,9,10,12,13,14)</td>
<td>2</td>
<td>123</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Market Cap ($million)</th>
<th>Code</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large/Mega Cap (≥10,000&gt;200,000) (1,2)</td>
<td>1</td>
<td>139</td>
</tr>
<tr>
<td>Small/Mid Cap (≥50&lt;10,000) (3,4)</td>
<td>2</td>
<td>50</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Motivation to Attack</th>
<th>Code</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Gain (1)</td>
<td>1</td>
<td>110</td>
</tr>
<tr>
<td>Political Expression (2,3)</td>
<td>2</td>
<td>79</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Code</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion Attack (1,2,5)</td>
<td>1</td>
<td>67</td>
</tr>
<tr>
<td>Inaccessibility Attack (4,6)</td>
<td>2</td>
<td>77</td>
</tr>
<tr>
<td>Other Attacks (3)</td>
<td>0</td>
<td>45</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>189</strong></td>
</tr>
</tbody>
</table>

5 All numbers in parentheses refer to the previous, specific subsample groups, merged into these general subsamples.
Appendix D: Industry coding

<table>
<thead>
<tr>
<th>Industry Name</th>
<th>Industry Abbreviation</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business services</td>
<td>SECBUSSER</td>
<td>3</td>
</tr>
<tr>
<td>Finance</td>
<td>SECFIN</td>
<td>67</td>
</tr>
<tr>
<td>Internet &amp; E-commerce</td>
<td>SECINTEC</td>
<td>23</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>SECMAN</td>
<td>10</td>
</tr>
<tr>
<td>Media</td>
<td>SECMDA</td>
<td>2</td>
</tr>
<tr>
<td>News</td>
<td>SECNWS</td>
<td>1</td>
</tr>
<tr>
<td>Real estate</td>
<td>SECRLEST</td>
<td>1</td>
</tr>
<tr>
<td>Retail</td>
<td>SECTAIL</td>
<td>12</td>
</tr>
<tr>
<td>Software</td>
<td>SECSOFTW</td>
<td>19</td>
</tr>
<tr>
<td>Technology</td>
<td>SECTECH</td>
<td>22</td>
</tr>
<tr>
<td>Telecom</td>
<td>SECTELCM</td>
<td>13</td>
</tr>
<tr>
<td>Tourism, Food &amp; Hospitality</td>
<td>SECTOFOHO</td>
<td>12</td>
</tr>
<tr>
<td>Transportation</td>
<td>SECTRANSP</td>
<td>2</td>
</tr>
<tr>
<td>Utility</td>
<td>SECUTLT</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>189</td>
</tr>
</tbody>
</table>

Appendix E: Normality tests after outlier removal (30-day window)

<table>
<thead>
<tr>
<th></th>
<th>Kolmogorov-Smirnov</th>
<th>Shapiro-Wilk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Statistic</td>
<td>df</td>
</tr>
<tr>
<td>All Firms Before</td>
<td>0,095</td>
<td>172</td>
</tr>
<tr>
<td>All Firms After</td>
<td>0,112</td>
<td>172</td>
</tr>
<tr>
<td>Inaccessability Before</td>
<td>0,120</td>
<td>69</td>
</tr>
<tr>
<td>Inaccessability After</td>
<td>0,171</td>
<td>69</td>
</tr>
<tr>
<td>Intrusion Before</td>
<td>0,096</td>
<td>61</td>
</tr>
<tr>
<td>Intrusion After</td>
<td>0,091</td>
<td>61</td>
</tr>
<tr>
<td>Large/Mega Before</td>
<td>0,103</td>
<td>125</td>
</tr>
<tr>
<td>Large/Mega After</td>
<td>0,124</td>
<td>125</td>
</tr>
<tr>
<td>Small/Medium Before</td>
<td>0,135</td>
<td>48</td>
</tr>
<tr>
<td>Small/Medium After</td>
<td>0,168</td>
<td>48</td>
</tr>
<tr>
<td>Personal Gain Before</td>
<td>0,075</td>
<td>98</td>
</tr>
<tr>
<td>Personal Gain After</td>
<td>0,075</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Kolmogorov-Smirnov</td>
<td>Shapiro-Wilk</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>Statistic</td>
<td>df</td>
</tr>
<tr>
<td>All Firms Before</td>
<td>0.112</td>
<td>178</td>
</tr>
<tr>
<td>All Firms After</td>
<td>0.116</td>
<td>178</td>
</tr>
<tr>
<td>Inaccessability Before</td>
<td>0.126</td>
<td>69</td>
</tr>
<tr>
<td>Inaccessability After</td>
<td>0.167</td>
<td>69</td>
</tr>
<tr>
<td>Intrusion Before</td>
<td>0.137</td>
<td>66</td>
</tr>
</tbody>
</table>

* This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Appendix F: Normality tests after outlier removal (5-day window)
<table>
<thead>
<tr>
<th>Category</th>
<th>Before</th>
<th>After</th>
<th>Before T</th>
<th>After T</th>
<th>Before 5</th>
<th>After 5</th>
<th>Before 30</th>
<th>After 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion After</td>
<td>0.135</td>
<td>0.004</td>
<td>0.867</td>
<td>0.000</td>
<td>0.135</td>
<td>0.004</td>
<td>0.867</td>
<td>0.000</td>
</tr>
<tr>
<td>Large/Mega Before</td>
<td>0.116</td>
<td>0.000</td>
<td>0.923</td>
<td>0.000</td>
<td>0.116</td>
<td>0.000</td>
<td>0.923</td>
<td>0.000</td>
</tr>
<tr>
<td>Large/Mega After</td>
<td>0.126</td>
<td>0.000</td>
<td>0.925</td>
<td>0.000</td>
<td>0.126</td>
<td>0.000</td>
<td>0.925</td>
<td>0.000</td>
</tr>
<tr>
<td>Small/Medium Before</td>
<td>0.113</td>
<td>0.171</td>
<td>0.923</td>
<td>0.004</td>
<td>0.113</td>
<td>0.171</td>
<td>0.923</td>
<td>0.004</td>
</tr>
<tr>
<td>Small/Medium After</td>
<td>0.221</td>
<td>0.000</td>
<td>0.833</td>
<td>0.000</td>
<td>0.221</td>
<td>0.000</td>
<td>0.833</td>
<td>0.000</td>
</tr>
<tr>
<td>Personal Gain Before</td>
<td>0.103</td>
<td>0.008</td>
<td>0.942</td>
<td>0.000</td>
<td>0.103</td>
<td>0.008</td>
<td>0.942</td>
<td>0.000</td>
</tr>
<tr>
<td>Personal Gain After</td>
<td>0.133</td>
<td>0.000</td>
<td>0.878</td>
<td>0.000</td>
<td>0.133</td>
<td>0.000</td>
<td>0.878</td>
<td>0.000</td>
</tr>
<tr>
<td>Political Expression Before</td>
<td>0.113</td>
<td>0.027</td>
<td>0.932</td>
<td>0.001</td>
<td>0.113</td>
<td>0.027</td>
<td>0.932</td>
<td>0.001</td>
</tr>
<tr>
<td>Political Expression After</td>
<td>0.105</td>
<td>0.055</td>
<td>0.956</td>
<td>0.016</td>
<td>0.105</td>
<td>0.055</td>
<td>0.956</td>
<td>0.016</td>
</tr>
<tr>
<td>Technology Before</td>
<td>0.080</td>
<td>0.200</td>
<td>0.948</td>
<td>0.010</td>
<td>0.080</td>
<td>0.200</td>
<td>0.948</td>
<td>0.010</td>
</tr>
<tr>
<td>Technology After</td>
<td>0.163</td>
<td>0.000</td>
<td>0.906</td>
<td>0.000</td>
<td>0.163</td>
<td>0.000</td>
<td>0.906</td>
<td>0.000</td>
</tr>
<tr>
<td>Traditional Before</td>
<td>0.105</td>
<td>0.004</td>
<td>0.933</td>
<td>0.000</td>
<td>0.105</td>
<td>0.004</td>
<td>0.933</td>
<td>0.000</td>
</tr>
<tr>
<td>Traditional After</td>
<td>0.093</td>
<td>0.019</td>
<td>0.962</td>
<td>0.003</td>
<td>0.093</td>
<td>0.019</td>
<td>0.962</td>
<td>0.003</td>
</tr>
<tr>
<td>Diff Technology</td>
<td>0.071</td>
<td>0.200</td>
<td>0.983</td>
<td>0.535</td>
<td>0.071</td>
<td>0.200</td>
<td>0.983</td>
<td>0.535</td>
</tr>
<tr>
<td>Diff Traditional</td>
<td>0.037</td>
<td>0.200</td>
<td>0.994</td>
<td>0.922</td>
<td>0.037</td>
<td>0.200</td>
<td>0.994</td>
<td>0.922</td>
</tr>
<tr>
<td>Diff Small/Medium</td>
<td>0.084</td>
<td>0.200</td>
<td>0.976</td>
<td>0.422</td>
<td>0.084</td>
<td>0.200</td>
<td>0.976</td>
<td>0.422</td>
</tr>
<tr>
<td>Diff Large/Mega</td>
<td>0.066</td>
<td>0.200</td>
<td>0.983</td>
<td>0.094</td>
<td>0.066</td>
<td>0.200</td>
<td>0.983</td>
<td>0.094</td>
</tr>
<tr>
<td>Diff Personal Gain</td>
<td>0.087</td>
<td>0.045</td>
<td>0.951</td>
<td>0.001</td>
<td>0.087</td>
<td>0.045</td>
<td>0.951</td>
<td>0.001</td>
</tr>
<tr>
<td>Diff Political Expression</td>
<td>0.078</td>
<td>0.200</td>
<td>0.982</td>
<td>0.392</td>
<td>0.078</td>
<td>0.200</td>
<td>0.982</td>
<td>0.392</td>
</tr>
<tr>
<td>Diff 30 Days (All firms)</td>
<td>0.109</td>
<td>0.000</td>
<td>0.950</td>
<td>0.000</td>
<td>0.109</td>
<td>0.000</td>
<td>0.950</td>
<td>0.000</td>
</tr>
<tr>
<td>Diff 5 Days (All firms)</td>
<td>0.097</td>
<td>0.000</td>
<td>0.959</td>
<td>0.000</td>
<td>0.097</td>
<td>0.000</td>
<td>0.959</td>
<td>0.000</td>
</tr>
<tr>
<td>Diff Inaccessibility</td>
<td>0.070</td>
<td>0.200</td>
<td>0.988</td>
<td>0.721</td>
<td>0.070</td>
<td>0.200</td>
<td>0.988</td>
<td>0.721</td>
</tr>
<tr>
<td>Diff Intrusion</td>
<td>0.132</td>
<td>0.006</td>
<td>0.936</td>
<td>0.002</td>
<td>0.132</td>
<td>0.006</td>
<td>0.936</td>
<td>0.002</td>
</tr>
<tr>
<td>Diff Traditional (Even sample sizes)</td>
<td>0.054</td>
<td>0.200</td>
<td>0.994</td>
<td>0.961</td>
<td>0.054</td>
<td>0.200</td>
<td>0.994</td>
<td>0.961</td>
</tr>
<tr>
<td>Diff Small/Medium (Even sample sizes)</td>
<td>0.153</td>
<td>0.006</td>
<td>0.815</td>
<td>0.000</td>
<td>0.153</td>
<td>0.006</td>
<td>0.815</td>
<td>0.000</td>
</tr>
<tr>
<td>Diff Large/Mega (Even sample sizes)</td>
<td>0.097</td>
<td>0.170</td>
<td>0.977</td>
<td>0.230</td>
<td>0.097</td>
<td>0.170</td>
<td>0.977</td>
<td>0.230</td>
</tr>
</tbody>
</table>

* This is a lower bound of the true significance.

a. Lilliefors Significance Correction
Appendix G: Examples of distribution graphs, before & after removing outliers

Histogram 1 - Tech industry (30 days, before outlier)

Histogram 2 – Tech industry (30 days, after outlier)

Histogram 3 - All firms (5 days, before outlier)

Histogram 4 – All firms (5 days, before outlier)
Appendix H: Example of Normal Q-Q plots

**Note:** Graphs and plots provided in the appendix are just examples picked out from a very large quantity of similar figures. Arranging the appendix this way is a conscious choice taken in order to decrease the extensive amount of pages that would be needed if figures from all subsamples were to be included. Subsample specific figures or exact event dates will happily be furnished upon any reader’s request. For such inquires we refer to our e-mail addresses listed below:

Erik Collin: erikcollin89@gmail.com

Gustav Juntti: juntti26@gmail.com