9-2023

Do hacker groups pose a risk to organizations? Study on financial institutions targeted by hacktivists

Mikko Samuli NIEMELAE
Singapore Management University, msniemelae.2018@dba.smu.edu.sg

Citation

NIEMELAE, Mikko Samuli. Do hacker groups pose a risk to organizations? Study on financial institutions targeted by hacktivists. (2023). 1-72.
Available at: https://ink.library.smu.edu.sg/etd_coll/539

DO HACKER GROUPS POSE A RISK TO ORGANIZATIONS? STUDY ON FINANCIAL INSTITUTIONS TARGETED BY HACKTIVISTS

MIKKO SAMULI NIEMELAE

SINGAPORE MANAGEMENT UNIVERSITY

2023

Do Hacker Groups Pose a Risk to Organizations?

Study on Financial Institutions Targeted by Hacktivists

Mikko Samuli Niemelae

Submitted to Lee Kong Chian School of Business

in partial fulfilment of the requirements

for the Degree of Doctor of Business Administration (Innovation)

Dissertation committee

Ang Ser Keng (Chair)

Principal lecturer of Finance

Singapore Management University

Jussi Keppo (Co-supervisor)

Professor of NUS Business School

National University of Singapore

Say Gui Deng

Assistant Professor of Strategic Management

Singapore Management University

SINGAPORE MANAGEMENT UNIVERSITY

2023

I hereby declare that this dissertation is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in this dissertation.

This dissertation has also not been submitted for any degree in any university previously.

Mikko Samuli Niemelae

September 5 2023

Do Hacker Groups Pose a Risk to Organizations?

Study on Financial Institutions Targeted by Hacktivists

Mikko Samuli Niemelae

Abstract

In the digital era, technological progress has been shadowed by an escalation in cybersecurity threats, notably impacting the financial sector. This research critically examines the influence of hacktivist campaigns—particularly those led by groups like Anonymous—on the cyber exposure of financial services firms listed on the NYSE. Employing Synthetic Controls and analyzing 22 treated firms, the study found that such campaigns significantly enhance the target institutions' deep and dark web exposure, with an average increase of 65% per annum in the subsequent two years from the campaign initiation. Crucially, smaller firms display a heightened susceptibility to these campaigns. The outcomes suggest that financial entities, especially smaller ones, should be proactive, adopting strategies like improved cybersecurity measures, continuous deep and dark web monitoring, employee training, and possibly cyber insurance. Additionally, maintaining ethical business practices and prioritizing transparency can potentially reduce the risk of becoming a hacktivist target.

Table of Contents

List of Tables

List of Figures

Acknowledgement page

I would like to thank my committee Dr. Ser Keng Ang, Assistant Prof. Gui Deng Say & Prof Jussi Keppo for extensive and extended support through this process!

Introduction

The digitalization of crime has created a landscape rife with both opportunities and dangers. Globally, the exponential growth of digital and cybercrime is a cause for grave concern (Driessen & Gustafson, 2020). The darkweb, a nebulous portion of the internet known for facilitating anonymous criminal activity, tops this list of concerns (Branwen, 2021).

This progression is paralleled by the rise of hacktivism, a complex and multifaceted form of activism that blends hacking techniques with various motivations. These motivations can be categorized based on political, economic, social, technological, environmental, and legal aspects (Nurmi & Niemelä, 2018). This shift from traditional activism to a form that utilizes cyber tools for orchestrated operations has been led by groups like Anonymous, targeting institutions that represent injustice or exploitation (Zannettou et al., 2018).

Scholarly opinions diverge on the impact of hacktivism, with some claiming it as consequential while others regard it as a minor nuisance. This debate remains unresolved, as previous studies often omit the level of exposure, a critical aspect when assessing the threat. This research addresses this oversight by directly measuring exposure.

This study builds on the understanding of hacktivism as a politically motivated use of technical expertise, such as coding, to address network infrastructure for political or social change (Milan, 2015). As hacktivism is a highly contested concept with different objectives and tactics, Milan's exploration of hacktivism as a radical media practice provides valuable insight into the phenomenon, including hacktivists' tactics, their approach to institutions and social norms, and the challenges they face.

Titled "Do Hacktivists Pose a Threat to NYSE-Listed Financial Services Companies?", this study investigates the symbolic threats posed by hacktivist activities towards NYSE-listed financial services firms. Hacktivists often target financial institutions not for financial gains, but to protest and raise awareness against perceived systemic injustices and exploitations that such firms might represent. While these institutions are also attractive to cybercriminals for monetary reasons, it's essential to distinguish between hacktivist intentions and those of profit-driven cybercriminals (Van der Werf, 2020). For this study, data has been compiled from various sources, including hacktivist campaign motives, target lists, and leaked passwords and documents from the darkweb and deepweb. Datasets from COMPUSTAT and Sustainalytics, detailing companies' ESG and unmanaged risks, further complement the analysis.

The sample consists of NYSE-listed financial services firms targeted by hacktivists (treatment group) and those not targeted (control group). The study employs several statistical techniques, including Propensity Score Matching (PSM), Synthetic Controls, Difference-in-Differences (Dif-in-Dif), and regression analysis, to conduct a comprehensive analysis.

This research advances under the premise of three distinct hypotheses. Hypothesis 1 contends that the cyber exposure of financial institutions intensifies in the aftermath of a hacktivist campaign's announcement. This anticipated surge in exposure can be attributed to the peculiar dynamics of hacktivism. Unlike traditional hackers who operate in shadows, hacktivists operate in the limelight, broadcasting their campaigns to maximize their impact. This public revelation inadvertently attracts other malicious actors, leveraging the initial exposure and further augmenting the risk profile of the targeted entity. Moreover, when these institutions find their data or references on the deep and dark web, their vulnerability to subsequent threats multiplies, drawing them deeper into the quagmire of cyber risks.

Building upon the intricate web of cybercrime, Hypothesis 2 postulates that the repercussions of hacktivist campaigns on cyber exposure are particularly pronounced for financial institutions whose cleartext passwords—obtained from previous leaks—are accessible on the darkweb or deepweb. These unencrypted passwords not only represent vulnerabilities but also potent gateways for unauthorized intrusions, magnifying the cyber risk landscape.

Diving deeper into the firm dynamics, Hypothesis 3 explores the potential difference in cyber exposure between smaller and larger firms in the aftermath of hacktivist campaigns. The underpinning rationale is rooted in the conventional belief that the size of a firm, and by extension its resources and cybersecurity infrastructure, could influence its vulnerability to such external cyber threats.

Scholarly opinions diverge on the impact of hacktivism, with some claiming it as consequential while others regard it as a minor nuisance (Mansfield-Devine, 2011). This debate remains unresolved, as previous studies often omit the level of exposure, a critical aspect when assessing the threat. This research addresses this oversight by directly measuring exposure (Anonymous, 2011).

Literature Review and Hypotheses Development

Cyber exposure in the dark web

The deep and dark web, characterized by illicit activities, are recognized for hosting hacktivist campaigns targeting businesses (Holt & Bossler, 2016). The anonymity and encrypted features of the dark web, prominently facilitated by Tor (The Onion Router), make it a primary choice for users seeking online privacy against traffic analysis and network surveillance. This widespread demand for privacy, coupled with Tor's encryption, renders it a dominant protocol for dark web activities, making it a favorable environment for coordinating hacktivist campaigns and cyber-attacks.

Liu, Wang, & Wesselman (2018) highlight the dual use of exposed information within the dark web for cyber threat intelligence, emphasizing its potential defensive and offensive applications. Hackers can leverage leaked target-specific information to craft precise phishing messages, incorporating details such as personal hobbies, credit card numbers, or internal organizational communications. Rajivan & Gonzalez (2018) found that attackers, equipped with exposed data, could increase their phishing success rates by tailoring deceptive messages. Their research underscored the importance of understanding how such exposure amplifies threats and vulnerabilities.

Hacktivism, traditional activism and traditional hacking

Hacktivism and Activism Hacktivism, a portmanteau of "hacking" and "activism," is a form of protest that involves using hacking techniques to advance political or social objectives (Manion & Goodrum, 2000). Similar to traditional activism, hacktivism aims to affect change, draw attention to a cause, or influence policy. However, unlike traditional activism, hacktivism leverages the power of digital tools and the internet to achieve these goals (Samuel, 2004). Both hacktivism and traditional activism stem from a desire to disrupt the status quo and challenge existing power structures (Della Porta & Diani, 2009; Dreyfus, 2014). They share a common philosophical underpinning grounded in advocating for change, often in response to perceived social, political, or economic injustices (Nurmi, 2018). However, the methods employed by hacktivists and traditional activists differ significantly. While traditional activists might organize protests, sit-ins, or strikes to voice their concerns, hacktivists may use techniques such as website defacement, Distributed Denial of Service (DDoS) attacks, or data leaks to disrupt their targets and draw attention to their cause (Sauter, 2014; Manion & Goodrum, 2000).

Milan (2015) further explores the complexity of hacktivism as a radical media practice, highlighting the politically motivated use of technical expertise. She notes that hacktivism is a highly contested concept, encompassing different objectives and tactics that are not always compatible. For instance, while some hacktivists might engage in digital protests through website defacements or information leaks, others might resort to more aggressive measures such as cyberattacks on infrastructure. These diverse approaches arise from differing motivations, ideologies, and definitions of success within the hacktivist community. Her insights illuminate the multifaceted nature of hacktivist tactics and their approach to institutions and social norms, emphasizing the challenges faced in terms of repression, accountability, and impact..

Though their methods may differ, both forms of activism aim to bring about change by drawing attention to issues, influencing public opinion, and exerting pressure on individuals, organizations, or governments to act (Earl & Kimport, 2011; Denning, 2001). Stefania Milan's exploration into hacktivism identifies significant challenges faced by this form of activism, adding to its complexity (Milan, 2015). Increasing repression and surveillance, accountability to the broader society, and the assessment of real impact define the nuanced dynamics of hacktivism. As this method gains prominence, the issues of transparency and potential coerciveness add to the debate surrounding its efficacy and societal role. Milan's insights highlight the multifaceted nature of hacktivism, examining the balance between its radical intentions and the practical implications of its tactics, thus enriching our understanding of this modern form of protest.

In contrast to traditional hacking campaigns typically seek personal gain, espionage, or corporate benefits (Shackelford, 2013), and they often employ more precise and sophisticated methods leading to more significant direct losses. Effectiveness may vary based on its definition, and traditional hacking might be seen as more effective in terms of immediate financial or operational damage. In the realm of cyber theft, attackers often hoard the acquired information for personal benefit, either using it directly or monetizing it in underground markets. Conversely, hacktivists are more inclined to share or publicize the data to further their cause, rather than for direct monetary profit.

The demarcation between hacktivism and traditional hacking, while evident in their core motivations, can become convoluted in practice. Indeed, both involve unauthorized intrusions into digital systems, yet their primary objectives diverge. Hacktivists, fueled by advocacy, aim to spotlight certain issues or causes, whereas traditional hackers may be motivated by personal gain, espionage, or corporate benefits (Shackelford, 2013).

An insightful perspective to adopt is viewing hacktivism as a process with two interconnected stages. The first stage involves the initial exposure by hacktivists. Here, the primary intention is not personal enrichment but amplification of firm vulnerabilities and drawing attention to their chosen cause. Once this information is in the open, a second stage can ensue, where the exposed data becomes a ripe target for traditional hackers. Devoid of advocacy motivations, these entities seize the exposed data to further their specific objectives, which can lead to significant financial or reputational damage to the targeted entity.

Although some campaigns might bear characteristics of both hacktivism and traditional hacking, understanding their foundational differences is paramount. Differentiating the deep/dark web's utility in hacktivist activities from the essence of hacktivism is crucial. The consequences of breaches, in terms of data exposure and financial ramifications (Hammouchi, Cherqi, Mezzour, Ghogho, & El Koutbi, 2019), emphasize the varied effectiveness of hacktivist campaigns compared to traditional hacking endeavors.

The effect of hacking campaign announcements by hacktivists on a firm’s cyber exposure

Hacktivist campaigns have increasingly garnered attention for their political or social underpinning, aiming to disrupt targeted businesses and spotlight specific causes (Holt & Bossler, 2016). Two notable examples include the attack on MasterCard and Visa in retaliation for their decision to stop serving WikiLeaks (Greenberg, 2010) and the hack on the U.S. Sentencing Commission website, which Anonymous claimed was a response to the prosecution and subsequent suicide of Aaron Swartz (Whittaker, 2013; Davies, 2013). Such campaigns have empirically evidenced effectiveness, leading targeted entities to face consequences like financial loss, reputational impairment, and escalated risks on the deep and dark web (Zetter, 2015; Mansfield-Devine, 2011).The deep and dark web are acknowledged platforms for illicit activities, including cyberattacks, and a mere mention on these platforms can dramatically heighten a company's risk profile (Chen, 2011; Rajamanickam et. al. 2021).

Hacktivist campaigns, as described by Nurmi, J., & Niemelä, M. S. (2018) are driven by political or ideological objectives, and they strive for societal change or highlighting specific issues. They may release exposure information rather than stealing digital assets or blocking access to websites. This public-facing nature and symbolic message can attract more attention than traditional hacking attacks, and their impacts can ripple beyond the immediate victims, shaping public opinion and generating wider societal consequences. However, it is important to clarify that while hacktivist campaigns may organize on the deep/dark web, the exposure information becomes public, aligning with their ideological incentives and symbolic actions. It is essential to recognize, however, that hackers are inherently opportunistic. Their initial attacks may not be discriminative, targeting any perceived vulnerability. Only after gaining access might they evaluate the nature of the firm and determine the value of the information they have accessed.

In the context of this study, the hacktivist group Anonymous has garnered significant attention for its high-profile campaigns, which often target governments, corporations, and other powerful entities. These campaigns are characterized by a unique operational approach that leverages the collective power of anonymous online actors to enact change (Olson, 2013; Sauter, 2014).

Anonymous campaigns typically begin with the publication of a manifesto, which outlines the group's objectives and grievances (Fuchs, 2013). This manifesto is often disseminated across social media platforms and other digital channels to reach a broad audience. The aim is to resonate with like-minded individuals and encourage them to participate in the planned hacktivist actions (Uitermark, 2017).

Once potential participants have been recruited, Anonymous proceeds to the next phase, often referred to as "weaponization." This involves providing participants with the tools and instructions necessary to carry out coordinated cyberattacks (Coleman, 2014). The collective nature of Anonymous's operations means that the more people the manifesto resonates with, the larger the scale of the resultant cyberattack will be (Milan, 2015).

While the public face of Anonymous campaigns often emphasizes social or political change, their actions have deeper implications. By mobilizing volunteers to engage in cyberattacks, including data breaches and password leaks, Anonymous can leverage the dark web as a platform for exposing sensitive information. This not only resonates with the hacktivist goal of challenging power structures but also amplifies the target's risk of cyber exposure. For financial institutions, a breach of security could mean a substantial increase in their deep web and dark web exposure, making them more vulnerable to subsequent attacks and financial risks. Such deliberate strategies used by Anonymous can be seen as serving as a catalyst, amplifying the repercussions of the initial attack and providing 'resources' and 'opportunity structures' for broader impact. This continuous potential for damage contrasts sharply with traditional activism, which tends to be limited to a particular protest event. Drawing from the relational approaches to collective action, as highlighted by Diani and McAdam (2003), hacktivism, as practiced by groups like Anonymous, goes beyond the immediate act, creating conditions conducive for subsequent actions by other entities in the digital realm. This study, therefore, seeks to explore the evolving relationship between hacktivism and cyber exposure in this broader context.

Successful cyberattacks have been known to influence firm performance in terms of sales growth, risk management, and stock prices (Kamiya et al., 2020). Beyond direct consequences for the firm, a successful hacktivist campaign often translates into broader political implications. As the Stuxnet case illustrated, media narratives shape public perception and can influence political discourse. Similarly, Anonymous strategically publicizes their actions, through formal media channels or the dark web, to ensure their message gains traction and reaches a wider audience (Dunn Cavelty, 2018; Sauter, 2013).

Taken together, I propose that

> **Hypothesis 1: The cyber exposure of targeted financial institutions rises after the announcement of a hacktivism campaign.**

The moderating effect of clear text passwords on the relationship between hacktivism campaign and cyber exposure

Recent studies have illuminated an intricate web of specialized cybercrime. Unethical developers produce malware, which is subsequently employed to target potential victims, primarily via methods like email attachments. When these attacks are successful, vital data, including cleartext passwords, is sold on underground platforms such as the Genesis Market.

Cleartext, or unencrypted passwords, function as more than mere vulnerabilities; they act as powerful entry points for cybercriminals seeking unauthorized access (Verizon, 2017; Das, 2014; Bonneau, 2012). These compromised credentials frequently resurface for resale on platforms within the Tor network, like the Database Market, enhancing the future risk landscape for financial institutions (Nurmi et al., 2023).

Prior research has underscored leaked passwords and existing vulnerabilities as pivotal elements in successful cyberattacks (Verizon, 2017; Das, 2014; Bonneau, 2012). The vulnerability inherent in cleartext passwords is underscored by their directness; they bypass the need for attackers to exploit software vulnerabilities or employ complex methods. Their availability on the deep or dark web magnifies the risk, offering attackers a tactical edge.

The sequence of cyber incidents, especially those that capitalize on exposed passwords, can span a considerable period—beginning from when a vulnerability is detected to its eventual resolution, which some reports suggest can extend up to six months (Tndel et al., 2015). The financial and reputational repercussions can amplify the efficacy of a successful hacktivist campaign.

This threat can be further dissected through the lens of information asymmetry—a knowledge imbalance between entities like an organization and a hacker (Cavusoglu et al., 2019). When cleartext passwords are available on platforms like the dark or deep web, the advantage often held by institutions diminishes, favoring cybercriminals.

It's essential to clarify that while cleartext passwords act as vulnerabilities, their presence on the dark or deep web contributes to an institution's cyber exposure, although they don't constitute the entirety of it.

Though vulnerabilities, even direct ones like exposed passwords, don't guarantee exploitation, reduced information asymmetry enables cybercriminals to evaluate potential targets better, hone their strategies, and concentrate on the most exploitable weaknesses. Observations have confirmed that when cybercriminals access such critical information, they often utilize these vulnerabilities for complex cyberattacks (Verizon, 2017; Das, 2014; Bonneau, 2012).

Therefore, I hypothesize that:

> **Hypothesis 2: The effect of hacktivism campaigns on the cyber exposure is stronger for financial institutions with some cleartext passwords available in the dark web or deep web than for those institutions that did not have leaked passwords.**

The moderating effect of firm size on the relationship between hacktivism campaign and cyber exposure

The size of a firm can often influence its allocation of cybersecurity resources, and by extension, its resilience against cyber threats (Romanosky, Hoffman, & Acquisti, 2014; Chatterjee, Sarker, & Valacich, 2015). The employee count provides an insight into this vulnerability; a larger workforce might lead to more potential intrusion points, which can be further magnified by human errors, susceptibility to social engineering, and operational lapses.

On one hand, smaller companies, due to their limited resources, might face challenges in instituting strong cybersecurity defenses, potentially increasing their vulnerability during hacktivist campaigns (Gordon & Loeb, 2002; Romanosky et al., 2014). Empirical studies have also shown that cyberattacks can impact smaller businesses more severely (Johnson, 2015; Ponemon, 2018; Setiawan et al., 2019). Conversely, larger corporations, while being perceived as more lucrative targets due to the abundance of data, generally possess advanced security infrastructures. Such infrastructures can deter the likelihood of a successful cyberattack (Cavusoglu, Mishra, & Raghunathan, 2019).

However, it's worth noting that from a hacktivist perspective, while larger entities offer tempting targets, their robust security systems might discourage attempts of infiltration. In contrast, smaller firms, despite their perceived lesser value, might become more appealing due to their perceived vulnerabilities, especially for hacktivists working with limited resources.

Given these considerations:

> **Hypothesis 3: The effect of hacktivism campaigns on a firm’s cyber exposure is greater for smaller Firms.**

Research Methodologies and Sample

3.1 Data Collection & variable description

Cyber Exposure Data: To gather data on cyber exposure, scraping techniques were employed across both the dark web and deep web. Using advanced web crawling and spidering tools, specific types of unintended information exposures were systematically detected and documented. This specifically pertained to instances where companies inadvertently leaked sensitive information, including but not limited to passwords, proprietary data, and personal identifiers, in these online realms. This data aggregation resulted in a comprehensive database that illuminated the technical vulnerabilities and the patterns of unintended information release among the targeted companies.

Compustat Financial Data: The financial information related to the companies under investigation was primarily extracted from Compustat. Known for its broad spectrum of financial, market, and statistical data, Compustat was a comprehensive source for this study. In situations where Compustat had missing data, specifically relating to employee count, Macrotrends.net, a well-established and reliable financial data platform, was used to fill the gaps.

Data Verification through Yahoo Finance: To confirm the listing of the investigated companies on the New York Stock Exchange (NYSE), listing identifiers were procured from Yahoo Finance. This additional step was crucial in validating the inclusion of these companies in this study.

Definition of Variables

Exposure: Exposure is operationalized as the presence of a company's domain name within data sources from the dark web or deep web. Specifically, it captures instances where company-associated information is identified within these digital territories, irrespective of the nature of the information. The data encompass various exposures, such as the discovery of encrypted or plain text passwords, mentions of the company's domain in hacker forums or discussions, instances where sensitive company-specific documents or source codes are found, or scenarios where the company's domain name appears without a clear surrounding context. This variable serves to provide a consistent and unbiased representation of a company's cyber exposure in the dark and deep web, treating all companies with the same systematic approach.

Leaked: The dummy variable "Leaked" is a more specific component of the broader "Exposure" category. It pinpoints occurrences where unencrypted, readable passwords related to the company are discovered within the dark web or deep web realms. The presence of such unencrypted passwords suggests a unique type of cybersecurity threat that the company is facing. It's noteworthy that while "Leaked" is correlated with the overall "Exposure" measurement, each metric encapsulates different facets of a company's total cyber susceptibility. Essentially, the "Leaked" variable monitors the occasions when a company's unprotected information becomes accessible in potentially detrimental digital zones. The value is 1 if company had leaked passwords within 2 quarters (180 days) to 6 quarters (545 days) before the announced campaign starting date and 0 otherwise.

Size: The "Size" variable is the natural logarithm of the number of employees.

After: A dummy variable that is 1 after the campaign's start date.

Return on assets (ROA): A financial ratio that measures the profitability of an organization relative to its total assets.

Treated: A dummy variable for companies that have been the target of hacktivist attacks, with a value of 1 if the company was the target and 0 otherwise (control company).

3.2 Sample Creation

The sample includes NYSE-listed financial services firms, which have been subjected to hacktivist attack campaigns. The rationale behind the selection of these firms is the frequency of their encounters with cyberattacks, substantiating their relevance to this study. The remaining NYSE-listed financial services firms not included in the hacktivist attack campaigns are used to form a control group.

The subject pool for this study consists of NYSE-listed financial services firms that have been victims of hacktivist attack campaigns. These firms were selected due to the regularity of their run-ins with cyberattacks, thus demonstrating their significance to this study. A control group was subsequently formed using the remaining NYSE-listed financial services firms not involved in the hacktivist attack campaigns. Yahoo Finance assisted in identifying these firms, leading to a complete list of 1,223 firms, inclusive of those originally identified as targets of hacktivist campaigns.

The collected tickers from Yahoo Finance were used to filter the COMPUSTAT database, selecting only companies whose industry format (INDFMT) was financial services (FS) and the years 2011, 2013, and 2015 preceding each attack campaign. This filtering resulted in the retention of 181 companies, one of which lacked data for 2011 as obtained from macrotrends.net and the company's 10-K report. The sample then consists of 159 control firms and 22 treated firms.

3.3 Variable Selection for Matching

In order to compare the treatment and control groups, this research selected two variables for matching: Return on Assets (ROA) and the logarithmically transformed count of employees, denoted as ln(EMP+1).

Return on Assets (ROA): ROA, calculated by dividing Income Before Extraordinary Items (IB) by Total Assets (AT) from COMPUSTAT, is a measure used to assess the efficiency at which a company's operational assets generate profits. Gordon, Loeb, & Sohail (2010) have pointed out its significance in the context of a firm's ability to invest in cybersecurity infrastructure. A firm with a higher ROA may have more resources available, which could be allocated to cybersecurity measures.

Logarithmically Transformed Employee Count ln(EMP+1): This variable serves as a proxy for a company's size, encompassing its infrastructure and workforce dimensions. Both the scale of a company and its ROA can influence its overall vulnerability, which hacktivists might weigh when selecting targets. In scenarios where the vulnerabilities—gauged by employee count and ROA—are comparable between firms, one might find itself in the crosshairs of hacktivist activities, while the other remains untouched. Such variations allow for a nuanced exploration via the Difference-in-Differences (DID) methodology. For data sourcing, when employee count details were not accessible from COMPUSTAT, Macrotrends.net was consulted as an alternate. If both sources proved unyielding, a linear estimation approach was employed. Of the 518 observations, 9 lacked employee count data: 5 of these were sourced from Macrotrends, while the remaining 4 were estimated.

Year and Industry Dummies: To account for unobserved year-specific effects, such as changes in the overall economic environment, and industry-specific variations, which might influence a firm's cyber exposure irrespective of its financial performance or size, year and industry dummies were incorporated into the analysis. These dummies ensure that the effect being measured is purely due to hacktivist activities and not influenced by external year or industry dynamics.

Matching based on these variables ensures that the groups are comparable, thereby allowing a systematic examination of the influence of hacktivist campaigns on the companies studied. This method aims to maintain the consistency and validity of the subsequent analyses.

Following the creation of the sample, the next step implemented was Synthetic Controls matching. This technique is beneficial when there's a limited number of treated units, and when these units might be subject to unobservable influences. The detailed results from this matching process are available in Appendix D. Initial observations after applying Propensity Score Matching (PSM) and Synthetic Controls matching suggest that results from the Synthetic Controls method are consistent, though the observed treatment effect appears to be more subdued than that from PSM. Detailed interpretations of these findings will be presented in the following sections.

There were three distinct periods during which firms were targeted by hacktivist attacks. For each of these periods, procedures were carried out for each group of treated firms and all control firms. The quarterly cyber exposure data was combined with financial data from COMPUSTAT. Subsequently, control firms were matched with treated firms. The final sample comprised 1,056 firm-quarter observations, divided between 44 firms (22 treated and 22 control).

3.4 Main model

Upon matching ROA and employee count between the treatment and control groups, the sample preparation phase is concluded. This ensures a robust foundation for the succeeding analytical steps in this research.

The primary model for this research is formulated as follows:

$$log(Exposure_{i,t}) = \alpha + \beta \cdot (Treated_i \cdot After_t) + Size_i + ROA_i + \gamma_j + \delta_y + \varepsilon_{i,t} \qquad (1)$$

Where:

- $log(Exposure_{i,t})$ represents the risk exposure level in deep and dark web.
- $Treated_i$ designates the treatment variable indicating if company i was the target of a hacking campaign.
- $After_t$ denotes the time variable marking whether the quarter is post the campaign event.
- α is a constant.
- β signifies the treatment effect, which is the main variable of interest.

- $Size_i$ is the logarithmic representation of the employee count in the year preceding the hacking campaign.
- ROA_i stands for the return-on-assets, represented in 100%, from the year prior to the hacking campaign.
- γ_j is the fixed effect for industry j.
- δ_y denotes the fixed effect for year y.
- $\varepsilon_{i,t}$ is the error term.

The NAICS labels extracted from COMPUSTAT data, coupled with cyber exposure data years, were used to implement industry and year fixed effects. The study incorporated seven unique six-digit NAICS codes and cyber exposure data spanning from 2009 to 2019.

It's worth highlighting that the dataset features a significantly smaller number of treated companies compared to control entities. To rectify this disproportion, the synthetic control method, as outlined by Abadie & Gardeazabal (2003) and subsequent works by Abadie, Diamond, & Hainmueller (2010, 2011, 2014), is applied for matching purposes. Specifically, for each treated company, a synthetic counterpart is constructed by evaluating pre-campaign exposure levels juxtaposed against company size and fiscal performance. This assists in determining the suitable weights to be attributed to each control entity. This strategy is instrumental in minimizing selection bias and ensuring the parallel trends assumption inherent in the difference-in-differences analysis. For every matched pair, the synthetic entity within the control group is designated the time variable After, mirroring its treated equivalent.

Observations in this research's dataset are perceived as independent, given the assurance against contamination between the treatment and control firms, the chronological autonomy of observations, and the accounting for industry and annual specific shocks. The process of selection, deeply anchored in lucid criteria related to firms targeted by Anonymous juxtaposed with their untargeted counterparts sharing identical industry characteristics, solidifies the robustness of the ensuing comparisons.

A comprehensive list of variables, accompanied by descriptive statistics among the 44 firms in the matched sample, is systematically presented in Table 1.

Table 1. Descriptive statistics - SC (N = 1,056)

The table provides summary statistics for the key variables used in hypothesis tests. The sample period comprises the twelve quarters preceding and following each of the three campaign dates in 2012, 2014, and 2016. There are a total of 1,056 observations during the period. The variable definitions are contained in Chapter 3.

	Mean	*St. Dev.*	*Min*	*Pctl(25)*	*Median*	*Pctl(75)*	*Max*
After	0.500	0.500	0.000	0.000	0.500	1.000	1.000
Treated	0.500	0.500	0.000	0.000	0.500	1.000	1.000
log(Exposure)	4.015	2.940	0.000	1.686	3.630	5.990	12.847

Size	3.678	1.212	0.700	2.760	3.557	4.413	5.580
ROA	1.540	2.758	-0.061	0.714	0.848	1.202	13.850
Leaked	0.909	0.288	0.000	1.000	1.000	1.000	1.000

Table 2. Correlation matrix of the variables – SC

The table illustrates the correlation between the variables used in hypothesis tests.

	After	*Treated*	*log(Exposure)*	*Size*	*ROA*	*Leaked*
After	1.000	0.000	0.389	0.000	0.000	0.000
Treated	0.000	1.000	0.123	0.000	0.003	-0.316
log(Exposure)	0.389	0.123	1.000	0.458	-0.055	0.293
Size	0.000	0.000	0.458	1.000	-0.220	0.244
ROA	0.000	0.003	-0.055	-0.220	1.000	0.000
Leaked	0.000	-0.316	0.293	0.244	0.000	1.000

Table 3. 12-Quarter comparative metrics after treatment: treated vs. control exposure – SC

The table compares the average exposure between treated and control groups in the 12 quarters following treatment.

	Treated	*Control*	*Difference*	*Absolute diff.*
Exposure	11,859	1,890	+ 527 %	9,969
Exposure (in log)	5.639	4.676	+ 21 %	0.963

Results

4.1 Hypothesis 1

The first hypothesis, “The cyber exposure of targeted financial institutions rises after the announcement of a hacktivism campaign,” is tested using the baseline model, and the results are presented in Table 4. These results suggest that the impact of a hacking campaign on a company’s risk exposure level in the deep and dark web is consistently significant and positive, as shown in columns (1) – (3). The campaign effect (Treatedi · Aftert) is reduced to 0.475 when additional control variables are included (column 3), but it remains substantial. This significance translates to treatment companies having an average of 52 more records of cyber exposure than the control group over 12 quarters, with the control group averaging 86 records. While the severity of each record is variable, ranging from potentially harmless to severely devastating, even a single record might suffice for a hacker to compromise the institution.

Table 4. Baseline model results

The table presents the results of the baseline model used to test the first hypothesis. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:		
		log(Exposure)	
	(1)	(2)	(3)
Treated		0.487***	0.493***
		(0.154)	(0.144)
After		-0.195	-0.106
		(0.203)	(0.190)
Size			0.757***
			(0.062)
ROA			-0.282*
			(0.148)
Treated*After	0.816***	0.475**	0.475**
	(0.141)	(0.217)	(0.203)
Constant	3.245***	2.876***	-0.020
Industry and Year FE	(0.434)	(0.441)	(0.484)
Observations	1,056	1,056	1,056
R^2	0.640	0.646	0.690
Adjusted R^2	0.635	0.639	0.684
Residual Std. Error	1.777 (df = 1038)	1.766 (df = 1036)	1.653 (df = 1034)

F Statistic	108.740*** (df = 17; 1038)	99.378*** (df = 19; 1036)	109.748*** (df = 21; 1034)
Note:			*p<0.1; **p<0.05; ***p<0.01

Figure 1 illustrates the risk exposure trends of the treatment and control companies, indicating that the parallel trends assumption holds. The overlap between the risk exposures of the two groups starts to diminish after the campaign date, and their trends completely diverge approximately three quarters later, with treated companies experiencing significantly higher exposures.

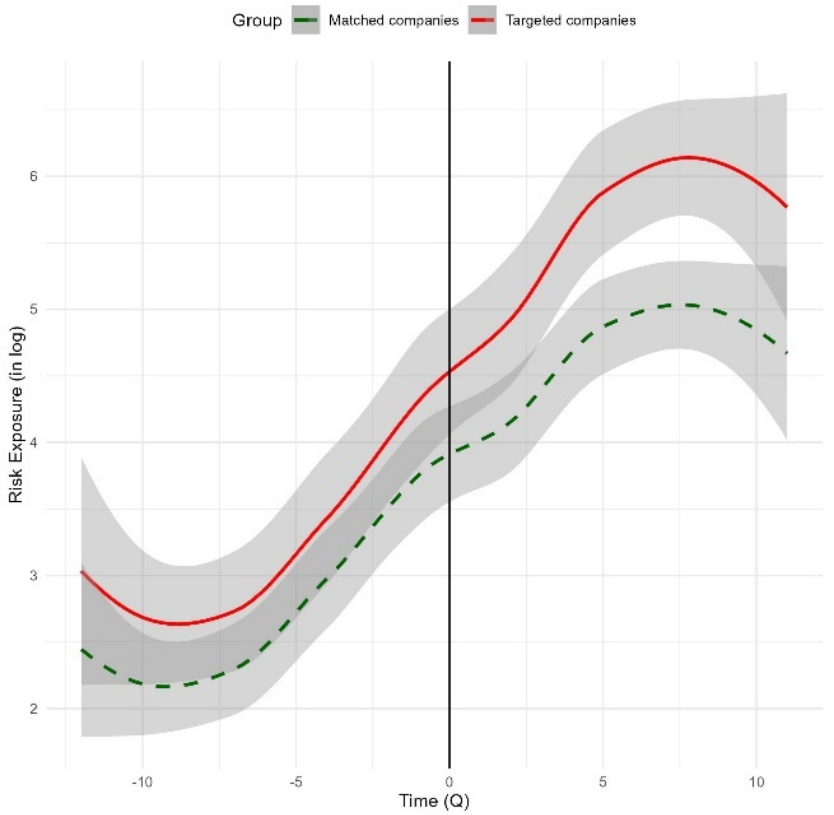


Figure 1: *Risk exposure trends of the treatment and control companies*

4.2 Hypothesis 2

The second hypothesis "The effect of hacktivism campaigns on the cyber exposure is stronger for financial institutions with some cleartext passwords available in the dark web or deep web than for those institutions that did not have leaked passwords" is tested by analyzing the role of cleartext password leaks prior to the campaign, considering the potential for hackers to begin preparations in advance. A binary variable (Leakedi) is created, which equals one if company i has a cleartext password leaked between 2 and 6 quarters before the campaign date, and zero otherwise. Results presented in Table 5 indicate that companies with cleartext password leaks before the campaign consistently and significantly experience higher risk exposure in the deep and dark web. Notably, this translates to an increase of 129 more records of cyber exposure for these companies compared to the control group over 12 quarters, with the control group averaging 86 records. A second interaction term is added in the model below.

$$log(Exposure_{i,t}) = \alpha + \beta_1 \cdot (Treated_i \cdot After_t) + \beta_2 \cdot (Treated_i \cdot After_t \cdot Leaked_i) + Size_i + ROA_i + \gamma_j + \delta_y + \varepsilon_{i,t} \qquad (2)$$

Table 5. The impact of cleartext passwords leaked prior to campaign

The table presents the results of the model used to test the second hypothesis. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:		
	log(Exposure)		
	(1)	(2)	(3)
Treated			0.819^{***}
			(0.146)
After			0.013
			(0.181)
Leaked	1.869^{***}		1.831^{***}
	(0.219)		(0.287)
Size	0.715^{***}	0.746^{***}	0.701^{***}
	(0.061)	(0.061)	(0.059)
ROA	0.048	-0.152	0.081
	(0.149)	(0.146)	(0.145)
Treated*After	1.160^{***}		-0.276
	(0.133)		(0.354)
Treated*After*Leaked		1.361^{***}	0.918^{**}
		(0.140)	(0.362)
Constant	-1.508^{***}	0.225	-2.023^{***}
Industry and Year FE	(0.511)	(0.469)	(0.544)
Observations	1,056	1,056	1,056
R^2	0.706	0.701	0.721
Adjusted R^2	0.701	0.695	0.714
Residual Std. Error	1.609 (df = 1035)	1.624 (df = 1036)	1.571 (df = 1032)
F Statistic	124.435^{***} (df = 20; 1035)	127.563^{***} (df = 19; 1036)	115.724^{***} (df = 23; 1032)
Note:			*p<0.1; **p<0.05; ***p<0.01

4.3 Hypothesis 3

The third hypothesis postulates, “The effect of hacktivism campaigns on a firm’s cyber exposure is greater for smaller firms.” To examine the influence of company size on the impact of hacking campaigns, three methodological tests were executed: the Bifurcation Analysis, Bootstrapping Test, and Three-Way-Interaction Analysis.

Bifurcation Analysis

In the conducted Bifurcation Analysis, the primary sample was divided into two distinct subsamples: small and large companies. This division was based on the median employee count of treated companies; those exceeding this median were categorized as large, while the rest were considered small. Synthetic counterparts for each of these subsamples were subsequently identified. By employing the main model, the analysis was systematically executed for both groups. Table 6 showcases the outcomes of this analysis and highlights a notable impact on smaller companies, which significantly outstrips the baseline model's implications evident in Table 4. Delving into the results of Table 6, small firms experienced an estimated 61.3% increase in log(Exposure) after the treatment. In contrast, their larger counterparts registered a 33.7% uptick. On the front of statistical significance, the difference-in-differences (DiD) estimate for small enterprises proves to be significant at the 5% threshold, reflecting a positive effect subsequent to the treatment. Contrarily, for the larger firms, the available data doesn't present convincing evidence of a substantial post-treatment influence. Upon juxtaposition, it's discernible that the DiD coefficient for small companies is both considerably more substantial and statistically relevant than that for their larger counterparts.

Table 6. The impact of company size

The table presents the results of the model used to test the third hypothesis. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:					
	log(Exposure)					
	Small companies (1) - (3)			Large companies (4) - (6)		
	(1)	(2)	(3)	(4)	(5)	(6)
Treated		0.362*	0.362*		0.613***	0.633***
		(0.189)	(0.185)		(0.210)	(0.208)
After		-0.168	0.200		0.691**	0.640**
		(0.242)	(0.255)		(0.301)	(0.307)
Size			0.726***			0.347**
			(0.189)			(0.148)
ROA			1.537***			-0.547***
			(0.422)			(0.170)
Treated*After	0.851***	0.613**	0.613**	1.057***	0.337	0.337
	(0.172)	(0.267)	(0.262)	(0.197)	(0.297)	(0.293)
Constant	2.551***	2.280***	-0.438	4.079***	3.892***	2.615**

Industry and Year FE	(0.467)	(0.478)	(0.781)	(0.722)	(0.729)	(1.098)
Observations	528	528	528	528	528	528
R^2	0.629	0.634	0.648	0.649	0.656	0.666
Adjusted R^2	0.618	0.621	0.634	0.640	0.646	0.655
Residual Std. Error	1.540 (df = 511)	1.533 (df = 509)	1.506 (df = 507)	1.722 (df = 514)	1.708 (df = 512)	1.685 (df = 510)
F Statistic	54.177*** (df = 16; 511)	48.887*** (df = 18; 509)	46.659*** (df = 20; 507)	73.143*** (df = 13; 514)	65.110*** (df = 15; 512)	59.916*** (df = 17; 510)
Note:						*p<0.1; **p<0.05; ***p<0.01

Bootstrapping Test

In the Bootstrapping Test, resampling was conducted on the subsamples of both small and large companies. This process was repeated a thousand times, during which the treatment effect difference was computed. The methodology employed to estimate the 95% confidence interval for this difference involved subtracting the treatment effects of larger firms from those of smaller ones. The graphical representation of this differential can be found in Figure 4, while Figures 2 and 3 provide detailed insights into the bootstrapped treatment effects for each respective subsample. Analyzing Figure 4, the confidence interval (CI) bounds are notable, indicating that the true variance in the coefficients from models 3 and 6 spans from -1.0758331 to 0.5008049. A critical observation is that zero is encompassed within this interval, suggesting an absence of compelling evidence to differentiate the coefficients from models 3 and 6. This insight brings to the fore the practical implications of the analysis: the bootstrapped confidence interval underscores an inherent uncertainty concerning the difference in the point estimate presented in Table 6.

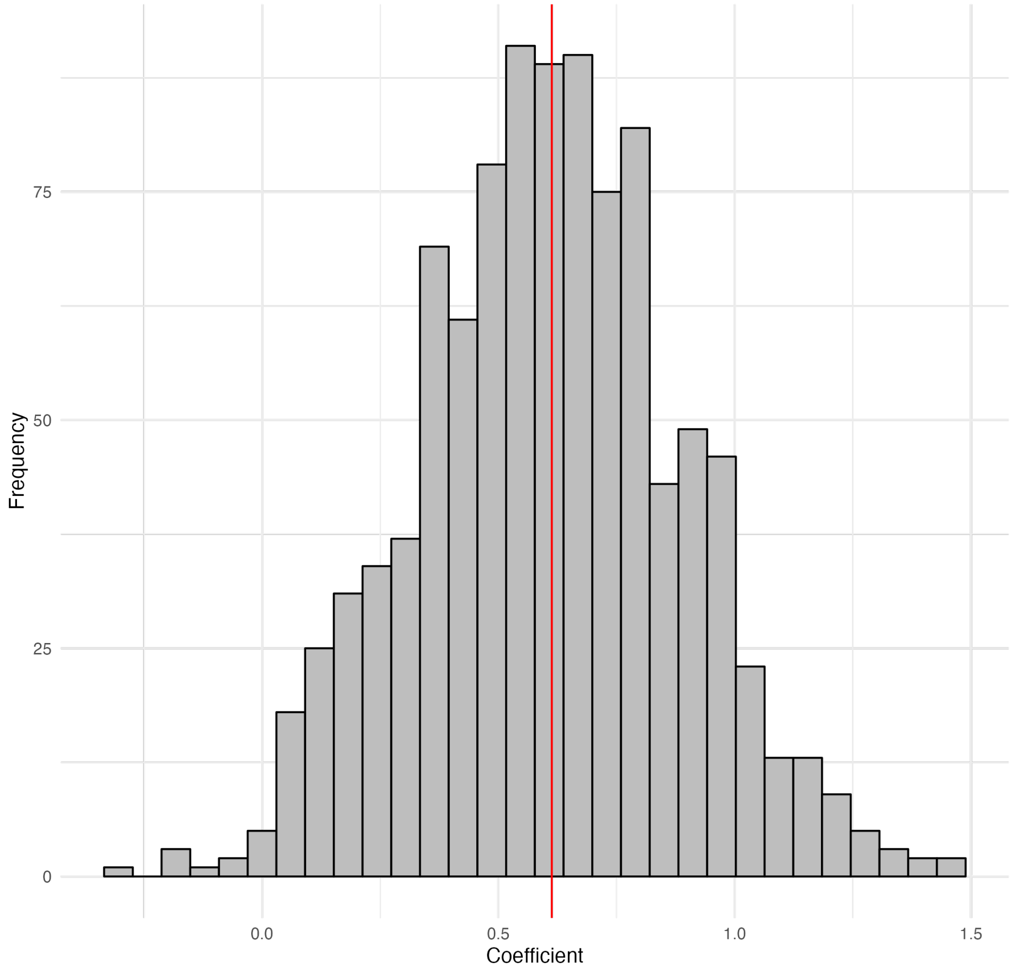


Figure 2: *Small companies (Treated*After: 0.613 – red line)*

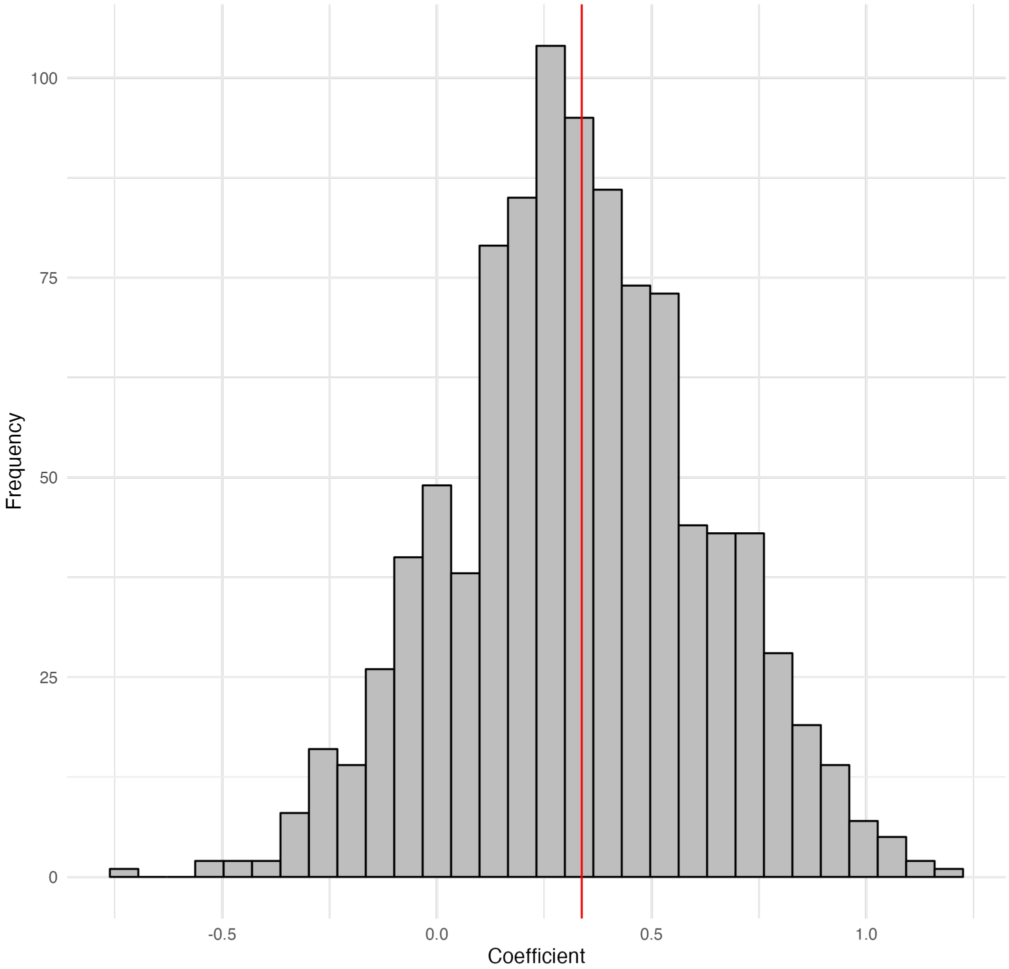


Figure 3: *Large companies (Treated*After: 0.337 – red line)*

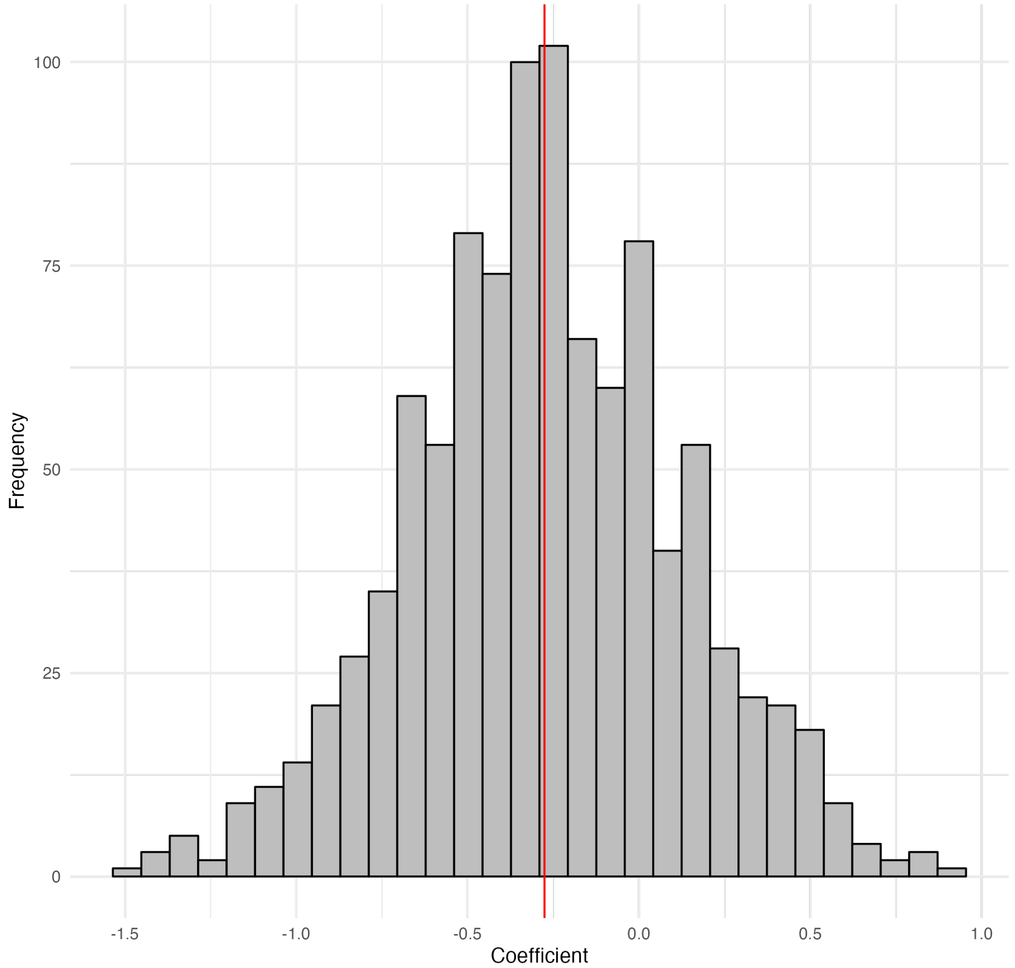


Figure 4: *Large companies DiD coeff - small companies DiD coeff. (-0.276 – red line)*

In Figure 4, the bootstrapping analysis is presented. The confidence interval (CI) bounds, based on the bootstrap results, show that the difference in the "TreatedAfter" coefficients between models 3 and 6 lies between -1.0758331 and 0.5008049 at a 95% confidence level. Since the interval includes zero, we cannot reject the null hypothesis that there's no difference between the "TreatedAfter" coefficients in models 3 and 6 at the 5% significance level. This means that the bootstrap analysis does not provide strong evidence of a significant difference between the coefficients in these two models. While the point estimate from Table 6 might suggest a difference, the bootstrapped confidence interval highlights the uncertainty around this estimate. In summary, even though the regression analysis in Table 6 might indicate some difference in the "Treated*After" coefficients of models 3 and 6, the bootstrapped confidence interval shows this difference is not statistically significant at the 5% level.

Three-Way-Interaction Analysis

This section details the analysis that incorporates a three-way interaction among the Treated, After, and Size variables in the main model, represented by model (3).

The equation for this model is:

$$log(Exposure_{i,t}) = \alpha + \beta_1 \cdot (Treated_i \cdot After_t) + \beta_2 \cdot (Treated_i \cdot After_t \cdot Size_i) + Size_i + ROA_i + \gamma_j + \delta_y + \varepsilon_{i,t}$$

In the three-way interaction analysis, the dependent variable utilized is the logarithmically transformed measure, log(Exposure). When interpreting the coefficients, specific attention is paid to the variables "Treated," "After," "Size," "ROA," "TreatedAfter," and "TreatedAfter*Size" as they hold particular significance in this model. Notably, the results indicate that while the size of a firm consistently impacts its exposure, the effect of hacktivist campaigns does not exhibit a consistent difference based on firm size. Furthermore, from a statistical perspective, the models demonstrate reasonable R-squared values. The F-statistics further validate the overall significance of the models.

Table 7. 3-way interaction between "Treated*After*Size"

The table presents the results of the model with three-way interaction that was used to test the third hypothesis. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:		
		log(Exposure)	
	(1)	(2)	(3)
Treated			0.493^{***}
			(0.144)
After			-0.102
			(0.190)
Size		0.734^{***}	0.732^{***}
		(0.067)	(0.067)
ROA	0.083	-0.262^{*}	-0.286^{*}
	(0.154)	(0.149)	(0.148)
Treated*After	-1.028^{***}	0.469	0.110
	(0.385)	(0.390)	(0.418)
Treated*After*Size	0.505^{***}	0.104	0.099
	(0.098)	(0.100)	(0.099)
Constant	3.052^{***}	0.377	0.060
Industry and Year FE	(0.445)	(0.488)	(0.491)
Observations	1,056	1,056	1,056
R^2	0.650	0.686	0.691
Adjusted R^2	0.643	0.680	0.684

Residual Std. Error	1.756 (df = 1036)	1.664 (df = 1035)	1.653 (df = 1033)
F Statistic	101.165^{***} (df = 19; 1036)	113.017^{***} (df = 20; 1035)	104.804^{***} (df = 22; 1033)
Note:			*p<0.1; **p<0.05; ***p<0.01

Synthesis of H3 Test Findings

The combined influence of a hacktivist campaign and company size offers mixed results. The evidence does not consistently affirm that company size determines the hacktivist campaign's impact magnitude.

Robustness testing

Quantifying the shifts in cyber exposure of financial institutions post a hacktivist campaign demands rigor in methodological approach and analytical scrutiny. At the heart of such an investigation is the quintessential need to ensure that the control group is representative, effectively mirroring the treated firms, so as to draw reliable inferences. In light of this, and acknowledging the complexity inherent in the nature of firms, the Propensity Score Matching (PSM) technique was employed. This methodological choice stemmed from its potential to neutralize biases arising from observable characteristics and thereby buttressing the credibility of our causal deductions on the influence of hacktivist campaigns on cyber exposure.

In the sections that follow, the robustness of the study's findings will be assessed using several methodologies:

1. **Difference-in-differences models with propensity score matching**: An approach that seeks to substantiate the core findings by leveraging PSM to isolate the genuine effects of hacktivist campaigns.
2. **Placebo Tests**: Utilized to discern the validity of observed causal effects, ensuring that the connections made are not just coincidences or random occurrences.
3. **Sustainalytics Analysis**: A deeper exploration into the ESG dimensions to appreciate the broader governance context that firms operate in and its implications for cyber resilience.

Through these methods, the chapter aims to illuminate the strength, depth, and nuances of the research's primary outcomes.

5.1 Difference-in-differences models with propensity score matching

In a study centered on the quantification of changes in cyber exposure of financial institutions following a hacktivist campaign, ensuring that the selected control group closely resembles the treated firms is crucial for drawing valid inferences. Given the multifaceted nature of firms and the numerous underlying confounding factors that could affect their susceptibility to cyber threats, the Propensity Score Matching (PSM) technique was utilized. This method enabled the systematic selection of matches from a pool of 159 control firms for the 22 treated firms in the sample. By using PSM, observable characteristics between the treated and control firms were balanced, mitigating potential biases and strengthening the validity of causal inferences regarding the effect of hacktivist campaigns on cyber exposure.

In this section, the study replicates the difference-in-differences analyses leveraging an alternative matched sample grounded in propensity score matching. For each treated entity, a score is computed, representing the likelihood of a control company being targeted. This scoring is derived considering two primary variables: company size, as depicted by ($Size_i$), and the firm's financial performance, marked by ROA_i.

The methodology adopted is the one-to-one nearest neighbor matching, systematically pairing each treated company ($Treated_i$=1) with its corresponding control ($Treated_i$=0). Every pair's control entity receives the assignment of the " $After_t$ " time variable, mirroring that of its treated peer. Comprehensive statistics of the 44 firms in the propensity-score-matched sample are detailed in Table 8.

Table 11 and Table 12 highlight the core findings of Equations (1) and (2), respectively. Further, Table 13 elucidates the implications of company size, particularly within the cohort matched via propensity scores. Notably, these insights remain in harmony with the primary analysis executed with synthetic controls. However, an anomaly surfaces when examining Figure 1. The trajectories of the two groups begin to show variance preceding the campaign date. A comparative review of Figure 1 against Figure 5 accentuates a pivotal observation: the sample constituted through propensity scores doesn't uphold the parallel trends assumption as robustly or transparently as its synthetic controls counterpart.

Table 8. Descriptive statistics - PSM (N = 1,056)

The table provides summary statistics for the key variables used in hypothesis tests. The sample period comprises the twelve quarters preceding and following each of the three campaign dates in 2012, 2014, and 2016. There are a total of 1,056 observations during the period. The variable definitions are contained in Chapter 3.

	Mean	*St. Dev.*	*Min*	*Pctl(25)*	*Median*	*Pctl(75)*	*Max*
After	0.500	0.500	0.000	0.000	0.500	1.000	1.000
Treated	0.500	0.500	0.000	0.000	0.500	1.000	1.000
log(Exposure)	3.591	3.256	0.000	0.000	3.178	5.921	12.847
Size	3.776	1.191	0.501	3.123	3.799	4.430	5.700
ROA	1.610	2.823	-0.417	0.596	0.799	1.398	13.971
Leaked	0.705	0.456	0.000	0.000	1.000	1.000	1.000

Table 9. Correlation matrix of the variables - PSM

The table illustrates the correlation between the variables used in hypothesis tests.

	After	*Treated*	*log(Exposure)*	*Size*	*ROA*	*Leaked*
After	1.000	0.000	0.314	0.000	0.000	0.000
Treated	0.000	1.000	0.242	-0.082	-0.022	0.249

log(Exposure)	0.314	0.242	1.000	0.403	-0.161	0.567
Size	0.000	-0.082	0.403	1.000	-0.346	0.412
ROA	0.000	-0.022	-0.161	-0.346	1.000	-0.181
Leaked	0.000	0.249	0.567	0.412	-0.181	1.000

Table 10. 12-Quarter comparative metrics after treatment: treated vs. control exposure – PSM

The table compares the average exposure between treated and control groups in the 12 quarters following treatment.

	Treated	*Control*	*Difference*	*Absolute diff.*
Exposure	11859	3,014	+ 293 %	8,844
Exposure (in log)	5.639	3.588	+ 57 %	2.051

In Table 11. The coefficient of 0.955 for the "Treated*After" term in the Difference-in-Differences model indicates that after the intervention, the treated group experienced an approximately 159.6% higher Exposure compared to the control group, controlling for other variables in the model. This effect is statistically significant at the 1% level, suggesting strong evidence of a treatment effect.

Table 11. Baseline model results

The table presents the results of the baseline model used to test the first hypothesis. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:		
	log(Exposure)		
	(1)	(2)	(3)
Treated		1.899^{***}	1.950^{***}
		(0.220)	(0.212)
After		-0.785^{***}	-0.424^{*}
		(0.244)	(0.232)
Size			0.902^{***}
			(0.080)

ROA			-0.045
			(0.040)
Treated*After	1.754***	0.955***	0.955***
	(0.205)	(0.274)	(0.257)
Constant	2.339***	1.327**	-2.248***
Industry and Year FE	(0.568)	(0.545)	(0.608)
Observations	1,056	1,056	1,056
R^2	0.484	0.541	0.598
Adjusted R^2	0.474	0.531	0.588
Residual Std. Error	2.362 (df = 1034)	2.230 (df = 1032)	2.089 (df = 1030)
F Statistic	46.262*** (df = 21; 1034)	52.953*** (df = 23; 1032)	61.337*** (df = 25; 1030)
Note:			*p<0.1; **p<0.05; ***p<0.01

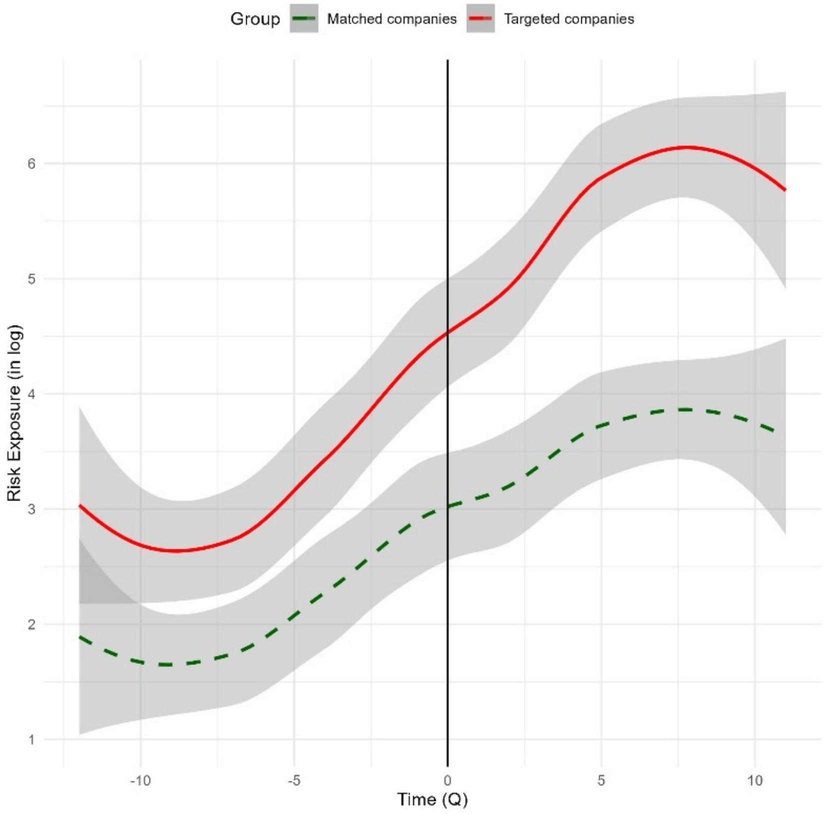


Figure 5: *Risk exposure trends of the treatment and control companies*

Table 12. The impact of cleartext passwords leaked prior to campaign

The table presents the results of the model used to test the second hypothesis. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:		
	log(Exposure)		
	(1)	(2)	(3)
Treated			0.597***
			(0.207)
After			-0.148
			(0.207)
Leaked	3.460***		3.017***
	(0.174)		(0.202)
Size	0.296***	0.896***	0.375***
	(0.077)	(0.081)	(0.079)
ROA	0.094**	-0.113***	0.098***
	(0.037)	(0.040)	(0.037)
Treated*After	1.171***		0.217
	(0.170)		(0.387)
Treated*After*Leaked		2.388***	0.902**
		(0.196)	(0.380)
Constant	-1.170**	-1.345**	-1.563***
Industry and Year FE	(0.535)	(0.613)	(0.545)
Observations	1,056	1,056	1,056
R^2	0.675	0.572	0.681
Adjusted R^2	0.667	0.563	0.672
Residual Std. Error	1.878 (df = 1031)	2.153 (df = 1032)	1.865 (df = 1028)
F Statistic	89.166*** (df = 24; 1031)	60.067*** (df = 23; 1032)	81.105*** (df = 27; 1028)
Note:			*p<0.1; **p<0.05; ***p<0.01

Table 13. The impact of company size

The table presents the results of the model used to test the third hypothesis. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:					
	log(Exposure)					
	Small companies (1) - (3)			Large companies (4) - (6)		
	(1)	(2)	(3)	(4)	(5)	(6)
Treated		2.128^{***}	2.799^{***}		1.850^{***}	2.337^{***}
		(0.251)	(0.331)		(0.319)	(0.326)
After		-0.505^{**}	-0.307		0.193	0.349
		(0.256)	(0.256)		(0.407)	(0.387)
Size			0.787^{***}			0.881^{***}
			(0.158)			(0.161)
ROA			0.079^{*}			-1.444^{***}
			(0.046)			(0.261)
Treated*After	1.871^{***}	1.055^{***}	1.055^{***}	2.224^{***}	0.854^{**}	0.854^{**}
	(0.232)	(0.293)	(0.285)	(0.303)	(0.420)	(0.396)
Constant	1.876^{***}	0.842^{*}	-2.062^{***}	3.332^{***}	2.450^{**}	-0.813
Industry and Year FE	(0.546)	(0.510)	(0.785)	(1.035)	(1.012)	(1.251)
Observations	528	528	528	528	528	528
R^2	0.567	0.642	0.661	0.445	0.483	0.540
Adjusted R^2	0.551	0.627	0.645	0.429	0.466	0.523
Residual Std. Error	1.844 (df = 508)	1.682 (df = 506)	1.640 (df = 504)	2.492 (df = 512)	2.410 (df = 510)	2.278 (df = 508)
F Statistic	35.082^{***} (df = 19; 508)	43.151^{***} (df = 21; 506)	42.667^{***} (df = 23; 504)	27.400^{***} (df = 15; 512)	28.035^{***} (df = 17; 510)	31.416^{***} (df = 19; 508)
Note:						*p<0.1; **p<0.05; ***p<0.01

5.2 Placebo Test

Placebo tests were utilized as a robustness check to corroborate the causal effects observed in the primary analysis. The purpose was to discern if the relationships between hacktivist campaigns and changes in cyber exposure were genuine or merely coincidental. Employing these tests fortifies the study's findings by ruling out spurious correlations, highlighting the distinct impact of hacktivist campaigns on financial institutions' cyber vulnerabilities.

The methodology for the placebo test, as proposed by Agarwal et al. (2015) and Keppo and Korte (2018), was meticulously followed. It entailed randomly shuffling the treatment and control companies within the Propensity Score Matching (PSM) matched sample, an exercise executed a thousand times. Figure 6 offers a histogram of the placebo difference-in-differences coefficients, similar in style to Table 11, Column 3. The authentic coefficient, denoted by a vertical red line, stands at 0.955. It's pivotal to note that the placebo coefficients are notably lower than the genuine coefficient, further underscoring the tangible influence of hacking campaigns on exposures in the deep and dark web.

To enrich the analysis, a supplementary model was incorporated. Instead of using a singular 'After' marker, a series of interaction terms were introduced, spanning from Treated * year2009 through to Treated * year2019. This approach refrains from presuming a consistent impact. Each term, which signifies the treatment group in a given year, captures the evolving effect over time. Hence, every term indicates the treatment effect for that particular year, keeping other model variables constant. By accounting for potential time-varying effects, this method imparts a more intricate understanding of the annual ramifications of hacking campaigns on deep and dark web exposures. The introduction of these year-specific terms significantly bolsters the reliability of the placebo test.

*Baseline - (1): log(Exposure) ~ Treated*After + Size + ROA + factor(naics) + factor(year)*

*Supplementary - (2): log(Exposure) ~ Treated*factor(year) + Size + ROA + factor(naics)*

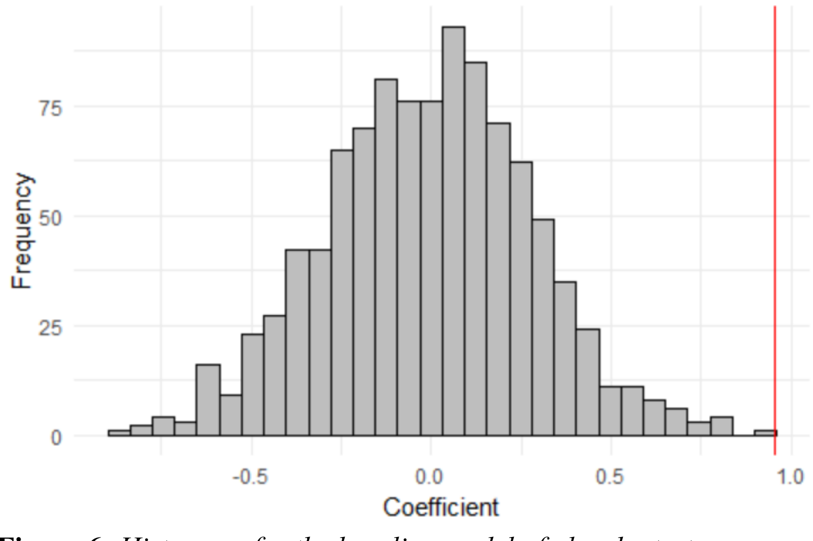


Figure 6: *Histogram for the baseline model of placebo test*

Interpreting the results from the supplementary model presents further validation of the primary findings. The coefficients, especially for the Treated variable, indicate a strong and consistent impact of hacktivist campaigns on cyber exposure across different time points. In both columns, the Treated coefficients are significant, underscoring the continued influence of such campaigns. Moreover, the varying impacts as the years progress suggest that the consequences of these campaigns can oscillate.

For instance, the coefficients for Treated*factor(year)2018 and Treated*factor(year)2019 are positive, while some earlier years showcase negative coefficients. This may allude to a progressive intensification of the impacts of hacktivist campaigns over time, warranting further investigation. The regularity and significance of the factor(year) terms further highlight how the annual consequences of hacking campaigns are pronounced and cannot be dismissed as mere fluctuations.

Interestingly, while the ‘After’ coefficient in the baseline model is negative and significant, its interaction with the ‘Treated’ variable is positive and highly significant. This affirms that while there might be a general decline in cyber exposure, entities targeted by hacktivist campaigns witnessed an upswing in their vulnerabilities post the campaign.

These findings collectively bolster the argument that the effects observed are not due to random chance or spurious relationships. The magnitude and direction of these coefficients, in conjunction with their statistical significance, lend strong support to the hypothesis that hacktivist campaigns indeed have a measurable and, at times, escalating impact on the cyber vulnerabilities of financial institutions. The supplementary model not only complements the primary analysis but also enriches the understanding by offering a granular view of the year-on-year effects.

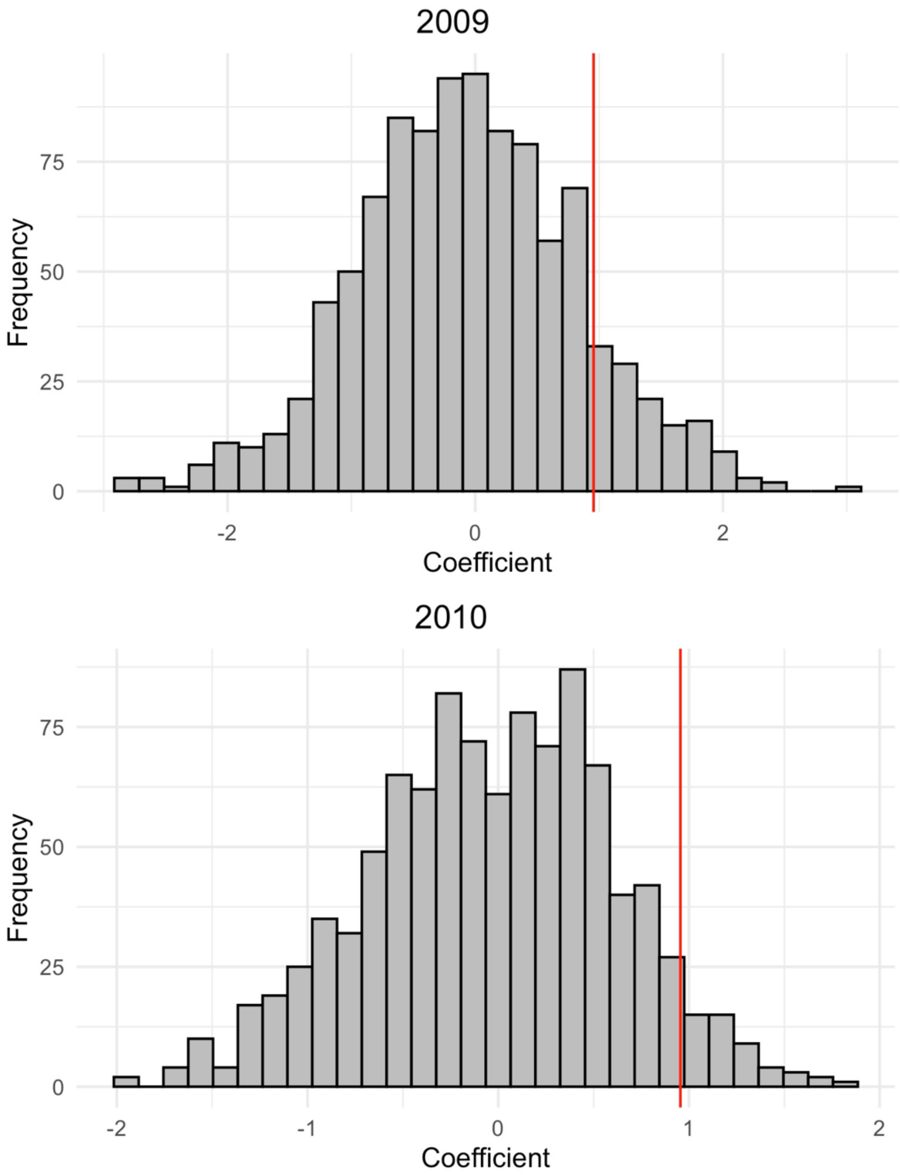
Table 14. Supplementary model results

The table presents the results of the placebo test using the supplementary model (Treated*year[2009-2019]). The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:	
	log(Exposure)	
	(1)	(2)
Treated	1.950***	2.497**
	(0.212)	(1.007)
After	-0.424*	
	(0.232)	
Size	0.902***	0.929***
	(0.080)	(0.079)
ROA	-0.045	-0.089**
	(0.040)	(0.041)
Treated*factor(year)2010		-1.333
		(1.100)
Treated*factor(year)2011		-1.088
		(1.095)

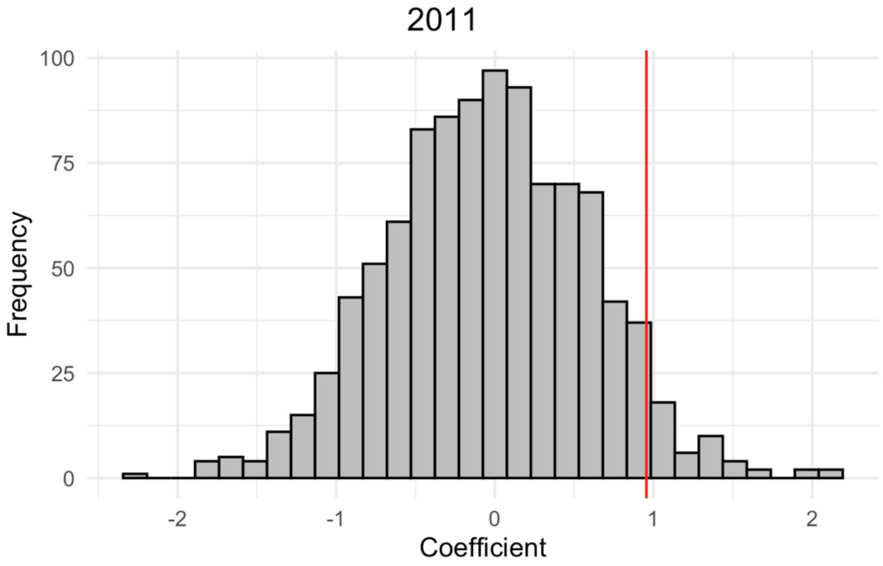
Treated*factor(year)2012		-1.452
		(1.091)
Treated*factor(year)2013		-0.036
		(1.068)
Treated*factor(year)2014		-0.410
		(1.040)
Treated*factor(year)2015		-0.375
		(1.047)
Treated*factor(year)2016		0.152
		(1.084)
Treated*factor(year)2017		0.252
		(1.088)
Treated*factor(year)2018		1.119
		(1.092)
Treated*factor(year)2019		0.340
		(1.119)
factor(year)2010	-1.082**	-0.416
	(0.551)	(0.778)
factor(year)2011	-0.464	0.083
	(0.548)	(0.774)
factor(year)2012	-0.979*	-0.235
	(0.548)	(0.771)
factor(year)2013	1.494***	1.574**
	(0.553)	(0.755)
factor(year)2014	0.207	0.487
	(0.530)	(0.733)
factor(year)2015	0.577	0.843
	(0.533)	(0.737)
factor(year)2016	3.133***	3.162***
	(0.550)	(0.761)
factor(year)2017	2.526***	2.542***
	(0.590)	(0.763)
factor(year)2018	4.972***	4.556***
	(0.593)	(0.766)
factor(year)2019	3.552***	3.526***
	(0.606)	(0.785)
Treated*After	0.955***	
	(0.257)	
Constant	-2.248***	-2.710***
	(0.608)	(0.773)
Observations	1,056	1,056
R^2	0.598	0.602
Adjusted R^2	0.588	0.589

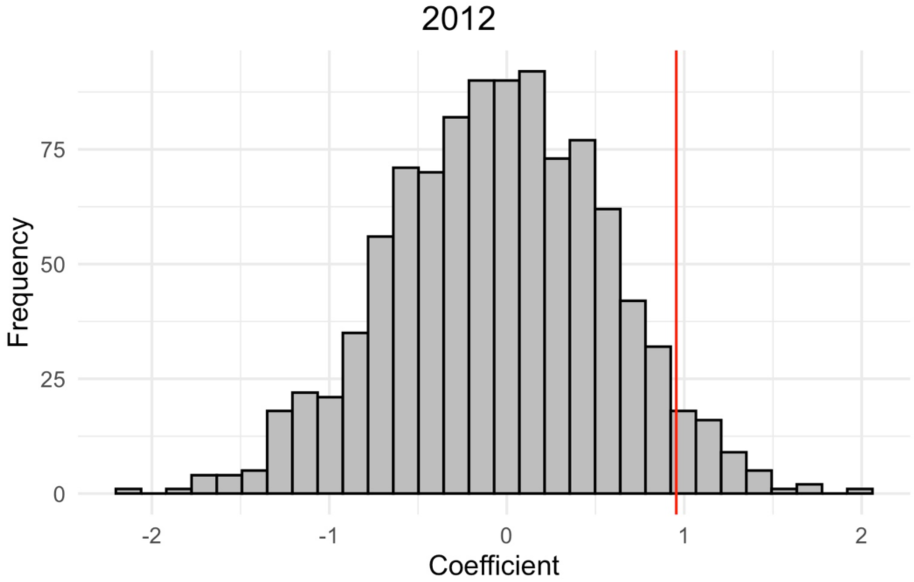
Residual Std. Error	2.089 (df = 1030)	2.087 (df = 1022)
F Statistic	61.337*** (df = 25; 1030)	46.865*** (df = 33; 1022)
Note:	*p<0.1; **p<0.05; ***p<0.01	

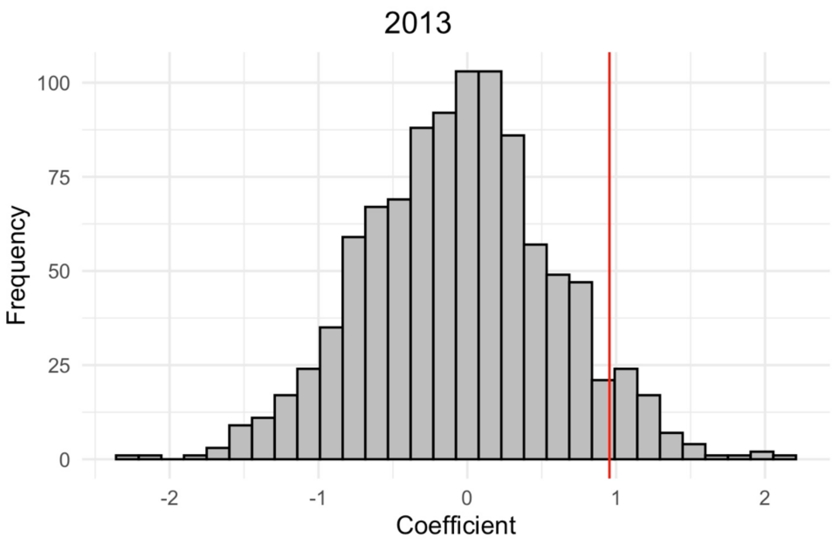


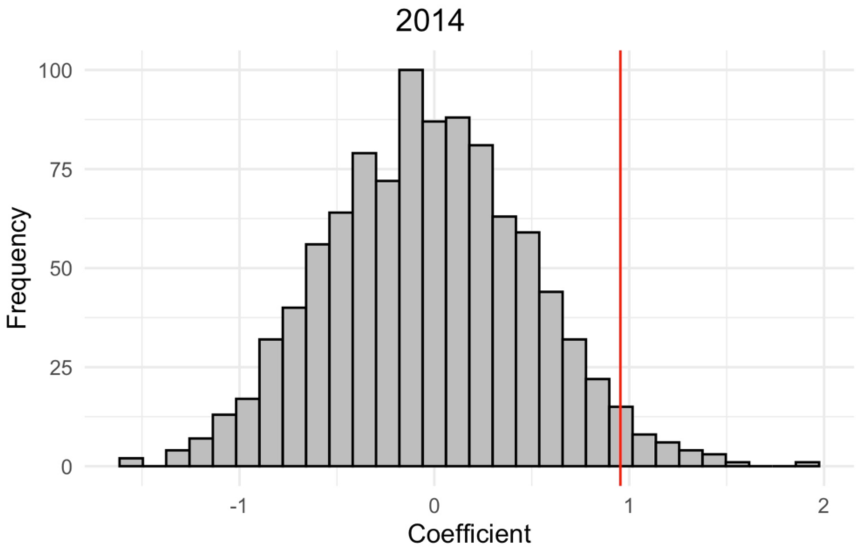
2009

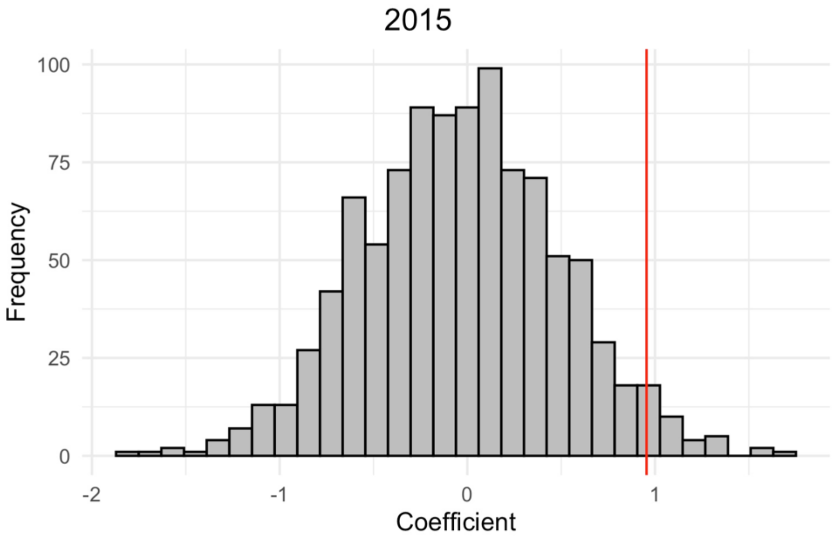
2010

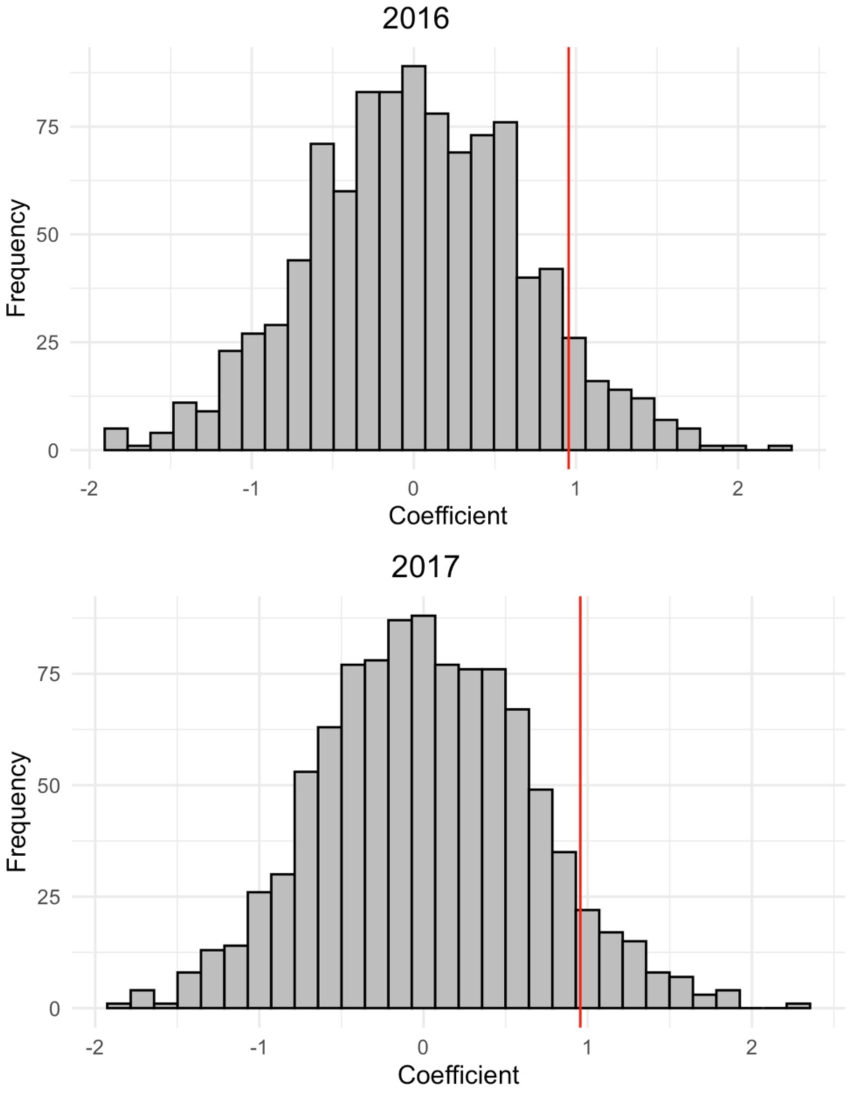

2011
Frequency
100
75
50
25
0
-2
-1
0
1
2
Coefficient


2012
Frequency
75
50
25
0
-2
-1
0
1
2
Coefficient


2013
Frequency
100
75
50
25
0
-2
-1
0
1
2
Coefficient


2014
Frequency
100
75
50
25
0
-1
0
1
2
Coefficient


2015
Frequency
100
75
50
25
0
-2
-1
0
1
Coefficient


2016
Frequency
75
50
25
0
-2
-1
0
1
2
Coefficient
2017
Frequency
75
50
25
0
-2
-1
0
1
2
Coefficient

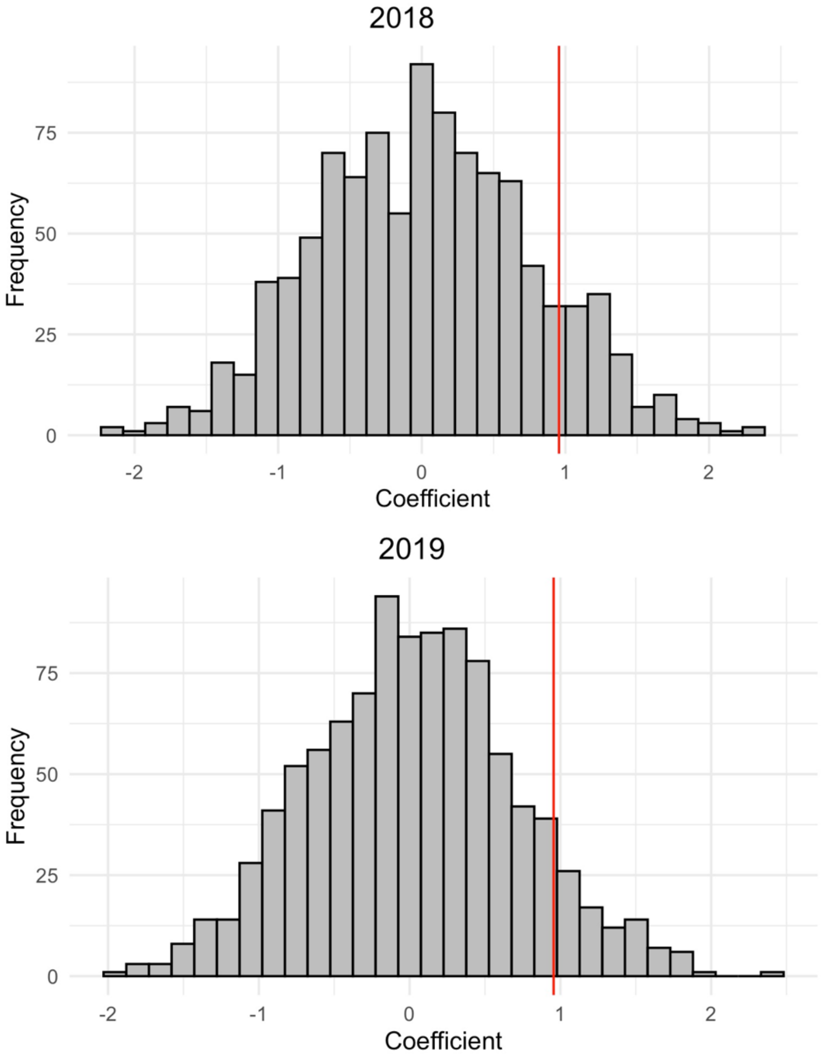


Figure 7: *Year-by-year histograms of the supplementary model results (Treated*year[2009-2019])*

5.3 Sustainalytics Analysis

The core of this study is the evaluation of cyber exposure and hacktivist campaigns. However, to provide a comprehensive understanding of potential factors influencing a firm's susceptibility or resilience to these threats, the Sustainalytics ESG database was incorporated. This database provides a lens into the Environmental, Social, and Governance (ESG) aspects of firms. High ESG scores may suggest a robust overall governance, encompassing strong cybersecurity measures. This becomes crucial, as a well-governed firm may be better equipped to navigate cyber threats.

It is important to underline that while hacktivist campaigns were charted in 2012, 2014, and 2016, the ESG data became accessible only from 2018 onwards. This implies a latent effect where the subsequent ESG data might reflect the prolonged outcomes and possibly the governance adaptations made by firms post-attacks. By weaving in this database, the research not only delves into the immediate fallout of hacktivist interventions but also elucidates the extended interplay of corporate governance factors, providing a richer perspective of the cybersecurity milieu.

For a more robust assessment, the Sustainalytics database via the Wharton Research Data Services (WRDS) platform was used to gauge the lasting influence of hacking campaigns on ESG factors. The framework from Sustainalytics measures the manageable yet unaddressed risks. Pertinent to this study are the cybersecurity and privacy parameters that counteract risks firms can navigate. In essence, significant security incidents can amplify cybersecurity deficits.

Six ESG indicators were extracted from the Sustainalytics data, which directly relate to privacy and risk. This data was then merged with deep and dark web exposures on a quarterly basis, spanning October 2018 to December 2021. To discern the enduring impact of hacking campaigns, the focus was narrowed to the PSM-matched firms, both treated and control.

Table 14 presents these six ESG indicators. Each column, from (1) to (6), stands for an individual indicator. A thorough breakdown of these indicators is cataloged in Appendix C. The primary independent variable here is "Treated." The assessment captures three hacking campaigns with relative lags of six, four, and two years from when ESG indicators were observed. Intriguingly, even after several years, the ESG risk ratings of firms subjected to hacking campaigns exhibit significant perturbations.

Table 15. ESG model results

The table presents the results of linear regressions, with columns (1) – (6) representing the six ESG indicators (as detailed in Appendix C). The analysis includes three hacking campaigns with delays of six (2012), four (2014), and two (2016) years. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:					
	DPSBeta	DPSManagement Score	DPSUnmanageableRisk Score	DPSRisk Score	ESGRisk ScoreMomentum	ESGRisk Score
	(1)	(2)	(3)	(4)	(5)	(6)
	Subsample: Hacking Campaign in 2012					
Treated	0.112**	-2.895	0.117*	0.106	3.387***	-3.382*
	(0.055)	(3.313)	(0.061)	(0.261)	(1.144)	(2.022)
	Subsample: Hacking Campaign in 2014					
Treated	0.087	-11.823	0.658***	2.641**	-1.220	-1.248
	(0.193)	(7.930)	(0.234)	(1.098)	(1.240)	(3.209)
	Subsample: Hacking Campaign in 2016					
Treated	0.154***	4.335	0.138**	0.195	4.383***	2.396
	(0.052)	(3.245)	(0.061)	(0.262)	(0.864)	(1.628)
Note:						*p<0.1; **p<0.05; ***p<0.01

Table 16: Fixed effects panel model results

The table presents the results of the fixed-effects panel models used to illustrate the impact of exposure to the deep and dark web on ESG risk ratings. The asterisk ***, ** and * denote significance at the 1%, 5% and 10%, respectively.

	Dependent variable:					
	DPSBeta	DPSManagement Score	DPSUnmanageableRisk Score	DPSRisk Score	ESGRisk ScoreMomentum	ESGRisk Score
	(1)	(2)	(3)	(4)	(5)	(6)
log(Exposure)	0.016^{***}	-0.178	0.018^{***}	0.083^{***}	0.125^{**}	0.623^{***}
	(0.003)	(0.146)	(0.004)	(0.014)	(0.050)	(0.128)
Observations	2,379	2,379	2,379	2,379	2,379	2,379
R^2	0.012	0.001	0.011	0.015	0.003	0.011
Adjusted R^2	-0.071	-0.083	-0.071	-0.067	-0.080	-0.072
F Statistic (df = 1; 2195)	25.772^{***}	1.488	25.486^{***}	33.488^{***}	6.204^{**}	23.597^{***}
Note:						*p<0.1; **p<0.05; ***p<0.01

Discussion

The results of this study shed light on the notable effects hacktivist campaigns exert on the cybersecurity landscape of financial institutions.

The analysis underscores that financial institutions targeted by hacktivist campaigns face a marked escalation in their exposure on the deep and dark web. The quantitative data attests to a 60% surge in risk exposure for the targeted companies when contrasted with control entities. Approximately three-quarters into a campaign, discernible trends emerge, indicating a divergence between the targeted institutions and control groups. The former experiences a significantly heightened exposure. Such findings robustly substantiate the first hypothesis, thereby emphasizing the linkage between hacktivist campaigns and an amplified cyber risk for the impacted firms.

Moreover, the collected data unveils a compelling correlation between pre-campaign cleartext password leaks and the trajectory of cyber risk exposure. Institutions with prior incidents of leaked passwords undergo a heightened exposure, lending weight to the second hypothesis. Such insights suggest that prior password leaks might be more than mere indications of cybersecurity vulnerabilities. They could potentially heighten an institution's susceptibility to severe breaches, especially during hacktivist campaigns.

Turning attention to the third hypothesis, though the study hints at a potential relationship between the size of a company (particularly those with employee counts below the median of targeted entities) and its vulnerability to hacktivist campaigns, the findings did not yield statistically significant results. Multiple models and robustness tests were employed, yet the data did not conclusively affirm that smaller firms are more vulnerable. While the observed trends suggest that smaller financial entities might be at a heightened risk, the lack of statistical significance indicates a need for further investigation in this domain.

Collectively, while the results offer a comprehensive insight into the dynamics of hacktivist campaigns, they also underscore the criticality of financial institutions revisiting and bolstering their cybersecurity frameworks.

Limitations

However, it's paramount to situate these findings within the context of the study's limitations.
The study is concentrated on NYSE-listed financial services companies. While this focus was deliberate to ensure a specific and intensive examination, it inevitably constrains the extrapolation of the findings. There remains an uncertainty regarding the applicability of these findings to entities listed on other exchanges, those operating in different industries, or privately held firms.
Additionally, the study employs Return on Assets (ROA) as a proxy for the available capital of these companies. While ROA serves as a functional metric, the reliance on it does introduce potential for variance. A richer dataset with detailed internal accounting could potentially refine our understanding of the capacity of these firms to allocate resources towards cybersecurity.
One significant limitation is the absence of a direct measure of firms' cybersecurity defense or any quantifiable data on their prior breaches. Without this data, it's challenging to determine the baseline

cybersecurity posture of the institutions in question or to contextualize the implications of prior breaches on subsequent hacktivist campaigns.

Another area the study didn't explore is the subsequent behavior of targeted firms. While increased cyber exposure following a hacktivist campaign is evident, this study doesn't delve into whether these institutions exhibited any behavioral changes in response. Such modifications could range from enhancing cybersecurity defenses to making operational or ethical adjustments in line with hacktivist demands. The ultimate objective of activism is to induce change, but this research does not ascertain whether the targeted firms acquiesced to the demands or bolstered their defenses against potential future attacks.

The methodological design of the study, while rigorous, might not encapsulate potential concurrent events within institutions during the period of observation. The multifaceted nature of business environments suggests that the observed patterns could also be influenced by an array of factors, be they organizational shifts, unrelated security incidents, or significant market dynamics.

Lastly, sourcing data from the dark and deep web, while invaluable, carries its set of limitations. The clandestine nature of hacktivist campaigns and other cyber threats means that there's a possibility that some pertinent data might remain concealed or go undetected.

Future Work

The results of this study are indicative of the profound implications hacktivist campaigns have on the cybersecurity landscape of financial institutions. The analysis reveals that financial institutions targeted in hacktivist campaigns experience a notable escalation in their exposure on the deep and dark web. The quantitative analysis confirms that there is a 60% increase in risk exposure for such targeted companies in comparison to control companies. The data suggests that approximately three quarters after the onset of a campaign, there's a discernible divergence in the trends between the targeted and control groups, with the former enduring significantly greater exposure. This finding lends substantial support to the first hypothesis, underscoring the correlation between hacktivist campaigns and amplified cyber risk for the targeted entities.

Further, the data brings forth an intriguing relationship between pre-campaign cleartext password leaks and the trajectory of cyber risk exposure. It is evident that institutions with prior leaked passwords experience an exacerbation in their exposure, reinforcing the second hypothesis. This suggests that prior password leaks may not only be symptomatic of cybersecurity weaknesses but might also predispose institutions to more severe breaches in the face of hacktivist campaigns.

In exploring the third hypothesis concerning the correlation between the size of a financial institution and its susceptibility to hacktivist campaigns, the results did not yield statistically significant findings. One plausible interpretation of these results is the inherent nature of hacktivist campaigns and their decision-making processes. It is noteworthy that many hacktivist groups, such as Anonymous, often operate with collective decision-making frameworks, involving mechanisms like target lists or even communal voting to decide on their subsequent targets. This suggests that the criteria for targeting might be driven by factors other than company size, possibly focusing more on the institution's perceived ideological misalignments or other extrinsic factors. Thus, while company size might intuitively seem like a determinant of cyber vulnerability, in the realm of hacktivism, it might not always serve as a primary criterion for target selection.

Collectively, the results not only provide a nuanced understanding of the dynamics surrounding hacktivist campaigns but also emphasize the imperative for financial institutions to reassess and fortify their cybersecurity postures.

Conclusion and Recommendations

This research offers a compelling insight into the manifold effects of hacktivist campaigns on the cyber exposure of NYSE-listed financial services firms. Distinctly evident is the substantial rise in cyber exposure, especially for institutions with prior cleartext password breaches. Interestingly, the anticipated heightened vulnerability of smaller firms was not statistically substantiated by the study, raising questions about the underlying factors influencing hacktivist target selection.

Gleaning from the findings, the ensuing recommendations are proffered:

1. **Recognize the Threat of Hacktivists**: Hacktivists, regardless of their diverse motivations, have the potential to inflict significant damage. Understanding and addressing this risk is imperative.

2. **Preemptively Diminish Target Appeal**: Grasping common catalysts for hacktivist campaigns can serve as a proactive defense. Adopting transparent operations, endorsing ethical practices, and ensuring favorable ESG outcomes might deflect hacktivist attention.

3. **Prioritize Exposure Surveillance**: Equipping institutions with advanced cybersecurity tools to continually monitor deep and dark web exposures is paramount. Periodic risk benchmarking against industry peers can facilitate early threat detection.

4. **Empower Through Cybersecurity Education**: Continuous training can foster a workforce well-versed in recognizing and countering cyber threats.

5. **Strategize Incident Management**: A robust incident response mechanism can significantly minimize the damage from cyber incursions. Regular evaluations and updates to this strategy are crucial.

6. **Endorse Cyber Insurance**: In light of potential financial repercussions, cyber insurance can provide a safety net.

7. **Legislative and Regulatory Recommendations**: Given the societal implications of cyber breaches, there's a pressing need for regulatory enhancements. Stricter cybersecurity standards, especially in the financial sector, can bolster systemic resilience. Enhanced penalties for cyber miscreants can act as a deterrent. Given the global nature of cyber threats, fostering international cooperation in cybercrime investigations is recommended.

References

Abadie, A., & Gardeazabal, J. (2003). The Economic Costs of Conflict: A Case Study of the Basque Country. American Economic Review, 93(1), 113-132.

Abadie, A., Diamond, A., & Hainmueller, J. (2010). Synthetic Control Methods for Comparative Case Studies: Estimating the Effect of California's Tobacco Control Program. Journal of the American Statistical Association, 105(490), 493-505.

Abadie, A., Diamond, A., & Hainmueller, J. (2011). Synth: An R Package for Synthetic Control Methods in Comparative Case Studies. Journal of Statistical Software, 42(13), 1-17.

Abadie, A., Diamond, A., & Hainmueller, J. (2014). Comparative Politics and the Synthetic Control Method. American Journal of Political Science, 59(2), 495-510.

Agarwal, S., Chomsisengphet, S., Mahoney, N., Stroebel, J. (2015). "Regulating consumer financial products: Evidence from credit cards." Quarterly Journal of Economics, 130 (1), 111-164.

Anonymous. (2011, August 17). Anonymous Is Not Unanimous. Pastebin. http://pastebin.com/4vprKdXH.

Branwen, G. (2021). Darknet Market mortality risks. Crime Science, 10(1), 1-16.

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

Chatterjee, S., Sarker, S., & Valacich, J.S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. Journal of Management Information Systems, 31(4), 49-87.

Chen, H. (2011). From terrorism informatics to dark web research. Counterterrorism and Open Source Intelligence (pp. 317-341). Springer, Vienna.

Coleman, G. (2014). Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. Verso.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014, February). The tangled web of password reuse. In NDSS (Vol. 14, No. 2014, pp. 23-26).

Davies, L. (2013, January 26). Anonymous takes down US Sentencing Commission website. The Guardian. https://www.theguardian.com/technology/2013/jan/26/anonymous-hacking-takes-down-sentencing-commission-website

Della Porta, D., & Diani, M. (2009). Social Movements: An Introduction (2nd ed.). Blackwell Publishing.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), Networks and netwars: The future of terror, crime, and militancy (pp. 239-288). RAND Corporation.

Diani, M., & McAdam, D. (2003). Social Movements and Networks: Relational Approaches to Collective Action.

Dreyfus, S. (2014). Underground: Tales of hacking, madness, and obsession on the electronic frontier. Random House.

Driessen, J., & Gustafson, N. (2020). A Criminological Internet of Things: Implications for our Darkweb Desires. Journal of Crime and Justice, 43(2), 143-157.

Dunn Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. Politics and Governance, 6(2), 22–30.

Earl, J., & Kimport, K. (2011). Digitally enabled social change: Activism in the Internet age. MIT Press.

Fuchs, C. (2013). The Anonymous movement in the context of liberalism and socialism. Interface: A Journal for and About Social Movements, 5(2), 345-376.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. MIS Quarterly, 34(3), 567-594.

Gordon, L.A., & Loeb, M.P. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438-457.

Greenberg, A. (2010, December 8). MasterCard.com Taken Down By WikiLeaks Supporters, Twitter Next? Forbes. https://www.forbes.com/sites/andygreenberg/2010/12/08/mastercard-taken-down-by-wikileaks-supporters-twitter-next/

Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & el Koutbi, M. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. Procedia Computer Science, 151(2018), 1004–1009. https://doi.org/10.1016/j.procs.2019.04.141

Holt, T. J., & Bossler, A. M. (2016). Technology and Violence. In C. A. Cuevas & C. M. Rennison (Eds.), Technology and the Politics of Crime, Policing, and Security. https://doi.org/10.1002/9781118303092.ch30

Johnson, M.E. (2015). Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain. Journal of Management Information Systems, 32(2), 7-25.

J. Bonneau, "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 2012, pp. 538-552, doi: 10.1109/SP.2012.49.

Kamiya S., Kang J., Kim J., Milidonis A., Stulz R. (2020), Risk management, firm reputation, and the impact of successful cyberattacks on target firms, forthcoming in Journal of Financial Economics.

Karagiannopoulos, V. (2020). A Short History of Hacktivism: Its Past and Present and What Can We Learn from It.

Keppo, J., Korte, J. (2018). "Risk Targeting and Policy Illusions - Evidence from the Announcement of the Volcker Rule," Management Science, 64, 215-234.

Liu, A., Wang, Q., & Wesselman, A. (2018). Cyber threat intelligence sharing: A survey. ACM Computing Surveys (CSUR), 51(4), 1-38.

Manion, Mark and Abby Goodrum. 2000. "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic." Computers and Society 30(2): 14-19. Retrieved April 15, 2013 (http://www.csis.pace.edu/cis101/CIS_101_Fall_2007_Spring_2008/LearningPod Topics/SocialResponsibility/Terrorism-or-Civil-Disobedience.pdf).

Mansfield-Devine, S. (2011). Anonymous: serious threat or mere annoyance? Netw. Secur., 2011, 4-10.

Milan, S. (2015). Hacktivism as a radical media practice.

Nurmi, J., & Niemelä, M. S. (2017). Tor De-anonymisation Techniques. In Lecture Notes in Computer Science (Vol. 10394). Presented at the International Conference on Network and System Security. https://doi.org/10.1007/978-3-319-64701-2_52

Nurmi, J., & Niemelä, M. S. (2018). PESTEL analysis of hacktivism campaign motivations. In Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23 (pp. 323-335). Springer International Publishing.

Nurmi, J., Niemelä, M., & Brumley, B. B. (2023). Malware Finances and Operations: a Data-Driven Study of the Value Chain for Infections and Compromised Access. ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1–12). https://doi.org/10.1145/3600160.3605047

Nurmi, J., Niemelä, M., & Brumley, B. B. (2023). Malware Finances and Operations: a Data-Driven Study of the Value Chain for Infections and Compromised Access. ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1–12). https://doi.org/10.1145/3600160.3605047

Olson, P. (2013). We are anonymous. Random House.

Ponemon (2018). 2018 Cost of Cyber Crime Study.

Rajamanickam, D. S., & Zolkipli, M. F. (2021). Review on Dark Web and Its Impact on Internet Governance. Journal of ICT in Education, 8(2), 13–23. https://doi.org/10.37134/jictie.vol8.2.2.2021

Rajivan, P., & Gonzalez, C. (2018). Creative persuasion: A study on adversarial behaviors and strategies in phishing attacks. Frontiers in psychology, 9, 135.

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

Samuel, A. W. (2004). Hacktivism and the future of political participation. Harvard University.

Sauter, M. (2013). “LOIC Will Tear Us Apart”: The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. American Behavioral Scientist, 57(7), 983-1007.

Sauter, Molly. (2014). The Coming Swarm: DDoS Activism, Hactivism, and Civil Disobedience on the Internet. New York: Bloomsbury.

Setiawan, I., Hartog, F., & Zahir, S. (2019). Information security in small and medium enterprises in Indonesia. Information & Computer Security.

Shackelford, S. J. (2013). Should your firm invest in cyber risk insurance? Business Horizons, 55(4), 349-356.

Tndel, I. A., Meland, P. H., Omerovic, A., Gjære, E. A., & Solhaug, B. (2015). Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research.

Uitermark, J. 2017. Complex Contention: Analyzing Power DynamicsWithin Anonymous. Social Movement Studies 16(4): 403–417

Verizon (2017). 2017 Data breach investigations report.

Van der Werf, M. (2020). Exploring the Cyber Threat Landscape: Analysing Cyber Threats and Attacks on Financial Services. Journal of Cyber Security and Mobility, 9(2), 103-126.

Whittaker, Z. (2013, January 25). Anonymous hacks US Sentencing Commission, distributes files. ZDNet. https://www.zdnet.com/article/anonymous-hacks-us-sentencing-commission-distributes-files/

Zannettou, S., Bradlyn, B., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (2018). What is Gab? A Bastion of Free Speech or an Alt-Right Echo Chamber. Companion Proceedings of The Web Conference 2018, 1007-1014.

Zetter, K. (2015). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown.

Appendix

Appendix A: Synthetic Controls

Synthetic Controls (SC) represent a robust methodological approach for comparative case studies. The core concept of Synthetic Controls stems from the objective to construct a comparison group that accurately reflects the circumstances that the treatment group would have experienced in the absence of the intervention or event.

Synthetic Controls were utilized in the current study to account for the difference in sample sizes between the treatment group, consisting of 22 companies, and the control group of 161 companies. This size disparity can potentially impose analytical challenges, and Synthetic Controls have been employed to bridge this gap and enhance the robustness of the analysis.

Definition and Use of Synthetic Controls

The Synthetic Control Method (SCM) was first introduced by Abadie and Gardeazabal (2003), and further developed by Abadie, Diamond, and Hainmueller (2010). The primary objective of SCM is to estimate the causal effect of an intervention, or 'treatment', on the treated unit, when there's only one or a few treated units, and there's no suitable or comparable control unit available.

SCM creates a 'synthetic' control group by taking a convex combination of potential control units that approximates the characteristics of the treated unit pre-treatment. In the context of this study, SCM was used to construct a Synthetic Control group that mirrors the 22 treated companies by combining a subset of the 161 control companies.

Applicability of Synthetic Controls

The application of the Synthetic Control Method is particularly suitable when dealing with instances characterized by a limited number of treated units, non-random assignment of the treatment, and a lack of suitable comparable control units. Given that the study is dealing with a smaller treatment group compared to the control group, SCM is a suitable and appropriate methodological choice.

It's also pertinent to note that SCM works well with time-series cross-sectional data, which typically arise in comparative case studies, as the combination of units to form the Synthetic Control is based on the match of the pre-intervention outcomes.

Benefits and Limitations of Synthetic Controls

One of the key advantages of the SCM is its ability to provide an intuitive and data-driven method to select a comparison group in observational studies. This method ensures more accurate results and inferences in cases where the treatment group is significantly smaller than the control group, as seen in the study.

However, it's also important to recognize some limitations of the SCM. Firstly, the quality of the synthetic control depends on the pool of potential control units; if the control units are not diverse or numerous enough, the synthetic control may not be an accurate reflection of the treated unit. Secondly, the results from the SCM may not be as robust to unobserved time-varying confounders as other methods like difference-in-differences. Finally, uncertainty estimates for SCM effects are typically based on permutation methods, which may not fully reflect the true uncertainty.

Overall, the Synthetic Control Method has provided a valuable tool to address the analytical challenges imposed by the size disparity between the treatment and control groups in this study.

Appendix B: Regression Analysis

Regression analysis, a staple in the realm of statistical modeling, is an indispensable tool in modern quantitative research. Used extensively in diverse fields, such as economics, psychology, and engineering, regression analysis is an invaluable asset for exploring relationships between variables, predicting future observations, and determining the effectiveness of interventions.

In the present study, regression analysis was used to explore the relationships between various factors impacting the company's performance. This Appendix will delve into the concept of regression analysis, its application, and its limitations, with specific attention to Ordinary Least Squares (OLS) regression.

Definition and Use of Regression Analysis

Regression analysis is a set of statistical processes used for estimating the relationships among variables. It includes techniques for modeling and analyzing several variables, focusing on the relationship between a dependent variable and one or more independent variables.

The Ordinary Least Squares (OLS) regression, specifically, is a type of linear regression analysis, which aims to minimize the sum of the squares of the differences between the observed dependent variable in the given dataset and those predicted by the linear function of the independent variable(s).

In the current study, OLS regression was applied to evaluate the relationships between various company performance indicators and their respective contributing factors.

Applicability of Regression Analysis

OLS regression is applicable in various scenarios, particularly when the goal is to understand how the typical value of the dependent variable changes when any one of the independent variables is varied while the other independent variables are held fixed. This method assumes that the relationship between each predictor and the response variable is linear and that errors are normally distributed and have constant variance — assumptions that were verified in this study before OLS regression was applied.

Benefits and Limitations of Regression Analysis

Regression analysis, especially OLS regression, is widely used due to its several benefits. It is relatively easy to implement and understand. OLS, in particular, provides unbiased and minimum-variance estimates, assuming that the model fits the assumptions of linearity, independence, homoscedasticity, and normality.

However, it is important to note the limitations of regression analysis. The accuracy and reliability of the OLS estimates heavily depend on the fulfillment of its assumptions. For instance, the presence of multicollinearity, heteroscedasticity, or endogeneity can lead to biased or inefficient estimates. Additionally, OLS regression is not suitable for non-linear data, and it may be sensitive to outliers.

Overall, despite its limitations, regression analysis has proven to be an essential tool in this study, providing valuable insights into the factors affecting company performance.

Appendix C: Forming the Sustainalytics dataset

Three datasets were acquired from Wharton Research Data Services (WRDS):

- ESG Risk Rating Focus data
- ESG Risk Rating Indicator data
- ESG Risk Rating MEI data

The dataset comprises information from October 2018 to February 2023. This study focuses specifically focus on six variables listed below.

- DPSBeta
  - **Name:** Issue - Data Privacy and Security-Beta
  - **Description:** A factor that assesses the degree to which a company's exposure deviates from its subindustry's exposure on a material ESG issue. The beta is multiplied with the subindustry issue exposure score to derive a company-specific issue exposure score for a material ESG issue. It normally ranges from 0 to 2, with 0 indicating no exposure, 1 indicating the subindustry average (as represented by the subindustry exposure score), and 2 indicating exposure that is twice the subindustry average. In exceptional cases the issue beta for a company might be set at above 2 to reflect overwhelming risks or circumstances that distinguish a company in an extraordinary manner from its peers in the same subindustry (for example by having certain types of additional business activities). Setting the beta to above 2 requires a special sign-off procedure. The issue beta is derived either from quantitative model (see quantitative issue beta) that captures multiple factors that have an influence on company-specific risk or a qualitative overlay (see issue beta overlay) that allows analysts to reflect factors that are not captured by the quantitative model, and includes also issue exposure adjustments in case of category 4 or 5 events.
- DPSManagementScore
  - **Name:** Issue - Data Privacy and Security-Management Score
  - **Description:** Measures a company's handling of a single material ESG issue and is used to calculate the issue managed risk score. The score ranges from 0 to 100, with 0 indicating no (evidence of) management of the issue and 100 very strong management of the issue. The score is calculated as the sum of all indicator weighted scores in an issue.

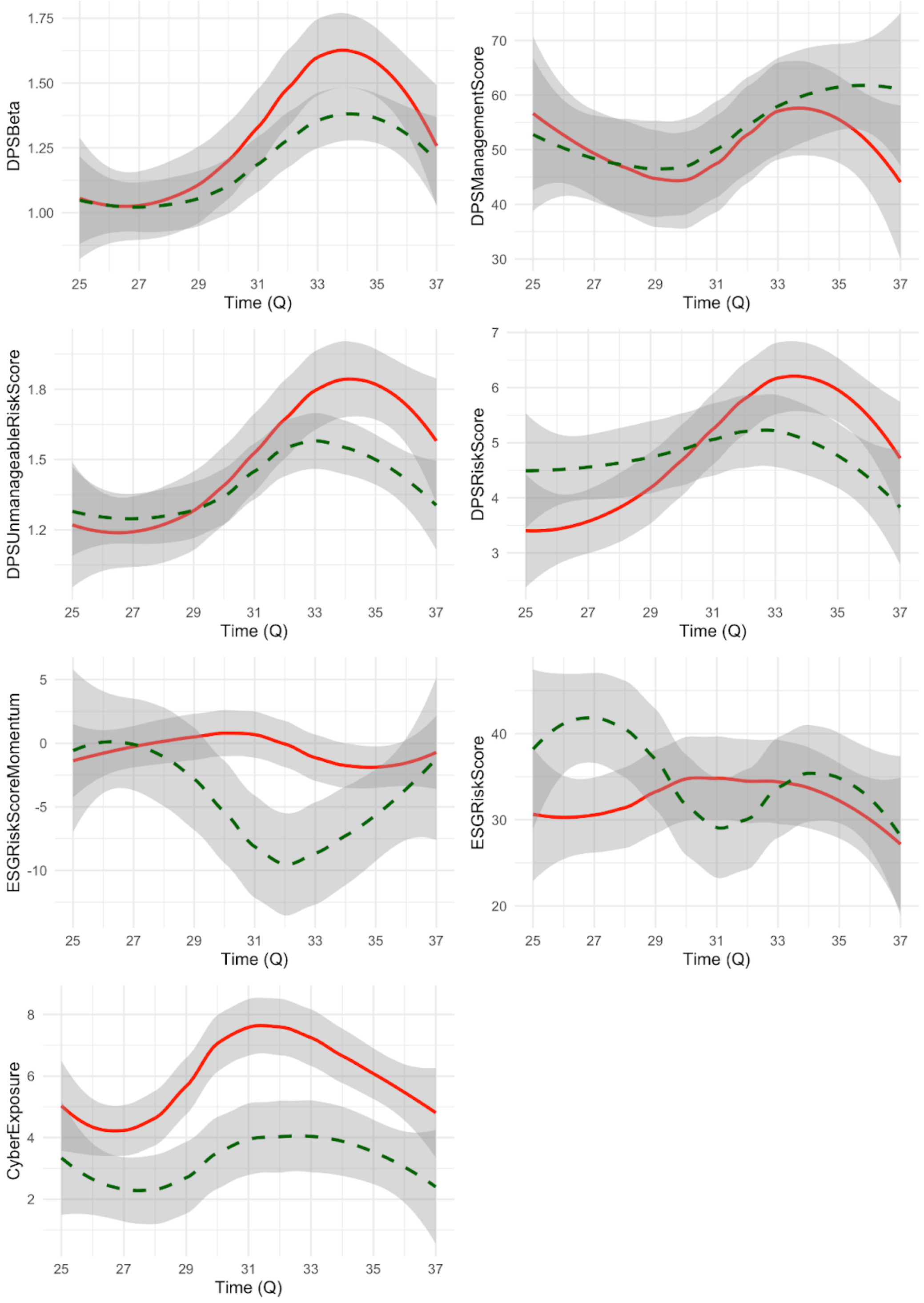
- DPSUnmanageableRiskScore
  - **Name:** Issue - Data Privacy and Security-Unmanageable Risk Score
  - **Description:** Refers to the amount of issue exposure that is deemed "unmanageable" and which cannot be mitigated by the company through management initiatives; it is calculated by subtracting the issue manageable risk score from the issue exposure score. The score ranges from 0 to the issue exposure score, with 0 indicating that the issue risk is fully manageable, and a score equaling to the issue exposure score indicating that none of the issue risk is manageable.
- DPSRiskScore
  - **Name:** Issue - Data Privacy and Security-Risk Score
  - **Description:** Refers to the unmanaged risk for a company on a material ESG issue; it is calculated by subtracting the issue managed risk score from the issue exposure score. Indicates the amount of exposure that is not (or cannot be) addressed by the company through management initiatives.
- ESGRiskScoreMomentum
  - **Name:** ESG Risk Score-Momentum
  - **Description:** Refers to the y-o-y absolute change in ESG risk score, comparing the current score with the historical score as of 12 months before, calculated on a rolling basis: ESG Risk Score (current) - ESG Risk Score (-12m).

- ESGRiskScore
  - **Name:** ESG Risk Score
  - **Description:** The company's overall score in the ESG Risk Rating. It applies the concept of risk decomposition to derive the level of unmanaged risk for a company, which is assigned to one of five risk categories. The score ranges from 0 and 100, with 0 indicating that risks have been fully managed (no unmanaged ESG risks) and 100 indicating the highest level of unmanaged risk. It is calculated as the difference between a company's overall exposure score and its overall managed risk score, or alternatively by adding the Corporate Governance unmanaged risk score to the sum of the company's issue unmanaged risk scores.

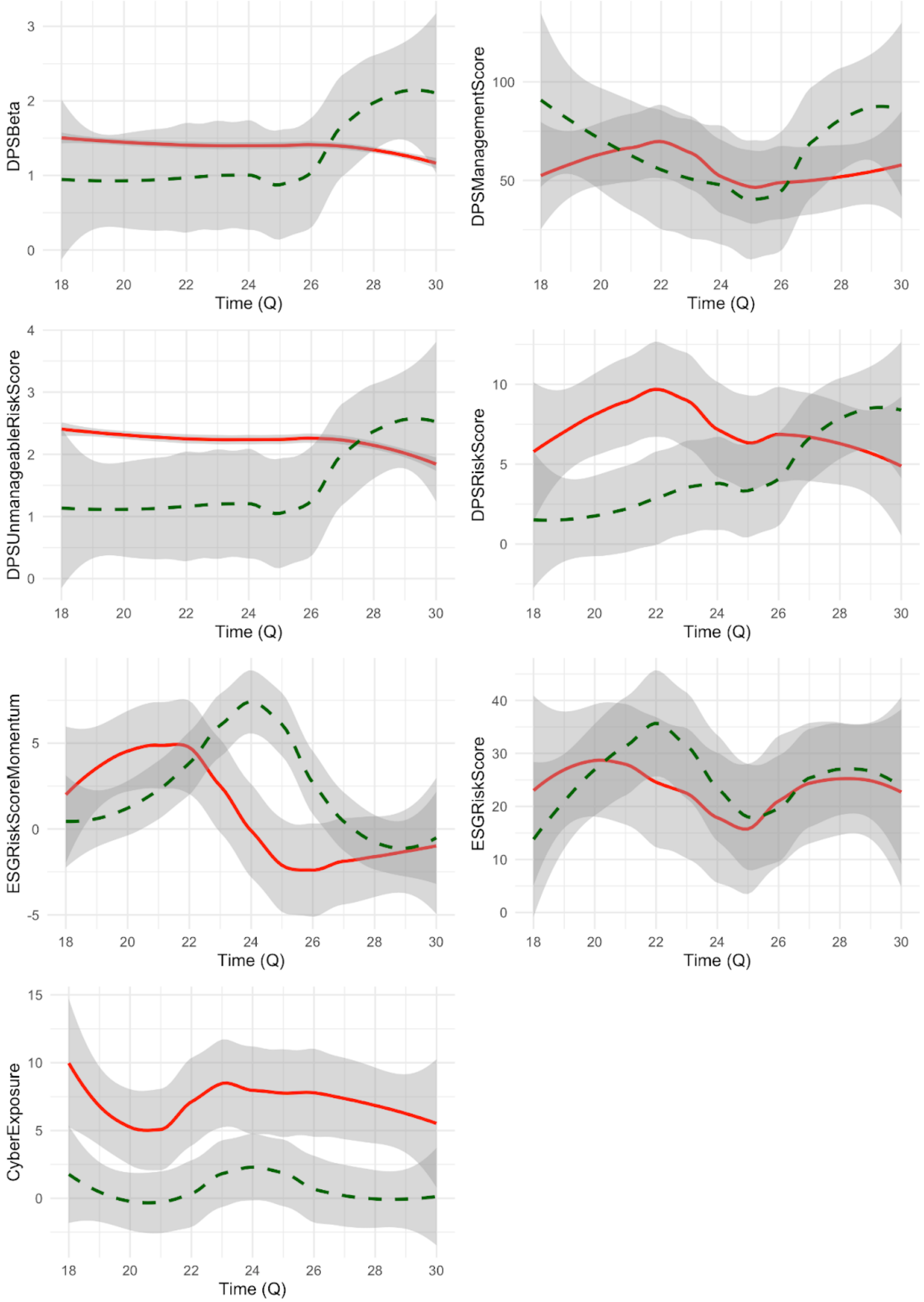
Sustainalytics (and cyber exposure) figures

Red = Targeted financial institutions
Green = PSM matched financial institutions
Time (Q) = quarters after the hacking campaign startDate

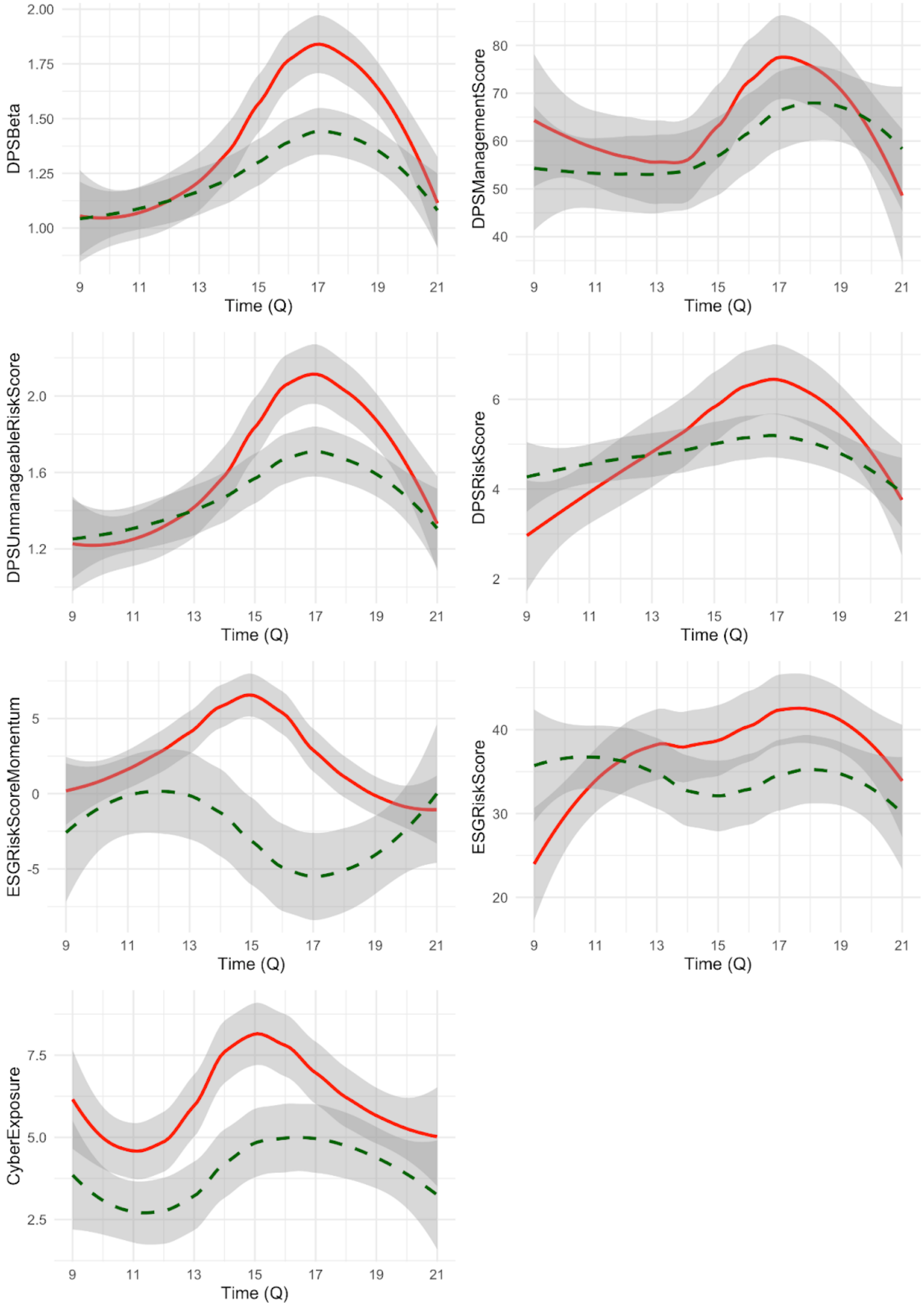
Subsample: Hacking Campaign in 2012



Subsample: Hacking Campaign in 2014



Subsample: Hacking Campaign in 2016



Appendix D: Matching Tables

The ROA and EMP numbers in matched company tables are from the previous year to the Campaign StartDate.

Table of control & treatment companies

Company	*Treated / Control*	*Campaign StartDate*
AFFILIATED MANAGERS GRP INC	Control	
AFLAC INC	Control	
ALLEGHANY CORP	Control	
ALLSTATE CORP	Control	
ALLY FINANCIAL INC	Treated	2012-09-18 UTC
AMBAC FINANCIAL GROUP INC	Control	
AMERICAN EQTY INVT LIFE HLDG	Control	
AMERICAN EXPRESS CO	Treated	2012-09-18 UTC
AMERICAN FINANCIAL GROUP INC	Control	
AMERICAN INTERNATIONAL GROUP	Control	
AMERIPRISE FINANCIAL INC	Treated	2012-09-18 UTC
AON PLC	Control	
ARGO GROUP INTL HOLDINGS LTD	Control	
ASSOCIATED BANC-CORP	Control	
ASSURANT INC	Control	
ASSURED GUARANTY LTD	Control	
AXIS CAPITAL HOLDINGS LTD	Control	

AXOS FINANCIAL INC	Control	
BANC OF CALIFORNIA INC	Control	
BANCO BBVA ARGENTINA SA	Control	
BANCO DE CHILE	Control	
BANCO LATINOAMERICANO DE COM	Control	
BANCO MACRO SA	Control	
BANCO SANTANDER BRASIL -ADR	Control	
BANCO SANTANDER MEXICO -ADR	Control	
BANCO SANTANDER SA	Control	
BANCO SANTANDER-CHILE	Control	
BANCOLOMBIA SA	Control	
BANK OF AMERICA CORP	Treated	2016-08-25 UTC
BANK OF HAWAII CORP	Control	
BANK OF MONTREAL	Control	
BANK OF NEW YORK MELLON CORP	Control	
BANK OF NOVA SCOTIA	Control	
BANK OF NT BUTTERFIELD & SON	Control	
BANKUNITED INC	Control	
BARCLAYS PLC	Control	
BARINGS BDC INC	Control	
BBVA	Treated	2016-08-25 UTC
BERKLEY (W R) CORP	Control	
BERKSHIRE HILLS BANCORP INC	Control	
BLACKROCK INC	Control	
BLACKSTONE GROUP INC	Control	

BRADESCO BANCO	Control	
BROOKFIELD ASSET MANAGEMENT	Control	
BYLINE BANCORP INC	Control	
CADENCE BANCORPORATION	Control	
CANADIAN IMPERIAL BANK	Control	
CAPITAL ONE FINANCIAL CORP	Treated	2012-09-18 UTC
CENTRAL PACIFIC FINANCIAL CP	Control	
CHUBB LTD	Control	
CI FINANCIAL CORP	Control	
CITIGROUP INC	Treated	2016-08-25 UTC
CITIZENS FINANCIAL GROUP INC	Treated	2016-08-25 UTC
CITIZENS INC	Control	
CNA FINANCIAL CORP	Control	
CNO FINANCIAL GROUP INC	Control	
COHEN & STEERS INC	Control	
COMERICA INC	Treated	2016-08-25 UTC
COMMUNITY BANK SYSTEM INC	Control	
CREDICORP LTD	Control	
CULLEN/FROST BANKERS INC	Control	
CUSTOMERS BANCORP INC	Control	
DEUTSCHE BANK AG	Control	
DISCOVER FINANCIAL SVCS	Control	
EMPLOYERS HOLDINGS INC	Control	
ENOVA INTERNATIONAL INC	Control	
EVERCORE INC	Control	

EVEREST RE GROUP LTD	Control	
F N B CORP/FL	Control	
FB FINANCIAL CORP	Control	
FEDERAL AGRICULTURE MTG CP	Control	
FEDERATED HERMES INC	Control	
FIDELITY NATL FINL FNF GROUP	Control	
FIRST AMERICAN FINANCIAL CP	Control	
FIRST BANCORP P R	Control	
FIRST COMMONWLTH FINL CP/PA	Control	
FIRST HORIZON CORP	Control	
FIRST REPUBLIC BANK	Control	
FLAGSTAR BANCORP INC	Control	
FRANKLIN RESOURCES INC	Control	
GAMCO INVESTORS INC	Control	
GENWORTH FINANCIAL INC	Control	
GLACIER BANCORP INC	Control	
GLOBAL INDEMNITY GROUP LLC	Control	
GLOBE LIFE INC	Control	
GOLDMAN SACHS GROUP INC	Treated	2016-08-25 UTC
GREENHILL & CO INC	Control	
GRUPO AVAL ACCIONES VALORES	Control	
GRUPO SUPERVIELLE	Control	
HANOVER INSURANCE GROUP INC	Control	
HARTFORD FINANCIAL SERVICES	Control	
HCI GROUP INC	Control	

HDFC BANK LTD	Control	
HERCULES CAPITAL INC	Control	
HERITAGE INSURANCE HOLDINGS	Control	
HILLTOP HOLDINGS INC	Control	
HOME BANCSHARES INC	Control	
HORACE MANN EDUCATORS CORP	Control	
HSBC HLDGS PLC	Control	
ICICI BANK LTD	Control	
INTERCONTINENTAL EXCHANGE	Treated	2012-09-18 UTC
INVESCO LTD	Control	
ITAU CORPBANCA	Control	
ITAU UNIBANCO HLDG SA	Control	
JPMORGAN CHASE & CO	Treated	2016-08-25 UTC
KB FINANCIAL GROUP	Control	
KEMPER CORP/DE	Control	
KEYCORP	Control	
LAZARD LTD	Control	
LINCOLN NATIONAL CORP	Control	
LLOYDS BANKING GROUP PLC	Control	
LOEWS CORP	Control	
M & T BANK CORP	Control	
MAIN STREET CAPITAL CORP	Control	
MANULIFE FINANCIAL CORP	Control	
MARKEL CORP	Control	
MASTERCARD INC	Control	

MBIA INC	Control	
MERCURY GENERAL CORP	Control	
METLIFE INC	Control	
METROPOLITAN BANK HLDNG	Control	
MGIC INVESTMENT CORP/WI	Control	
MITSUBISHI UFJ FINANCIAL GRP	Control	
MIZUHO FINANCIAL GROUP INC	Control	
MOELIS & CO	Control	
MORGAN STANLEY	Treated	2016-08-25 UTC
NATIONAL BANK HLDGS CORP	Control	
NATWEST GROUP PLC	Control	
NELNET INC	Control	
NEW YORK CMNTY BANCORP INC	Control	
OCWEN FINANCIAL CORP	Control	
OFG BANCORP	Control	
OLD REPUBLIC INTL CORP	Control	
OPPENHEIMER HOLDINGS INC	Control	
PENNANTPARK INVESTMENT CORP	Control	
PIPER SANDLER COS	Control	
PJT PARTNERS INC	Control	
PNC FINANCIAL SVCS GROUP INC	Treated	2016-08-25 UTC
PRIMERICA INC	Control	
PROASSURANCE CORP	Control	
PROGRESSIVE CORP-OHIO	Control	
PROSPERITY BANCSHARES INC	Control	

PROVIDENT FINANCIAL SVCS INC	Control	
PRUDENTIAL FINANCIAL INC	Control	
PZENA INVESTMENT MANAGEMENT	Control	
RADIAN GROUP INC	Control	
RAYMOND JAMES FINANCIAL CORP	Control	
REGIONAL MANAGEMENT CORP	Control	
REGIONS FINANCIAL CORP	Treated	2012-09-18 UTC
REINSURANCE GROUP AMER INC	Control	
RENAISSANCERE HOLDINGS LTD	Control	
RLI CORP	Control	
ROYAL BANK OF CANADA	Control	
SCHWAB (CHARLES) CORP	Treated	2012-09-18 UTC
SERVISFIRST BANCSHARES INC	Control	
SHINHAN FINANCIAL GROUP LTD	Control	
SIRIUSPOINT LTD	Control	
STATE STREET CORP	Treated	2012-09-18 UTC
STEWART INFORMATION SERVICES	Control	
STIFEL FINANCIAL CORP	Control	
SUMITOMO MITSUI FINANCIAL GR	Control	
SUN LIFE FINANCIAL INC	Control	
SUNTRUST BANKS INC	Treated	2016-08-25 UTC
SYNCHRONY FINANCIAL	Control	
SYNOVUS FINANCIAL CORP	Control	
TD AMERITRADE HOLDING CORP	Control	
TORONTO DOMINION BANK	Treated	2016-08-25 UTC

TRAVELERS COS INC	Control	
TRUIST FINANCIAL CORP	Control	
UNIVERSAL INSURANCE HLDGS	Control	
UNUM GROUP	Control	
US BANCORP	Treated	2016-08-25 UTC
VISA INC	Treated	2014-06-12 UTC
WALKER & DUNLOP INC	Control	
WEBSTER FINANCIAL CORP	Control	
WELLS FARGO & CO	Treated	2012-09-18 UTC
WESTERN ALLIANCE BANCORP	Control	
WESTERN UNION CO	Control	
WESTWOOD HOLDINGS GROUP INC	Control	
WHITE MTNS INS GROUP LTD	Control	
WOORI FINANCIAL GROUP INC	Control	

Table of PSM matched companies

Company	*Treated / Control*	*Campaign StartDate*	*roa*	*log(emp)*
ALLY FINANCIAL INC	Treated	2012-09-18 UTC	-0.060850054	2.76000994
AMERICAN EXPRESS CO	Treated	2012-09-18 UTC	3.1949236	4.151039906
AMERIPRISE FINANCIAL INC	Treated	2012-09-18 UTC	0.847849775	2.49642341
AON PLC	Control	2012-09-18 UTC	3.299269085	4.143134726
BROOKFIELD ASSET MANAGEMENT	Control	2012-09-18 UTC	2.149980013	3.17805383

CAPITAL ONE FINANCIAL CORP	Treated	2012-09-18 UTC	1.578980579	3.482531563
HDFC BANK LTD	Control	2012-09-18 UTC	1.538468402	4.038690898
HSBC HLDGS PLC	Control	2012-09-18 UTC	0.657267883	5.700443573
INTERCONTINENTAL EXCHANGE	Treated	2012-09-18 UTC	1.409967128	0.699626147
LOEWS CORP	Control	2012-09-18 UTC	1.411608624	2.957511061
RADIAN GROUP INC	Control	2012-09-18 UTC	4.538991537	0.500775288
REGIONS FINANCIAL CORP	Treated	2012-09-18 UTC	0.148760331	3.325503537
SCHWAB (CHARLES) CORP	Treated	2012-09-18 UTC	0.795924571	2.714694744
STATE STREET CORP	Treated	2012-09-18 UTC	0.885498577	3.425564738
TRUIST FINANCIAL CORP	Control	2012-09-18 UTC	0.738347682	3.490428515
WELLS FARGO & CO	Treated	2012-09-18 UTC	1.207808705	5.580484258
WOORI FINANCIAL GROUP INC	Control	2012-09-18 UTC	0.683147282	3.337405249
FRANKLIN RESOURCES INC	Control	2014-06-12 UTC	13.97113766	2.302785073
VISA INC	Treated	2014-06-12 UTC	13.85026143	2.351375257
AMERICAN INTERNATIONAL GROUP	Control	2016-08-25 UTC	0.441901788	4.210645018
BANCO SANTANDER SA	Control	2016-08-25 UTC	0.445137483	5.272296748

BANK OF AMERICA CORP	Treated	2016-08-25 UTC	0.740935571	5.367283571
BANK OF NEW YORK MELLON CORP	Control	2016-08-25 UTC	0.801970644	3.955082495
BBVA	Treated	2016-08-25 UTC	0.352230059	4.934243691
CITIGROUP INC	Treated	2016-08-25 UTC	0.999070015	5.446737372
CITIZENS FINANCIAL GROUP INC	Treated	2016-08-25 UTC	0.607779579	2.928523524
COMERICA INC	Treated	2016-08-25 UTC	0.724849395	2.312832409
DEUTSCHE BANK AG	Control	2016-08-25 UTC	-0.417032426	4.625991902
GOLDMAN SACHS GROUP INC	Treated	2016-08-25 UTC	0.706180092	3.632309103
GRUPO AVAL ACCIONES VALORES	Control	2016-08-25 UTC	0.942113782	4.122300138
HDFC BANK LTD	Control	2016-08-25 UTC	1.752977929	4.483623828
HSBC HLDGS PLC	Control	2016-08-25 UTC	0.561158937	5.579729826
JPMORGAN CHASE & CO	Treated	2016-08-25 UTC	1.039334132	5.462126963
LOEWS CORP	Control	2016-08-25 UTC	0.341974773	2.87356464
MANULIFE FINANCIAL CORP	Control	2016-08-25 UTC	0.310937595	3.540959324
MIZUHO FINANCIAL GROUP INC	Control	2016-08-25 UTC	0.346814816	4.356183047
MORGAN STANLEY	Treated	2016-08-25 UTC	0.780098163	4.046868534

PNC FINANCIAL SVCS GROUP INC	Treated	2016-08-25 UTC	1.145350118	3.979924615
SUNTRUST BANKS INC	Treated	2016-08-25 UTC	1.013012467	3.220594347
TORONTO DOMINION BANK	Treated	2016-08-25 UTC	0.716424614	4.412592212
TRUIST FINANCIAL CORP	Control	2016-08-25 UTC	0.992631474	3.642835516
US BANCORP	Treated	2016-08-25 UTC	1.393613415	4.196193921

Table of SC matched companies

Matched control companies have the same id as treated companies, but with the equation id*1000.

Company	*Treated / Control*	*Campaign StartDate*	*roa*	*log(emp)*	*id*
AMERICAN EXPRESS CO	Treated	2012-09-18 UTC	3.1949236	4.151039906	4
REGIONS FINANCIAL CORP	Treated	2012-09-18 UTC	0.148760331	3.325503537	16
ALLY FINANCIAL INC	Treated	2012-09-18 UTC	-0.060850054	2.76000994	21
WELLS FARGO & CO	Treated	2012-09-18 UTC	1.207808705	5.580484258	26
STATE STREET CORP	Treated	2012-09-18 UTC	0.885498577	3.425564738	32
SCHWAB (CHARLES) CORP	Treated	2012-09-18 UTC	0.795924571	2.714694744	51
CAPITAL ONE FINANCIAL CORP	Treated	2012-09-18 UTC	1.578980579	3.482531563	108
INTERCONTINENTAL EXCHANGE	Treated	2012-09-18 UTC	1.409967128	0.699626147	149
AMERIPRISE FINANCIAL INC	Treated	2012-09-18 UTC	0.847849775	2.49642341	152

NA (synthetic)	Control	2012-09-18 UTC	3.194922469	4.151039831	4000
NA (synthetic)	Control	2012-09-18 UTC	0.148760954	3.325503527	16000
NA (synthetic)	Control	2012-09-18 UTC	-0.060817218	2.760003732	21000
NA (synthetic)	Control	2012-09-18 UTC	1.20068315	5.575683703	26000
NA (synthetic)	Control	2012-09-18 UTC	0.885498582	3.42556476	32000
NA (synthetic)	Control	2012-09-18 UTC	0.795921519	2.714694816	51000
NA (synthetic)	Control	2012-09-18 UTC	1.578980558	3.482531455	108000
NA (synthetic)	Control	2012-09-18 UTC	1.409967204	0.699628255	149000
NA (synthetic)	Control	2012-09-18 UTC	0.847849816	2.496423407	152000
VISA INC	Treated	2014-06-12 UTC	13.85026143	2.351375257	164
NA (synthetic)	Control	2014-06-12 UTC	13.8502609	2.351252708	164000
JPMORGAN CHASE & CO	Treated	2016-08-25 UTC	1.039334132	5.462126963	11
COMERICA INC	Treated	2016-08-25 UTC	0.724849395	2.312832409	13
CITIGROUP INC	Treated	2016-08-25 UTC	0.999070015	5.446737372	14
US BANCORP	Treated	2016-08-25 UTC	1.393613415	4.196193921	18
BANK OF AMERICA CORP	Treated	2016-08-25 UTC	0.740935571	5.367283571	25

PNC FINANCIAL SVCS GROUP INC	Treated	2016-08-25 UTC	1.145350118	3.979924615	27
SUNTRUST BANKS INC	Treated	2016-08-25 UTC	1.013012467	3.220594347	35
MORGAN STANLEY	Treated	2016-08-25 UTC	0.780098163	4.046868534	41
BBVA	Treated	2016-08-25 UTC	0.352230059	4.934243691	57
TORONTO DOMINION BANK	Treated	2016-08-25 UTC	0.716424614	4.412592212	66
CITIZENS FINANCIAL GROUP INC	Treated	2016-08-25 UTC	0.607779579	2.928523524	84
GOLDMAN SACHS GROUP INC	Treated	2016-08-25 UTC	0.706180092	3.632309103	124
NA (synthetic)	Control	2016-08-25 UTC	0.626742122	5.460640088	11000
NA (synthetic)	Control	2016-08-25 UTC	0.724852038	2.312832395	13000
NA (synthetic)	Control	2016-08-25 UTC	0.999009165	5.445290364	14000
NA (synthetic)	Control	2016-08-25 UTC	1.393614045	4.196192775	18000
NA (synthetic)	Control	2016-08-25 UTC	0.74089677	5.366502739	25000
NA (synthetic)	Control	2016-08-25 UTC	1.145451124	3.979770571	27000
NA (synthetic)	Control	2016-08-25 UTC	1.013086401	3.220535433	35000
NA (synthetic)	Control	2016-08-25 UTC	0.780099474	4.046867118	41000
NA (synthetic)	Control	2016-08-25 UTC	0.355411654	4.934233169	57000

NA (synthetic)	Control	2016-08-25 UTC	0.716428615	4.412587198	66000
NA (synthetic)	Control	2016-08-25 UTC	0.607780589	2.928523013	84000
NA (synthetic)	Control	2016-08-25 UTC	0.70618303	3.63230908	124000