THE IMPACTS OF CYBERATTACKS ON PRIVATE FIRMS' CASH HOLDINGS

NURLANA GADIROVA

Thesis submitted to the University of Ottawa in partial Fulfillment of the requirements for the degree of M.Sc. in Management – Finance

Telfer School of Management
University of Ottawa

Abstract

This research investigates 202 data breach events occurring between 2015 and 2019 and the related financial effects on the USA's impacted private firms. From examining previous research, it is obvious that no known studies evaluate the financial impacts of cybercrimes on private firms. Prior studies mostly focus on public firms and stock market reactions even though there is the increasing number of cyberattacks on private firms too. This study seeks to fill the gap by providing the empirical evidence of the impacts on those firms' cash holding after experiencing a cybersecurity attack. Overall, the results of this research show if the private firms that have been cyberattacked face the connate aftermath and follow the similar precautions as public firms with data breaches or not. I find that the firms that experienced an attack two years ago increase their cash holdings significantly, while an attack that happened a year ago can only impact cash holdings while interacting with tangibility and ROA of a firm. These results are essential as the private firms draw up a budget and reform strategies for coping with cyber incidents.

Keywords: cybersecurity, private firms, data breaches, cash holdings.

Table of Contents

List of Tables

1. Introduction

1.1.What are the objectives of this research?

This paper investigates the effect of cyber attacks on private organizations and the consequences on their cash holdings. To understand the importance of cybersecurity in the firms, first I examine the inducing determinants of cybercrimes and identify the financial outcomes for those companies. The substantial influence that cyberattacks have on businesses and regulators raises still unresolved questions about the economics of information security and, ultimately, the factors and actual effect of cybercrime on attacked firms. I aim to answer some of these important questions in this research. This paper's main *objective* is to identify the importance and the impacts of cyberattacks on the private firms and the consequences on their cash balances. This study's *research questions* is "How do data breaches affect private companies' cash holdings? ".

1.2.Why is this research important?

Several recent reports indicate that cyberattacks have become one of the biggest threats facing nearly every company in the world. Reports of past breaches and other cyberattacks indicate an increasing volume (higher than anticipated) of such incidents year by year, in the both USA and worldwide. These annual reports also indicate a clearer explanation of challenges faced by firms. According to a Statista report (2019), there were 1,473 data breaches with over 164.68 million sensitive data expos in 2019.

According to the World Economic Forum's report (2019), cyberattacks are counted within the top 10 risks to universal solidity, at number seven for the effect and five for the probability. Other additional reports also evince that cyberattacks have become one of the biggest threats facing most companies globally. For example, according to the 2019 Global Risks Report, cyberattacks are not

only ranked by executives as the top risk for enterprises in North America, but it also edged out all other risks to occupy the top spot for the first time in France, Germany, Italy and the UK (GRR, 2019).

Before 2002, it was not mandatory to disclose data breach events publicly in the US. California took the initiative and enacted the law of data breach disclosure for the first time in 2002, followed by almost all other states between 2002 and 2016. The law's root idea is publicly sharing data security breaches, although the law's technicalities may differ from state to state. Mandating firms to announce a data breach provokes risks and direct & indirect costs to them (Boasiako & Keefe, 2020).

Cyber incidents are among the most dangerous and rapidly thriving crimes against organizations and threats to national security. To put it more explicitly, once the cyber-criminal can access the system, the targeted firm is open to substantial direct costs that can include the loss of millions of dollars or core assets, such as intellectual property, that can threaten the company's viability. Studies claim that a new type of war is rising, and, cyberattacks' targets cannot afford to lose. In compliance with federal regulations and their business models, private sector and large financial institutions acquire, collect, and retain significant volumes of confidential information. Control over and possession of this sensitive data make these organizations and institutions desirable targets for hackers.

1.3.What are the contributions of this research?

This study outlines the changes in the private firms' cash holdings, which have not been studied before since the most available research focuses on the public sector. Cyberattacks are a serious threat to all organizations including private companies worldwide. I conduct this research in the

USA context. Nevertheless, this work can also apply to other countries internationally. This work is of interest to the private sector and also law enforcement agencies, businesses, consumers and legislators worldwide.

It contributes to the research on cyber security and cash holding strategies. Furthermore, it might help firms enhance security and financial decisions and formulate policies that lead to better social outcomes.

1.4.What is the structure of this research?

I conduct a comprehensive review of the literature on cybercrimes, which constitutes the first building block of my thesis. Firstly, I identify the types and determinants of cyberattacks by analyzing the suggested definitions. Then, I examine the studies that investigate some aspects of cybercrime consequences on firms and financial markets. I probe the effects of cyberattacks on the cost of financing and cash holdings of firms that were the target of cyberattacks. The review of the literature confirms that there are massive concerns and problems regarding cyber crime. In the following section, the conceptual framework is outlined along with hypothesis development of this thesis. The next section includes the sample's exhaustive dissection and the methodology used in this research, followed by analyses and empirical results. Lastly, I conclude the paper and discuss the limitations of the research and potential future study areas.

2. Literature Review

2.1. Cyber Attacks

2.1.1. What is a cyber attack?

Gordan & Ford (2006) state that there are different kinds of cyberattacks – cyber incidents, cyber terrorism, cyber warfare, cybercrime, etc. Despite the popularity of these concepts, there are no universally adopted definitions for these terms. Existing definitions of "cyberattack" vary widely and capture a diverse array of behaviors, motivations, actors, actions and activities. The mentioned scholars refer to cyber activity that violates legal standards as cybercrime; cybercrime involves prohibited activity "facilitated or committed using a computer, network, or hardware device." Cybercrimes also involve the use of computers or computer technology to commit a crime or "to engage in activity that threatens a society's ability to maintain internal order."

Johnson (2017) also characterizes the cyberattacks' definitions and divides them into five categories. The first is "lone wolf" which are executed by individual hackers with the purpose of compromising networks. The attacks of this category are mostly for fame or fun. The second type of hackers involves "hacktivists" which try to draw attention to political or social concerns. The third category of attacks includes "fraud and criminal activity." As stated in its name, this type of attack aims to access customers' private information for fraud or their advantage. These attackers target financial institutions and retailers, mostly because of the vast customer information they have. The next category involves "industrial espionage", targeting the financial assets. These crimes require highly technical methods and deception. The final (fifth) type of cyberattacks contains "cyber warfare", which is against a nation-state (e.g. military or political campaign). These cybercrimes and data breaches affect businesses or corporations by stealing their private

information, including their customers' social security numbers, credit card and debit card numbers, email addresses, and telephone numbers.

Another categorization for cybercrime was given by Shim (2010) – whether the attacks are targeted or untargeted. "Untargeted" attacks are designed to fasten on millions of potential victims wishing to ruin as many computer systems as possible (Dzung, Naedele, Von Hoff, & Crevatin, 2005; Tally, 2009). Thus, opponents attempting untargeted attacks aim to contaminate any vulnerable system obtained on a network (Dzung, et al., 2005; Turk, 2005). Widespread instances of untargeted attacks contain spyware, worms, viruses, trojan horses, etc.

"Targeted" attacks intend to damage specific information assets of an organization or communication system with the objectives of monetary gains, industrial spying or even terrorism (Dzung, et al., 2005; Tally, 2009). Attackers using such methods ordinarily gather information about the target, design attacks separately for each particular victim, and, therefore, know who will be attacked (Dzung, et al., 2005; Turk, 2005). Common examples of targeted attacks are whaling and malicious hacking.

There can be another type of attack which was not examined in Shim's study: hybrid attacks. Hybrid attacks are designed as a combination of targeted and untargeted attacks and possess two levels. In the first level, opposers start untargeted attacks by spreading malicious software. In the second level, the attackers attempt the final targeted attacks. This type of aggression is essential to investigate. This categorization explores only some cases where the combination of targeted and untargeted attacks also impacts an organization's security risk management strategies. To set an example, in the first type of hybrid attacks, the targeted attack following an untargeted attack can be avoided if servers can be protected from the initial infection wave by untargeted attacks (Kurt et al. 2018).

NASDAQ (one of the largest international securities exchanges) admitted that its computer network was attacked. Most of the personal documents were accessed (Barrett, 2011), which shocked the market participants and impacted the market prices and economic stability worldwide. Johnson also states that, since financial institutions are highly dependent on technology to conduct their businesses, it is critically suggested to follow the regulations and policies to survive in the domestic and international economy. Another example given in this study is the Yahoo scandal, which occurred in 2016. Yahoo confirmed that 500 million users' account information was stolen (Perlroth, 2016).

Such data breach examples raise questions regarding the companies' reliability and accountability and impact all the market actors. As a result, the organizations' cost becomes more detrimental than the funds spent on prevention applications far-sightedly (Johnson, 2017). Johnson's statements and findings of data breaches' effect on the whole economy were re-examined in 2019 by Garg, who studied the spillover effect of cyberattacks. Overall, her study results indicate that the data breach outcomes are not only crucial to the attacked firms but also to the peers in the industry. Gande and Lewis (2009) find that an industry's litigation concentration acts as a strong predictor of a firm's actual litigation risk. Arena and Julio (2011) extend that to see that peer firms increase their cash holdings after a firm in their industry was involved in litigation. Lei et al. (2018) state that firms sensitive to credit shocks from peers build up cash reserves, serving as a precautionary motive for corporate liquidity management. As a result, prior literature shows that firms do not operate in isolation and any attack on one of the peers can affect the balance of all industry.

2.1.2. Geographical factors

The role of geography is significantly critical for monitoring companies' strategies and financing policies. There is also a rich literature on this concept, which considers the effect of geography on analyzing company's activities. Some of these studies again provide evidence on the similarities on the behaviour of geographically close companies (Gao, Ng and Wang, 2011). They conclude that such common strategies are related to social and cultural interaction between administrations rather than financial factors.

While some kinds of cyber incidents are specific to some countries or regions, other types, such as false statements or identity theft, cut across all countries; Wada (2011) discusses the types of cybercrimes in Nigeria that have an economic impact not only directly but also indirectly on the financial system of the nation and even facing trans frontier ripple effects. Longe and Chiemeke (2008) stripped the list of undesired outcomes (such as credit card frauds, ATM frauds, spamming, phishing, criminal activities, identity theft, and other related cyber crimes) of Information and Communication Technologies (ICT) to include acts like phishing, cyber terrorism, electronic spam mails, cyberstalking, and fake copy-cat websites. Wada expand the work of Longe and Chiemeke by attempting to peruse cybercrime and its impact on Nigeria's banking institutions. Wada also examines the institutional countermeasures' success in dealing with cybercrime and the banking industry's existing policy framework. Analysis of this study shows a significant relationship between electronic banking services and cybercrime. IT support and training, access control, and other internal banking security factors are found not to have a relationship to electronic banking services and cybercrime in Nigeria.

Mshvidobadze (2014) examines how modern Russia's economic, social and political features have induced multiple cyber threats to neighbouring countries and the U.S. The paper demonstrates the Russian approach to information warfare (IW) and its subset – cyber warfare. The study also illustrates how Russia's IW doctrine is tied to its geopolitical ambitions and how the relationship between the government and cybercriminals is formed in this regard. This paper also inquires about the cyberattacks in the countries such as Estonia, Georgia and Ukraine, which displayed the world-embracing characteristic of the cyber threats.

Alternatively, I can check into Adonis's research in 2016 which concerns with financial institutions of South Africa. This research aims to examine the exiguousness of information security on financial institutions and further explore whether business processes are responsive to an organization's needs in South Africa. Duncan (2015) also remarked on the unique challenges South Africa faces, corresponding with hacking and the intentions of stealing personal information. It is, thereby, significant for South African companies and institutions to understand their vulnerabilities.

The geographical differences and the worldwide prevalence of cybersecurity are discussed above with the guidance of previous scholars. These nuances are again conferred in the articles of Labbé (2018), who investigates banks concerning data breaches and cybercrimes. She states that since the digital landscape changes rapidly and continuously, there is no single prudent solution to stay safe from threats that banks face. Labbé also mentions the importance of ISO standards (such as ISO 27001, the international standard for best-practice information security management systems), which assist the banks and other organizations (mainly in Europe) in preventing the cyberattacks and be prepared for future potential breaches. Furthermore, she links up these realities to the

particulars of geographical requirements, which can make concordance very challenging to protect.

2.1.3. What causes companies to be attacked?

We are currently living with numerous devices continuously connected to the Internet in a hyperlinked world. The increasing addiction to such devices brings multifarious cybersecurity threats with itself as well. This growing connectivity demonstrates that vulnerabilities can be presented at any stage of the software development period. Hence, risk management on cybersecurity is more significant than ever not only to organizations from all industries and of all sizes but also to regimes at all progression stages. The awareness of cyber threats helps us understand the magnitude of certification and standards as a prevention approach (Peng, 2018). In other words, in our modern world, it is almost inescapable to be exposed to cyberattacks.

Purposes of cyberattacks differ from criminal to criminal. I found several previous works that indicate the various reasons as an incentive for cybercrimes. Al Saadi (2016) conducted the study to contribute to the knowledge and conceptual insight into terrorist financing and comprehend the trending terrorist funding strategies and the methods to prevent them. The main goal of this research is to understand how terrorism financing is formed and create policy frameworks on fundamental mechanisms for mitigating the terrorism financing regimes. As far back as 2012, Biller also conferred the attacks with political and criminal purposes, which are on the march worldwide. He states a lack of existing law to directly address cyberterrorism because of the absence of one standard working definition. Therefore, the author reaches at the definition by analyzing the different meanings which were previously suggested by security experts and were used by governmental institutions. This paper also recommends enshrining cybersecurity in law to fight terrorism around the world as a precursor to Al Saadi's research in 2016. Cyberterrorism is

the least common type of all cyberattacks, however, it is likely the most destructive (Johnson 2015).

Growing technology is at all levels of our life as stated in Peng. It is also undeniable that the finance sector includes innovations more than estimated. The concept of "financial innovation" was investigated by Stankovska (2019) and was described as establishing and improving new financial services and products, promoting new processes to organize new structures for financial institutions, interacting with customers, and expedite financial operations. The financial innovations offer the mechanism to finance innovative technological strategies while traditional origins of funds are missing because of high investment risk. Digital design is an essential part of financial innovations, which causes cyber threats by providing less time-consuming but risky solutions. The relation between the emergence of Fintech (trend of adopting emerging technologies for financial services) and cybersecurity in a global financial centre is also discussed in Ng and Kwok (2017).

Mester (2019) describes the financial system as a dynamic and continuously evolving system. He adds the rapid pace of technological changes by considering artificial intelligence, machine learning and other advanced technologies. The author also identifies the outputs of these innovations, such as making our payments easier and smoother, hastening our daily transactions and building more efficient analytical means to analyze and control the risk. However, these advances also bring some difficulties and even new dangers with themselves. With the incidence of technological innovations, some companies are suggesting the financial services can not fit into the current regulatory framework anymore, and even analyzing the risks outside of the traditional banking sector furnishes some rigours. In a rapidly changing financial system, firms' experience and wisdom can quickly become outmoded, as can the methodologies we use to inspect and control

the risks to financial balance. The author also indicated that we should guarantee that our monitoring strategies are agile enough to adopt new technologies since the dangers are evolving.

The literature on the financial innovations stated above demonstrates that cyberattacks are quite inevitable in modern life. However, Romanosky (2016) remarks that all cyber events might not be noticed, and even if noticed, they can not be mentioned in the dataset. Nevertheless, I try to explain most of the characteristics of the common cyberattacks.

2.1.4. Impacts of cyber attacks

After investigating the geographical factors and the researches in different countries, I can easily state that cyberthreats are prospective for across the world. Nonetheless, in this research I specifically deal with the USA context. According to "Cost of Data Breach Study" of IBM (2020), the USA is the most expensive country for a data breach's average total cost at $8.64 million.

The impacts on the organizations and consumers should not be confused as they have typical outcomes, as Coram (2018) states in his dissertation. He also examines another independent study by the Ponemon Institute (which is an independent organization that leads researches and offers to consult services to guide companies on developing data protection, privacy, and security applications) and Accenture (2017a), which demonstrates that cyberattacks cost companies in the United States approximately $21 million, that is 21.22% higher than in the previous year. Moreover, the research states that worldwide costs have also increased by 62% over the past five years.

Also, there are *intangible costs* to the organizations that are considerable to a data breach's total costs. These costs are root in the results of attacks on the consumers. Possible intangible costs to the firm include the loss of reputation, customer confidence and loyalty, low consumer satisfaction,

and investor trust loss (Acquisti, Friedman, & Telang, 2006; Lawrence et al., 2014; Yayla & Hu, 2011). The other authors indicate that data breaches can cost the firms the threat of lost revenues as a consequence of unfavourable publicity and unsatisfied consumers, additionally the potential penalties, fines or lawsuits (Gatzlaff & McCullough, 2010; Lawrence et al., 2014).

Janakiraman (2018) researches data breach announcements (DBA) outcomes directly related to customer reactions. He uses each transaction data of the retailer's consumers to inspect a systematic and detailed empirical study of a DBA's impacts on consumer expenses and behaviour. Janakiraman compares customer decisions before and after the DBA by conducting a treatment group (consumers whose personal data is attacked) and a control group (consumers whose personal data is not attacked). He concludes that the information breach ends up in a massive decrease in consumers' expenses. Nevertheless, customers of the attacked company migrate to the channels of the retailers that are not breached. Another very similar research is investigated by Rosati (2017) which analyzed the results of data breach announcements on market efficiency, especially, on the bid-ask spread and the trading volume. The author indicates the data breach announcements as an asymmetric information source and suggests a new dimension to the current market activity debate. He finds that DBAs have a positive short-term effect on both trading volume and bid-ask spread. However, the impact is only experienced on the day of the event and the market efficiency returned to regular market activity quickly.

Meisner does his research on financial outcomes of cyber attacks that are resulting in data breaches in the healthcare sector in 2017. The writer identifies the healthcare sector as significantly vulnerable to digital data breaches and damages, which are welded by illegal access to patients' confidential and personal data. The article also states that, medical organizations exposed to such dangerous attacks should anticipate financial results of possible cybercrime. This

study's objective is to explain the outcomes of a digital data breach in the healthcare sector and their economic effect – by comparing Polish and global perspectives. The study results suggest that approximations of total digital data breach costs differ widely among numerous analyses and reports. The fundamental reasons are the implementation of several methods for anticipating and the lack of reliable dataset because of incomplete disclosure of cyberattacks. Lastly, the study's most significant conclusion is that there is an emerging necessity to research possible data breach costs in the Polish healthcare sector, since studies have not covered Poland yet.

The previous researchers analogize the consequences of cyberwarfare on conventional armed attacks (Hathaway, 2012). As was previously stated, Garg (2019) also examines the effects of cybersecurity and suggests that the companies increase their cash balances after the cyber incidents. More interestingly, even if the organizations are not experienced any attack, they still follow their peers' behaviour as a spillover effect.

Considering the width of critical infrastructure resources found in Johnson's (2017) study, his research limits its focus to cyber threats against domestic and international financial markets and payment systems. It does not include the political effects of cybercrime. The author argues that these types of attacks on financial markets threaten to undermine the integrity of market operating systems and the domestic and international economy's stability. Johnson adds that despite the rich literature on cybersecurity, there is a limited number of detailed studies on attacked companies' stock market value.

Coronado (2012) states in his thesis that the data breaches, as a generic category (e.g. availability, confidentiality and integrity), have a particularly negative effect on firm's market returns. The researcher also mentions that the different results in information breaches can be the output of several factors. The aforementioned factor is the lack of an accurate definition of what composes

a personal information breach. Another factor is that various studies are conducted by different estimation methods. Lastly, the sample sizes differ significantly in size, which may also impact the findings' reliability (Coronado). However, Morse, Raval, and Wingender (2011) also find a statistically significant and negative effect on stock returns as an outcome of data breaches. They lastly state that the financial industry suffered more significant impacts on negative abnormal returns across the different sectors studied in the previous researches.

"The disclosure of data breaches can potentially subject firms to regulatory investigations and fines, litigation, media scrutiny and reputation damage, customer loss, revenue decline, and increased cash flow risks and possibly threaten a firm's bottom line, as well as shareholder value, among other things." (Boasiako & Keefe)

2.2. Cash Holdings

Next, I review the prior studies on cash holdings since this thesis's critical portion discusses cash hoarding behaviour and its determining factors after a data breach. There are numerous valuable studies on the cash reserves of private firms. Nevertheless, most of these researches are focused on Europe and other non-US locations. The actual number of articles in the US context is quite limited due to private organizations' challenging data availability.

Gao, Harford and Li (2012) compare the public and private firms' cash policies in the USA and stated that examining private firms' cash policy is of tremendous interest to financial analyzers & economists since there is a lack of data before their research. The scholars also suggest that private organizations' cash holding is about half as much of public companies. Even though private firms are supposed to have more powerful precautionary actions and these firms have conceivable less

external financing opportunities, the results are significant. They also provide evidence that an average private firm keeps less cash than the average public firm does. In my research I also speak about the contrasts between private and public firms for their cash management and the cautious motives by comparing our results to the previously researched public firms.

Another research in the US context is conducted by Boasiako & Keefe, who look into the changes in corporations' cash policies after mandatory data breach disclosure laws. The scholars state that firms are inclined to increase their cash levels after laws mentioned above get mandatory. Moreover, they find that facing an attack induces high cash hoardings in corporations and lowers their external financing and investments. The scholars also demonstrate that breached firms continue to keep high cash balances in the next year which aligns with Garg's findings. The severity of a data breach also affects cash holdings in a positive correlation, according to Boasiako & Keefe.

3. Hypothesis Development

This research examines how data breaches impact private firms' cash holdings and the other triggering reasons behind the cash holdings' volatility after an attack. There are various losses that data breaches can result in. These losses may be tangible or intangible, as I discussed in previous studies' findings. To the best of my knowledge, no prior research has analyzed the private companies' cash holdings after being exposed to a data breach as in this thesis. I use a conceptual framework for private firms that mirrors Garg's conceptual framework for public firms.

By investigating the firms' *credit risk*, Kamiya et al. (2018) find out that attacked companies experience more bankruptcy, superior decline in credit ratings and finally, increased cash flow volatility. They also mention that the attacked firms might have to stop investing externally to keep more cash available to cope with the undesired results of a breach. Additionally, several studies also focus on cash holding as a precautionary motive; Acharya, Davydenko, & Strebulaev (2012) suggest that companies are more inclined to hold cash when they experience high credit risk and financial incompatibility. The scholars also confirm the intuitive correlation between saving cash and being a "safer" firm. Similarly, Opler, Pinkowitz, Stulz and Williamson (1999) state that firms increase their cash holdings when they face escalated cash flow fluctuation in the market. The same researchers find evidence that operating losses' accruing is the primary reason for significant variance in surplus cash.

Thus, I hypothesize:

H1: Private firms increase their cash holdings after experiencing a data breach.

4. Data & Methodology

To construct the data on cybercrime, I use mainly the PRC (Privacy Rights Clearinghouse) database since it contains the information of the attacks that are publicly announced. It is also used in prior similar researches (Garg, 2019; Kamiya et al., 2018; Coram, 2018, etc.). I also gather the data from the annual reports (for the same years) of ITRC (Identity Theft Resource Center) and via Google search. I first select all the data breach events between 2015 and 2019 which contains 3136 records. The reason for the period selection is because the majority (50%) of the data breaches since 2005 are reported in the years starting in 2015 (Coram). Kamiya et al. also show a typically rising trend in the number of data breaches happening over the years by showing only four breaches recorded in 2005, compared with 46 records in 2017 in their study. In other words, more data breach incidents have been experienced in recent years.

Subsequently, I remove government and military entities, non-profit organizations, non-US firms and educational institutions from my dataset, which drops the number of records to 2591. The collected events have exact information of the date of public announcement, type of breach, type of organization, link to the source and whenever possible, description of incident and the total number of records that are breached.

Next, I verify every attacked firm to be a private firm and manually match them with the firms listed in Capital IQ, a useful database for finding detailed information of private firms. Organizations are categorized as private or public according to their most current status in Capital IQ. This database has been widely used in the prior literature (Kamiya et al., 2018; Gao et al., 2012, 2013, 2017). Huasheng Gao and his colleagues (2012) state a considerable rise in the number of private firms covered by Capital IQ since 2004.

After narrowing my sample down by requiring organizations to have an annual income statement and balance sheet data available for the periods right before and after a data breach, the final sample size decreases to 202 incidents. Since the private firms with assets less than $10 million are not required to disclose their financial statements, they need hand-collected data separately.

All tables can be found in the Tables section. Table 1 represents a chronological distribution of the collected data breaches by industry (SIC two-digit codes). The distribution shows that the most attacked sector is Service Industries (48.53%), pursued by Finance (43.63%), Wholesale trade and retail trade (4.90%), Manufacturing (0.98%) and Mineral & Construction industry (0.98%). These results also align with the previous research's (Kamiya, et al., 2018) findings and support that the most frequently cyberattacked companies are the ones working with numerous clients.

To test Hypothesis 1, the basic regression model for testing whether an organization increases cash holdings after an attack is specified as:

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\varepsilon_t \quad (1)$$

Where CH_t, the dependent variable, denotes the cash holdings of private firms after an attack. Cash holding is the ratio of total cash & cash equivalents to total assets. *Attack* is a dummy variable of interest that indicates the data breaches recorded in the last three years (impact of these cyberattacks are denoted by β_1, β_2, β_3, according to the attack year). It equals one if there was an attack and equals zero otherwise. The vector X is a set of control variables with firm characteristics from the year-end immediately preceding the attack. These variables include the logarithm of Sales (to control for firm Size), Leverage, ROE, ROA, Tangibility of assets, Sales Growth. I include the random error term which is denoted as ε_t. Furthermore, I am using robust standard error for the regression to mitigate the risk that my data are heteroskedastic.

After my primary analysis, I conduct a robustness check for industries. Following Garg, I use two-digit SIC codes to define the industries.

5. Analysis & Results

To start the analysis, I first check all linear regression assumptions to see if I need to transform my data. After visualizing the dataset's diagnostic plots, I delete some of the outliers that violate the linearity assumptions but do not affect the results. Then, I check the summary statistics of the data. Table 2.1 makes it visible that the dataset needs to be standardized to avoid creating a bias. Because the various inputs have large differences between their ranges. Table 2.2 presents the standardized data statistics, which are used for the following analysis.

This research's primary analysis includes the possible effect of cyberattacks that occurred in the last three years besides the firm-specific independent variables. The results of the estimations are presented in Table 3.1. I start my investigation with 205 data breach events that happened at (t-1), then add extra data points when there was no attack at (t-1), but there were attacks either at (t-2) or at (t-3) or at both. The findings are quite striking at this point. I find a strong link between attacks at (t-2) and the dependent variable in my analysis.

Since the previous literature on public companies mostly ended up with the significant relation between attacks and cash holdings (Garg), interestingly, it does not seem valid for private firms. To comprehend the reasons behind this difference, prior studies on cash holdings of private firms should be analyzed. In this particular respect, my findings are consistent with Gao et al. (2013), who compared cash policies in public and private firms in the USA. Their results indicate that the

mean cash holding of public firms is significantly greater than that of private firms. In other words, public firms hold twice more cash than private companies. The scholars also testify that public companies typically increase their cash holdings every year, approximately three times more than private firms do. The general conclusion is that financial frictions do not sway private firms to hold more cash, and they tend to use their money as a guard against losses instead of accumulating it as public firms do (Gao et al.). My results also accord with the research conducted in Europe by Poti et al. (2020) and Mortal et al. (2020). Mortal and his colleagues provide evidence that private firms are not sensitive to precautionary motives and do not accumulate cash for cautious reasons, because debt financing or borrowing the money is costlier for private firms.

It is also shown in Table 3.1 that the company *size* and *tangibility* of a firm are negatively and significantly affecting the cash holdings of private firms. At the same time, *sales growth* is positively correlated with the dependent variable. These estimations are consistent with Gao et al.'s research, in which the companies with higher sales growth hoard more cash but the larger firms accumulate less. When it comes to the *leverage* - debt indicator variable, it is found to harm cash holdings. However, higher leverage ratio would lead companies to hold more cash reserves to decrease the debt level. A negative correlation between leverage and cash reserves is consistent with both free cash flow and pecking order theories (Ali and Yousaf 2013). A significantly high level of leverage in private firms can be explained by the fact that these companies do not have access to the public equity market like public firms. Consequently, they must rely on debt more (Bray, 2009 and Asker et al. 2012).

Next, I check the effect of the interaction of independent variables on cash holdings. Among all possible interactions, I selected the interaction of Attack (t-1) with Tangibility and ROA; followed by Attack (t-2) with Tangibility, Leverage and Size; and Attack (t-3) with Tangibility, ROA and

ROE. These selections are according to the prior researches, which are discussed after the models below.

The new findings based on different interactions are quite multifaceted. Table 3.2 demonstrates the estimations of a new model, including two separate interactions with *Attack (t-1)* in the 1st and 2nd column accordingly:

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\beta_4 Attack_{(t-1)}*Tangibility+\varepsilon_t \quad (2)$$

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\beta_4 Attack_{(t-1)}*ROA+\varepsilon_t \quad (3)$$

With reference to the Drobetz & Grüninger (2007) study, tangibility negatively sways cash holdings, which is also proved by Uyar & Kuzey (2014) for the Turkish market. Later in 2019, similar findings are shown by Jebran et al. - a significant and negative correlation between cash holdings and tangibility. The scholars also state the reason for this negative correlation: being able to sell tangible assets when they need cash promptly or using them as collateral while issuing debt. My results cohere with the prior literature and add a new perspective that cyber-attacked firms with more tangibility decrease cash holdings more than the firms with no attack at (t-1). In other words, the effect of tangibility on cash holdings depends on if the firms are attacked or not. If a firm is attacked and tangibility is lower, then cash holdings do not decrease as much as it would if the tangibility was higher for the same attacked companies.

When it comes to including the interaction of return on assets and attack at (t-1), I detect that the attacked firms with higher ROA do increase their cash holdings significantly while the same firms with no attack do decrease their cash reserves at 10% significance level. In other saying, the impact of ROA is also dependent on the occurrence of a data breach.

While reviewing the prior studies about the relation of ROA and cash holdings, multifarious results came up. Arena et al. (2011) describe ROA as a reflection of companies' overall performance. This result of negative impact is in line with Thu et al.(2018) who also attained a negative interrelation between return on asset and cash reserves in the Vietnamese stock market. The trade-off theory also supports this negative impact of ROA on cash holdings (Ozkan et al., 2004, Kim et al., 1998). However, some of my analyses indicate a positive relationship, supported by the pecking order theory (Almeida et al. 2004). The same correlation is proved in the research of Ogundipe et al. (2012) as well. Thus, ROA has mixed effects on cash reserves and the impact is significantly dependent on attacks at (t-1) and (t-3) (Table 3.2 and Table 3.4).

Next, I consider the interaction of attacks that happened at (t-2) with Tangibility, Leverage and Size. The empirical results are listed in Table 3.3. The new regression equations are below:

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\beta_4 Attack_{(t-2)}*Tangibility+\varepsilon_t \quad (4)$$

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\beta_4 Attack_{(t-2)}*Leverage+\varepsilon_t \quad (5)$$

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\beta_4 Attack_{(t-2)}*Size+\varepsilon_t \quad (6)$$

Although the leverage itself is found to have a negative impact on cash holdings, it increases the cash holdings while interacting with Attack (t-2) variable. In other words, leverage can only raise the firms' cash reserves which were cyber attacked two years ago.

When it comes to the interaction of size and attack at (t-2), it still affects the cash holdings adversely but with less significance. In other saying, being attacked at (t-2) decreases the severity of the decrease in cash reserves, which is related to firms' size. Prior studies also prove that size is negatively correlated to cash holdings (Al-Najjar 2013, Ferreira & Vilela 2004). This finding is

supported by the pecking order theory, which promotes the idea that small firms have fewer credit limits, consequently, higher interest expenses and costly external funding. Hence, small firms save more cash reserves against possible financial distress (Al-Najjar & Belghitar, 2011).

Table 3.4 reports the results for the following regression models:

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\beta_4 Attack_{(t-3)}*Tangibility+\varepsilon_t \quad (7)$$

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\beta_4 Attack_{(t-3)}*ROA+\varepsilon_t \quad (8)$$

$$CH_t=\beta_0+\beta_1 Attack_{(t-1)}+\beta_2 Attack_{(t-2)}+\beta_3 Attack_{(t-3)}+\beta' X_{(t-1)}+\beta_4 Attack_{(t-3)}*ROE+\varepsilon_t \quad (9)$$

I have explained the impact of interactions of Tangibility and ROA with attacks in the previous paragraphs. Explanations are valid for these models, too, since the results are in line.

When it comes to our new interaction variable – ROE, it is found to have a significantly negative effect on cash balances while interacting with Attack at (t-3). ROE measures the expected profitability of a firm (Palazzo 2012). Both return on asset and equity seem to have a similar explication since they both measure the profitability, but the analyses show a remarkable difference in the impacts of these variables. The essential difference between ROE and ROA is considering the debt of a firm.

Although there are limited studies on the relation of ROE and cash holdings, the found correlation is in line with the previous research of Al-Najjar, who find opposite relevancy (contradictory with pecking order theory) between profitability and cash holdings for US sample. Whereas, the positive correlation is ascertained during a study conducted in Brazil by Manoel et al. (2018). Another interesting study is undertaken by Fernandes et al. (2020), who deduced a concave and nonmonotonic rapport between the aforesaid variables while investigating the impact of cash

reserves on profitability, which is a reverse of our test. The discussed studies have various findings pursuant to different industries, periods, locations, which lead to the need of future research. It is also worth noting that the impact of return on equity in my analyses is material only when there is a data breach at (t-3), which should be studied particularly in times to come.

Lastly, Table 4 displays the empirical outcomes of robustness check. Cash holdings of financial firms and banks are regulated, which could mislead analyses (Garg). Therefore, I select and employ only financial firms and banks' observations according to their two-digit SIC code. The test indicates that my conclusions are robust regardless of the industry.

6. Conclusion

This research analyzes the cyber attacks occurring between 2015 and 2019 and the associated effects on private firms' cash holdings. The previous investigations concentrate on the short-term market reactions to cybercrime events even though it is shown that experiencing long-term financial impacts on companies is also possible. Additionally, there is no known research discussing the effect of cyberattacks on private firms. This thesis aims to fill this gap by providing empirical evidence of the financial impact of data breaches on private organizations. It is evident that breached public firms experience increased cash holdings for at least three years after an incident (Garg), which I also investigate for the private firms by noting the last three years' data breach events. According to Boasiako & Keefe, the current empirical finance literature has not dealt with cyber incidents and security regulations elaboratively, in spite of stupendous media attention to data breach events.

My empirical findings are essential since the firms estimate their budgets and adjust their cash keeping strategies to overcome cybercrime events. My research aims to contribute to businesses, consumers and legislators while facing such unlikeable incidents. Additionally, financial managers, consultants and investors get benefit from this study's findings.

This research provides a detailed introduction to a cyber incident phenomenon facing businesses nowadays and their prudent actions. I find a significant correlation between cash reserves and the attacks that occurred two years ago. Also, the attacks in the last year interact with tangibility and ROA of a firm separately and affect cash hoardings positively. Whereas, tangibility, leverage and size affect the cash holdings significantly while interacting with attacks that occurred two years ago. Furthermore, tangibility and profitability (ROA and ROE) of a firm are found to affect adversely and considerably its cash hoarding if there was a data breach event three years ago.

However, the analyses do not show any direct impact of last year's cyber incidents on firms' cash holding behaviour which is in contrast with the prior researches on public firms. The reason to this contradiction is shown to be rooted in the different cash hoarding strategies of public and private firms. Because holding more cash is comparatively costlier for private organizations, which brings down the precautionary motives (Mortal et al.). In sum, high borrowing costs (Mortal et al. and Saunders & Steffen 2011), expensive lines of credit (Campello et al. 2011) and fewer agency conflicts (Gao et al.) lead to low cash hoardings in private firms.

Despite significant enhancements to the current literature, this study still has some *limitations*. First, the used sample is not large because it is restrictive to find all private companies who have both publicly announced their data breach accident and shared their annual statements. In other words, I face the constraint of data collection, which can be improved and extended by *future* scholars. Covering more years would bring up new impressive outcomes since it will include significant and minor crises and other important happenings in the USA over the years. Second, this study has only focused on US businesses, the results of which might vary across different locations. Even, updated findings can be generalized for developed and emerging markets down the line. More further studies are required to define the ways for companies to apply cybersecurity solutions in a detailed and timely manner. Since the private sector continues to be a high-profile target for cybercriminals, cybersecurity strategies will always be demanded research area. Lastly, how the risk management should decide to address past and potential future attacks will be the critical question for many years to come.

7. References

Acharya, V., Davydenko, S. A., & Strebulaev, I. A. (2012). Cash holdings and credit risk. *The Review of Financial Studies*, *25*(12), 3572-3609.

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

Adonis, R. (2016). *An empirical investigation into the information management systems at a South African financial institution* (Doctoral dissertation, Cape Peninsula University of Technology).

Al Saadi, T. (2016). *Cyber terrorist finance methods* (Doctoral dissertation, Utica College).

Ali, A., & Yousaf, S. (2013). Determinants of cash holding in German market. *Journal of Business and Management*, *12*(6), 28-34.

Almeida, H., Campello, M., & Weisbach, M. S. (2004). The cash flow sensitivity of cash. *The Journal of Finance*, *59*(4), 1777-1804.

Al-Najjar, B. (2013). The financial determinants of corporate cash holdings: Evidence from some emerging markets. *International business review*, *22*(1), 77-88.

Al-Najjar, B., & Belghitar, Y. (2011). Corporate cash holdings and dividend payments: Evidence from simultaneous analysis. *Managerial and decision Economics*, *32*(4), 231-241.

Arena, M. & Julio, B. (2011). *Litigation risk, cash holdings, and corporate investment*. Working paper, Marquette University and London Business School.

Arena, M., & Julio, B. (2011). Litigation risk, cash holdings, and corporate investment. *Marquette University and London Business School Working Paper*.

Asker, J., Farre-Mensa, J., & Ljungqvist, A. (2011). *Comparing the investment behavior of public and private firms* (No. w17394). National Bureau of Economic Research.

Biller, J. T. (2012). Cyber-terrorism: Finding a common starting point. *Case W. Res. JL Tech. & Internet*, *4*, 275.

Boasiako, K. A., & Keefe, M. O. C. (2020). Data breaches and corporate liquidity management. *European Financial Management*.

Brav, O. (2009). Access to capital, capital structure, and the funding of the firm. *The Journal of Finance*, *64*(1), 263-308.

Campello, M., Giambona, E., Graham, J. R., & Harvey, C. R. (2011). Liquidity management and corporate investment during a financial crisis. *The Review of Financial Studies*, *24*(6), 1944-1979.

Clement, J. (2020). U.S. Data Breaches and Exposed Records 2020. *Statista*, 1 Oct., www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-ofbreachesandrecordsexposed/#:~:text=In%202019%2C%20the%20number%20of,164.68%20million%20sensitive%20records%20exposed

Coram, S. (2018). *Data breaches and the financial impacts on firms* (Order No. 11017760). Available from Business Premium Collection; ProQuest Dissertations & Theses Global. (2151555237). Retrieved from https://searchproquestcom.proxy.bib.uottawa.ca/dissertations-theses/data-breaches-financial-impacts-on-firms/docview/2151555237/se2?accountid=14701

Coronado, A. S. (2012). Market reactions to publicly announced privacy and security breaches suffered by companies listed on the United States stock exchanges: A comparative empirical investigation.

Cost of a Data Breach Study. (2020). *IBM*, www.ibm.com/security/data-breach.

Devlin Barrett et al. (Feb. 7, 2011). *Nasdaq Confirms Breach in Network*, Wall St. J. http://www.wsj.com/articles/SB10000142405274870398950457612863256880233 2

Drobetz, W., & Grüninger, M. C. (2007). Corporate cash holdings: Evidence from Switzerland. *Financial Markets and Portfolio Management*, *21*(3), 293-324.

Duncan, A. (2015). *Hackers steal 1 billion personal data points* – IBM.

Dzung, D., Naedele, M., Von Hoff, T., & Crevatin, M. (2005). Security for industrial communication systems. *Proceedings of the IEEE*, *93*(6), 1152-1177.

Fernandes, G., dos Santos Mendes, L., & de Oliveira Leite, R. (2020). Cash holdings and profitability of banks in developed and emerging markets. *International Review of Economics & Finance*, *71*, 880-895.

Ferreira, M. A., & Vilela, A. S. (2004). Why do firms hold cash? Evidence from EMU countries. *European financial management*, *10*(2), 295-319.

Gande, A. & Lewis, C. (2009). Shareholder-initiated class action lawsuits: Shareholder wealth effects and industry spillovers. *Journal of Financial and Quantitative Analysis*, 44, 823–850.

Gao, H., Harford, J., & Li, K. (2013). Determinants of corporate cash policy: Insights from private firms. *Journal of Financial Economics*, *109*(3), 623-639.

Gao, H., Harford, J., & Li, K. (2017). CEO turnover–performance sensitivity in private firms. *Journal of financial and quantitative analysis*, *52*(2), 583-611.

Gao, H., Li, K., & Lemmon, M. L. (2012). Are CEOs in public US firms overpaid? New evidence from private firms. *New Evidence from Private Firms (March 15, 2012)*.

Gao, W., Ng, L., & Wang, Q. (2011). Does corporate headquarters location matter for firm capital structure?. *Financial Management*, *40*(1), 113-138.

Garg, P. (2019). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*.

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

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13-20.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 817-885.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85-105.

Jebran, K., Iqbal, A., Bhat, K. U., Khan, M. A., & Hayat, M. (2019). Determinants of corporate cash holdings in tranquil and turbulent period: evidence from an emerging economy. *Financial Innovation*, *5*(1), 3.

Joe Myers. (2019). "These Are the Biggest Risks Facing Our World in 2019." *World Economic Forum*, www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/

Johnson, K. N. (2015). Managing cyber risks. *Ga. L. Rev.*, *50*, 547.

Johnson, K. N. (2017). Innovating to new heists: regulating cyber threats in the financial services industry. *The Most Important Concepts in Finance.* Edward Elgar Publishing.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). *What is the impact of successful cyberattacks on target firms?* (No. w24409). National Bureau of Economic Research.

Kim, C. S., Mauer, D. C., & Sherman, A. E. (1998). The determinants of corporate liquidity: Theory and evidence. *Journal of financial and quantitative analysis*, 335-359.

Kurt, M. N., Yılmaz, Y., & Wang, X. (2018). Real-time detection of hybrid and stealthy cyber-attacks in smart grid. *IEEE Transactions on Information Forensics and Security*, *14*(2), 498-513.

Labbé, A. (2018). PRIMER: Banks and cyber security (part 1). *International Financial Law Review*.

Lei, J., Qiu, J.,Wan, C., & Yu, F. (2018). *Credit risk spillovers and cash holdings.* Claremont McKenna College Robert Day School of Economics and Finance Research Paper no. 3140958. Claremont, CA: Claremont McKenna College

Longe, O. B., & Chiemeke, S. C. (2008). CYBER CRIME AND CRIMINALITY IN NIGERIA: WHAT ROLES ARE INTERNET ACCESS POINTS IN PLAYING?

Manoel, A. A. S., Moraes, M. B. C., Nagano, M. S., & Sobreiro, V. A. (2018). Cash holdings and corporate governance: The effects of premium listing in Brazil. *Review of development finance*, *8*(2), 106-115.

Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63-73.

Mester, L. J. (2019). Cybersecurity and Financial Stability.

Morse, E. A., Raval, V., & Wingender Jr, J. R. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263-273.

Mortal, S., Nanda, V., & Reisel, N. (2020). Why do private firms hold less cash than public firms? International evidence on cash holdings and borrowing costs. *Journal of Banking & Finance*, *113*, 105722.

Mshvidobadze, K. (2014). *Cyber bear: Russian cyber threat to its neighbors and America* (Doctoral dissertation, Utica College).

Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre. *Journal of Financial Regulation and Compliance*.

Nicole Perlroth. (Sept. 23, 2016). Yahoo Hackers Plundered Data on 500 Million, NY Times, http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

Ogundipe, L. O., Ogundipe, S. E., & Ajao, S. K. (2012). Cash holding and firm characteristics: Evidence from Nigerian emerging market. *Journal of Business, Economics*, *1*(2), 45-58.

Opler, T., Pinkowitz, L., Stulz, R., & Williamson, R. (1999). The determinants and implications of corporate cash holdings. *Journal of financial economics*, *52*(1), 3-46.

Ozkan, A., & Ozkan, N. (2004). Corporate cash holdings: An empirical investigation of UK companies. *Journal of banking & finance*, *28*(9), 2103-2134.

Palazzo, B. (2012). Cash holdings, risk, and expected returns. *Journal of Financial Economics*, *104*(1), 162-185.

Peng, S. Y. (2018). Private Cybersecurity Standards: Cyberspace Governance, Multistakeholderism, and the (Ir) Relevance of the TBT Regime. *Cornell Int'l LJ*, *51*, 445.

Potì, V., Pattitoni, P., & Petracci, B. (2020). Precautionary motives for private firms' cash holdings. *International Review of Economics & Finance*, *68*, 150-166.

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

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, *49*, 146-154.

Saunders, A., & Steffen, S. (2011). The costs of being private: Evidence from the loan market. *The Review of Financial Studies*, *24*(12), 4091-4122.

Shim, W. (2010). *Interdependent risk and cyber security: An analysis of security investment and cyber insurance*. Michigan State University. Communication Arts and Sciences-Media and Information Studies.

Stankovska, A., Dimitrieska, S., & Stamevska, E. (2019). Finance Innovations. *Economics and Management*, *16*(2), 51-57.

Tally, G. (2009). *Phisherman: A Phishing Data Repository*. Paper presented at the Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications & Technology

The Office of the Privacy Commissioner of Canada's blog. (2019, October 31) "A full year of mandatory data breach reporting: What we've learned and what businesses need to know" [Blog post] Retrieved from: https://www.priv.gc.ca/en/blog/20191031/

Third, A., Forrest-Lawrence, P., & Collier, A. (2014). Addressing the Cyber Safety Challenge: from risk to resilience.

Thu, P. A. (2018). Factors effect on corporate cash holdings of the energy enterprises listed on Vietnam's stock market.

Turk, R. J. (2005). *Cyber incidents involving control systems:* Idaho National Engineering and Environmental Laboratory.

Uyar, A., & Kuzey, C. (2014). Determinants of corporate cash holdings: evidence from the emerging market of Turkey. *Applied Economics*, *46*(9), 1035-1048.

Wada, F. J. (2011). The Impact of Information Communication Technology on Banking Institutions: A Theoretical Policy Perspective of Cyber Crime in Nigeria. *Faculty of the Graduate School Southern University and A & M College Baton Rouge, Louisiana In Part*.

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

8. Tables

Table 1. Distribution of data breaches by year and industry

The table shows the chronological and industry (SIC two-digit codes) order of 205 data breaches occurred between 2015 and 2019 to private firm in the US, covered in Capital IQ. The percentages of successful breaches happened in a given year for each column (industry) are demonstrated in parentheses. The percentage of successful breaches happened in the entire industry between 2015 and 2019 are shown in brackets.

Calendar year	Mineral, construction (10-17)	Manufacturing (20-39)	Electric, gas and sanitary services (49)	Wholesale trade and retail trade (50-59)	Finance (60-69)	Service Industries (70-89)	Housing programs (95)	Total
2015	0 (0.00)	0 (0.00)	0 (0.00)	2 (20.00)	8 (9.00)	23 (23.23)	1 (100.00)	34 (16.67)
2016	0 (0.00)	1 (50.00)	1 (100.00)	3 (30.00)	11 (5.37)	32 (32.32)	0 (0.00)	48 (23.53)
2017	0 (0.00)	1 (50.00)	0 (0.00)	2 (20.00)	11 (5.37)	14 (6.86)	0 (0.00)	28 (13.73)
2018	1 (50.00)	0 (0.00)	0 (0.00)	2 (20.00)	32 (15.61)	14 (6.86)	0 (0.00)	49 (24.02)
2019	1 (50.00)	0 (0.00)	0 (0.00)	1 (10.00)	27 (30.34)	16 (7.84)	0 (0.00)	45 (22.06)
Total	2 (100.00) [0.98]	2 (100.00) [0.98]	1 (100.00) [0.49]	10 (100.00) [4.90]	89 (100.00) [43.63]	99 (100.00) [48.53]	1 (100.00) [0.49]	204 [100.00]

Source: Kamiya et al., 2018

Table 2.1. Summary Statistics A

The table represents summary statistics for a sample of 205 data breaches occurred between 2015 and 2019 to private firm in the US, covered in Capital IQ. This table shows statistics before standardizing our dataset. Appendix A displays detailed descriptions of the construction of the variables.

Variable	Minimum	Maximum	Mean	Median	SD	1st Qu.	3rd Qu.
Cash Holding at t	0.00000	1.00000	0.12118	0.06160	0.1829409	0.01875	0.13085
Sales growth	-10109.194	9244.000	221.449	7.490	1478.982	-0.051	79.919
Size	0.00	85594.00	5878.20	177.77	14157.06	25.57	2153.92
LEVERAGE	0.0000	1.2894	0.5520	0.6018	0.3405219	0.2352	0.8702
ROA	-0.408828	0.368893	0.018678	0.009665	0.08592005	0.002695	0.041613
TANGIBILITY	0.0000	1.0000	0.5355	0.4933	0.3886494	0.1660	0.9904
ROE	-1.23418	2.75378	0.06522	0.06486	0.2894627	0.02296	0.10481

Table 2.2. Summary Statistics B

The table represents summary statistics for a sample of 205 data breaches occurred between 2015 and 2019 to private firm in the US, covered in Capital IQ. This table shows statistics after standardizing our dataset. Appendix A displays detailed descriptions of the construction of the variables.

Variable	Minimum	Maximum	Mean	Median	SD	1st Qu.	3rd Qu.
Cash Holding at t	-0.662375	4.803871	0.000000	-0.325639	1.000000	-0.559883	0.052877
Sales growth	-6.984968	6.100513	0.000000	-0.144666	1.000000	-0.149765	-0.095694
Size	-0.415213	5.630816	0.000000	-0.402656	1.000000	-0.413407	-0.263069
LEVERAGE	-1.6209890	2.1656842	0.000000	0.1461690	1.000000	-0.9301638	0.9344476
ROA	-4.975615	4.076064	0.000000	-0.104896	1.000000	-0.186018	0.266935
TANGIBILITY	-1.3777699	1.1952432	0.000000	-0.1084611	1.000000	-0.9507592	1.1705125
ROE	-4.488996	9.288130	0.000000	-0.001221	1.000000	-0.145984	0.136792

Table 3.1 Results A (Main)

The table represents estimates of linear regressions in which the dependent variable is cash holding of a firm and no interaction variable is included. The sample consists of 205 data breach events over the period 2015 to 2019. All independent firm-specific variables are measured one year before the event, unless otherwise specified. Appendix A provides descriptions of all variables in detail. P-values are reported in parentheses and robust standard error is used for all the regression to mitigate the risk of heteroskedasticity. "***", "**", "*" and "." denote statistical significance levels at 0.1%, 1%, 5% and 10% respectively.

	Dependent variable: Cash Holdings
Attack (t-1)	0.079619 (0.6002467)
Attack (t-2)	-0.284765 (0.0366712 *)
Attack (t-3)	0.038867 (0.7922122)
Sales Growth	0.067983 (0.0258248 *)
Size	-0.284488 (0.0003468 ***)
Leverage	-0.096599 (0.1516670)
ROA	0.156137 (0.1013067)
Tangibility	-0.276286 (5.64e-05 ***)
ROE	-0.026570 (0.5439382)
Observations	227
Adj R^2	0.1194

Table 3.2 Results B

The table represents estimates of linear regressions in which the dependent variable is cash holding of a firm. Additionally, an interaction of **(1)** *Attack (t-1)* and *Tangibility* and **(2)** *Attack (t-1)* and *ROA* is included. The sample consists of 205 data breach events over the period 2015 to 2019. All independent firm-specific variables are measured one year before the event, unless otherwise specified. Appendix A provides descriptions of all variables in detail. P-values are reported in parentheses and robust standard error is used for all the regression to mitigate the risk of heteroskedasticity. "***", "**", "*" and "." denote statistical significance levels at 0.1%, 1%, 5% and 10% respectively.

	Dependent variable: Cash Holdings	
	(1)	**(2)**
Attack (t-1)	0.020594 (0.8886362)	0.052188 (0.727977)
Attack (t-2)	-0.312366 (0.0253014 *)	-0.270524 (0.048360 *)
Attack (t-3)	0.023730 (0.8731180)	0.037646 (0.797984)
Sales Growth	0.068144 (0.0304204 *)	0.070331 (0.020305 *)
Size	-0.281649 (0.0003643 ***)	-0.293379 (0.000263 ***)
Leverage	-0.093086 (0.1640736)	-0.105423 (0.118245)
ROA	0.161090 (0.0885648 .)	-0.225459 (0.053903 .)
Tangibility	-0.043674 (0.6553876)	-0.280916 (4.332e-05 ***)
ROE	-0.028197 (0.5169276)	-0.026173 (0.548609)
Attack (t-1) * Tangibility	-0.257012 (0.0370144 *)	
Attack (t-1) * ROA		0.395186 (0.003739 **)
Observations	227	227
Adj R^2	0.1208	0.1213

Table 3.3 Result C

The table represents estimates of linear regressions in which the dependent variable is the cash holding of a firm. Additionally, an interaction of **(1)** *Attack (t-2)* and *Tangibility*; **(2)** *Attack (t-2)* and *Leverage* ; and **(3)** *Attack (t-2)* and *Sales* is included. The sample consists of 205 data breach events over the period 2015 to 2019. All independent firm-specific variables are measured one year before the event, unless otherwise specified. Appendix A provides descriptions of all variables in detail. P-values are reported in parentheses and robust standard error is used for all the regression to mitigate the risk of heteroskedasticity. "***", "**", "*" and "." denote statistical significance levels at 0.1%, 1%, 5% and 10% respectively.

	Dependent variable: Cash Holdings		
	(1)	**(2)**	**(3)**
Attack (t-1)	0.136695 (0.3638936)	0.0154716 (0.9129855)	-0.0032466 (0.9825635)
Attack (t-2)	-0.193537 (0.1283938)	-0.3048812 (0.0201971 *)	-0.3287735 (0.0150356 *)
Attack (t-3)	0.028946 (0.8384108)	0.0025502 (0.9856322)	-0.0134396 (0.9276392)
Sales Growth	0.070709 (0.0265146 *)	0.0651922 (0.0291713 *)	0.0526215 (0.1119752)
Size	-0.294648 (0.0003639 ***)	-0.2935251 (0.0002132 ***)	-0.3580618 (0.0003962 ***)
Leverage	-0.086292 (0.1958532)	-0.1240285 (0.0890353 .)	-0.0938719 (0.1619953)
ROA	0.167927 (0.0758421 .)	0.1637875 (0.0846300 .)	0.1619796 (0.0871056 .)
Tangibility	-0.315848 (4.785e-05 ***)	-0.2721840 (6.527e-05 ***)	-0.2814608 (4.892e-05 ***)
ROE	-0.029009 (0.5030998)	-0.0211391 (0.6379646)	-0.0300543 (0.4895439)
Attack (t-2) * Tangibility	0.282112 (0.0178316 *)		
Attack (t-2) * Leverage		0.2245418 (0.0636704 .)	

Attack (t-2) * Size			0.3081860 (0.0320098 *)
Observations	227	227	227
Adj R^2	0.1244	0.1209	0.1207

Table 3.4 Results D

The table represents estimates of linear regressions in which the dependent variable is cash holding of a firm. Additionally, an interaction of **(1)** *Attack (t-3)* and *Tangibility;* **(2)** *Attack (t-3)* and *ROA;* **(3)** *Attack (t-3)* and *ROE* is included. The sample consists of 205 data breach events over the period 2015 to 2019. All independent firm-specific variables are measured one year before the event, unless otherwise specified. Appendix A provides descriptions of all variables in detail. P-values are reported in parentheses and robust standard error is used for all the regression to mitigate the risk of heteroskedasticity. "***", "**", "*" and "." denote statistical significance levels at 0.1%, 1%, 5% and 10% respectively.

	Dependent variable: Cash Holdings		
	(1)	**(2)**	**(3)**
Attack (t-1)	0.086653 (0.5622901)	0.093358 (0.5301889)	0.082184 (0.5843290)
Attack (t-2)	-0.287631 (0.0299423 *)	-0.310166 (0.0211737 *)	-0.306317 (0.0273709 *)
Attack (t-3)	0.054598 (0.7033495)	0.156340 (0.2757415)	0.062634 (0.6512243)
Sales Growth	0.073501 (0.0181602 *)	0.071894 (0.0187543 *)	0.075279 (0.0155872 *)
Size	-0.288224 (0.0003644 ***)	-0.292879 (0.0002444 ***)	-0.287823 (0.0002568 ***)
Leverage	-0.098048 (0.1438506)	-0.106077 (0.1156701)	-0.098519 (0.1424344)
ROA	0.157724 (0.0968204 .)	0.167115 (0.0791601 .)	0.163903 (0.0864289 .)
Tangibility	-0.300744 (5.402e-05 ***)	-0.284054 (3.874e-05 ***)	-0.279742 (4.737e-05 ***)
ROE	-0.026247 (0.5484563)	-0.022532 (0.6094822)	-0.022521 (0.6109723)
Attack (t-3) * Tangibility	0.251007 (0.0604402 .)		
Attack (t-3) * ROA		-0.776229 (0.0004824 ***)	

Attack (t-3) * ROE			-0.911300 (0.0060261 **)
Observations	227	227	227
Adj R^2	0.121	0.126	0.1216

Table 4. Robustness check

The table represents estimates of linear regressions in which the dependent variable is cash holding of a firm. Additionally, I excluded financial firms to check the robustness since their cash holdings are regulated. The sample consists of 115 data breach events over the period 2015 to 2019. All independent firm-specific variables are measured one year before the event, unless otherwise specified. Appendix A provides descriptions of all variables in detail. P-values are reported in parentheses and robust standard error is used for all the regression to mitigate the risk of heteroskedasticity. "***", "**", "*" and "." denote statistical significance levels at 0.1%, 1%, 5% and 10% respectively.

	Dependent variable: Cash Holdings
Attack (t-1)	-0.047918 (0.803189)
Attack (t-2)	-0.361759 (0.026804 *)
Attack (t-3)	-0.151385 (0.336157)
Sales Growth	0.090596 (0.136514)
Size	-0.353219 (0.001404 **)
Leverage	-0.048265 (0.613534)
ROA	0.151715 (0.202358)
Tangibility	-0.299765 (0.001909 **)
ROE	-0.041116 (0.391774)
Observations	126
Adj R^2	0.1062

9. **Appendix A.** Variable Descriptions

Variable	Description
Attack (t-1)	Dummy variable that equals to one if a firm has been breached in the fiscal year and zero otherwise.
Attack (t-2)	Dummy variable that equals to one if a firm had been breached a year before the fiscal year and zero otherwise.
Attack (t-3)	Dummy variable that equals to one if a firm had been breached two years before the fiscal year and zero otherwise.
Cash Holding at t	Cash plus cash equivalents divided by book value of total assets (immediately after the breach year).
Sales growth	Difference in sales revenue amount over a year (before and after a data breach).
Size at (t-1)	Logarithm of sales revenue at the fiscal year (before a data breach).
LEVERAGE	Total debt (short term and long-term liabilities) divided by total assets (before a data breach).
ROA	Net Income divided by total assets (before a data breach).
TANGIBILITY	Total Assets minus intangible assets (=net property, plant, and equipment) divided by total assets (before a data breach).
ROE at (t-1)	Net Income divided by total equity (before a data breach)