Influence board of directors on cyber security

Master Thesis

Name: *Robbert Johannes Benjamin Meeuwisse*

Student number: *481449*

Thesis supervisor: *prof. Jeroen Suijs*

Second assessor: *prof. Jochen Pierk*

Program: *Master Accounting and Finance*

Erasmus University Rotterdam – Erasmus School of Economics

Abstract

The board of directors is a known mitigation of the agency problem. Its job is to control managers and their decisions. To fulfil this job, the board should have enough knowledge about running a firm. An important topic of the last decade is the cyber security of firms. Due to growing amount of data and connectivity of the whole world via the internet, firms are more vulnerable for cyber-attacks. This paper studies if there is a relationship between the background of a board of directors and the cyber security of the firm. The main takeaway is that the presence of a cyber committee and board members with a cyber background is negatively related to the likelihood a firm suffers a data breach. Also the effectiveness of the board itself is studied via three factors: size of the board, fraction of insiders within the board and amount of busy directors in the board. There are mixed effects: the presence of insiders does not have a significant effect; the effect of the presence of insiders is depending on the age of the firm and the effect of the size of the board is not economic significant.

"The content of this thesis is the sole responsibility of the author and does not reflect the view of either the supervisor, second assessor, Erasmus School of Economics or Erasmus University."

Table of Content

1. Introduction

In 2020, the amount of data that exists was about 64.2 zettabytes (= 64.2 trillion Gigabytes). And in 2025 this amount will be tripled! (Holst, 2021). Every day, everybody has something to do with data. For example, a lot of people use social media like Twitter, Facebook and Instagram. Every one of those users give data to those companies.

The major benefit for firms is that they can reduce their costs, operate more efficiently and make better decisions. Unfortunately, there are also some major drawbacks. The combination of huge amounts of data and the connection of the world via the worldwide internet-network makes the data vulnerable for cyber-attacks or unintended disclosure to the wrong party. For example, Acer suffered a ransomware attack in May 2021 and the hackers demanded a ransom of USD 50 million. And KIA Motors had to pay a ransom of 20 million dollars after the attack of February 2021 (Wickramasinghe, 2021). Next to the amount of ransom that a firm needs to pay, the shutdown of the system also causes opportunity costs and reputation damage (Cavusoglu, Mishra, & Raghunathan, 2004). The estimation is that in 2023, there will be 15,4 million cyber-attacks. Therefore it is very important for firms to develop a good cyber security system.

But investments in cyber security are most of the time considered as expensive. The expectation is that in 2026 there will be a global spending on cyber security of more than $260 billion. That it is such a high number implies that it is important to invest the money in the right place, because money is limited. At the beginning of this century, it was shown by KPMG that there were a lot of companies that did not make optimal cyber investments (Gordon & Loeb, 2002).

The way money is used within a company is determined by the CEO and the other members of the management. But, they do not have the direct benefits of the investments, the shareholders do. Managers might be overinvesting because they do not want to take the blame for a cyber-attack due to a lack of investments, or they are underinvesting because the short term results are more important for their bonusses or rewards.

The interests of the managers might not be in line with the interests of the shareholders. This problem also refers to as the agency problem of agency theory (Ross, 1973). This problem is well discussed problem in the literature. The problem causes discrepancy between the managers and the shareholders. Managers act in their own interest and think about their own goals, while shareholders want to benefit from their interest in the company via dividend and profits.

Cyber attacks are something relatively new; the first cyber attack was in 1988 (FBI). And as said before, the amount of data and the worldwide connection is growing rapidly and so is the amount of cyber attacks. Therefore it is important that all the companies have sufficient knowledge about cyber attacks and how to provent those. To oversee the management and their choices, so to mitigate the agency problem, the shareholders can install a board of directors. They will control (and advise) the CEO and managers if that is necessary. To improve the cyber security of a firm, board members with a cyber background, or even a cyber committee might have a positive effect on the cyber security. But when is a board of directors really effective? Shareholders can appoint board members with a cyber background and even a cyber committee, but that all does not make any difference if the board of directors itself is not effective.

Therefore, in this paper the main question is: How does the board of directors influence the cyber security of a company? To answer this, I study the effect of board members with a cyber background, or even the appointment of a cyber committee, on the cyber security of a firm, which is measured by the occurrence of a data breach. But, next to that I also look at some factors that, according to the literature, influence the effectiveness of the board. I look at the independece of the board, the board size and the amount of busy directors in the board (example Fuzi et al., 2015; Fich and Shivdasani, 2006 and Lipton and Lorsch, 1992).

The findings are mostly in line with the main hyptohesis that having a board with a cyber background has a posititive statistic effect on the likelihood that a firm suffers a data breach during the sample period, the effect of the presence of a cyber committee is on average 24.3%. With regards to the effectivinvess of the board, there is no there is no statistic effect for the independece of the board on this likelihood; the effect of presence of busy directors on this likelihood is significantly positive in the sample, but only if the company is old enough; and the size of the board does not have a economic significant effect on the likelihood that a firms suffers a data breach.

The rest of this paper is constructed as follows. In the second part I discuss the relevant literature with regards to cyber security and the agency problem. I also give the reasoning for my hypotheses in this section. In the third part I discuss the methodology I use to test my hypotheses. After that I give a description of the data I use in this research. In the fifth part I give the results and the interpretation of them and in the last part I summarize and conclude.

2. Literature Review

2.1 Cyber security

In this paper, I will look at cyber security within a firm. It is assumable that if a firm has weak cyber security, it will be more vulnerable for cyber-attacks and data breaches. But the definition of cyber security is vague, unclear, and most of the time subjected to circumstances and points of view, see for example the definition in Von Solms & Van Niekerk (2012) (Craigen, Diakun-Thibault & Purse, 2014). In the end, they come up with a new definition of cybersecurity which they derived from nine other definitions: “Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights” (Craigen et al., p. 17, 2014). This definition contains a couple of broad terms, but there is one part that might be helpful, namly the part ‘used to protect cyberspace and cyberspace-enabled systems’. This includes, as Craigen et al. (2014) mention, that the the systems should be protected in the broadest sense from all threats.

But what are these threats? There are two common used terms if we talk about such threats: cyber attack and data breach. Those terms are often used interchangelby. According to Hathaway et al. (2012), “a cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose”(Hathaway et al., 2012, p. 826). ‘Any action’ means that the attack may consits of hacking, bombing etc. as long as the goal is to undermine the capabilities of the computer network. According to the ISO, a data breach is defined as follows: “compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed” (International Standards Organisation, 2016, ISO/IEC 27050, 3.3). So, with a data breach you have to think about an external hack or an insider who (by accident) leaks information to the outside world. In this paper I will use the term data breach because it captures the threats in the broadest sense as mentioned above.

Because the definition is pretty vague, it is difficult to directly adress the issue of preventing a data breach. In the early 2000s, KPMG found that companies do not make optimal investements with regards to cyber security (Gordon & Loeb, 2002). Such sub-optimal investments can make a company more vulnerable for data breaches. Those data breaches can have huge costs for the company as a direct effect of the data breach (Gordon et al., 2008). Next to that there might be significant economic effects due to the data breach. There is a negative effect on the stock price and market capitalization of the company, which is even more if the data is highly confidentinal, for example a customer database. Next to the direct effect of a data breach, there is also the indirect effect. If there is indeed a breach in a customer database, than this could cause a decrease in the firm’s future economic performances. (Campbell et al., 2003 and Cavusoglu et al., 2014). So, a sub-optimal investment in cyber secutiry can have an huge impact on a firm’s performances. Something that copmanies realize more and more. See for example that around 80% of the companies in the

2006 CSI/FBI Survey on Computer Crime and Fraud give cyber secutiry extra importance (Gordon et al., 2006).

But there might be a problem in allocating capital to the cyber security. In the end, a CFO decides how much money will be spend on cyber security, but this might give some difficulties for several reasons: 1) cyber systems are attacked frequently and the impact of those attacks might fluctuate heavenly; 2) because of the randomness it is hard to to measure the value of a cyber investment to the company (Chronopoulos, Panaousis, & Grossklags, 2018). Those difficulties can cause a friction between the CFO and the managers responsible for the cyber security (from now on: cyber manager). The CFO has the goal to allocate the capital as efficient as possible, so that the benefits of every investment are at least equal to the costs of that investment. While according to Gordon et al. (2003) the cyber manager wants to prevent the risk of a cyber attack as much as possible, because in the end he/she is responsible for preventing such an attack. But making such such a very expensive investment might not be worthwile (see Gordon & Loeb, 2002). So, in the short term the CFO might make the right choice, he is optimizing the benefits compared to the investments, but in the long run the firm might suffer huge losses from cyber attacks.

2.2 Agency Problem

One of the problems within an organisation is the difference between the interests of the shareholders and the interests of the managers. The main goal of the shareholders is that the company makes profit which creates shareholder value. For this, they hire managers and CEOs to run the daily activities of the company. Unfortunately for them, the managers and CEOs do not always have the interests of the company at heart, but they also look after their own interest. For example, CEOs want to boost short-term profit to increase their bonus, or they focus more on empire building than on developing the company. This problem is also referred to as the agency problem or agency theory.

Corporate governance is important to mitigate this problem. It gives the shareholders (and other stakeholders) ways to have control over the managers of the company to make sure that shareholders' interests are protected (John & Senbet, 1998). The shareholders could protect their own interests via the compensation of the managers. It can be made dependent of certain key performance indicators (KPIs) like sales, profit etc. Via this way the shareholders can decide which KPIs they think are important and influence the manager's behaviour via his compensation (Dalton et al. 2007). They can also include certain forms of equity in the manager's compensation formula. This should cause that the interests of the manager/CEO and the shareholders become more aligned, as the manager/CEO is a shareholder himself (Fama&Jensen, 1983).

Another way to mitigate the agency problem, is that the shareholders can install a board of directors. A lot of research is done on the role of the board of directors, see for example Hung (1998), Zahra and Pearce (1989), Hillman and Dalziel (2004) and Nicholson & Newton (2010). They all come up with several roles for a board of directors. For example, the board can advice managers about certain matters. But, the main role for the board of directors is the one of controlling and monitoring the CEOs and managers. They should control whether the choices and activities of the managers are in line with the preferences of the shareholders. This role is very important it is almost impossible for a single shareholder to monitor the managers himself (John & Senbet, 1998).

In their study, Nicholson & Newton (2010) give two different definitions for controlling; a narrow one and a broad one. In a narrow way it is only about firing and hiring managers and CEOs (Johnson et al., 1996). But in this paper I will use the broad definition that is also about the ability to monitor strategy implementation, approve or disapprove cetrain decisions and investments and rewarding the top management (Hillman & Daziel, 2003; Fama & Jensen, 1983).

2.3 Hypothesis

As said before, the CFO, in the end, decides how much the company invests in cyber security. There are several models to decide which amount is the most optimal amount to invest. See for example the Gordon-Loeb Model (GL-Model) (Gordon & Loeb, 2002). As said before, the cyber manager might want to over invest in cyber secutiry because he or she is respsonsible for preventing a cyber attack. But, if you look at the GL-Model, you can see that there is an optimal investment point where a 'simple' economic principle holds: the marginal costs of the investment are equal to the marginal benefits of the investment (Gorden & Loeb, Figure 1, 2002). This might imply that with simple economics, a CFO can determine the optimal level of investments. But, he does need a cyber manager, because there are two main factors that influence that optimal level: the vulnerability of the information and the expected loss if the the information is 'attacked'. So, it is very important that the cyber managers give a good overview of the reasoning behind their optimal amount of investment. He should inform the CFO in the best way possible.

There are a lot of cyber managers that feel support by their management about investing in cyber security and they indicate that they do not have any trouble to get enough budget for those investments (Moore et al., 2015). But, there are still a lot of COEs that are way to over optimistic about their current level of cyber security (RedSeal, 2016), which implies that you need to have cetrain knowledge about cyber security to be able to correctly judge the cyber security of a firm.

While controlling the firm, the board of directors is responsible for the oversight of the financial performance and to conrol the risk of the firm (the Enterprise Risk Management) (Gale et al., 2022). As cyber security is mostly based on reducing the risk on a cyber attack, this falls in the responsibility of the board of directors. And although the board should not control every single cyber investment and only interfer if there are major decisions to be made (Gale et al., 2022), it is still very important that the board knows what it is all about. The main goal of the board is that the managers act in line with the shareholder preferences. To make this judgement, the board of directors need to have alle the information available underlying the decisions made by management. But, with regards to cyber security, it turns out that 60% of the employees do not report security risks, until it is a serious risk (Martin, 2014). Also, recent studies shows that although boards are getting more involved in cyber security, there are still a lack of knowledge about it (Gale et al., 2022).

So, if there is indeed a lack of cyber security within a firm and the board is not aware of that, due to lack of reporting, or the board is aware and does not know what to do about it, due a lack of knowledge, the firm might be more vulnerable to cyber attacks. This is, of course, something the shareholders want to prevent as much as possible. Therefore they want to install a board that has a positive effect on the cyber security of the firm. This leads to the first hypothesis of this paper:

Hypothesis 1: A firm that has a board of directors with a cyber background has better cyber security.

The main issue in this paper will be the board of directors and their knowledge about cyber security. But it is also important to determine if the board itself is well functioning. There have been a lot of research about the functioning of the board of directors with regards to several subjects. For example, Carter et al. (2003) find that if a board contains more women, the value of the firm increases. And they also find that companies which have more women in their board, are more likely to have other minorities in the board. Fracassi and Tate (2012) study the power of the CEO, and conclude that if the CEO is powerful, he is more likley to have a say in appointing new board members. This could result in more board members that have a tie with the CEO which weakens the monitoring.

There are also studies that say that the monitoring weakens if the board is less independent from the firm. For example, Fuzi et al. (2015) say that independent board members are crucial for the performance of the company. An independent board member is more willing to challenge the CEO or other managers about certain choices, if the member has knowledge about cetrain topics. This implies that if a board has more independent board members with cyber knowledge, they will look more critically at the (lack of) cyber investments of the company, which should improve the quality of those investments.

But, on the other hand, Drymiotes (2007), find that fully independent boards have a negative effect on the firm performance. He find that boards need to have dependent directors to give the whole boards enough incentives to monitor in an effective way. There is also evidence that insiders in the board can be useful to outsiders to evaluate certain investments (Raheja, 2005), they could easier explain to the outside members what the (in)direct effects are of a cetrain investment. Especially cyber related investment might be very complicated to understand and to see the immediate effect of this. So, insiders are necessary for the board to optimally assess cyber related decisions made by the CEO and managers.

Somehow, Fuzi et al. (2015) also support the presence of insiders. This seems contradictionary, but they say, to optimal the firm value and the investments, that the balance between the dependent and independent board members should be guarded. This is also argued by Lipton and Lorsch (1992), they say that the board should exists of at least two-thirds independent directors. Combining this literature leads to the first sub-hypothesis:

Hypothesis 2a: The presence of insiders has a positive but diminishing effect on the cyber security of the firm.

Another issue in the literature about the board of directors is the amount of boards an individual director participate in. In the study of Beasley (1996) is concluded that there is a higher probability that there will be committed fraud within the company if there are more directors that are on multiple boards. Fich and Shivdasani (2006) find that in boards where the board members particiapte in three or more other boards, the firm performance is singnificant lower than in firms in which board members participate in less other boards. They have tested this on either a market performance measure and on an accounting performance measures. In both cases they find a negative relationship between the number of outside boards of a director and the firm performance.

Right across the view of Fich and Shivdasani, is the paper of Ferris et al. (2003). Their main finding is that the Busyness Hypothesis (directors who serve on multiple boards become so busy that they cannot monitor management adequately) does not hold and that having busy directors does not affect firm performance negatively. They even find that announcing a busy director for the first time, has a positive abnormal return.

Paradoxically, both views are supported by other literature. In other literature there is a split based on ‘the age’ of the company. If a company is relatively new, it recently had its IPO, the company has different demands for their board of directors than if a company is ‘old’. Field et al. (2013) say that because of the high amount of boards a busy director participates in, he is more experienced, and is seen as highly qualified for the job, and therefore can be very valuable for a new company. This, because those companies do not have the experience and the network to grow in their industry. But, they also support the view of Fich and Shivdasana by finding that five years after the IPO, there are almost 25% less companies that still have a busy board relative to the year of the IPO. After 10 years this is even more than 36% (see for similar results Cashman et al. (2012) and Ferris et al. (2020)).

How is this converted into a cyber security setting? The main task of the board of directors is, as discussed before, monitoring the CEO and managers. However, a company that recently had its IPO, requires more advising than monitoring. And the company that, for example, is present in the Forbes 500, should have more experienced managers and therfore needs more monitoring than advising (Field et al., 2013 and Ferris et al., 2020). The busyness of the directors might cause a shirking of the monitoring and then especially in cyber security, which is not a common part of the daily business and most of the time very complicated. Therefore this results in the following second sub-hypothesis:

Hypothesis 2b: The older the company, the more a board with busy directors has a negative relationship on the cyber security of the firm.

The last issue I discuss in this paper is one that is about the size of the board. One of the first papers that talks about this subject is the paper of Lipton and Lorsch (1992). They argue that one of the reasons that boards does not function optimal is the size of the board. They believe that if a board has more than ten board members, that this for instance causes a lack of cohesiveness. If a board has a maximum of ten, or preferably a size of eight or nine, they argue that the board should have enough combined knowledge to discuss all the issues arising make well-balanced decisions. So, the board will be beter in monitoring the CEO and managers and therefore improve the firm performance. But, Lipton and Lorsch did not provide any evidence to support their claim, their claim is only based on reasoning.

In the papers that also talk about this subject, there is evidence for the claim Lipton and Lorsch make. So does Yermack (1996) find that companies that have a smaller board have a higher Tobin's Q relative to companies with a larger board. And he also concludes that smaller board causes better financial ratios and stronger CEO performance. As an extension to this study, Eisenberg et al. (1998) find that the results of Yermack (1996) also hold for smaller firms. Yermack could not find a relationship between board size and firm performance with board that has less than six members. But in the study of Eisenberg et al. (1998), they do find this relationship for Finnish small and midsize firms.[1] Another study that confirms this theory is the study of Jenter et al. (2019). They study the effect of a mandatory increase in board members on the firm performance in Germany around the implementation of a new law. Their results indicate that the mandatory increase from 12 to 16 board members if a firm has more than 10,000 domestic employees causes a lower firm performance and a decreasing of the firm value.

Using the theory of Lipton and Lorsch which is supported with the emprical evidence of the studies discussed, I came up with the third subhypothesis of this paper:

Hypothesis 2c: If the board of directors is larger, the cyber security of the firm is worse.

Surprisingly, in the literature there are no studies about the minimum size of the board. All the studies discussed above only talk about the maximum size of the board and that it is better to have a board that is not that big. It is probably impossible to determine the optimal board size. But if we follow the theory of Lipton and Lorsch (1992), then we can say that a board should at least have three directors on it, two outsiders for every insider. But, I think it is common sense to say that a board with three people is inefficient because of the lack of knowledge. So, the closer the board to the 'optimal number' of nine people, the better. And it seems logical that this works two ways and that a small board is also inefficient and causes a worse cyber security. So therefore I will also look at the following hypothesis:

Hypothesis 2c': If the board size is too far from the optimal size, the cyber security of the firm is worse.

[1] Finnish and US boards are very similar and therefore it is assumable that the results for Finnish boards also hold for US boards.

3. Methodology

In this section I discuss the methodology I used to test the hypothesis as discussed in the previous section. I discuss both how I came up with the variables and the method I used to test the relationship between the dependent and independent variable(s).

3.1 First hypothesis

3.1.1 Variables

For the first hypothesis I looked at the background of the board members and the effect of that on the cyber security of the firm. In Figure 1 you see the predictive validity framework that conceptualizes the first hypothesis. Here you can immediately see which proxies I will use for both the dependent and the independent variable.

The independent variable for the fist hypothesis is the cyber background of the board members. To capture this, I used five proxies, four about the background of members of the board and one about the board of directors itself. First, I looked if the company has any cyber related committees. For this, I checked if the name of the committees consists of one of the (group of) words below. If this is not the case, I looked if the description of the activities contains one of those words. And lastly, I looked if any of the roles in the committee contains one of those words. This results in the dummy variable $CyberCommittee$, which either has the value of 1 (the company has a cyber related committee) or the value of 0 (the company does not have a cyber related committee).

- Cyber
- Cybertechnology
- Cyber safety or security
- Computer safety
- Artificial Intelligence
- Software

Next, I looked if the board member has or had any achievements, education, jobs and/or other activities that are cyber related. To check if those are cyber related, I looked if the achievement, description or title of the former job, (description of) degrees, description of other activities contained one of the (group of) words above.

This results in four different variables that count the number of degrees, achievements, former jobs and other activities that are cyber related:

- $Education$
- $Achievements$
- $Jobs$
- $Other\ Activities$

After this I aggregated each of those four director variables per company. This results in four numbers that give the amount of cyber related degrees, achievements, former jobs and other activities for the whole board of directors. For example, if company X has five board members

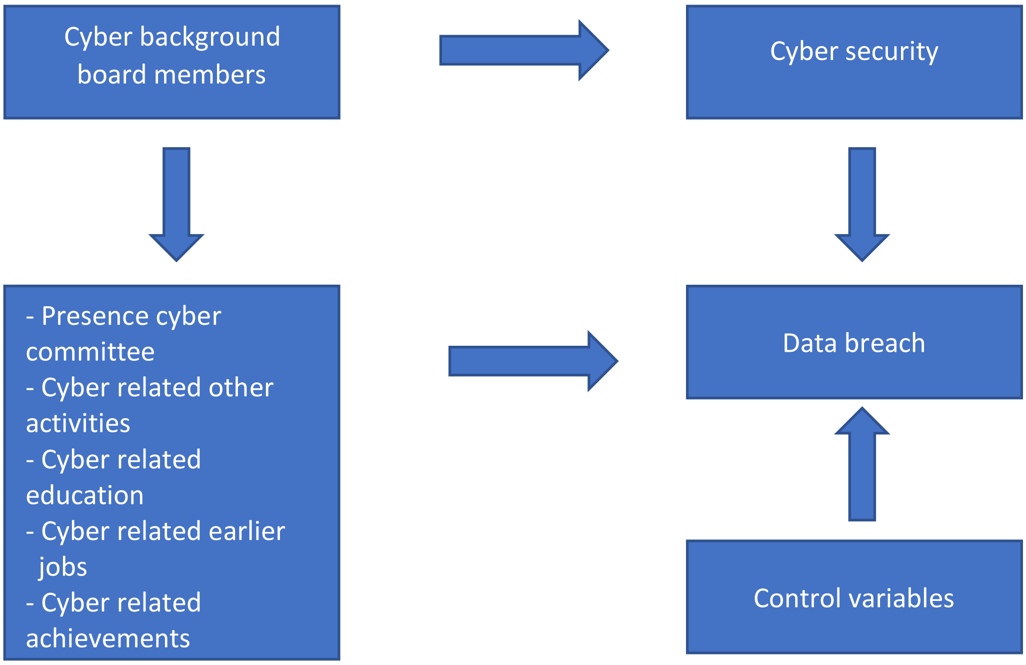
Cyber background board members
Cyber security
- Presence cyber committee
- Cyber related other activities
- Cyber related education
- Cyber related earlier jobs
- Cyber related achievements
Data breach
Control variables

Figure 1: Predictive Validity Framework Hypothesis 1

of which three have one cyber related achievement, the value of the variable $Achievement$ is 3.

The dependent variable is the cyber security of a firm. It is operationalised as the sufferance of a data breach during a certrain year. The variable is a dummy variable that takes the value of 1 in year t if the company suffers a data breach in year t, and 0 otherwise. To illustrate this, an example:

- Company A does not suffer a data breach in period 2005-2007 → variable $Data\ Breach$ takes value of 0 for 2005-2007
- Company A suffers a data breach in 2008 → variable $Data\ Breach$ takes value of 1 in 2008
- Company A does not suffer a data breach in period 2009-2015 → variable $Data\ Breach$ takes value of 0 for 2009-2017
- Company A suffers again a data breach in 2018 → variable $Data\ Breach$ takes value of 1 in 2018

3.1.2 Model

To test the likelihood that the firm suffers from a data breach, the dependent variable has the value 1, I used a binary model. In this case, a non-linear is preferred over a linear model because with a linear model the dependent variable can also take negative values and values greater than one. A non-linear model gives the probability that Y = 1 conditional on the explanatory variables (Savin & Horowitz, 2001). After ruling out the use of a linear model, there is still a choice between a probit and a logit model, both models would suit to tests the hypothesis. There is one difference between the two models: the underlying assumption of the distribution. The probit model assumes a cumulative normal distribution, while the logit model assumes a cumulative logistic distribution. Both models are very similar and only differ in extreme cases (Savin & Horowitz, 2001). In the study of Kamiya et al. (2018) they use a probit model to test if some firms are more likely to suffer from a cyber attack then others. Therefore, I also use the probit model for this study.

In model 1, I looked at the indicator for the presence of a cyber committee and see what this does with the probability that the firm suffers from a data breach. First I look if just the presence of a cyber committee is enough

$$P(Data\ Breach = 1) = \alpha + \beta_1 * CyberCommittee + \varepsilon \tag{1}$$

In model 2, I added the other proxies for the cyber background of the board of directors.

$$P(Data\ Breach = 1) = \alpha + \beta_1 * CyberCommittee + \beta_2 * OtherActivities + \beta_3 * Education + \beta_4 * Jobs + \beta_5 * Achievements + \varepsilon \tag{2}$$

In model 3, I added the control variables which results in the following model:

$$P(Data\ Breach = 1) = \alpha + \beta_1 * CyberCommittee + \beta_2 * OtherActivities + \beta_3 * Education + \beta_4 * Jobs + \beta_5 * Achievements + \beta_6 * ControlVariables + \varepsilon \tag{3}$$

In models 4, 5 and 6, I added an industry and a year effects and looked if those two have an effect on the different coefficients. The fixed effects cannot be used the same as in a lineair regression. This is because of the incidental parameter bias problem (IPP). The technical analysis is beyond the scope of this paper, for this I point to Neyman & Scott (1948) who mentioned this problem for the first time. In any model, if you increase in the ratio of observations to the number of parameters causes the prarameer estimates to converge to their true values. The IPP means that with fixed effects the number of parameters grows with the number of observations. This causes that the estimates can never converge to their true value as sample size increases which makes them unreliable.

I choose to solve this problem by adding the a dummy variable for every industry and year in the regression. This dummy variable gives the effect for every industry and every year on the probability that a company of that certrain industry in that certrain year suffers from a data breach. For the years (2005-2018), I use 13 different dummies, one for every year with 2005 as a baseline year. For the industries, I match the first two numbers of the SIC code of every company within the sample with one of the ten industry categories they belong to. For this classification I used the following industry classes (SIC Code):

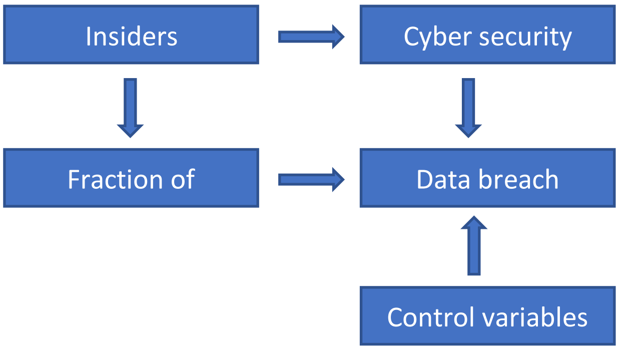

Figure 2: Predictive Validity Framework Hypothesis 2a

- 01-09: Agriculture, Foresty, Fishing
- 10-14: Mining
- 15-17: Construction
- 20-39: Manufacturing
- 40-49: Transportation & Public Utilities
- 50-51: Wholesale Trade
- 52-59: Retail Trade
- 60-67: Finance, Insurance, Real Estate
- 70-89: Services
- 91-99: Public Administration

3.2 Second hypothesis

The second hypothesis tests if there is an influence of certain board characteristics on the cyber security of the firm. In figure 2-4 you can see the predictive validity framework for the conceptualization and operationalization of all the sub-hypothesis.

3.2.1 Hypothesis 2a

The only thing that is different in the three sub-hypotheses, is the independent variable. For hypothesis 2a, I studied the effect of the presence of any insider on the board of directors on the cyber security of the firm (see Figure 2). For this, it is important to know when a board member is labeled as an insider. Partly, the dataset gives an indiciation if the boardmember was also active within in the company, so for these instances it was easy to label the members as insiders. But if this was unclear I looked if the role in the board contains any of the following words: CEO, CFO, COO, executive or other words that indicate that the member is an insder. I also looked the other way around; if the title contains the word ‘independent’, I did not label the member as an insider.

Because in the USA, there is a 1-tier board, insiders will always be present in the board of directors. Therefore the variabale is operationalised as the fraction of insiders in the board. This does not only correct for the fact that there are always insiders in an US board, but it also correct for the size of the board. It is calculated as:

$$FractionInsiders = \frac{Number\ of\ insiders\ in\ the\ board}{Number\ of\ members\ in\ the\ board}$$

For the model, I also used a probit model, because the dependent variable, the probability of a data breach, is the same as before I also included a quadratic term of 'FractionInsiders' to measure the diminishing effect of adding extra insiders.

First I looked at the effect of the two insider terms:

$$P(Data\ Breach = 1) = \alpha + \beta_2 * FractionInsiders + \beta_3 * FractionInsiders^2 + \varepsilon \quad (4)$$

After that, I added all the cyber related proxies[2], control variables and the industry and year dummies. This results in the following final model:

$$P(Data\ Breach = 1) = \alpha + \beta_1 * CyberBackground + \beta_2 * FractionInsiders + \beta_3 * FractionInsiders^2 + \beta_4 * Year + \beta_5 * Industry + \beta_6 * ControlVariables + \varepsilon \quad (5)$$

3.2.2 Hypothesis 2b

For the second sub-hypothesis I studied the effect between having a board with busy directors and the cyber security of the firm. As illustrated in Figure 3, I looked at the number of busy directors in the board. I first had to label the different directors in each board as busy or not busy. I did this in accordance with the study of Fich and Shivdasani (2006) who argue that if a director is active in three or more boards, the firm performance is significant lower than in firms in which board members participate in less other boards. So, if a director is active in three or more other boards, he or she is labeled as busy. Next, I aggregated the number of busy directors per company for every year to create the variable $BusyDirectors$.

I also hypothesize that the effect of busy directors depends on the age of the company. In accordance with the paper of Field et al. (2013), I set the variable Age as the time past after the year of the IPO. In the model I first look at the effect of adding extra busy directors and the aging of the firm. This gives the following model:

$$P(Data\ Breach = 1) = \alpha + \beta_1 * BusyDirectors + \beta_3 * Age + \varepsilon \quad (6)$$

After that, I added all the cyber related variables and the control variables. This gives the following model:

$$P(Data\ Breach = 1) = \alpha + \beta_1 * CyberBackground + \beta_2 * BusyDirectors + \beta_3 * Age + \beta_5 * Industry + \beta_6 * Year + \beta_7 * ControlVariables + \varepsilon \quad (7)$$

But this model is not the model of interest, because in this model you can only look at the separate effect of the age of a company and having busy directors at the board. To see the effect of having busy directors depending on the age of the company, I added an interaction effect between those two variables. This gives the following model:

[2] For simplicity, the cyber proxies are all labelled as 'CyberBackground', in the table I will split those proxies again.

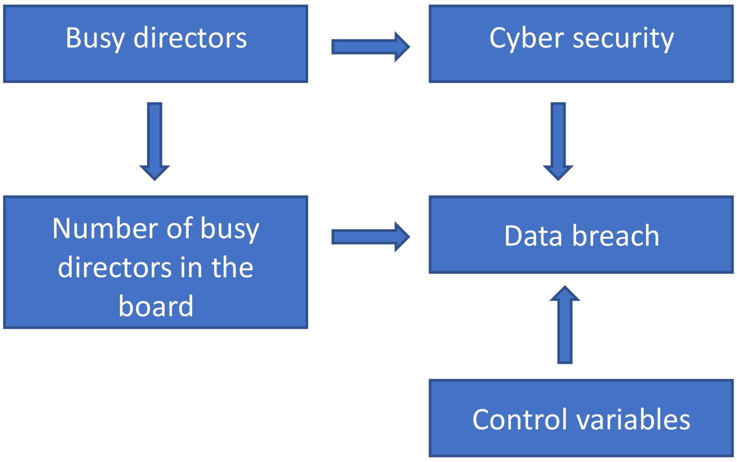

Figure 3: Predictive Validity Framework Hypothesis 2b

$$P(Data\ Breach = 1) = \alpha + \beta_1 * CyberBackground + \beta_2 * BusyDirectors + \beta_3 * Age + \beta_4 * Age * BusyDirectors + \beta_5 * Industry + \beta_6 * Year + \beta_7 * ControlVariables + \varepsilon \qquad (8)$$

3.2.3 Hypothesis 2c

For the last sub-hypothesis, I studied the relation between the size of the board of directors and the cyber security of the firm. In the predictive validity framework (figure 4), I show that I looked at the difference between the actual board size and the optimal board size.

Lipton and Lorsch (1992) argue that the optimal board size is eight or nine, but at maximum ten members. Another possibility might be given by Jenter et al. (2019). They show that the firm performance decreased when the board increases from twelve to sixteen members. Although, this threshold is set because of the regulation change and twelve might not be the ideal size. Therefore I decided to choose for an optimal board size of nine members (the middle of the three from Lipton and Lorsch).

This gives the following variable for hypothesis 2c:

$$\Delta Board\ Size = Actual\ Board\ Size - Optimal\ Board\ Size$$

In the model for hypothesis 2c, I only looked at the positive numbers because I only wanted to see the effect of a board size that is too large compared to the optimal board size.

For hypothesis 2c’, I adjusted the variable as follows:

$$\Delta Board\ Size' = |Actual\ Board\ Size - Optimal\ Board\ Size|$$

I took the absolute value of the difference between the actual and the optimal board size to make sure that also the negative values, when the board size is lower than the optimal, turned into a positive value. To test the hypothesis I used the model 9, only with the use of the other variable.

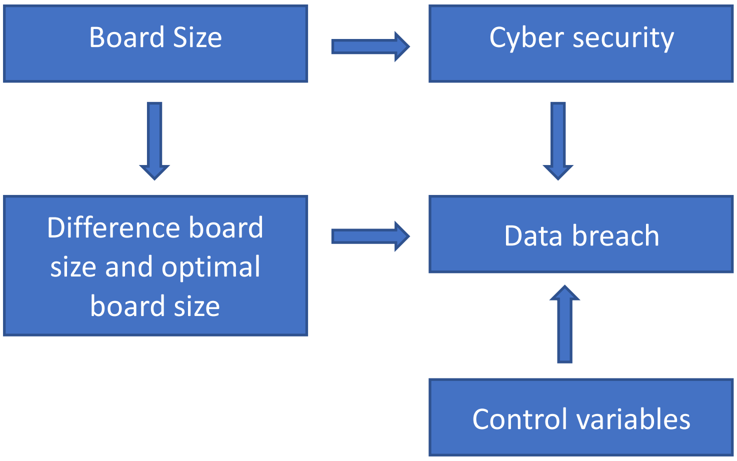

Figure 4: Predictive Validity Framework Hypothesis 2c

The model looked as follows:

$$P(Data\ Breach = 1) = \alpha + \beta_1 * CyberBackground + \beta_2 * \Delta Board\ Size + \beta_3 * Year + \beta_4 * Industry + \beta_5 * ControlVariables + \varepsilon \qquad (9)$$

4. Data

In this paper I used three different databases. I used the database of Privacy Rights Clearinghouse (PRC) to obtain data about data breaches[3] during the period 2005-2018 in the USA. Next to that I used the database BoardEx to obtain data about individual directors that are active in a board of directors and also to obtain data about all those board of directors itself. Last, I used the Wharton Research Data Services (WRDS) to collect data about the financial ratios, revenues and number of employees of the companies in question.

The PRC dataset consists of 9,015 data breaches at 7,625 different companies in the period 2005-2018. In the dataset are also data breaches that occurred at government firms, at educational institutions and at non-profit organizations, those are all removed from the data sample. This leaves 7,267 data breaches at 6,158 different companies. After the removal of the data breaches that are undefined, there are 7,178 data breaches left at 6,108 different companies. After this, I combined this data with the other data about the presence of a cyber committee, the cyber related background, and the proxies for insiders, boards size and busy directors. This leaves a total of 12,792 observations for 1,373 different companies during the period 2005-2018. Among these observations are 1,733 data breaches. See Table I for an overview of the number of data breaches.

As discussed before, I used several proxies to determine if the board of directors has a cyber background. First, I looked if there is a cyber committee in place. In Table II you can see that in about 5.6% of the observations there is a cyber committee in place. Important to understand is that if a company has a cyber committee for several years during the sample period, that these all count as single observations. So, the amount of companies that has a cyber related committee is even less than 77 companies (5.6% of 1,373).

In Table III you can see the descriptive statistics for the other four cyber proxies. You can see that on average, the board members do not have an elaborate cyber background. But there is a small group of board members that have a huge cyber background. This might have several reasons: (1) Cyber security gains more and more importance in the last two decades due to new technologies and the growing attacks on those technologies and some companies are further in the process than others; and (2) the board might rely on a very few, most of the times one, cyber specialists to assess the cyber investments of the company.

[3] For an explanation for this term, look at chapter 1

Table I: Summary data breaches

Type of data breach	Number of data breaches	Percentage of total
Credit card fraud	16	0.9%
Loss of stationary devices	42	2.4%
Insider breaches information	119	6.8%
Not specifiable	152	8.7%
Loss of portable devices	200	11.5%
Unintended disclosure to wrong party	335	19.3%
Physical loss of information	378	21.7%
Hack, malware or ransomware	498	28.7%
Total	**1733**	**100%**

Table II: Presence of cyber committee

Presence cyber committee	Number of firms	Percentage of total
Yes	716	5.6%
No	12.076	94.4%
Total	**12.792**	**100%**

Table III: Individual cyber proxies

Cyber proxy	Minimum	Median	Maximum	Mean
Other cyber activities	0	0	22	0.69
Cyber education	0	0	14	0.81
Cyber achievements	0	0	20	0.46
Cyber jobs	0	0	25	0.74

Table IV: Fraction of insiders, Board Size, Busy Directors and Age

	Minimum	Median	Maximum	Mean
Fraction of insiders	0.06	0.31	1	0.32
Δ Board Size	0	3	18	3.19
Busy Directors	0	4	21	4.13
Age	0	17	192	19.72

Table V: Control Variables

	Data Breach = 1		**Data Breach = 0**		**Total Sample**	
	N = 1,733		N = 9,792		N = 11,525	
	Median	Mean	Median	Mean	Median	Mean
Revenue*	1,296	8,152.74	1,476	10,043.30	1,318	8,549
Employees	3,100	18,237	3,900	21,257	3,200	18,420
Return on Assets	0.1000	0.0774	0.1050	0.0788	0.1030	0.0783
Return on Equity	0.0890	-0.0738	0.0960	-0.0238	0.0930	-0.0418
Return on capital employed	0.1120	0.0528	0.1170	0.0799	0.115	0.0701
Gross Profit/Total Assets	0.2640	0.2849	0.2700	0.2822	0.2680	0.2832
Assets Turn Over	0.7630	0.9626	0.7560	0.8970	0.7580	0.9208

* In millions of dollars

Table VI: Companies per industry

Industry	Amount of companies	Percentage of total
Agriculture, Foresty, Fishing	6	0.5%
Mining	33	2.4%
Construction	26	1.9%
Manufacturing	517	37.7%
Transportation & Public Utilities	92	6.7%
Wholesale Trade	85	6.2%
Retail Trade	99	7.2%
Finance, Insurance, Real Estate	253	18.4%
Services	261	19.0%
Public Administration	1	0.0%
	1,373	100%

Table VII: Observations per year

Year	Amount of observations
2005	780
2006	821
2007	849
2008	841
2009	856
2010	906
2011	934
2012	966
2013	922
2014	978
2015	1003
2016	1020
2017	1074
2018	842
	12.792

Table IV is about the composition of the board. It can be seen that in one third of the observations, about one third consists of insiders. This might imply that companies indeed follow the theory from Lipton and Lorsch (1992). They argue that for every insider there should be two independent directors, so the fraction of insiders should be at max 0.33.

Looking at the difference between the actual and the optimal board size, you can see that on average, the boards have three members to much. And there is even a board that is three times as big as the optimal board size. This might imply that there are boards which are less effective because they are too big.

The next part of Table IV is about the number of busy directors in the board. On average the boards in the sample have four directors that are active in three or more boards. This might imply that a lot of boards have ineffective board members that are participating in too much boards. There is even at least one board that has twenty-one directors that are too busy according to the literature.

The last part of Table IV is about the age of the companies in the sample. There are some companies that went public in 2018, and therefore have an age of 0. But there are also (at least one) companies that are older than 100 years. So, there is a huge difference between the oldest and the youngest company in the sample.

Tables V , VI and VII give the descriptive statistics for the control variables for the total sample and the distribution of the companies in the sample across the industries. I included several proxies for both firm performance and firm size. This to control for differences in cyber security between different kind of firms. Next to that it also gives the statistics for both the years that the firm suffered a data breach and the years that the firm did not suffer from a data breach. It is wort mentioning that there is not an equal distribution between all the industries, this is partly due to the matching based on the SIC codes, but important to remember when drawing conclusions. The distribution of the observations per year is more equal. It is not completely perfect, but every year has at least 780 observations and a maximum of 1074.

5. Results

This section is about the empirical results of the study. Section 5.1 discusses the results about the main hypothesis that a firm has better cyber security if it has a board of directors with a cyber background. Section 5.2, 5.3 and 5.4 will discuss the three (four) sub-hypotheses about the effect of the insiders in the board, size of the board and busyness of the directors.

Before I go to the results, I want to point out which results I am going to interpret. As said before, I used a probit regression to study the several hypotheses. But, there is an issue with the coefficients of the probit model. To explain this, I want to compare the probit model to the linear model. The interpretation of the coefficients of a linear model are quite simple and straight forward: a change in (one of) the independent variable(s), results in a change of the dependent variable with the corresponding coefficient.

The interpretation of the coefficients of a non-linear model, and then especially a probit model, is less straight forward. The coefficient has an effect on the Z-score of the dependent variable. A change in (one of) the independent variable(s), results in a change in the Z-score of the dependent variable with the corresponding coefficient. This is illustrated with an example:

- The dependent variable is $Y = living\ more\ than\ 80\ years$
- One of the dependent variables is $X = smoking\ the\ amount\ of\ cigarettes$
- The coefficient corresponding with X is $\beta_X = -0.037$

This does not mean that the probability of living more than 80 years is decreased by 0.037, this would have been the case if we were dealing with a linear regression. The coefficient of -0.037 in this example is the effect on the Z-score for each observation. To see what the change in probability is, you have to look at the marginal coefficient. In this study I looked at the Average Marginal Effect (AME). For this, you calculate the marginal effect for each individual observation, and take the mean of all those observations. The tables in this part will only show those AMEs, because those marginal coefficients are interpretable.

5.1 Hypothesis 1

For the first hypothesis I looked at the effect of having a cyber committee within the board on the cyber security of the firm. The first model in Table VIII shows that the presence of a cyber committee almost halves the probability that a firm suffers from a data breach. When adding the individual proxies for having a cyber background (model 2), this effect decreases.

After adding those, adding a cyber committee decreases the probability that a company suffers from a data breach with on average 24.3%. The four individual proxies are all significant. After testing for differences, it turns out that only the coefficient related to former cyber jobs and cyber achievements do not differ significantly from each other, in all the other comparisons there turns out to be a statistic difference between the coefficients (see A.1).

Those effects do change if you remove the variable $Cyber\ Committee$ from the probit regression. In this case, the marginal effects of the four individual proxies are as follows: 5.7%

($Cyber\ Education$); 3.8% ($Cyber\ Jobs$); 3.7% ($Cyber\ Achievements$); 2.9% ($Other\ Cyber\ Activities$). These changes seem not that high in absolute numbers, but the relative changes are respectively 62.9%, 22.5%, 32.1% and 38.1%. This implies that the presence of a cyber committee is of huge importance. Something that also follows from the high marginal coefficient of $Cyber\ Committee$.

In model 3, 4, 5 and 6 I first added the control variables and looked if the effects of the proxies are different after adding industry and year dummies. The results are in line with the first hypothesis that having a board of directors with a cyber background on average increases the cyber security of the firm. This supports the vision that having board members with a cyber background increases the awareness within the board about cyber security. This may result in better monitoring certain cyber investments and better communicating with the responsible managers (CFO, Cyber Manager) about the investment (costs) and security (benefits) of those investments to create the optimal amount of cyber investment.

For the industry dummies, only the effect of being active in the Transportation and the Wholesale Trade industry has a significant effect on the probability that one of those companies suffers a data breach, all the other industries do not have a significant effect (model 4).[4] For the Transportation industry the model gives a statistical decrease of 11.5% on average and for the Wholesale Trade the model gives a statistical decrease of 10.4% on average. Within the sample there are hardly any effects for adding year dummies. Only the year 2006 has a positive significant effect, the probability that a company suffers a data breach in that year is on average 3.3% higher than in the other years. It is important to keep Table VI in mind looking at those effects, because the Wholesale Trade and the Transportation industry have only 85 and 92 companies respectively, while there are some industries that contains much more companies and some that have less. The 'perfect' effect can be seen if there are equal amount of companies in every industry class.

[4] For practical purposes, the industries and year dummies are omitted in all tables

Table VIII: Likelihood of experiencing a data breach with respect to cyber background of the Board of Directors

This Table represents the marginal coefficients of the probit regression. The dependent variable takes the value of 1 if a firm suffers from a data breach and 0 if a firm does not suffer from a data breach. The sample consists of 11.525 firm year observations over the period 2005-2018. The Table shows the marginal coefficients and between the brackets the standard errors.

	Dependent Variable = Data Breach					
	(1)	(2)	(3)	(4)	(5)	(6)
Cyber Committee	- 0.473***	-0.243***	-0.241***	-0.240***	-0.241***	-0.240***
	(0.005)	-(0.006)	(0.006)	(0.006)	(0.006)	(0.006)
Cyber Achievements		-0.028***	-0.028***	-0.028***	-0.028***	-0.028***
		(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Cyber Education		-0.035***	-0.033***	-0.033***	-0.033***	-0.033***
		(0.003)	(0.003)	(0.003)	(0.003)	(0.003)
Cyber Jobs		-0.031***	-0.030***	-0.030***	-0.030***	-0.030***
		(0.002)	(0.002)	(0.002)	(0.002)	(0.002)
Other Cyber Activitie		-0.021***	-0.021***	-0.020***	-0.021***	-0.020***
		(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Log Revenue			-0.005	-0.004	-0.004	-0.004
			(0.004)	(0.004)	(0.004)	(0.004)
Log No Employees			-0.004	-0.003	-0.004	-0.003
			(0.004)	(0.004)	(0.004)	(0.004)
Return on Assets			0.023	0.022	0.020	0.019
			(0.020)	(0.021)	(0.020)	(0.021)
Return on Equity			0.000	0.000	0.000	0.000
			(0.001)	(0.001)	(0.001)	(0.001)
Return on Capital			-0.018**	-0.017**	-0.017	-0.015**
Employed			(0.007)	(0.007)	(0.007)	(0.007)
Assets Turnover			0.007	0.010**	0.007	0.010*
			(0.005)	(0.005)	(0.005)	(0.005)
Gross Proft/			-0.013	-0.010	-0.013	-0.010
Total Assets			(0.016)	(0.017)	(0.016)	(0.017)
Pseudo R^2	0.1842439	0.3039038	0.3555618	0.3861316	0.3867251	0.4073059

5.2 Hypothesis 2

In this section I will discuss the three sub-hypotheses as discussed before in this paper.

5.2.1 Hypothesis 2a

The first sub-hypothesis is about the presence of insiders in the board of directors. The hypothesis claims that there is a positive but diminishing effect of the presence of insiders in the board on the cyber security of the firm. First I looked if the fraction of insiders on its own has an effect on the cyber security (Table IX). In model 7 you can see that there is indeed a positive effect on the cyber security. If the fraction of insiders increases with 1, in this sample there is a positive effect on the cyber security of almost 30%. But, the fraction of insiders is between 0 and 1 and the minimum in the sample is 0.06 (see Table IV), so therefore the effect can be at maximum 28%. Next to that, there is indeed a diminishing return. In this sample there is first a decrease in the probability that a firms suffers a data breach, but if the fraction of insiders is above 0.3643 (36.43%) the probability that a firms suffers a data breach is increasing with every extra insider.

This is just little support for the first sub-hypothesis. In all the other models (model 8 till 11) the fraction of insiders does not have a significant effect on the probability of suffering a data breach. So, the first sub-hypothesis is rejected. In this sample, during this sample period, there is no direct effect of the fraction of insiders on the likelihood that the firms suffers a data breach.

5.2.2 Hypothesis 2b

The second sub-hypothesis discusses the effect of having busy directors on the cyber security of the firm, taking the age of the company into account as well. It says that the older the company, the more harm a board with busy directors does to the cyber security.

In model 12, I only looked at the effect of the busy directors and the age to the probability that a firm suffers from a data breach. The results (Table X) show that having a board with one more busy director makes it 2.6% less likely that a company suffers a data breach and that if a company is getting older, the probability that a firm suffers from a data breach decreases a little bit. In model 13, you can see that these effects decrease when adding the cyber related proxies and the control variables.

But, those effects are not the effects of interest. In model 14 till 17, I added the interaction effect of Busy Directors and Age. The meaning of that coefficient is best explained as follows: The baseline effect of having busy directors in the board is when the age of a company is equal to zero. This means that it is 0.8% less likely that a company suffers from a data breach if it has one more busy director and it has an age of zero. If the company is older, for example one year old, the effect of having one more busy director is equal to the marginal coefficient of Busy Directors plus the coefficient of the interaction effect Busy Directors*Age, which is equal to -0.008+0.001*1= -0.007. This means that if a company is one year old, having one more busy director, results in a 0.7% decrease in the probability that the firm suffers a data breach.

Table IX: Likelihood of experiencing a data breach with respect to the fraction of insiders in the Board of Directors

This Table represents the marginal coefficients of the probit regression. The dependent variable takes the value of 1 if a firm suffers from a data breach and 0 if a firm does not suffer from a data breach. The sample consists of 11.525 firm year observations over the period 2005-2018. The Table shows the coefficients and between the brackets the standard errors.

			Dependent Variable = Data Breach		
	(7)	(8)	(9)	(10)	(11)
Fraction of Insiders	-0.298***	-0.154	-0.156	-0.161	-0.160
	(0.75)	(0.188)	(0.190)	(0.189)	(0.191)
Fraction of Insiders	0.818***	0.143	0.148	0.116	0.163
squared	(0.081)	(0.116)	(0.119)	(0.163)	(0.119)
Cyber Committee		-0.244***	-0.244***	-0.243***	-0.243***
		(0.006)	(0.006)	(0.006)	(0.006)
Other Cyber Activities		-0.020***	-0.020***	-0.020***	-0.020***
		(0.001)	(0.001)	(0.001)	(0.001)
Cyber Jobs		-0.025***	-0.025***	-0.025***	-0.025***
		(0.002)	(0.002)	(0.002)	(0.002)
Cyber Education		-0.037***	-0.037***	-0.037***	-0.037***
		(0.003)	(0.003)	(0.003)	(0.003)
Cyber Achievements		-0.026***	-0.026***	-0.026***	-0.026***
		(0.001)	(0.001)	(0.001)	(0.001)
Log Revenue		-0.003	-0.002	-0.003	-0.002
		(0.004)	(0.004)	(0.004)	(0.004)
Log No Employees		-0.009**	-0.008**	-0.009**	-0.009**
		(0.004)	(0.004)	(0.004)	(0.004)
Return on Assets		0.066***	0.065***	0.062**	0.062**
		(0.024)	(0.025)	(0.024)	(0.024)
Return on Equity		-0.001	-0.001	-0.001	-0.001
		(0.001)	(0.001)	(0.001)	(0.001)
Return on Capital		-0.005	-0.006	-0.005	-0.006
Employed		(0.006)	(0.006)	(0.005)	(0.006)
Assets Turnover		0.017***	0.020***	0.017***	0.020***
		(0.005)	(0.005)	(0.005)	(0.005)
Gross Proft		-0.032**	-0.032*	-0.032**	-0.032*
/Total Assets		(0.016)	(0.0187)	(0.016)	(0.017)
Pseudo R^2	0.005887647	0.2984202	0.3386607	0.3395519	0.3597909

Table X: : Likelihood of experiencing a data breach with respect to Busy Directors and the company Age

This Table represents the marginal results of the probit regression. The dependent variable takes the value of 1 if a firm suffers from a data breach and 0 if a firm does not suffer from a data breach. The sample consists of 11,525 firm year observations over the period 2005-2018. The Table shows the coefficients and between the brackets the standard errors. The stars give the significance level of the coefficient.

	Dependent Variable = Data Breach					
	(12)	(13)	(14)	(15)	(16)	(17)
$Busy\ Directors$	-0.026***	-0.005***	-0.008***	-0.008***	-0.008***	-0.008***
	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)
Age	-0.006***	-0.000	-0.000	-0.000	-0.000	-0.000
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
$Busy\ Directors\ *\ Age$			0.001**	0.001**	0.001**	0.001**
			(0.000)	(0.000)	(0.000)	(0.000)
$Cyber\ Committee$		-0.244***	-0.244***	-0.243***	-0.243***	-0.242***
		(0.006)	(0.006)	(0.006)	(0.006)	(0.006)
$Other\ Cyber\ Activities$		-0.020***	-0.020***	-0.020***	-0.020***	-0.020***
		(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
$Cyber\ Jobs$		-0.025***	-0.025***	-0.025***	-0.024***	-0.025***
		(0.002)	(0.002)	(0.003)	(0.002)	(0.002)
$Cyber\ Education$		-0.037***	-0.037***	-0.037***	-0.037***	-0.037***
		(0.003)	(0.003)	(0.003)	(0.003)	(0.003)
$Cyber\ Achievements$		-0.026***	-0.026***	-0.026***	-0.026***	-0.026***
		(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
$Log\ Revenue$		0.001	0.001	0.001	0.001	0.001
		(0.004)	(0.004)	(0.004)	(0.004)	(0.004)
$Log\ No\ Employees$		-0.008**	-0.008**	-0.007*	-0.008**	-0.008*
		(0.004)	(0.004)	(0.004)	(0.004)	(0.004)
$Return\ on\ Assets$		0.060**	0.062**	0.060**	0.057**	0.056**
		(0.024)	(0.024)	(0.024)	(0.024)	(0.024)
$Return\ on\ Equity$		-0.001	-0.001	-0.001	-0.001	-0.001
		(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
$Return\ on$		-0.005	-0.005	-0.005	-0.005	-0.005
$Capital\ Employed$		(0.005)	(0.005)	(0.005)	(0.005)	(0.005)
$Assets\ Turnover$		0.014***	0.014***	0.018***	0.014***	0.018***
		(0.005)	(0.005)	(0.005)	(0.005)	(0.005)
$Gross\ Proft/Total\ Assets$		-0.035**	-0.036**	-0.035**	-0.036**	-0.035**
		(0.016)	(0.016)	(0.017)	(0.016)	(0.017)
$Pseudo\ R^2$	0.0195362	0.2980262	0.368232	0.2991229	0.2993965	0.3002981

This effect will be different for every year, because the company gets older. So, the last year that the marginal coefficient is negative, is when a company is four years old. In this year, it is 0.002% less likely that a firms with one more busy directors suffers a data breach. If a company is five years old, the sign of the coefficient changes; a company is 0.2% more likely to suffer from a data breach if it has one more busy director.

This means that the older the company, the more likely the company is suffering from a data breach if it has more busy directors. This is in line with the hypothesis. An effect of 0.2% might seem economically insignificant, but the average age of the company is 20 years old (see Table IV), the effect is than equal to a 1.2% increase in likelihood of suffering a data breach and this number will be increasing with age. So yes, there is support for the hypothesis, but only if the company is old enough.

5.2.2 Hypothesis 2c

The last sub-hypothesis discusses the board size of the board of directors. It says that if the board of directors is too large, the cyber security is weak. But, as extra part, it also says that if the board size is too far from the optimal size, the cyber security of the firm is weak as well. The first part only looks at boards that are too big, but the latter part also looks at boards that are too small. For this I split the sample in two samples. For model 18 and 21 I only used the observations which have a board size that is more than the optimal board size of nine. In model 19 and 22 I only used the observations that have a board size that is less than the optimal board size and in model 20 en 23 I used the complete dataset (see Table XI)

In panel A, I only looked at the effect of the difference between the optimal board size and the actual board size on the probability that a firm suffers a data breach. For model 18, it can be concluded that with a greater board of directors there is a decrease of 0.8% in the likelihood that a company suffers a data breach. For the whole sample, this is 0.9%. Only in model 19, there is no significant effect.

In Panel B, the more important tests for this hypothesis is done. Here I add all the cyber proxies and the control variables. In model 21 and 23, there is a slightly positive effect on the likelihood a firm suffers a data breach. For model 21 this implies that a board size that is greater than nine results in a 0.2% increase in the likelihood that a firm suffers a data breach. For model 23 this implies that a board size that is further away from the optimal size, results in a 0.2% increase in the likelihood that a firm suffers a data breach. In model 19 and 22 there is no significant effect. This implies that within the sample, during the sample period, a board that is smaller than nine members, does not have a significant effect on the likelihood that a firm suffers a data breach.

So, in two of the three samples there is a minor significant effect, and in the other case there is an insignificant effect. Although those effects are statistically significant, the economic significance of this coefficient is not that high. An effect of only 0.8% is not something a firm will look at first to improve its cyber security. So, economically the effect is not relevant.

Table XI: Likelihood of experiencing a data breach with respect to Board Size

This Table represents the marginal results of the probit regression. The dependent variable takes the value of 1 if a firm suffers from a data breach and 0 if a firm does not suffer from a data breach. For model (18) and (21), the sample consists of 10,490 firm year observations over the period 2005-2018. For model (19) and (21), the sample consists of 688 firm year observations over the period 2005-2018. For model (20) and (23), the sample consists of 11,525 firm year observations over the period 2005-2018. The Table shows the coefficients and between the brackets the standard errors.

PANEL A

	Dependent Variable = Data Breach		
	Larger than 9	Smaller than 9	Absolute difference from 9
	(18)	(19)	(20)
$\Delta Board\ Size$	-0.008***	-0.018	-0.009***
	(0.001)	(0.017)	(0.001)
$Pseudo\ R^2$	0.006882159	0.0009683185	0.008092086

PANEL B

	Dependent Variable = Data Breach		
	Larger than 9	Smaller than 9	Absolute difference from 9
	(21)	(22)	(23)
$\Delta Board\ Size$	-0.002**	-0.008	-0.002**
	(0.001)	(0.014)	(0.001)
$Cyber\ Committee$	-0.240***	-0.265***	-0.243***
	(0.007)	(0.024)	(0.006)
$Other\ Cyber\ Activities$	-0.020***	-0.016***	-0.020***
	(0.001)	(0.005)	(0.001)
$Cyber\ Jobs$	-0.024***	-0.050***	-0.025***
	(0.002)	(0.009)	(0.002)
$Cyber\ Education$	-0.037***	-0.034**	-0.037***
	(0.003)	(0.014)	(0.003)
$Cyber\ Achievements$	-0.025***	-0.028***	-0.026***
	(0.001)	(0.004)	(0.001)
$Log\ Revenue$	-0.004	-0.027	-0.001

	(0.004)	(0.017)	(0.004)
Log No Employees	0.006	-0.033*	-0.008*
	(0.005)	(0.018)	(0.004)
Return on Assets	0.064**	-0.074	0.060**
	(0.030)	(0.057)	(0.024)
Return on Equity	-0.001	-0.001	-0.001
	(0.001)	(0.006)	(0.001)
Return on Capital Employed	-0.002	-0.020*	-0.005
	(0.007)	(0.011)	(0.005)
Assets Turnover	0.020***	0.012	0.019***
	(0.006)	(0.015)	(0.005)
Gross Proft/Total Assets	-0.024	-0.063	-0.031*
	(0.019)	(0.052)	(0.017)
Pseudo R^2	0.2899429	0.4020144	0.2996043

6. Conclusion

Nowadays, companies give more attention to cyber security. But, there is still a lot to learn. This is for several reasons: 1) The definition of cyber security is unclear; 2) The technology, the possibilities with the data and the threats to the cyber systems are developing rapidly and; 3) Because of these reasons there are a lot of companies that do not make the optimal cyber investment. In this paper I first tried to have a clear definition of cyber security. After that I looked at the literature about the so-called agency problem. This well-known problem is the core of the differences in interests of shareholders and managers.

With regards to cyber security this problem arises when the higher management only think about their own bonusses and rewards instead of making the optimal investments with regards to cyber security. One of the ways to mitigate the agency problem is that the shareholders appoint a board of directors. A board of directors should control the CEO and the managers of the company. This includes hiring, rewarding and firing them, monitoring strategy implementation and approving or disapproving certain decisions and investments. A board is better able to control the decisions about certain subjects if it has knowledge about those subjects. And if the decisions are better controlled, the quality of the investments is increased. This leads to the main hypothesis of this paper that a board of directors with a cyber background has better cyber security.

The cyber security of a firm is measured via the likelihood a firm suffers a data breach during the sample period. If a firm does suffer a data breach, its cyber security is assumed to be worse. If the board of directors have a cyber background is measured via the presence of a cyber committee and if the board members have a cyber background. The latter is measured by looking at the individual history of a board member with regards to education, previous jobs, achievements and other activities.

The results show indeed that a firm with a cyber committee has a lower likelihood that this firm suffers a data breach during the sample period (2005-2018). Also, firms with board members with a cyber background have a lower likelihood that this firm suffers a data breach in the sample period.

Next to the main hypothesis, I also looked at three (four) sub-hypotheses with regards to the board of directors itself. I looked at the presence of insiders within the board, the size of the board and the amount of busy directors. It turns out that in the sample there is no significant effect in this sample for the presence of insiders. So, having more insiders does not impact the likelihood that the firm suffers a data breach. The presence of busy directors in the board makes it less likely that the firm suffers from a data breach when the firm is still young, but if the firm becomes older, it becomes more likely that it suffers a data breach. So, this effect is dependent on the age of the firm and grows with the age. Lastly, the size of the board does have a positive significant effect on the likelihood a firm suffers a data breach. Although, this effect is that small that it is economic insignificant.

The main question in this paper was: How does the board of directors influence the cyber security of a company? The main takeaway is that the presence of a cyber committee and board members with a cyber background is negatively related to the likelihood a firm suffers a data breach, and that the factors that effects the functioning of the board itself are mixed. But, that conclusion cannot be copy-paste to practice. There are still some limitations on this paper.

For example, the distribution of the companies across the different industries is not equal. There would be a better picture of possible industry effects if this distribution is equal. It is also very likely that there are more variables that influence the likelihood a firm suffers a data breach. Next to that, during 2007/2008 there was a financial crisis that might influence the behaviour of firms with regards to cyber security, therefore this might be an interesting topic for future research.

Another big limitation is that the research started with 9,015 data breaches and that after matching those breaches to the data about the firms and their board of directors there are only 1,733 data breaches left. Something that highly influences the results. Also, in the models I do not test for the effect of an earlier presence of a data breach. It might be interesting to see if companies suffer multiple times of a data breach during the sample period and what the effect is of a data breach on (the prevention of) a future data breach. In this, it might also be interesting to look at the impact of the different data breaches as names in Table I: is a firm more vulnerable for a hack or for an unintended disclosure to wrong party? And what is the most effective way to mitigate the probability of the different data breaches?

7. References

Beasley, M. S. (996). An Empirical Analysis of the Relation between the Board of Director Composition and Financial Statement Fraud. *The Accounting Review, 71*(4), 443-465.

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

Carter, D. A., Simkins, B. J., & Simpson, W. G. (2003). Corporate Governance, Board Diversity,and Firm Value. *The Financial Review, 38*, 33-53.

Cashman, G. D., Gillan, S. L., & Jun, C. (2012). Going overboard? On busy directors and firm value. *Journal of Banking & Finance, 36*(12), 3248-3259.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2014). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Secutiry Developers. *International Journal of Electronic Commerce, 9*(1), 70-104

Chronopoulos, M., Panaousis, E., & Grossklags, J. (2018). An Options Approach to Cybersecurity Investment. *IEEE Access*(6), 12175-12186.

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

Dalton, D. R. (2007). 'Chapter 1: The FundamentalAgency Problem and Its Mitigation. *The Academy of Management Annals, 1*(1), 1-64.

Drymiotes, G. (2007). The monitoring role of insiders. *Journal of Accounting and Economics, 44*(3), 359-377.

Eisenberg, T., Sundgren, S., & Wells, M. T. (1998). Larger board size and decreasing firm value in small firms. *Journal of Financial Economics, 48*(1), 35-54.

Fama, E. F., & Jensen, M. C. (1983). Seperation of Ownership and Control. *The Journal of Law and Economics, 26*(2), 301-325.

FBI. (sd). *Morris Worm*. Opgehaald van FBI History: https://www.fbi.gov/history/famous-cases/morris-worm

Ferris, S. P., Jagannatha, M., & Pritchard, A. C. (2003). Too Busy to Mind the Business? Monitoring by Directors with Multiple Board Appointments. *The Journal of Finance*, p. 1087-1111.

Ferris, S. P., Jayaraman, N., & Liao, M.-Y. (2020). Better directors or distracted directors? An international analysis of busy boards. *Global Finance Journal, 44*, p. 100437.

Fich, E. M., & Shivdasani, A. (2006). Are Busy Boards Effective Monitors? *The Journal of Finance*, p. 689-724.

Field, L., Lowrya, M., & Mkrtchyan, A. (2013). Are busy boards detrimental? *Journal of financial economics, 109*(1), pp. 63-82.

Fracassi, C., & Tate, G. (2012). External Networking and Internal Firm Governance. *The Journal of Finance, 68*(1), pp. 153-194.

Fuzi, S. F., Halima, S. A., & Julizaerma, M. K. (2016). Board Independence and Firm Performance. *Procedia Economics and Finance, 37*, pp. 460-465.

Gale, M., Bongiovanni, I., & Slalpnicar, S. (2022). Governing cyber security from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*(121).

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security, 5*(4), 438-457.

Gordon, L. A., Loeb, M. P., & Lucyshyn, M. (2003). Information security expenditures and real options: a wait-and-see approach. *Computer Security Journal*(19), 1-7.

Gordon, L. A., Loeb, M. P., Lucyshyn, M., & Richardson, R. (2006). 2006 CSI/FBI computer crimeand security survey. *Computer Security Journal, 22*, 1-2.

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C.-Y., & Zhou, L. (2008). Cybersecurity, Capital Allocations and Management Control Systems. *European Accounting Review*, 215-241.

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C.-Y., & Zhou, L. (2008). Cybersecurity, Capital Allocations and Mangement Control Systems. *European Accounting Review, 17*(2), 215-241.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack . *California law review*, pp. 817-887.

Hillman, A. J., & Dalziel, T. (2003). Boards of Directors and Firm Performance: Integrating Agency and Resource Dependence Perspectives. *Academy of Management Review, 28*(3), pp. 383-396.

Holst, A. (2021, June 7). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025*. Opgehaald van Statista.com: https://www.statista.com/statistics/871513/worldwide-data-created/

Hung, H. (1998). A Typology of the Theories of the Roles of Governing Boards. *Corporate Governance: An international Review*, pp. 101-111.

Jenter, D., Schmid, T., & Urban, D. (2019). Does board size matter? *Working Paper*.

John, K., & Senbet, L. W. (1998). Corporate governance and board effectiveness. *Journal of Banking & Finance, 22*(4), 371-403.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2018, July). What is the impact of successful cyberattacks on target firms. *Working Paper 24409*. Massachusetts: Natinoal Bureau of Economic Research.

Lipton, M., & Lorsch, J. W. (1992). A modest proposal for improved corporate governance. *The Business Lawyer, 48*, pp. 59-77.

Martin, S. (2014, April 16). *Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's 'Serious'.* Opgehaald van International Business Times: https://www.ibtimes.co.uk/cyber-security-60-techies-dont-tell-bosses-about-breaches-unless-its-serious-1445072

Moore, T., Dynes, S., & Chang, F. R. (2015, October 28). Identifying How Firms Manage Cybersecurity Investment. Dallas, Texas, USA: Darwin Deason Institute for Cyber Security.

Neyman, J., & Scott, E. L. (1948, Januari). Consistent Estimates Based on Partially Consistent Observations. *Econometrica, 16*(1), pp. 1-32.

Nicholson, G., & Newton, C. (2010). The role of the Board of Directors: Perceptions of managerial elites. *Journal of Management and Organization, 16*(2), 204-2018.

Privacy Rights. (sd). *Data Breaches*. Opgehaald van PrivacyRights.org: https://privacyrights.org/data-breaches

Raheja, C. G. (2005). Determinants of board size and composition: A theory of corporate boards. *Journal of financial and quantative analysis, 40*(2), pp. 283-306.

RedSeal. (2016, December). RedSeal CEO Survey: Summary & Key Findings . *The Rise of Cyber-Overconfidence in C-Suite*.

Ross, S. (1973). The economic theory of agency: The principal's problem. *American Economic Review*, pp. 134-139.

Savin, H. E., & Horowitz, J. L. (2001). Binary Response Models: Logits, Probits and Semiparametrics. *Journal of Economic Perspectives, 15*(4), 43-56.

SIC Code. (sd). *SIC Codes Lookup - Standard Industrial Classification*. Opgehaald van SIC Code: https://siccode.com/sic-code-lookup-directory

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

Wickramasinghe, S. (2021, November 23). *15 Biggest Cybersecurity Attacks in 2021*. Opgehaald van Privacy Affairs: https://www.privacyaffairs.com/cybersecurity-attacks-in-2021/

Yermack, D. (1996). Higher market valuation of companies with a small board of directors. *Journal of Financial Economics, 40*(2), pp. 185-211.

Zahra, S. A., & Pearce, J. A. (1989). Boards of Directors and Corporate Financial Performance: A Review and Integrative Model. *Journal of Management, 15*(2), pp. 291-334.

8. Appendix

Table A. 1: Statistic Differences Coefficients

	Cyber Achievements	*Other Cyber Activities*	*Cyber Jobs*	*Cyber Education*
Cyber Achievements				
Other Cyber Activities	0.000***			
Cyber Jobs	0.301	0.000***		
Cyber Education	0.024**	0.000***	0.2195	