Cyber security due diligence

How to reduce the information asymmetry between buyer and seller during an acquisition?

Hugo Atzema

February 2018

Abstract

When you buy a car you want to be sure that the brakes work and engine runs. In order to do this there is the possibility to make a test drive or take a look under the hood. When buying a company this is less straight forward because of the intangible character of the qualities of a company. One of the key qualities of modern companies is how it handles and protects its data. If data is considered the engine and cyber security as the brakes to protect it how would an acquiring arty assess the quality of these aspects? That is the main question of this research. In this thesis the current practical methods that are used to assess cyber security at a target company are described. Looking under the hood of a company is called due diligence and this method is also used for assessing cyber security risks. The current practice of due diligence works in silos depending on the requested expertise. The main forms of due diligence investigations are financial, legal and IT due diligence. Because data has become such an important aspect of modern corporate operations assessing cyber security will not be sufficiently covered by one of the three forms of due diligence. Therefore improvements could be made by combining expertise in cross functional teams and by asking better questions. This research has been done by interviewing a number of professionals in M&A sector consisting of investors who have the complete overview of the deal process and specialized experts that rely on their expertise. Combining the views of these two groups' people provided valuable insight into the current M&A practice and taught us how the role of cyber security could be improved.

Table of Contents

Chapter 1: Introduction to the topic

Introduction

Every year more money is being invested by organizations in cyber security in order to prevent data breaches, ddos attacks and other cyber security incidents. Companies are increasingly worried about their cyber security risks and their capabilities to manage them for a variety of reasons. From a layman's point of view this can be very straight forward; keeping criminals out of your network and making sure company-owned data is not getting in the wrong hands should have a certain necessity. There are incentives to invest in cyber security from a compliance point of view with the growing amount of legislation related to cyber security and data protection. Other incentives can be to protect intellectual property of a company or to reduce the risk of bad publicity due to big data breaches. But when we looking into the relationship between cyber security and the value of a company you can ask yourself why these investments in cyber security need to take place. What is the impact of cyber security risks for a company when looking at the complete corporate value?

Quantification of cyber risks remain, until today, the holy grail of cyber security. Many research is being spend on this topic with little and unsatisfying result. Putting a price on cyber security has turned out to be very challenging because of many reasons. The angle, scope and context of quantification researches differ a lot. Many research aims at quantifying cyber security risks for a complete economy of a country or continent.[1][2] Others try to quantify cyber security risks in a certain sector[3][4], all of these quantification exercises are very high level and have no practical approach. This makes it interesting to further investigate the topic from an original angle with a focus on practical execution of

---

[1] Yaakov Weber, Schlomo Tarba, and Christina Öberg, *A Comprehensive Guide to Mergers & Acquisitions*, 2014 <https://books.google.nl/books?hl=nl&lr=&id=YpZKAgAAQBAJ&oi=fnd&pg=PR7&dq=steps+in+M%26A+process&ots=jsB6iUmcDI&sig=EUM8Ab-56YMf-PtetkKfvZp4rOk#v=onepage&q=steps in M%26A process&f=false>.

[2] Linda Musthaler, 'A Cybersecurity Risk Assessment Is a Critical Part of M&A Due Diligence | Network World', 2017 <https://www.networkworld.com/article/3182139/security/a-cybersecurity-risk-assessment-is-a-critical-part-of-manda-due-diligence.html> [accessed 3 February 2018].

[3] D U E Diligence, 'Essential Cyber Due Diligence Considerations in M & A Deals Raised by Yahoo Breach', 2.20 (2016).

[4] Deloitte, 'Cyber Value at Risk in the Netherlands', 2016, 1–42 <https://www.thehaguesecuritydelta.com/images/deloitte-nl-risk-cyber-value-at-Risk-in-the-Netherlands.pdf>.

quantification. The more high level researches result in reports that might be interesting from a scientific, economic or political perspective but it provides no guidance for decision makers at companies who are interested in the value of cyber security risks for their business. And for them who need to make a decision on investments in cyber security want to know how that impacts the value of the firm. This relationship between cyber security and the value of a company is the general topic of this research.

There is literature available on the impact of cyber security on a company's value.[5][6] They give insight on the impact of cyber incidents on the value of a company but focus on stock prices of publicly traded companies. The value of a company based on stock price changes constantly so an important aspect in determining the impact of cyber security incidents and cyber risk management on a company's value is the period or moment in which it is measured. In the life cycle of a company there is a certain moment where the value of a company if being determined in a very precise and clear way. This is when a company is being acquired by investors or merged with another company. When this takes place the company must be valued and risks will be assessed by another party. This moment and the process around Mergers & Acquisitions (M&A) deals is chosen in this research as the setting in which parties assess how cyber security impacts a company's value. By narrowing the topic to this specific moment it provides a scoped course of actions and the possibility of a practical approach.

An M&A process can be divided in several steps, all aiming to eventually make a successful deal for the right price (see literature review in chapter 2 for a more detailed description of all steps). In this process there is one step that is part of every deal that is specifically designed to assess corporate risks of the company at sale. These risks are being investigated during a so-called *due diligence*. It is a type of corporate investigation that is designed to

[5] Ponemon Institute and Accenture, '2017 Cost of Cyber Crime Study', 2017, 56 <https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf>.

[6] Roger D . Feagin, 'THE VALUE OF CYBER SECURITY IN SMALL BUSINESS By Roger D . Feagin A Capstone Project Submitted to the Faculty of Utica College', 2015, 45 <http://0-media.proquest.com.oasis.unisa.ac.za/media/pq/classic/doc/3857701661/fmt/ai/rep/NPDF?hl=smaller,smallest,small,smaller,smallest,small,organisations,organisation,organizations,organization,organisations,organisation,organiz>.

provide insight regarding the risks that are present at a firm. Third parties involved in an M&A deal can use this information to make an informed decision on the course and value of a deal. To determine how current cyber security risks influence the value of a company during an M&A deal the due diligence is chosen as specific area of research.

Research question

The goal of this research is to determine if the current practice during an M&A process provides the right information for an investor to make an informed decision regarding the deal in general, and the deal value in particular. To answer this question concretely the focus will be on the practical methods of due diligence that are currently being used by professionals. The outcomes of these methods will than be evaluated in order to suggest certain improvements.

The main research question will be the following:

1. What methods are currently used to gather the information about cyber security risks at a company during an M&A process and how can it be improved?

This research question can be split in three sub questions:

1a. What are the current methods to assess cyber security risks during an M&A process?

1b. How can these methods be improved in order to provide better information?

Scope

To answer the research questions in a concrete and feasible way there are certain decision made to scope the area of research. These decisions are mainly made because of practical reasons aligned with my research method and to add focus to a quite broad topic

The object of my thesis will be limited by the following criteria:

1. Geographical: this research is limited to the European M&A market. This means that global literature and theories will be used to substantiate this thesis but the object of the research will focus on M&A deals taken place in Europe.

2. Deal types: this research will only focus on acquisitions of privately held companies. This is because at publicly listed companies the gathering of information of a target company is less of a problem due to disclosure obligations of these type of firms.
3. Cyber security risks: cyber security risks in this research are limited to risks associated with personal data[7] of consumers ("consumer data") and explicitly includes privacy risks. Without providing a limited list of threats or risks this research focuses on risks associated with large scale data breaches, non-compliance with (privacy) legislation, inability to use data because of legal restrictions, investments needed to become compliant with (upcoming) privacy legislation.
4. Company types: this research is focused on companies that are in a Business-to-Consumer ("B2C") market, preferably companies that rely heavily on the processing of consumer data. This is because it makes consumer data and important asset to the company and therefore an assumed important factor to into account when deciding on the deal.
5. Acquisitions: there are many (legal) ways to do a merger or an acquisition but in this research the focus will be on acquisitions in which the buying party ("the acquirer") gains ownership of a majority of the shares in a company ("the target").

Relevance of research

The assessment and valuation of the cyber security risks at a target company during an M&A process has become an increasing important topic for investors.[8][9] This is mainly driven by the fact that cyber security risks has become an increasing source of corporate costs.[10][11] This can lead to serious effects for shareholders or investors who are about to become shareholder.[12] Because of this there is a need to assess these risks by investors when they

[7] Personal data is defined by the General Data Protection Regulation (Regulation (EU) 2016/679, article 4.1) : 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[8] Deloitte USA, 'Cyber Risk in Advanced Manufacturing', 2017.

[9] Will Gangewere, 'Assessing the Impact of a Privacy Breach on a Firm 'S Market Value', 2013.

[10] Alessandro Acquisti and Allan Friedman, 'Is There a Cost to Privacy Breaches? An Event Study', in *Ywenty Seventh International Conference on Information Systems*, 2006, p. 23.

[11] By Jill Abitbol, 'Essential Cyber Due Diligence Considerations in M & A Deals Raised by Yahoo Breach', *Cyber Security Law Report*, 2.20 (2016), 1–9.

[12] Klaus Beucher and others, *Cyber Security in M&A*, 2014.

are considering the acquisition of a company. Prior research and available literature taught us that there is an increasing need for a good cyber security due diligence practice.[13][14] There is an increasing amount of literature available that describes the requested output of such a due diligence report but there is no widespread standard and documented method to do this.[15][16] This is a gap in the current knowledge in the world of cyber security and M&A and in this research we will see what current methods are used and how this can be improved. The outcomes of this research can be useful for deal makers, especially on the investment side of the deal table.

Information asymmetry

From an acquirer perspective the whole M&A process is a journey in which it tries to gather as much information about the target company to, in the end, pay the lowest possible price for it. But this information resides at the target company and this party will always aim to receive the highest price for the firm. Hence an information asymmetry that plays a very important role throughout the whole process. Where supply and demand meet there is market just like the players in M&A transactions form a market. And in markets there is always an asymmetry of information that can have certain effects on the players in the market but also on the market as a whole. This phenomenon was analyzed by Nobel price winner George Akerlof in his paper 'The market for Lemons' in 1970. When Akerlof introduced his concept of information asymmetry and the adverse selection problem, he used the infamous example of the market for used cars (in slang: "Lemons").[17] This market was used as example where the seller of a good (in this case a used car) has a knowledge advantage about the quality of the good in respect to the knowledge level of the buyer. Because the buyer is unable to determine the exact quality of the good it has become hard

---

[13] Sasha Romanosky, 'Examining the Costs and Causes of Cyber Incidents', *Journal of Cybersecurity*, 2016, tyw001 <https://doi.org/10.1093/cybsec/tyw001>.
[14] Ashish Garg, Jeffrey Curtis, and Hilary Halper, 'The Financial Impact of IT Security Breaches: What Do Investors Think?', *Information Systems Security*, 12.1 (2003), 22–33 <https://doi.org/10.1201/1086/43325.12.1.20030301/41478.5>.
[15] Kevin M. Gatzlaff and Kathleen A. McCullough, 'The Effect of Data Breaches on Shareholder Wealth', *Risk Management and Insurance Review*, 13.1 (2010), 61–83 <https://doi.org/10.1111/j.1540-6296.2010.01178.x>.
[16] Aswath Damodaran, 'Valuing Young, Start-Up and Growth Companies: Estimation Issues and Valuation Challenges', *SSRN Electronic Journal*, 2009, 1–67 <https://doi.org/10.2139/ssrn.1418687>.
[17] George A Akerlof, The Quarterly, and No Aug, 'The Market for " Lemons ": Quality Uncertainty and the Market Mechanism', 84.3 (2007), 488–500.

to decide on a suitable price for that good. This situation of information asymmetry results in a number of effects, both on the price of a good in a specific trade and on the market as a whole. His theory can be applied to the market for Mergers and Acquisitions, and this is used as the theoretical perspective for this research. The details of this theory, how it exactly links to the M&A market and how assessing cyber security during due diligence fits in it will be discussed in chapter 3. The general takeaway of this theoretical perspective is that an acquirer will always try to gather as much information about the quality of the target firm in order to be able to negotiate the right price. During all steps in the acquisition process, and especially the due diligence part, the knowledge about the target firm increases and therefore the information asymmetry decreases. How this (practically) works for information about a target's cyber security qualities is the main subject of this research.

Case study: Yahoo! Verizon case

Cyber security and the reality of mergers and acquisitions can be quite abstract and intangible. To make the subject of this research tangible the following case study can help. The impact of cyber security and data protection during an M&A process is graphically shown in the Yahoo! acquisition by Verizon in 2016. During this acquisition a rather large data breach of consumer personal data came to light and this has led to a lower price and changes in the deal terms. This shows the relationship between cyber security and privacy concerns at an acquirer and the course and value of a deal. The breach came as a surprise for Verizon at a very late stage of the deal. This raises the question if and how Verizon could have investigated this risk before finalizing the deal, hence the need for cyber security due diligence. [18]

Yahoo!

Yahoo was founded in 1994 by Stanford graduates David Filo and Jerry Yang, completed an initial public offering (IPO) in 1996 and was listed on the global NASDAQ under the ticker symbol "YHOO". The internet giant should be considered as one of the most important companies that played a role in the early development of commercial internet. According to

[18] Roland Trope and Tom Smedinghoff, 'The Importance of Cybersecurity Due Diligence in M&A Transactions', *Business Law Today*, 3.September (2017), 18–20 <https://doi.org/10.1053/j.jrn.2009.05.003>.

Yahoo, its value lies for advertisers in ""a streamlined, simple advertising technology stack that leverages Yahoo's data, content, and technology to connect advertisers with their target audiences. Advertisers can build their businesses through advertisements targeted to audiences on our online properties and services… and a distribution network of third-party entities"[19]. Besides the search engine and free email services there are many other activities that bring value to the company of which many is based on a rather large customer data base. Although this part of the business declined in value a lot to the point that Verizon's was able to acquire it there is another, more profitable, move Yahoo made in its existence. In October 2005 it acquired a share equity position in the Chinese e-commerce giant Alibaba. After its IPO and growth after that share position values around $55 billion.[2021] We should consider this share position as an important part of the business of Yahoo when further discussing the deal with Verizon. Besides the share position in Alibaba Yahoo showed a continues decline in financial results during the period between 2013 and 2015[2223].

The decline in earnings can be found by numerous reasons but in general it did not manage to reinvent itself enough and stay on track of the latest developments[24]. Shareholders wanted to keep their value and therefore actively planned for a spin-off of remaining shares in the Chinese company which basically means selling the core internet activities. The special 'Strategic Review Committee' was formed in January 2016 at Yahoo to facilitate the selling of its operating business. This committee exists of members of the Yahoo management advised by investment bankers of Goldman Sachs and J.P. Morgan and lawyers from Skadden Arps and Wilson Sonsini [25]. From this moment they had a very important say

---

[19] By Jill Abitbol, 'Cybersecurity Due Diligence in M & A Is No Longer Optional', *Cyber Security Law Report*, 2.17 (2017), 1–7.

[20] Steven Mellendez, 'Why Verizon's Due Diligence May Not Have Caught Yahoo's Massive Securi', 2016, p. 1 <https://www.fastcompany.com/3064765/why-verizons-due-diligence-may-not-have-caught-yahoos-massive-security-breach> [accessed 3 February 2018].

[21] By Amy and Terry Sheehan, 'Tackling Cybersecurity and Data Privacy Issues in Mergers and Acquisitions (Part One of Two)', *Cyber Security Law Report*, 1.12 (2015), 1–8; By Amy and Terry Sheehan, 'Tackling Cybersecurity and Data Privacy Issues in Mergers and Acquisitions (Part Two of Two)', *Cyber Security Law Report*, 1.13 (2015), 1–7.

[22] Michael J. Ryan, 'A Car and Brakes: Risk Management Is NOT Risk Avoidance', 2015, p. 1 <http://businessroundtable.org/media/blog/car-and-brakes-risk-management-not-risk-avoidance>.

[23] Colorado Boulder, 'Avoiding Lemons in M & A Deals', 2015.

[24] Yahoo! Inc., 'Yahoo! Inc., Report Filed on Form 10-K for the Fiscal Year Ended December 31, 2015', 2015, p. 171 <http://www.sec.gov/Archives/edgar/data/1011006/000119312514077321/d636872d10k.htm>.

[25] Lucinda Shen, 'Why Yahoo's Alibaba Stock Could Be a Bad Deal for Investors', *Fortune Finance*, 2017, p. 1 <http://fortune.com/2017/06/16/alibaba-stock-yahoo-altaba/> [accessed 16 August 2017].

in the direction of the deal for Yahoo. From February 2016, Financial Advisors of Yahoo were having sort of road shows to actively search for suitable parties that could acquire the operating business.

After a number of rounds in which Yahoo discussed draft offers with possible bidders in the months after, the due diligence continued on mainly financial terms. This resulted in the Strategic Review Committee advised that Yahoo "should proceed to negotiate definitive transaction agreements with Verizon on an expedited basis based upon the following stated and other factors:

a. Verizon's bid offered the highest base purchase price;
b. Verizon had submitted the transaction agreement mark-ups that were most responsive to the Strategic Review Committee's concerns regarding value, certainty of closing, and leaving the post-closing entity with limited liabilities unrelated to the assets retained by Yahoo;
c. Verizon had sufficient funds to finance the transaction, whereas the financing of the financial sponsor bidders was less certain; and
d. Verizon had substantially completed its due diligence review, whereas the financial sponsors needed additional time to complete their due diligence review"[26].

After Yahoo's board adopted this advice they negotiated the terms of the definitive transaction agreements with Verizon all signs on green from financial and legal advisors from both sides. This results in a Stock Purchase Agreement between Verizon Communications and Yahoo Holdings for the outstanding shares of for a cash purchase price of $4,825,800,000 and was signed on July 23 2016.[27]

The Breach

Actually there were two breaches at Yahoo reported short after each other. The first breach came out by a press statement from Yahoo 22 September 2016. The announcement stated that in late 2014 certain user account information was stolen of at least 500 million users. Stolen Information included names, email addresses, telephone numbers, dates of birth, hashed passwords and encrypted and unencrypted security questions and answers. [28] On 14

[26] Deepa Seetharaman, 'Yahoo Looks to Bright Side After Breach - WSJ', 2016, p. 1 <https://www.wsj.com/articles/yahoo-core-revenue-drops-again-1476822440> [accessed 16 August 2017].
[27] Yahoo! Inc.
[28] Deepa Seetharaman.

December 2016 the next data breach of Yahoo was announced. This time the breach occurred in 2013 and affected over 1 billion user accounts. Similar type of personal data was leaked but even less security questions and answers were encrypted which makes it even more intrusive for Yahoo customers. These two breaches gave Yahoo at the time the gold and silver medal in the world championship of data breaches. They were both defeated recently in a dubious race for largest data breaches in history by the River City Media hack that exposed almost 1.4 billion user accounts. [29]

At the time the breaches were announced the largest part of the due diligence had already taken place, the price was defined and the Stock Purchase Agreement was already signed. Therefore there is a lot of controversy around the timing of the announcement of at least the first data breach by Yahoo. Considering that the breach had took place two years before the announcement was made. The news came as a big shock and it was no surprise that Verizon demanded a thorough investigation, started making financial reservations for possible liabilities in the future and in December 2016 the media mentioned that Verizon is seeking a price cut of around $1 billion or even getting out of the deal.[30][31] While this was being discussed between the two parties Yahoo announced in January 2017 that is pushes back the projected closing date with 3 months. [32]

How did the data breach influence the Yahoo Verizon deal?

Both security and M&A specialists who were following this deal were holding their breath waiting on the outcome of the revised deal. By the end of February 2017 both parties announced that the deal price is lowered with $350 million. This price cut is considerable lower than the earlier mentioned $1 billion price cut. The reason can possibly be found in the fact that after the breaches were announced not many customers left Yahoo or complained about it. [33] Additionally, there is an agreement between Verizon and Altaba (the part of Yahoo that remained independent holding the Alibaba shares) that they share

---

[29] Lawrence J Trautman and Peter C Ormerod, 'Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach', *American University Law Review*, 66 (2017), 1–68.
[30] Trautman and Ormerod.
[31] SEC, 'Preliminary Special Proxy Pertaining to a Sale', 2016 <https://www.sec.gov/Archives/edgar/data/1011006/000119312516706578/d206374dprem14a.htm> [accessed 16 August 2017].
[32] Trautman and Ormerod.
[33] Dave Albaugh, 'The Biggest Data Breaches in History - Comparitech', *June* , 2017 <https://www.comparitech.com/blog/information-security/biggest-data-breaches-in-history/> [accessed 16 August 2017].

liability from any future lawsuits from both government organizations and commercial partners. The acquired part of Yahoo by Verizon is already under investigation by the Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) and it is expected that this will lead to fines and maybe other type of financial penalties. [34]

Verizon had other reasons not to push too hard for a new deal with Yahoo. One of them is because the total deal value can be considered 'pocket change' for Verizon. The company spend for instance $11 billion on building out its cellular network in 2016. In the end Verizon needs the Yahoo users in order to become the third player in online advertising (after Google and Facebook). The expected profit made from more detailed information to target customers is apparently worth more than possible damages caused by the data breaches. [35] With all these considerations and arrangements both parties closed the deal in June of 2017.

The impact of cyber security in an M&A deal

The two major changes in the deal after discovery of the breaches were a price cut of $350 million and a split in liability. How the amount of $350 million was established will probably never become public because this was subject of the re-negotiation. It is considerable lower than the $1 billion that was suggested by Verizon just after discovery of the breach. It is suggested that this was because major reduce of users or users' trust did not take place and therefor has no influence to the value of the consumer data of Yahoo!. Looking at the second agreement of liability sharing it strikes that Yahoo and Verizon expect the largest part of the costs as a result of the data breaches will come from law suits and liability claims. These arguments have probably been used during the renegotiations between the two parties but how this exactly took place is very confidential. Therefore it is hard to draw any conclusions regarding the exact price reduction because of a data breach in this case.

What the Yahoo!-Verizon case shows is that there is a connection between the deal value and the cyber security incident that took place. In the aftermath of this deal, specialists in the M&A business reacted by highlighting the necessity of having cyber security risk

---

[34] Claire Atkinson, 'Verizon Wants $1B Discount on Yahoo Deal after Reports of Hacking, Spying | New York Post', *New York Post*, 2016 <http://nypost.com/2016/10/06/verizon-wants-1b-discount-on-yahoo-deal-after-hacking-reports/> [accessed 16 August 2017].

[35] Scott Moritz and Brian Womack, 'Verizon Explores Lower Price or Even Exit From Yahoo Deal - Bloomberg', *Bloomberg*, 2016 <https://www.bloomberg.com/news/articles/2016-12-15/verizon-said-to-explore-lower-price-or-even-exit-from-yahoo-deal> [accessed 16 August 2017].

assessments during an M&A deal.[3637] All with the aim to provide valuable information to the acquiring party with regard to cyber security and privacy risks at a target company. High profile hacks and deals like the Yahoo!-Verizon case boost the attention for strong cyber due diligence.

Information Asymmetry

As described by Akerlof, there is always a certain level of information asymmetry between buyers and sellers in a market. This can lead to negative effects for the market as a whole and therefore there is a need to reduce this asymmetry. While the Yahoo data breaches are still under investigations of numerous federal commissions there are some interesting facts that can help us to assess whether measures against information asymmetry between buyer and seller in the M&A world is tried to be mitigated. In the US there are a number of legislative measures that try to reduce this asymmetry. The most important in the Yahoo case is the duty to disclose that means that if the board of a company is aware of a data breach of the magnitude of the ones at Yahoo in 2013 and 2014 it should disclose that information to shareholders, regulators and most importantly its potential acquirers. There a number of facts that proves that senior management of Yahoo and even the CEO herself was aware of the data breach before the end of July 2016. This was around the time of signing the stock purchasing agreement. Yahoo waited with announcing the data breach until end of September 2016 which will probably lead to a number of claims, even now the deal has already been closed.[38]

We can conclude that the measure against information asymmetry did not work in this case. Verizon did of course his own due diligence but the scope and level of detail of it did apparently not bring any questions with regard to information security at Yahoo. The reason for this can be found in the lack of good practices in these situations. Experienced deal

[36] Matthew Lynley, 'Yahoo Surprises No One by Pushing Back Its Verizon Acquisition Close Date | TechCrunch', *Techcrunch*, 2016 <https://techcrunch.com/2017/01/23/yahoo-unsurprisingly-pushes-back-its-verizon-acquisition-closing-date/> [accessed 16 August 2017].

[37] Brian Fung, 'Why Verizon Is Still Buying Yahoo on Sale , despite That Epic Security Breach', *Washington Post*, 2017, pp. 2–4.

[38] Abitbol, 'Essential Cyber Due Diligence Considerations in M & A Deals Raised by Yahoo Breach'.

makers have already expressed their concerns for this lack of knowledge and this might be subject for further studies [39].

For this example we assume that having a mature level of cyber security risk management is considered a quality aspect of a company. To keep using the automotive sector as an example we should consider a company as if it is a car and risk management as the breaks. Although some people might consider breaks as something that slows down a car you could argue the opposite; breaks enable a car to go fast. Without having proper breaks on a car you will not be able to drive fast in a responsible way. For a company to be profitable and have effective operations it needs to be aware of the risks and therefore risk management is needed[40]. Just as having proper breaks on a car is considered a quality aspect of a car, cyber risk management can be considered a quality aspect of a company. Following this assumption we will also have to conclude that having proper cyber security risk management comes with considerable investments to set it up and maintain it, just as good brakes of a car have costs and need maintenance.

This quality aspect is not obvious for the outside world so there is an information asymmetry between the target company and the acquiring company. To follow Akerlofs theory the adverse selection problem can exist in the corporate control market when it comes to investing in cyber security. Picture this: two firms are on the market, both ready to be acquired. Firm A has invested a lot in cyber security and firm B has not. Due to information asymmetry the investor is unable to determine which company had a certain quality level when it comes to cyber security risk management. Therefore this aspect will not be taken into account when deciding which of the two companies should be the eventual target. Investors will value them in that sense equally. The adverse selection problem might exist here in the fact that companies will not invest in cyber risk management because it will not influence the value of their company. This leads to a general negative effect on the quality of cyber risk management in companies in a market perspective. Another negative effect from the perspective of the investor is that not taking into account cyber risk management when acquiring a firm can lead to unwanted surprises

[39] Jeff Goldman, 'M&A Due Diligence, Cyber Security, and the Massive Yahoo Data Breach', 2016 <https://www.esecurityplanet.com/network-security/ma-due-diligence-cyber-security-and-the-massive-yahoo-data-breach.html> [accessed 3 February 2018].

[40] Ryan.

when these cyber security risks actually materialize once the acquisition has been completed. [41]

[41] Boulder.

Chapter 2: Literature review

The acquisition process

Before we dive deeper in the world of due diligence it is important to place that concept in the overall process of acquiring a company. Because this research focuses on the influence of cyber security on the acquisition of a firm we should not only focus on due diligence or at least be aware of the fact that there are more decisions influencing a deal. In practice, basically everybody can acquire a company and there are some mandatory legal steps someone has to go through before buying the shares of another company. Although these legal requirements are important and play a role in the overall process, in the following section we approach the process from a practical and strategic angle showing what steps are taken from an investor perspective.

There is no single approach for mergers and/or acquisitions worldwide but in general there are certain steps that can be identified. In general there are three stages in which an acquisition will take place:

Stage 1: Planning & strategic management;

Strategic planning

As an acquirer there is a need for having a strategy in place that in which growth through acquisition is the core. Part of that strategy can be the choice for a specific market segment and/or geographic focus. In this stage acquirers set certain strategic goals and focuses on synergy wins for combining their existing business with possible target companies.[42]

Selection

Once the strategy is in place it is time to identify companies that are open for acquisition. Investors have many ways in which they receive information in order to search, screen and select targets. In practice, specialized committees are set up to define the strategic framework in which M&A activities will take place. The use of external consultants and advisors can play an important role in this step.[43] This selection is made based on available information about the market in which it operates and (depending on the situation) some

---

[42] Weber, Tarba, and Öberg.

[43] Brian Coyle, *Mergers and Acquisitions*, ebook (Chicago: AMACOM, 2000) <http://web.a.ebscohost.com.ezproxy.leidenuniv.nl:2048/ehost/detail?sid=1aad445b-9e70-467e-ad74-035644fa333b@sessionmgr4006&vid=0&format=EB&lpid=lp_I&rid=0#AN=52734&db=nlebk> [accessed 10 February 2018].

information about the target company's (financial) performance. [44] There are several sources that can be used:

- "stock market analyst reports for listed public companies
- trade journals and publications
- trade associations
- business literature and online search facilities
- stockholder lists
- research studies
- contacts in the business, or other contacts with knowledge of the potential target, for example investment banks
- published financial accounts
- the company's own publicity brochures or product literature, including its website."[45]

The end of this stage is a shortlist of companies that might be suitable as a target and can be approached.

Stage 2: Negotiations, due diligence and agreement;[46]

The selected group of targets can be engaged, sometimes directly communicating with senior management or through advisors from both sides. During the first exploring conversations there is already the need for the acquirer to gather as much (inside) information about the target.

Valuation of target

Once a certain amount of information is gathered about a target the valuation of that firm can be executed by the acquirer. Valuating a company is partly a pure financial exercise in which the recent and future profits and cash flow are essential. On the other hand, the price of a company is always subject to negotiation between acquirer and target. Before the due diligence and actual negotiation takes place it is common for the acquirer to already have a maximum price for the target calculated. There are many methods to valuate a company:

---

[44] Mohsen Sharifi, Vijay Karan, and Zafar Khan, 'Your M&A Map for Success', *Journal of Corporate Accounting & Finance*, 16.2 (2005), 9–16 <https://doi.org/10.1002/jcaf.20082>.
[45] Coyle.
[46] Weber, Tarba, and Öberg.

a. Discounted Cash Flows (DCF), this method that is based on the present value of the future cash flow capacity that is available for the target which should be discounted using an appropriate discount rate. That discount rate considers the risk related to the business. The risks used for the discount are mainly related to financial risks like change in currency rates or debt and equity costs.[47][48] Other corporate risks, like cyber security risks, are not specifically part of this valuation method.[49][50]
b. Market Approach, her the value of a business is derived from valuation multiples of publicly traded firms in similar lines and transactions of comparable companies. The conditions and prospects of firms in similar lines of business depend on common factors such as overall demand for their products and services, implying that key value drivers like growth and risk should be similar.[51]

These valuation methods give an estimated value of the target and are mainly focusing on the financial situation of a company and its risks. The source for these valuation methods are mainly (historic) financial documents like balance sheets, profit and loss accounts. This information can be enriched by market information that are fed in models of valuation experts. Based on this valuation the price and focus of the key risk areas in the due diligence phase are decided.[52]

Due Diligence

After valuation of the target there is a general perception of what the company looks like and what value it represents based on financial information. This picture of the company will be tested during the due diligence in which more detailed information will be gathered and reviewed. This step of the process will be the main aim of this research and will be described in the following chapter.

---

[47] Damodaran.
[48] By A M Y Finkelstein and Kathleen Mcgarry, 'American Economic Association Multiple Dimensions of Private Information : Evidence from the Long-Term Care Insurance Market Author (S): Amy Finkelstein and Kathleen McGarry Source : The American Economic Review , Vol . 96 , No . 4 (Sep ., 2006), Pp .', 96.4 (2016), 938–58.
[49] Tim Koller, Marc Goedhart, and David Wessels, *Valuation: University Edition*, *Journal of Chemical Information and Modeling*, 2010 <https://doi.org/10.1017/CBO9781107415324.004>.
[50] Don Urbanowicz, 'The Seven Phases of M & A', 2015.
[51] Koller, Goedhart, and Wessels.
[52] Coyle.

Negotiation of deal terms

After due diligence is finalized the acquirer and the owners of the target will negotiate the price and further terms. Topics that are subject to negotiations are resulting from the previous steps in the process, especially the risks and issues following from the due diligence. Once both parties agree on the final terms the agreement will be captured in the Stock Purchase Agreement. Special attention should go to warranties, indemnifications and conditions to closing. These provisions are used to cover certain risks when these are not easy to quantify in the deal value.[53]

Stage 3: Integrating of the organizations.[54]

As with mergers in particular but also acquisitions can result in an integration of two companies, in general the target and (a part of) the acquirer. After the deal is finalized on legal and financial terms the target firm will be integrated with another organization. This is the case when the target is acquired by a company that has a competitive or complimentary position to the acquiring organization. This combination can result in certain synergies that can be a strong reason for an acquisition in the first place. It can also result in risks or other costs when two organizations have to become one. Especially the integration of IT systems can lead to a lot of unplanned costs and are therefore sometimes subject of an IT due diligence.[55]

Due diligence as part of the acquisition process

As described in the introduction, all steps in the acquisition process aims to gather information about the target firm in order acquire it for the right price. To do this the acquiring party wants to investigate the target business. It wants to have reliable information about the business to make an informed decision about the value and other contractual arrangements. Due diligence is the method of choice and can is defined by the American Management Association as "*a process whereby an individual, or an organization, seeks sufficient information about a business entity to reach an informed judgement as to its*

[53] Weber, Tarba, and Öberg.
[54] Weber, Tarba, and Öberg.
[55] Coyle.

value for a specific purpose".[56] It is important to mention that a due diligence is not in itself an audit but is a much broader investigation and much more focused on future profit potential then assessing the past. The investigation is normally divided between two general teams; a financial/strategic team and a legal team. Where the financial team focuses on the financial performance of the target company and is the legal team trying to discover legal issues that may result in impediments to the deal.[57] The higher the quality of information gathered during the investigation, the better informed decision will be made by the acquirer. The outcomes can be quantifiable and may lead to a change in deal value but the majority of the due diligence results are not easily quantifiable.[58] The two main challenges during due diligence are first to get the right information and secondly translate the findings into quantifiable outcomes or other solutions to manage the discovered risks.

Due diligence is never the same and can be very different, depending on the business, market and country in which the target company is operating. Traditional due diligence focuses on tangible assets or other types of information related to the operational side of the company that leads to legal or tax related matters.[59] Both from the field of scientific research and from practical experience there is a trend towards a growing attention of intangible assets because they seems to be a critical factor for the success of mergers or acquisitions.[60] Information regarding leadership, culture, employee retention and environmental issues can be very important for deal makers to have as well. According to the chapters in the American Management Association (AMA) handbook of Due Diligence that lists about thirty different areas that can be in a standard due diligence report with topics ranging from capitalization and ownership, marketing operations, physical distribution, human resources and legal affairs.[61] Very interesting detail is that in all standard checklist provided in the available handbook the terms 'personal data', 'privacy' or

---

[56] Andrew J. Crilly, William M., Sherman, *The AMA Handbook of Due Diligence.* (Americam Management Association, 2010).

[57] Crilly, William M., Sherman.

[58] GE Capital, 'Due Diligence : Main Steps and Success Factors', 2012, 4 <http://www.gecapital.eu/en/docs/GE_Capital_Overview_Due_Diligence.pdf>.

[59] Michael G Harvey and Robert F Lusch, 'EXPANDING THE NATURE AND SCOPE OF DUE DILIGENCE Puterbaugh Chair of American Free Enterprise Helen Robson Walton Chair of Marketing Strategy', 9026.94 (1995), 5–21.

[60] Alen Sacek, 'Due Diligence in Mergers and Acquisitions in Emerging Markets : Evaluated Risk Factors From the Academic and Practical View.pdf', 11.7 (2015), 363–72 <https://doi.org/10.17265/1548-6583/2015.07.004>.

[61] Crilly, William M., Sherman.

'cyber security' is not mentioned once. This is again an indication that this topic is not part of the standard way of working. Topics can of course always be added based on the wishes of the acquirer. What topics have more importance really depends on the attention and focus the acquiring party and specifics of the deal.

Traditional due diligence focuses on financial, legal and regulatory aspects of a business. Usually the acquiring company does an investigations that goes further than reviewing the annual reporting documentation. Other corporate documentation is also subject of due diligence research. To structure this, a Virtual Data Room ("VDR") is being setup by the target company and/or by (the advisors of) the acquirer. Back in the days there was no VDR but a physical room consisting of shelves with folders and binders with information about a company. Now a days this done via an online software as a service platform where acquirer, target and its advisors have access to. In this VDR all kinds or documents can be uploaded by the target upon request of the acquirer. Typical types of documents that can be found in a data room are financial reports and (corporate) contracts but also minutes of meetings of the board and shareholders and overviews of ongoing or finished legal litigation documents. Besides existing documents that are already available at the target company there is also the possibility to do further investigations through interviews with key stakeholders of the target or even technical assessments.[62]

The focus and scope of due diligence investigations are determined by investors and experts together. Lawyers and financial experts normally have a seat at the deal table and together with their clients they determine the areas of interest. The execution of the due diligence is divided between several experts. A financial due diligence will be executed by the financial expert, a lawyer does the legal part and, if decided, an environmental specialist could assess the environmental risks of a deal. The starting point of these investigations are normally existing and available documentation in the data room but will be supplemented with additional research if needed.[63] The result of a due diligence investigation will be captured in a report that shows key findings and possible next steps. These findings will generally be

[62] Vlado Sliskovic, 'Do Virtual Data Rooms Add Value To the Mergers and Acquisitions Process ?', 2007 <http://www.imaa-institute.org/docs/kummer-sliskovic_do virtual data rooms add value to the mergers and acquisitions process.pdf>.

[63] Crilly, William M., Sherman.

categorized per expertise in accordance with the type of due diligence executed. Not always are the results captured in one document or combined report. Especially because different parts of the entire due diligence report is written by different companies that do not necessary work together on it. A law firm provides the legal due diligence and a bank cyber security consultancy firms will conduct his part of the investigation. It is up to the investor to interpret these reports and go back to the negotiation table with it.[64] The risks identified during the due diligence phase can have some possible effects on the deal. When risks are unacceptable for the acquirer it might cause abortion of the deal entirely, the deal value can go down or additional contractual arrangements can be needed.

[64] GE Capital.

Chapter 3: Research method

Based on the literature there is general understanding of the process of an acquisition and the role and position of due diligence it has in it. The main takeaways that are important for the research are the following:

- During the several steps of the acquisition process the information level about the target firm increases depending on the focus of the acquirer during the due diligence.
- Current standard due diligence handbooks and other available literature mainly focuses on gathering financial information and the traditional legal aspects of due diligence.
- Several experts are involved during the execution of the acquisition in general and in due diligence in particular.

This research will investigate how the assessment of cyber security risks has a place in the described course of actions. This section describes how the research tries to answer the main research question: "What methods are currently used to gather the information about cyber security risks at a company during an M&A process and how can it be improved?"

In order to answer the research questions in a practical way the chosen approach has been the execution of semi-structured interviews with professionals in the M&A business. This group of professionals consists of valuators, M&A lawyers, bankers, investors and cyber security professionals. The information that is gathered during these interviews provides a decent overview of the current business standard. Based on the received information from these professionals and available literature we are able to provide recommendations for improvement of the current practice.

Semi-structured interviews are the most appropriate scientific method because there is very little literature available and the topic has a very practical nature. The object and area of this research was expected to be very non-scientific and it lacks existence of scientific theories and literature. Especially because of the practical focus of this research and because the focus is basically on the research of behavior of professionals and their business decisions. Therefore finding out what these professionals do and think via open discussions will lead to the most interesting input for this research.

Interviews:

For the interviews a selection is made of a variety of people with different backgrounds. The interviewees were selected based on two selection criteria: first it was determined whether the person was experienced in M&A deals and secondly it was determined whether they had some experience in M&A deals where personal data and associated (cyber security) risks were involved. Resulting from these criteria the group of interviews consisted of investors, bankers, lawyers and other advisors active in the M&A market.

This complete group of interviewees can be split in two type of people based on their role in the M&A process and how they are involved in the due diligence step:

Group 1: “Investors”

One group is formed by the investors, mostly working for private equity firms, investment funds or having a senior management position at large corporations. This group consists of people that oversee the complete process of an acquisition deal and are not specialists in a certain topic, like cyber security. Therefore they appreciate the influence of cyber security risks from a certain distance and place it in a certain perspective in relation to overall acquisition. Because of their position they decide what focus a due diligence should have and what impact the outcomes will have on the deal.

Group 2: “Experts”

The second group of interviewees consists of specialized advisors like lawyers and consultants who have a more narrow view on the course of an acquisition deal and are mainly experts in due diligence. These people have a specialized area of expertise and use this during due diligence investigations. The experts all have a different expertise that can be grouped in three sub groups; finance, IT or legal.

Both groups consist of people with varying experience as a player in an acquisition deal, either on the acquirer or target side. As set out in the introduction, the focus is on the perspective of the acquirer for this party is aiming on reducing the information asymmetry. It is interesting to see that these two type of interviewees have a different view on the matter associated with their role in the process. These groups will be referred to as ‘Investors’ or ‘Experts’.

The total group of interviewees consists of sixteen professionals, all working in M&A with varying experience, ages and market focus. The group of Investors consists of eight people who all work or have worked at investment funds, private equity firms or were in a senior management position at large corporations in Europe, mostly located in the Netherland. The group of Experts consists of eight professionals. Three lawyers, specialized in M&A with a strong focus on technology. Three cyber security consultants who have experience in advise acquiring parties in M&A deals. And two financial advisors; one banker and one financial consultant who both had experience with advising M&A deals from a financial perspective.

The interviewees are approached with a predefined set of questions that are the same for all interviewees. The interview questions were designed to get the right information in a considerable short time due to the limited availability of the interviewees. Besides certain administrative information the following questions were asked:

1. How many deals have you worked on in your professional career?
2. In how many of these deals there was a substantial focus on IT and data as intangible assets?
3. Would you describe the level of attention to data and the associated risks and value during an M&A deal sufficient?
4. What methods are used to assess the risks and opportunities associated with data at companies?
5. Are there generally accepted frameworks or standards that play an important role in executing due diligences?
6. To what extent do these due diligence frameworks spend attention to data and cyber risks?
7. What are the most common identified outcomes of due diligences with regard to data and cyber risks/opportunities?
8. How do these outcomes influence the deal value?
9. Do you have examples of deals where in hindsight, data security and privacy issues were raised that should have been addressed during the DD?
10. How would you qualify the accuracy of the discussed course of actions?

11. What recommendations would you have to improve the experienced way of working?

All the interviews took place via phone calls in which the questions as listed above were discussed and additional information around the topic was discussed. As described earlier, the main goal of the interviews was to determine how cyber security plays a role in the acquisition process and what current methods are in place. This led to a quite fractured picture but it also gave a lot of inside information on how different roles within an M&A process work together.

Theoretical framework

As mentioned in the introduction, the theoretical framework for this research lies in the theory of information asymmetry. In 1970, George A. Akerlof published his famous article in The Quarterly Journal of Economics called *The Market for "Lemons": Quality Uncertainty and the Market Mechanism.* In this article he explains his economic theory of information asymmetry between buyers and sellers and what consequences this has in a particular market. Information asymmetry exists when the selling party has more information about the quality of a product than the buying party. This leads to uncertainty about the quality of goods in a market and this has certain negative effects.

Akerlof used the market for cars as an example to explain his theory. In American slang a used car with a hidden defect is called a 'lemon', a good quality car is called a 'peach'. For the example it is assumed that the buyer cannot asses the car in a way that he knows the quality of the car, in other words if he is buying a lemon or a peach. In general the buyer will assume that car has average quality. This results in the fact that a buyer will only be willing to pay the price for a car with average quality. Owners of good quality cars will now have less incentives to place their cars on the market because they will not be able to receive the right price for it. As a result they will leave the market and the average quality of cars within the market will drop, as will the price.[65]

Following the reasoning of this theory, asymmetric information make bad products drive out the good ones in a market. This effect is also described by Greseham's Law when looking

[65] Akerlof, Quarterly, and Aug.

at the market for money and the effect of exchange rates.[66] This has a negative effect on both buyers, sellers and eventually on the market itself.

Another possible result of asymmetric information is adverse selection. This happens when traders that have more information about the quality of a product will selectively step in a trade when it will benefit him, at the expense of the other party in the trade. A proved example of adverse selection in a real market is that of life insurances[67]. To understand this a bit better we will discuss a hypothetical example in this market. Imagine that the market for life insurances consists of two type of people; one unhealthy type that smokes and eats unhealthy food and the other healthy type that does not smoke and eats healthy. Both of these types are searching for a life insurance but the insurance company is unable to differentiate. The insurance company would like to demand higher premiums for the unhealthy type of people but because there is no tool to his disposal of determining the healthiness of the persons it will demand the same high premium for both types. This resulting behavior of the insurance company is called adverse selection and leads to a great disadvantage for the healthy people.

When applying the theory of Akerlof towards the M&A market there is a need for some assumptions. For this example we assume that having a mature level of cyber security, or cyber risk management, is considered a quality aspect of a company. To keep using the automotive sector as an example we should consider a company as if it is a car and risk management as the breaks. Although some people might consider breaks as something that slows down a car you could argue the opposite; breaks enable a car to go fast. Without having proper breaks on a car you will not be able to drive fast in a responsible way. For a company to be profitable and have effective operations it needs to be aware of the risks and therefore risk management is needed[68]. Just as having proper breaks on a car is considered a quality aspect of a car, cyber risk management can be considered a quality aspect of a company. Following this assumption we will also have to conclude that having proper cyber

[66] J Law, *A Dictionary of Finance & Banking* (Oxford Uniersity press, 2015).
[67] Lillian Ablon and others, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, *RAND Institute*, 2016.
[68] Manuel Ritt-Huemer, 'Austria: Overcoming Information Asymmetry in M&A', 2017, p. 2 <http://roadmap2017.schoenherr.eu/overcoming-information-asymmetry-in-ma/>.

security risk management comes with considerable investments to set it up and maintain it, just as good brakes of a car have costs and need maintenance.

This quality aspect is not obvious for the outside world so there is an information asymmetry between the target company and the acquiring company. To follow Akerlofs theory the adverse selection problem can exist in the corporate control market when it comes to investing in cyber security. Picture this: two firms are on the market, both ready to be acquired. Firm A has invested a lot in cyber security and firm B has not. Due to information asymmetry the investor is unable to determine which company had a certain quality level when it comes to cyber security risk management. Therefore this aspect will not be taken into account when deciding which of the two companies should be the eventual target. Investors will value them in that sense equally. The adverse selection problem might exist here in the fact that companies will not invest in cyber risk management because it will not influence the value of their company. This leads to a general negative effect on the quality of cyber risk management in companies in a market perspective. Another negative effect from the perspective of the investor is that not taking into account cyber risk management when acquiring a firm can lead to unwanted surprises when these cyber security risks actually materialize once the acquisition has been completed.

Following the two negative effects as described above there is enough reason, especially from the perspective of the investor to improve the information asymmetry in an M&A process. The risk of information asymmetry in the M&A market can be mitigated in different ways; ownership solutions, contractual solutions and market solutions but the most practical one is due diligence.[69] Due diligence is the main focus for this research and the quality of this method will be assessed. The theory of information asymmetry is used to define the quality of the current due diligence practice. For this research we assume that the best method is the one that provides the best information about the ability of the target company to manage the cyber security risks and the capability to get the most value out of the data. During the interviews the main focus will be to assess how the professional think they can receive the most valuable information to make this assessment.

[69] Boulder.

Chapter 4: Results

The results of the interviews provides a picture of how the professionals approach cyber security during the acquisition process in general and how due diligence plays a role in this. Before we dive into the specific answers to the questions and start drawing conclusions it is interesting to start with some general observations. Besides discussing the eleven predetermined questions other observations were made during the conversations with the professionals. It was striking that when discussing the attention to cyber security during acquisition deals the majority of the interviewees were convinced of the fact that is an important topic and that its importance is increasing. They were all convinced that since cyber security and privacy has become so-called 'board room topics' the attention in the M&A market is growing. Acquirers are interested in the maturity of cyber security and data protection at a target company, especially if data plays a vital role in the business model.

All interviewees were convinced that data in general and consumer data in particular are useful when it can provide information that is valuable for a company. If business models drive on data of consumers/clients directly, for instance companies in the online marketing or sales business, it is obvious. But also when customer data may not provide the direct revenue stream it is still of value because data can provide insight. Insight in customers, (but also in employees, work streams or even competitors) can result in improved decision making.[70] When used correctly, data is essential to become an Insight Driven Organization (IDO). Research has proven that IDOs are more successful than others and are also better prepared for the future.[71] A majority of the interviewees were becoming aware of the fact that there is value in data and that it can be an important reason in valuating and assessing a company. With the increasing value comes the risks and the general awareness of these growing risk factor was present at the majority of the interviewees. The cyber security risks associated with data are considered to be information security risks and privacy risks although this distinction is not made by the majority of the interviewees. This is an example of the knowledge level with regard to this topic at the professionals, especially at the

[70] Ron Bergerss and Jasper Meijerink, 'The New Gold', *Deloitte*, 2017, p. 2.
[71] Forrester, *Global Business Technographics® Data And Analytics Survey, 2016*, 2016 <https://www.forrester.com/Global+Business+Technographics+Data+And+Analytics+Survey+2016/-/E-sus3014>.

Investors group. From the conversations with the professionals an image came forward of a group of people who are consciously aware of the importance of the topic but are in search of a solid method to approach it. The methods that are being used at the moment are considered imperfect by all interviewees but they see it improving over the years. This was a confirmation for the need of this research and was one the reasons why the interviewees were open to discuss this topic in an exploring manner.

Interview answers

Before we dive deeper in the outcome and conclusions of our research we first want to give a general overview on how the two different groups (Investors and Experts) responded to the eleven questions. For some questions the answers varied a lot, especially between the two groups. Therefore, in the following section the answers to the eleven questions are sometimes discussed with distinction between the two groups.

Question 1 How many deals have you worked on in your professional career?

The group of Investors had an average experience of around thirty deals per person with an average of five till ten deals a year. The average experience of Experts differed a lot depending on the profession. Lawyers can be involved in over hundred deals, mainly involved by executing legal due diligence. Investors are generally more involved then Experts in a deal because they handle a deal from start till finish where Experts only fulfill a small role in the process. Therefore the difference in number of deals between the two groups makes sense.

Question 2: In how many of these deals there was a substantial focus on IT and data as intangible assets?

Both groups scoring with an average of five deals where the value of data and the according risks played a vital role. Besides the absolute number it is important to mention that all interviewees confirm the trend of an increasing attention to data and the cyber security risks that come with it.

Question 3: Would you describe the level of attention to data and the associated risks and value during an M&A deal sufficient?

Especially the Investors were very clear in stating that the attention is not sufficient but all professionals agreed that it is improving. The answers from Experts, especially the IT and

cyber security consultants, to this question give a bit of a distorted picture because when they are involved in a deal the attention is there while they are not involved when the attention is not present. The fact that specialists in the field of cyber security are becoming more involved in acquisitions is a sign that confirms the growing attention to the subject.

Question 4: What methods are used to assess the risks and opportunities associated with data at companies?

All interviewees confirmed that during due diligence these kind of risks are being investigated. Investors expect these topics to be handled by their advisors and rely heavily on their specialized expertise and experience. Among the Experts, especially the lawyers and the IT consultants confirmed that this during legal due diligence or an IT due diligence this topic is addressed. The financial Experts could think of only one instance where the topic has become part of his due diligence.

Question 5: Are there generally accepted frameworks or standards that play an important role in executing due diligences?

Investors were not aware of any standard frameworks accept for one Investor who mentioned the Environmental Social and Governance (ESG) framework and the United Nations Principles for Responsible Investments (UNPRI) framework that his firms uses. Although these frameworks do steer the attention of Investors towards general Governance, of which general risk management is considered part of, this does not result in practical tools to assess cyber security risks during due diligence.[72] Experts stated that they all use certain frameworks and industry standard to structure their due diligence. IT consultants use industry standards like ISO 27001 or NIST frameworks. Lawyers do not have a general accepted due diligence framework but stated that every professional law firm uses their own framework that are constantly updated and adapted to the client they serve.

Question 6: To what extent do these due diligence frameworks spend attention to data and cyber risks?

Investors were in general not able to answer this question because of their lack of in-depth knowledge of used frameworks. The group of Experts had different reactions to this questions. Lawyers stated that there was increasing attention in their frameworks for cyber

[72] PRI Association, 'About the PRI | Principles for Responsible Investment' <https://www.unpri.org/about> [accessed 11 February 2018].

security and privacy risks. The financial advisors stated there was no attention in general frameworks to cyber security or the data whatsoever. They stated that they would only take (consumer) data into consideration if it is put on the balance sheet of a company. This has never took place in the experience of the financial Experts that were interviewed. Lawyers stated that with cyber security laws and regulation growing, especially with the upcoming General Data Protection Regulation (GDPR), this will be a standard part of their legal due diligence.

Question 7: What are the most common identified outcomes of due diligences with regard to data and cyber risks/opportunities?

A due diligence report provides an overview of risks in a specific area (legal, IT or financial) to provide input for the negotiations at the deal table. If observations during a due diligence is considered as a high risks this will be mentioned as a so-called 'red flags'.

Question 8: How do these outcomes influence the deal value?

If and how due diligence reports impact a deal differs a lot according to the answers of the professionals. One Investor made very clear to me that the proceeding of the deal and the deal value will only be impacted if the outcomes of the due diligence reports are extremely unexpected. He made clear that the decision to acquirer a company is normally already made in steps preceding the due diligence step in the acquisition process. The professionals could not recall an example where cyber security risks discovered during due diligence lead to a significant drop in deal value. The reason for this can, among other reasons, be found in the fact that risks in general and especially cyber security risks are extremely hard to quantify. For example the risk of getting a fine due to non-compliance with privacy and security legislation resulting from possible data breaches in the future was considered by the majority of the Experts. But to calculate the chance of having a data breach occurring in the future and the amount of the fine resulting from it is considered to complex and therefore to uncertain to make it result in significant changes in deal value. When the professionals were asked how this relates to the value drop in the Yahoo! Verizon case the majority of the Investors considered it as just bold negotiation skills from Verizon. Basically saying that a large scandal at a target company will always be used as breaker at the deal table.

Question 9: Do you have examples of deals where in hindsight, cyber security and privacy issues were raised that should have been addressed during the due diligence?

None of the professionals could think of concrete examples where cyber security or privacy issues were raised after he had worked on it. One Expert was involved in a 'post-merger' integration project at a large med-tech company where one database of consumer data had to be divided in two after a split of the company. Although this was foreseen during the acquisition, the efforts (and costs) of this project were underestimated. This could have been prevented if they had analyzed this further during the due diligence. The Expert did noticed that projected the costs for these kind of projects are again extremely hard and would normally not be part of a due diligence because of the costs and efforts it would bring.

Question 10: How would you qualify the accuracy of the discussed course of actions?

Especially the Investors were negative with regard to the accuracy of the way cyber security is currently being handled. All professionals agreed that there is a lot of room for improvement in this. It is interesting to see that they basically point to each other for the solution. Investors expect their advisors to bring the right attention, methods and knowledge in the process in order to cope with this topic. Meanwhile the majority of the Experts stated that because Investors are not interested enough in the topic and are not willing to allocate budget for thorough investigation of cyber security it remains underexposed.

Question 11: What recommendations would you have to improve the experienced way of working?

Investors state that the raise of awareness of the topic will result in more attention and budget for the topic. Increasing legislation on data protection is expected to raise awareness and many of the professionals were convinced that with every major cyber hack in the news people will be more interested in the topic. Almost all Experts had another interesting recommendation for improving the way cyber security can be addressed during due diligence and the key-word is collaboration. As also set out during the literature review there are different 'streams' of due diligence assessments, each focusing on a certain specialism like finance, IT, legal or sometimes even culture or environment. Many of the

Experts acknowledged that in order to address cyber security fully at least the IT and legal experts involved should work together.

Main results: different types of due diligence

The interviewed professionals provided a sometimes scattered image of the current reality and because of the limited size of the group of interviewees it has the most value to focus on the answers that provided a congruent image. To go back to the main research question we can conclude the method for assessing cyber risks during an acquisition is due diligence. None of the interviewed professionals named another method where these kind of risks would or should be addressed. Therefore it is interesting to further investigate how due diligence investigations are structured in order to assess cyber security risks. The Experts were able to provide a clear image of how this works in practice. It is important to remember that there is not one type of due diligence. What is being assessed during a due diligence will vary based on the wishes of the acquirer, the type of target, the market in which it operates and the experience of the Investor and the Experts. The execution of due diligence is normally split up in several streams, all focusing on different substantial topics. In general there are three different types of due diligence where the topic of data and risks associated with it might play a role; financial, legal and IT due diligence. What the Experts and the Investors made clear is that the cyber security risks and is part of these three different forms of due diligence, all from another angle.

Financial due diligence

During a financial due diligence the acquirer mainly looks at the profitability and financial status of the target company. This is done by evaluating financial documentation like balance sheets, profit & loss accounts and other accounting documentation. The financial Experts explained that consumer data becomes part of a financial due diligence when it is put on the balance sheet. Although this is not yet seen a lot, a recent study from Gartner predicts that this will increase in the coming years.[73] Currently, consumer data might also be part of the financial due diligence if it is considered as goodwill. Experts explained that when

[73] Gartner, 'Gartner Says Within Five Years, Organizations Will Be Valued on Their Information Portfolios', *Gartner Newsroom*, 2017, p. 1 <https://www.gartner.com/newsroom/id/3600817>.

there is large and valuable commercial database that play an important role for the revenue streams of a target company, it can be part of the goodwill on a balance sheet. Investors and experts are not only interested in the sole numbers and financial results they also evaluate the business case that is behind it. If the target is able to produce revenue from the commercial data is possesses this will surely be part of the financial due diligence.

Legal due diligence

With a legal due diligence the acquirer tries to discover legal liabilities and regulatory risks. Liabilities can exist towards clients or customers but also against shareholders and directors of the company itself. Cyber risks can cause liability issues, especially when looking at the risk of data breaches, which can also be considered as an operational risk as one Expert explained. Especially in the US it is a hot topic because of the many law suits following from giant data breaches. In Europe this has not been the case yet but with stricter cyber security and privacy legislation in place this might come to the continent as well. Experts assess these risks by reviewing the past and requesting an overview of data breaches that occured and try to use this information to predict the risk in the future. Liabilities will also be assessed by reviewing contracts with vendors and other third parties. The Experts that were interviewed admitted that although contract review is the base of every legal due diligence, they did not always have the time and expertise to review the material provisions in the contracts on security requirements, arrangements with regard to handling data breaches or data localization. Contract reviews during legal due diligence might be limited to general reviews of liabilities, warranties, contractual notice periods and change of control provisions. Regulatory risks can rise from all sorts of non-compliance with legislation. With the arrival of the General Data Protection Regulation (GDPR) this becomes a more important topic but this is still very immature and the exact way of assessing whether an organization complies with the GDPR is not yet in place. Some Experts have recently started reviewing privacy policies and (consent) statements in order to assess whether the consumer data in the target databases gives the acquirer the right to process it for the purposes it has envisioned. This happens however very little and only when the target relies very heavily on consumer data for their main business model.

IT due diligence

Assessing the IT infrastructure of a target is becoming more standard in recent years but is still very immature as well. Especially when it comes to cyber security as part of an IT due diligence. IT due diligence 'historically' focuses on assessing the status of the IT assets which basically meant that it reviews the replacements costs of the hardware and the costs of long-term software licenses. When an acquisition leads to combing or connecting two corporate IT infrastructures, the acquirer wants to know what additional costs will come with that from an IT perspective. Although these topics touch upon risks associated with data storing from a technical point of view, it has nothing to do with cyber security. Cyber security assessments as part of the IT due diligence are developing since recent years. In these assessments not only the purely IT side of cyber security is assessed but it also dives into the organizational measures that are taken to manage cyber risks. Experts explained that industry standards like the NIST and ISO frameworks are used to assess the cyber security maturity of an organization. In very rare cases even specific penetration tests are being conducted on vital systems of the target. In some cases the source code of (self-developed) software is being reviewed. It is worth mentioning that a IT due diligence, let alone a cyber security due diligence, is certainly not yet part of standard due diligence.

These three forms of due diligence can address parts of the cyber security risks that are associated with consumer data, all from their own perspective. Both Investors and Experts explained that it really depends on the structure, the experience and the focus of the deal team whether these three due diligence reports are combined into one overall report. Experts stated that the different streams in the due diligence team sometimes don't communicate at all. A fully integrated due diligence approach is not common yet.

What is missing?

Market standards

Based on the interviews with Investors and Experts a picture can be derived that there is a general understanding of the value of (consumer) data and the importance of assessing the risks that are associated with it. Investors may differ in knowledge about the topic and it is quite often purely based on coincidental experience from previous deals. Investors also rely

heavily on what their advisors advise them to do. It is interesting to see that in the fairly mature M&A market there is a general lack of industry standards or best practices on how to assess risks in general and especially cyber security risks. All the lawyers that were interviewed stated that their firm had its own catalogue of due diligence questions and methods to answer them. This provides certain flexibility to Experts to tailor investigations to their clients' needs but from a research perspective it is hard to draw conclusions from it. Experts in the field of IT and technical cyber security use a lot more industry standards because this is very common in that market. Especially the security standards like NIST and ISO can provide a framework for experts to score a target organization to. It still remains very hard to quantify any of the results into something useful.

Awareness

As described in the previous chapter, cyber security is currently a topic that is becoming more important for investors and because it has become a 'boardroom topic' it will increasingly be addressed during deals. Although Investors and Experts state that the topic is not being addressed sufficiently enough there is an increasing attention for it. All the different type of Experts will address the topic more and include it in their current way of working. The financial advisor will be more focused on addressing the value and financial risks of data in the financial due diligence, as will the lawyer for the legal due diligence and the IT expert for the IT due diligence. Because of this development, the expectation is that the topic will find its way to the negotiation table.

Working in silos

A part from the answers to the questions there was another major takeaway that was not envisioned before the start of the research. That results from the way M&A deals are structured from an organizational perspective. Investors normally guide the deal and are the ones taking the strategic decisions, select the targets and determine the conditions of the deal. They are in the lead and will be assisted by a varying group of Experts. Deciding on what specialists will be used during a deal and what type of due diligence should be executed is the responsibility of the Investor. The reason for Investors to decide to make cyber security a priority in their due diligence can be quite arbitrary. One Investor explained

that they once decided to look into cyber security risks in very late stage of the deal because the son of one of their senior manager started a cyber security minor on university and raised the topic at the dining table. This shows that it strongly depends on the wishes and knowledge of Investors. Experts can be hired from different consultancy or law firms, depending on their expertise. They will be assigned with a separated task and scope in which they will do their investigation. The outcome will be put in a report and this reports will be used as input for the investors during the negotiations. These reports will not be combined or aligned with each other and any other type of corporation is missing. In this lack of collaboration between Investors and the different type of Experts lies a major risk that results from the segregation of knowledge. The thoroughness of their investigations and the quality of their reports may be from the best possible level but in solitary it does not address the full picture of the values and risks of consumer data.

To conclude the results of the research in relation to the research question we have to see whether it provides the right amount of information to the acquiring party in order to make an informed decision about the 'quality' of the company. As stated before we assume here that having the right capabilities in place to manage cyber security risks should be considered as a 'quality' of the target firm. Based on the interviews it is fair to say that the current practice of assessing cyber security during due diligence provides a considerable amount of information but there is room for improvement. By improving awareness, agreement on market standards and better collaboration between involved parties the amount and quality of information produced by due diligence would be much better. How 'cyber security due diligence' could look like is discussed in the next chapter.

Chapter 5: How cyber security due diligence could be improved

When the goal of an acquirer is to gather as much information about the cyber security situation at the target there are a couple of improvements to current practice of due diligence. In this chapter a selection of proposed improvements are discussed based on available (scientific) literature and the outcomes of the interviews. Besides the discussed improvements discussed in this chapter there might be many more but these improvements are mainly focused on the practical process on the one hand and on the content of what should be investigated on the other hand.

Collaboration

One of the weaknesses of the current practice is the fact that due diligence experts are working in silos.[74] A lot of improvements can be achieved with setting up cross-functional teams working together on one due diligence report.[75] This is especially the case for the IT due diligence and the legal due diligence teams. IT experts normally lack legal knowledge and vice versa while cyber security and privacy are both highly connected with the topic areas of expertise. For example when an acquirer wants to know what the capabilities of the target firm are to handle data breaches there a number of ways to assess this. An IT expert would probably focus on the ability of the security architecture to detect intrusion on a company network or the average level of technical security measures that are taken against hackers. Even if the IT experts would broaden its scope it might even look to internal procedures on how to handle data breaches and at best it might even check whether the data protection officer is part of this procedure. Assessing all these qualities would provide a pretty good image of the capabilities of the target company on how it can handle data breaches in the future. But it is missing a vital part that a lawyer would have looked into. A legal specialist working on a due diligence with the same task of finding out how good the target company is prepared for data breaches would probably review the contracts with third parties where data of the company resides. These contracts would be checked on provisions regarding the obligations in possible data processing agreements on when to

---

[74] James A. Scherer, Taylor M. Hoffman, and Eugenio E. Ortiz, 'Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices', *Richmond Journal of Law & Technology*, 21.2 (1979), 243–58 <https://doi.org/10.3366/ajicl.2011.0005>.

[75] James McLetchie and Andy West, 'Perspectives on Merger Integration', *McKinsey: Perspectives on Merger Integration*, 31.June (2010).

inform about data breaches to the target company. A lawyer with a broader look would even check if the practical execution of the notification between parties is functional. There are not many lawyers who would even check the definition of data breach in the contract with the right technical knowledge. This example shows that two different experts aiming on finding answers to the same question will provide a completely different outcome and with totally different aspects of the target company assessed, despite the best intentions of both experts. Another upside of combining different types of expertise is the creation of synergies within an M&A deal team resulting from collaboration. Because data has become such an important aspect of business operations in general it touches all aspects of the acquisition process and provides input for the valuation.[76]

What to assess

The previous described improvement to the current practice of 'cyber due diligence' was aiming to provide more information by combining teams and expertise to create synergies within the acquisition team. This does not mean that every expert should remain to have a certain focus that suits his expertise. Combining knowledge is one thing but the knowledge to be combined should also be from a high quality. In this section we highlight a number of topics that should be part of a due diligence:

Assessing policies and procedures

Cyber security is not only an IT issue or a legal issue but has also a very strong operational aspect and therefore is reviewing internal policies and procedures essential. An acquirer should want to know whether the target has effective incident response plans, Bring Your Own Device (BYOD) policies, password policies and business continuity plans in place.[77] Besides checking whether these kind of policies and procedures are in present it should also be assessed whether they are regularly updated.

---

[76] John Reed Stark, 'Cyber-Security Due Diligence: A New Imperative.', *Compliance Week*, 13.150 (2016), 76–77 <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=116627581&site=eds-live>.

[77] John Reed Stark, *The Cybersecurity Due Diligence Handbook:* (Bookaby.com, 2016) <https://www.scribd.com/read/315345305/The-Cybersecurity-Due-Diligence-Handbook-A-Plain-English-Guide-for-Corporations-Contemplating-Mergers-Acquisitions-Partnerships-Vendors-or-Other-S> [accessed 10 February 2018].

Assessing the technical systems

The systems that are processing the valuable data or make it available should be state of the art when an acquirer wants it to be. This can be assessed by requesting information about data mapping, data loss prevention techniques, encryption, patching and updating. The most obvious technical measurement is of course see if decent anti-virus software is installed on the vital systems within the organization.[7879]

Assessing the people

A considerable amount of cyber risks are the result on human mistakes, mostly from inside the organization. Therefore it is extremely valuable to see whether the staff are able to manage cyber security. Is the right governance structure in place? Is the board aware and engaged in managing cyber security? Are there good training programs available? Is there an active recruitment program aiming on getting the right expertise into the organization? All these questions should be asked in order to provide a full picture about the organization.[80]

Possible influence of the GDPR

Normally is new and strict legislation not best friends with the average acquirer in the M&A market. Extra compliance pressure means delay in the process and especially during a deal time means money. Especially the GDPR, the new reality of privacy in Europe, is not famous for improving business practice due to stricter accountability requirements.[81] But as a result of one of the accountability requirements in the new law there might be a positive effect for acquirers doing due diligence. All the above proposed improvements are aiming on getting information about how data and according risks is being managed. Although targets provide normally a considerable cooperation with the due diligence experts there might a challenge in finding the right answer within the organization. This will probably be reduced by the requirements of article 30 of the GDPR. This requirement means that every responsible data

---

[78] Stark, *The Cybersecurity Due Diligence Handbook:*

[79] Amy and Sheehan, 'Tackling Cybersecurity and Data Privacy Issues in Mergers and Acquisitions (Part One of Two)'; Amy and Sheehan, 'Tackling Cybersecurity and Data Privacy Issues in Mergers and Acquisitions (Part Two of Two)'.

[80] Stark, *The Cybersecurity Due Diligence Handbook:*

[81] Maciej Sobolewski, Joanna Mazur, and Michał Paliński, 'GDPR: A Step towards a User-Centric Internet?', *Intereconomics*, 52.4 (2017), 207–13 <https://doi.org/10.1007/s10272-017-0676-5>.

controller must have an up-to-date record of their processing activities. This overview must contain a number of aspects that can immediately provide valuable information if being reviewed during a due diligence. It should provide information about the type of data being processed, the purposes of processing, retention periods and security measures taken to protect the data.[82] With all this information in one place could function as a kick start for the due diligence process and shows immediately where additional research might be needed.

[82] Article 30 General Data Protection Regulation (Regulation (EU) 2016/679).

Chapter 6: Conclusion

During this research a lot is discovered about the world of M&A and how cyber security plays a role. With the value of data remaining to increase and the risks associated with it the methods of assessing these risks will too. At the moment due diligence is the methods used for assessing cyber security risks. The different forms of due diligence cover a piece of the puzzle but for a complete picture improvements should be made. The improvements proposed in this thesis are all aiming on providing better and more complete outcome of the current due diligence practice with regard to cyber security. These improvements are based on the idea that better and more complete information about a target's cyber security organization is helping to reduce the information asymmetry that is present during an M&A deal. Full disclosure of all information that resides at a target will probably never happen so complete information symmetry cannot be reached with regard to cyber security. With the current development in this area of expertise the asymmetry is expected to be reduced to a level that the negative effects as described by Akerlof might not emerge. When the right mechanisms are in place to assess cyber security at an organization during an acquisition there will be a greater incentive for management of future target companies to invest in cyber security.

Bibliography

Abitbol, By Jill, 'Cybersecurity Due Diligence in M & A Is No Longer Optional', *Cyber Security Law Report*, 2 (2017), 1–7

———, 'Essential Cyber Due Diligence Considerations in M & A Deals Raised by Yahoo Breach', *Cyber Security Law Report*, 2 (2016), 1–9

Ablon, Lillian, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, *RAND Institute*, 2016

Acquisti, Alessandro, and Allan Friedman, 'Is There a Cost to Privacy Breaches? An Event Study', in *Ywenty Seventh International Conference on Information Systems*, 2006, p. 23

Akerlof, George A, The Quarterly, and No Aug, 'The Market for " Lemons ": Quality Uncertainty and the Market Mechanism', 84 (2007), 488–500

Amy, By, and Terry Sheehan, 'Tackling Cybersecurity and Data Privacy Issues in Mergers and Acquisitions (Part One of Two)', *Cyber Security Law Report*, 1 (2015), 1–8

———, 'Tackling Cybersecurity and Data Privacy Issues in Mergers and Acquisitions (Part Two of Two)', *Cyber Security Law Report*, 1 (2015), 1–7

Atkinson, Claire, 'Verizon Wants $1B Discount on Yahoo Deal after Reports of Hacking, Spying | New York Post', *New York Post*, 2016 <http://nypost.com/2016/10/06/verizon-wants-1b-discount-on-yahoo-deal-after-hacking-reports/> [accessed 16 August 2017]

Bergerss, Ron, and Jasper Meijerink, 'The New Gold', *Deloitte*, 2017, p. 2

Beucher, Klaus, Bertram Burcher, Chris Forsyth, and Matt Friedrich, *Cyber Security in M&A*, 2014

Boulder, Colorado, 'Avoiding Lemons in M & A Deals', 2015

Coyle, Brian, *Mergers and Acquisitions*, ebook (Chicago: AMACOM, 2000) <http://web.a.ebscohost.com.ezproxy.leidenuniv.nl:2048/ehost/detail?sid=1aad445b-9e70-467e-ad74-035644fa333b@sessionmgr4006&vid=0&format=EB&lpid=lp_I&rid=0#AN=52734&db=nlebk> [accessed 10 February 2018]

Crilly, William M., Sherman, Andrew J., *The AMA Handbook of Due Diligence.* (Americam

Management Association, 2010)

Damodaran, Aswath, 'Valuing Young, Start-Up and Growth Companies: Estimation Issues and Valuation Challenges', *SSRN Electronic Journal*, 2009, 1–67 <https://doi.org/10.2139/ssrn.1418687>

Dave Albaugh, 'The Biggest Data Breaches in History - Comparitech', *June* , 2017 <https://www.comparitech.com/blog/information-security/biggest-data-breaches-in-history/> [accessed 16 August 2017]

Deepa Seetharaman, 'Yahoo Looks to Bright Side After Breach - WSJ', 2016, p. 1 <https://www.wsj.com/articles/yahoo-core-revenue-drops-again-1476822440> [accessed 16 August 2017]

Deloitte, 'Cyber Value at Risk in the Netherlands', 2016, 1–42 <https://www.thehaguesecuritydelta.com/images/deloitte-nl-risk-cyber-value-at-Risk-in-the-Netherlands.pdf>

Diligence, D U E, 'Essential Cyber Due Diligence Considerations in M & A Deals Raised by Yahoo Breach', 2 (2016)

Feagin, Roger D ., 'THE VALUE OF CYBER SECURITY IN SMALL BUSINESS By Roger D . Feagin A Capstone Project Submitted to the Faculty of Utica College', 2015, 45 <http://0-media.proquest.com.oasis.unisa.ac.za/media/pq/classic/doc/3857701661/fmt/ai/rep/NPDF?hl=smaller,smallest,small,smaller,smallest,small,organisations,organisation,organizations,organization,organisations,organisation,organiz>

Finkelstein, By A M Y, and Kathleen Mcgarry, 'American Economic Association Multiple Dimensions of Private Information : Evidence from the Long-Term Care Insurance Market Author (S): Amy Finkelstein and Kathleen McGarry Source : The American Economic Review , Vol . 96 , No . 4 (Sep ., 2006), Pp .', 96 (2016), 938–58

Forrester, *Global Business Technographics® Data And Analytics Survey, 2016*, 2016 <https://www.forrester.com/Global+Business+Technographics+Data+And+Analytics+Survey+2016/-/E-sus3014>

Fung, Brian, 'Why Verizon Is Still Buying Yahoo on Sale , despite That Epic Security Breach', *Washington Post*, 2017, pp. 2–4

Gangewere, Will, 'Assessing the Impact of a Privacy Breach on a Firm 'S Market Value', 2013

Garg, Ashish, Jeffrey Curtis, and Hilary Halper, 'The Financial Impact of IT Security Breaches:

What Do Investors Think?', *Information Systems Security*, 12 (2003), 22–33 <https://doi.org/10.1201/1086/43325.12.1.20030301/41478.5>

Gartner, 'Gartner Says Within Five Years, Organizations Will Be Valued on Their Information Portfolios', *Gartner Newsroom*, 2017, p. 1 <https://www.gartner.com/newsroom/id/3600817>

Gatzlaff, Kevin M., and Kathleen A. McCullough, 'The Effect of Data Breaches on Shareholder Wealth', *Risk Management and Insurance Review*, 13 (2010), 61–83 <https://doi.org/10.1111/j.1540-6296.2010.01178.x>

GE Capital, 'Due Diligence : Main Steps and Success Factors', 2012, 4 <http://www.gecapital.eu/en/docs/GE_Capital_Overview_Due_Diligence.pdf>

Goldman, Jeff, 'M&A Due Diligence, Cyber Security, and the Massive Yahoo Data Breach', 2016 <https://www.esecurityplanet.com/network-security/ma-due-diligence-cyber-security-and-the-massive-yahoo-data-breach.html> [accessed 3 February 2018]

Harvey, Michael G, and Robert F Lusch, 'EXPANDING THE NATURE AND SCOPE OF DUE DILIGENCE Puterbaugh Chair of American Free Enterprise Helen Robson Walton Chair of Marketing Strategy', 9026 (1995), 5–21

Koller, Tim, Marc Goedhart, and David Wessels, *Valuation: University Edition*, *Journal of Chemical Information and Modeling*, 2010 <https://doi.org/10.1017/CBO9781107415324.004>

Law, J, *A Dictionary of Finance & Banking* (Oxford Uniersity press, 2015)

Lucinda Shen, 'Why Yahoo's Alibaba Stock Could Be a Bad Deal for Investors', *Fortune Finance*, 2017, p. 1 <http://fortune.com/2017/06/16/alibaba-stock-yahoo-altaba/> [accessed 16 August 2017]

Lynley, Matthew, 'Yahoo Surprises No One by Pushing Back Its Verizon Acquisition Close Date | TechCrunch', *Techcrunch*, 2016 <https://techcrunch.com/2017/01/23/yahoo-unsurprisingly-pushes-back-its-verizon-acquisition-closing-date/> [accessed 16 August 2017]

McLetchie, James, and Andy West, 'Perspectives on Merger Integration', *McKinsey: Perspectives on Merger Integration*, 31 (2010)

Mellendez, Steven, 'Why Verizon's Due Diligence May Not Have Caught Yahoo's Massive Securi', 2016, p. 1 <https://www.fastcompany.com/3064765/why-verizons-due-

diligence-may-not-have-caught-yahoos-massive-security-breach> [accessed 3 February 2018]

Moritz, Scott, and Brian Womack, 'Verizon Explores Lower Price or Even Exit From Yahoo Deal - Bloomberg', *Bloomberg*, 2016 <https://www.bloomberg.com/news/articles/2016-12-15/verizon-said-to-explore-lower-price-or-even-exit-from-yahoo-deal> [accessed 16 August 2017]

Musthaler, Linda, 'A Cybersecurity Risk Assessment Is a Critical Part of M&A Due Diligence | Network World', 2017 <https://www.networkworld.com/article/3182139/security/a-cybersecurity-risk-assessment-is-a-critical-part-of-manda-due-diligence.html> [accessed 3 February 2018]

Ponemon Institute and Accenture, '2017 Cost of Cyber Crime Study', 2017, 56 <https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf>

PRI Association, 'About the PRI | Principles for Responsible Investment' <https://www.unpri.org/about> [accessed 11 February 2018]

Ritt-Huemer, Manuel, 'Austria: Overcoming Information Asymmetry in M&A', 2017, p. 2 <http://roadmap2017.schoenherr.eu/overcoming-information-asymmetry-in-ma/>

Romanosky, Sasha, 'Examining the Costs and Causes of Cyber Incidents', *Journal of Cybersecurity*, 2016, tyw001 <https://doi.org/10.1093/cybsec/tyw001>

Ryan, Michael J., 'A Car and Brakes: Risk Management Is NOT Risk Avoidance', 2015, p. 1 <http://businessroundtable.org/media/blog/car-and-brakes-risk-management-not-risk-avoidance>

Sacek, Alen, 'Due Diligence in Mergers and Acquisitions in Emerging Markets : Evaluated Risk Factors From the Academic and Practical View.pdf', 11 (2015), 363–72 <https://doi.org/10.17265/1548-6583/2015.07.004>

Scherer, James A., Taylor M. Hoffman, and Eugenio E. Ortiz, 'Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices', *Richmond Journal of Law & Technology*, 21 (1979), 243–58 <https://doi.org/10.3366/ajicl.2011.0005>

SEC, 'Preliminary Special Proxy Pertaining to a Sale', 2016 <https://www.sec.gov/Archives/edgar/data/1011006/000119312516706578/d206374

dprem14a.htm> [accessed 16 August 2017]

Sharifi, Mohsen, Vijay Karan, and Zafar Khan, 'Your M&A Map for Success', *Journal of Corporate Accounting & Finance*, 16 (2005), 9–16 <https://doi.org/10.1002/jcaf.20082>

Sliskovic, Vlado, 'Do Virtual Data Rooms Add Value To the Mergers and Acquisitions Process ?', 2007 <http://www.imaa-institute.org/docs/kummer-sliskovic_do virtual data rooms add value to the mergers and acquisitions process.pdf>

Sobolewski, Maciej, Joanna Mazur, and Michał Paliński, 'GDPR: A Step towards a User-Centric Internet?', *Intereconomics*, 52 (2017), 207–13 <https://doi.org/10.1007/s10272-017-0676-5>

Stark, John Reed, 'Cyber-Security Due Diligence: A New Imperative.', *Compliance Week*, 13 (2016), 76–77 <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=116627581&site=eds-live>

———, *The Cybersecurity Due Diligence Handbook:* (Bookaby.com, 2016) <https://www.scribd.com/read/315345305/The-Cybersecurity-Due-Diligence-Handbook-A-Plain-English-Guide-for-Corporations-Contemplating-Mergers-Acquisitions-Partnerships-Vendors-or-Other-S> [accessed 10 February 2018]

Trautman, Lawrence J, and Peter C Ormerod, 'Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach', *American University Law Review*, 66 (2017), 1–68

Trope, Roland, and Tom Smedinghoff, 'The Importance of Cybersecurity Due Diligence in M&A Transactions', *Business Law Today*, 3 (2017), 18–20 <https://doi.org/10.1053/j.jrn.2009.05.003>

Urbanowicz, Don, 'The Seven Phases of M & A', 2015

USA, Deloitte, 'Cyber Risk in Advanced Manufacturing', 2017

Weber, Yaakov, Schlomo Tarba, and Christina Öberg, *A Comprehensive Guide to Mergers & Acquisitions*, 2014 <https://books.google.nl/books?hl=nl&lr=&id=YpZKAgAAQBAJ&oi=fnd&pg=PR7&dq=steps+in+M%26A+process&ots=jsB6iUmcDI&sig=EUM8Ab-56YMf-PtetkKfvZp4rOk#v=onepage&q=steps in M%26A process&f=false>

Yahoo! Inc., 'Yahoo! Inc., Report Filed on Form 10-K for the Fiscal Year Ended December 31,

2015', 2015, p. 171
<http://www.sec.gov/Archives/edgar/data/1011006/000119312514077321/d636872d10k.htm>