12-2019

Insufficient Due Diligence as a Security and Privacy Issue

Cynthia Konan
zw0398ov@go.minnstate.edu

Insufficient Due Diligence as a Security and Privacy Issue

by

Amoin Cynthia Joceline Konan

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Information Assurance

December 2019

Starred Paper Committee:
Abu Hussein, Abdullah, Chairperson
Kasi, Balasubramanian
Lynn, Collen

Abstract

Organizations face the rapid and constant evolution of technology and must adapt quickly to that fast pace changing environment. It is in that perspective that companies dive into adopting a new technology without a proper investigation on how the technology works or without knowing if they have the adequate resources to use it; thus, underestimating possible security threats. One of the most common threats related to organization rushing into acquiring a new technology is insufficient due diligence. Insufficient due diligence is the lack of proper measures taken to ensure the credibility of the technology provider. Insufficient due diligence happens when organizations try to move too quickly to the adopt technology without thoroughly understanding it. Organizations rushing in the decision making of which technology to choose, skip some important steps such as conducting a proper evaluation of the technology they want to adopt, which cause security threats. This is a problem mainly because of lack of research on the subject, ignorance and lack of attention to details. This starred paper will present the state of art of insufficient due diligence when adopting technology, its root causes, and the different aspect of the problem and propose recommendation to improve security in organizations. This work aims to raise the security bar for organizations adopting technology and improve security.

Acknowledgments

Thank you to Professor Abu Hussein for his patience, understanding and availability throughout the completion of this work. Thank you to my Family for their love and support. Special thank you to the person special to my heart, for being encouraging and present during the whole process.

Table of Contents

Chapter Page

List of Tables

Table Page

List of Figures

Figure Page

Chapter I: Introduction

Finding ways to achieve complete cyber security has been the main concern for many organizations. Therefore, to succeed in any project, there are important measures that need to be taken to ensure that nothing will interrupt the smooth development of that project. One of the steps taken by most organization to ensure complete security of their business is the implementation of due diligence in every step of the development.

Due diligence is when the top management of an organization take adequate security measures to ensure that the assets of the corporation such as information, for example, are protected and at the same time, to ensure that the organization complies with the law and different contractual obligations.

Due diligence is also ensuring that the product or service of the provider meets the security requirements and customers' expectations before engaging in a contract. Implementing due diligence can be expensive, however it is a necessary cost that every organization should assume. Although, awareness about due diligence is increasing in most companies, there are still some existing challenges.

Insufficient due diligence or lack of due diligence is when the necessary measures are either not considerable or nonexistent at all to ensure proper security and credibility of the service provider. Insufficient due diligence is ranked in the top nine severe security threats, according to The CSA (Cloud Security Alliance) in their article *The Notorious Nine cloud computing top threats in 2013.* Insufficient due diligence or the lack of due diligence can lead to costly consequences for the organization (CSA,

2013). Studying the impact of insufficient due diligence or lack of due diligence will reflect its importance of due diligence in the development of the organization.

The composition of this paper is as follows: Chapter II will present a literature review about the problem followed by a literature review about the possible solutions and recommendations. Chapter III is a methodology of the study, which includes the importance of due diligence and its benefits for the organization, the drivers of insufficient / lack of due diligence and possible solutions related to those issues.

Problem Statement

Lack of due diligence or insufficient due diligence in security is the cause of a wide spectrum of security and privacy issues in organizations. Currently, there is not much effort done in trying to identify the root causes of insufficient due diligence. To address this issue properly, it is important to thoroughly investigate the problem and raise awareness because many organizations give little to no attention to the issue.

Nature and Significance of the Problem

Insufficient due diligence or lack of due diligence is a considerable issue because it is ranked among the most severe security threats (CSA, 2013). It is often taken lightly when it should be under deeper investigation. In fact, insufficient/ lack of due diligence in organization can lead to the loss of personnel information, loss in company's assets and integrity and reliability. This study will be useful because it will raise security awareness and provide possible solutions regarding the problem.

Objective of the Study

The main objective in conducting this study is to solve the issue of insufficient/ lack of due diligence. The steps that will be taken to achieve this objective are as follows: Identify the root causes of the problem, investigate and try to find solutions to the problem, provide a framework of recommendation to organization that are already victims of this issue and finally raise awareness, among top management of organizations to prevent insufficient due diligence or lack of due diligence in security.

In addition to those steps, a checklist will be provided. This checklist will contain a list of items that will be used by organizations to verify and check if they are meeting all requirements regarding the implementation of due diligence. The purpose of the checklist will be to reduce and, in some cases, eliminate completely insufficient due diligence in security. Organization will be able to compare their security checklist to the elaborated checklist to ensure that they are following due diligence.

The checklist will also help organization to establish the link between the How and Five (5w) of Insufficient Due Diligence or Lack of Due Diligence. In fact, companies will know what Insufficient Due Diligence is, why it happens, where it happens, which is mostly in the security, development and engineering teams. Companies will also know who is responsible for that issue, when the issue occurs and finally how to solve the issue.

Definition of Terms

Insufficient due diligence has been and continue to be a grand mal of the security world today. Unfortunately, there are few people who know what this phenomenon is that affect the confidentiality, integrity and availability of information in companies. To solve an issue, it is important to have a deep knowledge of the issue and of all the terms related to it.

A better understanding of those terms will make it easier to understand the problem, its implications and how to solve it. This part of the paper will focus on a list of terms related to insufficient due diligence. Those terms will be defined to give the reader a better understanding of what this paper is about.

Due diligence

"Providing demonstrated assurance that management is exercising adequate protection of the corporate assets and compliance with legal and contractual obligations" (Harold, 2006). In other words, it is when the organization takes proper measures to ensure the security of the business.

Insufficient due diligence

It is ranked as one of the severe security threats. It is when all the security measures are not taken to protect the organization assets (CSA, 2013).

Lack of due diligence

This is when due diligence is nonexistent in a company's security protocol.

Compliance

In general, compliance means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws, policies, and regulations.

Compliance officer

A compliance officer is an employee whose responsibilities include ensuring the company complies with outside regulatory requirements and internal policies.

Compliance education program

A corporate compliance program is generally defined as a formal program specifying an organization's policies, procedures, and actions within a process to help prevent and detect violations of laws and regulations.

Information security management system (ISMS)

According to the definition provided in the article *9 reasons to implement Information Security Management System (ISMS),* an ISMS is "a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and

improving an organization's information security to achieve business objectives" (IT Governance, 2016).

Legal obligations

Obligation - Legal Definition. n. A moral or legal duty to perform or to not perform some action. A binding, formal arrangement or an agreement to a liability to pay a specified amount or to do a certain thing for a person or group of persons. See also duty and liability ("Dictionary", n.d.).

Contractual obligations

Something that a person is legally forced to do through having signed a contract. Usage to fulfil your contractual obligations ("Dictionary", n.d.).

Awareness program

Security awareness training is a formal process for educating employees about computer security. A good security awareness program should educate employees about corporate policies and procedures for working with information technology (IT) ("Dictionary", n.d.).

Ethics program

Compliance and ethics ("C&E") programs are organizational policies put in place to promote law abiding and ethical conduct. To be effective, they must be supported by procedures, communications efforts, and cultural attributes ("Dictionary", n.d.).

Security

"The state of being free for danger or threats” (“Dictionary”, n.d.).

Threat

"A statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done." (“Dictionary”, n.d.).

Risk

Is define as the fact of exposing (someone or something valued) to danger, harm, or loss; or a situation involving exposure to danger (“Dictionary”, n.d.).

Encryption

"The process of converting information or data into a code, especially to prevent unauthorized access." (“Dictionary”, n.d.).

Incidence response procedures

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs (“Dictionary”, n.d.).

Risk Assessment

A systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking (“Dictionary”, n.d.).

Risk Management

The forecasting and evaluation of financial risks together with the identification of procedures to avoid or minimize their impact (“Dictionary”, n.d.).

Experiential knowledge

Experiential knowledge is knowledge gained through experience, as opposed to a priori (before experience) knowledge: it can also be contrasted both with propositional (textbook) knowledge, and with practical knowledge (“Dictionary”, n.d.).

Summary

The first chapter of the paper was to enlighten the readers about the existence of insufficient due diligence or lack of due diligence in organizations and the threat that this issue can constitute for those organization, if not taken seriously. The next step in this study will be essentially about gathering facts regarding the consequences of insufficient due diligence but also the possible solution that can be elaborated to prevent or solve this issue.

Chapter II: Background and Review of Literature

Introduction

Insufficient due diligence or lack of due diligence in security is an existing problem. Even though not much research is available, researchers have tried to identify the causes of the issues and possible solutions through their work and study. Here are some reals world incidents that underline the massive impact that insufficient due diligence can have on companies. In this section of the study, the literature review related to the problem and literature review related to the methodology, as well as the background on the issue will be elaborated.

Literature Related to the Problem

1. *Security Breaches in Healthcare: How these 7 recent cases happened*

Jake Olcott (2016) lists several recent incidents that happened in the healthcare department because of insufficient due diligence. This article is about the consequences of insufficient due diligence. The author mentioned the name of the companies that were attacked, how it happened, the data that was compromised and their losses. There were millions of records compromised, and those numbers are frightening. Those incidents can endanger the integrity of those companies (Olcott, 2016).

2. *IRS, EITC and other refundable credits: consequences of not meeting your due diligence requirements.*

The IRS published an article (“consequences of not meeting”, 2017) that shows the financial retribution that one will have to pay if due diligence is not met. The consequences will be for all party involved. In fact, the client, the tax preparer and the employer can all become liable.

- The client will have to pay the money back with interest and could be banned from claiming for two to ten years depending on whether the error is due to fraud.
- The tax prepare will pay a penalty ranging from $500 to $5000 according to the reason why the error occurred.
- Finally, the employer will a penalty between $500 and $1,530.

3. *INTERFIRMA, the Aegis journal: Due diligence failures (2015).*

This article is pointing the fact that due diligence should start from the top management. Due diligence was existent and successful in this case, but management was not practicing it, which lead to costly consequences (Burke, 2015). The article is giving advices on what should have been done from the management side. The author few points that should be avoided while implementing due diligence. Those points are:

- Cheap due diligence.
- Insufficient resources (time, budget, subject matter expertise)
- Too much time and money.
- Wrong selection of people.

- Failure to understand the true meaning of due diligence as a process and not a thing.

4. *The consequences of inadequate due diligence (2019)*

This article is about the consequences of inadequate due diligence when selecting third party partners. In fact, most companies rely on third parties to assist in developing their business (Anjum, 2019). However, those organization cannot always control if due diligence is applied by those third party, which can result in a damaged reputation and brand devaluation for companies. Inadequate due diligence can be costly for companies.

5. *Failure to perform due diligence*

This article is about the civil consequences that insufficient due diligence can generate. Insufficient due diligence can lead to criminal penalties under Sarbanes-Oxley. Failure to perform due diligence is punishable by law. Therefore, it is important for companies that would like to succeed in a very competitive market, to conduct proper due diligence to avoid unnecessary costs and waste of time (Bukh, n.d.). The company will ensure to request and acquire all necessary documents to conduct a proper due diligence.

6. *Due diligence: definition and history of precautionary risk assessment (2019)*

This article is about the possible risks generated by insufficient due diligence. In fact, lack of due diligence can lead to reputation damage, economic risks of a purchase, financial risks in existing business relationships and legal consequences. A company reputation could be damaged if a proper due diligence is not conducted during acquisitions and mergers (“Due diligence: definition”, 2019). Also, if due diligence is not performed, hidden information will not be uncovered and that will constitute a financial risk and generated legal consequences.

7. *How integrity due diligence can protect your company from risk (2017)*

This article enumerates the potential consequences of not using due diligence. Some examples of consequences will be, reputational damage, impact to the revenue and profit of the acquirer, vulnerabilities and ineffective compliance programs. This article presents another proof that insufficient due diligence is not beneficial for companies. In fact, the cost of lack of due diligence will be higher than the one to implement due diligence (“How integrity due diligence”, 2017). When companies take the time to implement proper due diligence from the start, it will minimize the impact on revenue and profit.

8. *The top 10 due diligence disasters,* By Debbie Stephenson March 7, 2013

This article elaborates a list of the consequences that lack of due diligence can create for companies. This list clearly show how much insufficient due diligence can be costly. Because those companies did not take the time to properly conduct due diligence and take a deeper look at what they were getting involved with. Those are well known companies that could have afford to have proper due diligence implemented but decided otherwise (Stephenson, 2013). The consequences were disastrous on the financial aspect.

9. The Importance of Due Diligence Investigations: Failed Mergers and Acquisitions of the United States' Companies by Wendy B.E. Davis

In this article, the author talked about the fact that companies most of the time must use merge and acquisition to expand their business. However, In the process of doing so, companies do not take the time to conduct proper due diligence. Companies will then face costly consequences that ranges in millions of dollars (Davis, 2009).

The author gives examples of companies that did not properly conduct due diligence and ended up losing a considerable amount of money to correct the mistakes that were made. Once more, it is important to notate that, implementing due diligence from the beginning of the process, will save companies in time and money rather than trying to fix mistakes due to insufficient due diligence.

10. 7 Consequences of Improper Regulatory Due Diligence (2018)

In this article, the focus is on the merger and acquisitions ventures particularly on health and products industries. In fact, when merging with or acquiring other business,

companies do not complete proper due diligence and therefore face multiple risks (“7 Consequences of improper”, 2018). The author elaborated the following list to accentuate the risks of improper due diligence:

- Delays or cancellation of product launches
- Rebranding of products
- Costs of coming into compliance
- Increased market liability
- Increased exposure to government enforcement
- Failure to meet commitments to third parties

11. *Lack of Due Diligence: How It Can Hurt Your Company – iCorps*

In this article the author emphasizes on the fact that security threat is not always related to new virus or a piece of malware (“Lack of due diligence”, 2014). It is usually due to improper due diligence established by companies. Lack of due diligence can be costly for companies like tech companies. For example, according to the article, the average cost of downtime is running an average of $7,900 per minute across industries.

Literature Related to the Methodology

1. *Multi-dimensional enterprise-wide security: Due diligence*

In this paper the author Rebecca Herold highlights the definition of due diligence and the benefit that could occur when applied in the company. The author emphasizes the fact that top management should be involved in promoting due diligence among

their employees (Herold, 2006). She also gives solution on how to prevent insufficient due diligence. Among those solutions are:

- Implementation of training and awareness program
- An effective and executive supported information security education
- The role the leaders should not be only to publish information on security and privacy policies but to also understand them.
- Information privacy, security and compliance education program should be in place

2. *Security Breaches in Healthcare: How these 7 recent cases happened*

This article provides steps that should have been used by the healthcare organizations to prevent those attacks (Olcott, 2016). The author Jake Olcott elaborated those few points as solution:

- Know the security performance of the vendors
- Incorporate due diligence during the selection stage of the product or service
- Monitor security performance in real time
- Ensure third-party software are up to date
- Possible vulnerabilities must be fixed quickly

3. *Nine reasons to implement an information security management system (ISMS)* (2016).

This article is covering the use of ISMS to ensure security in the company. The author Lewis Morgan mentioned in that article that one of the benefits for implementing ISMS is that it demonstrates due diligence. Implementing due diligence, gives credibility with staff, clients and partner organizations (Morgan, 2016). Earning credibility will be beneficial for companies. Credibility is a key point for companies to maintain customers and therefore develop their businesses.

4. *Warning: Be sure your due diligence is thorough*

This article is about the benefit of implementing proper due diligence. In fact, when proper due diligence is performed, it will provide detail information on the possible risk related to the choice of a third party, the compliance followed, evidence through proper documentation and validation (Ritter, 2017). Due diligence can help uncover and quantify risk according to the article.

5. *Due diligence: definition and history of precautionary risk assessment*

This article provides the different areas that are most frequently examine in due diligence and should be followed to avoid costly consequences. Those areas are financial due diligence that will focus on considering strength and weaknesses, market and commercial due diligence this will help evaluate the suppliers and the contracts involved in the negotiation, tax due diligence, operational due diligence, technical due diligence and environmental due diligence (“Due diligence: definition and history”, 2019).

6. *How integrity due diligence can protect your company from risk*

This article is about a specific type of due diligence called integrity due diligence can be beneficial for companies. In fact, this due diligence will help identify possible risks the company could avoid while selecting business partners and contractors (“How integrity due diligence”, 2017).

7. T*he Importance of Due Diligence Investigations: Failed Mergers and Acquisitions of the United States’ Companies*

In this article, the author elaborates the reasons why it is important to do a due diligence investigation (Davis, 2019). According to the author that investigation should include:

- Ascertain purchase price and method of payment
- Determine details about acquisition agreement
- Evaluate legal and financial risks of the transaction
- Evaluate the condition of tangible and intangible property, physical plant and equipment
- Analyze potential antitrust issues
- Determine compliance with relevant laws and disclose any regulatory restrictions

- Discover liabilities or risks that may be deal-breakers

8. *Understanding the Importance of Due Diligence*

This article underlines the importance of due diligence. In fact, implementing due diligence is critical because it will help save time and money, ensure the quality of financial information, ensure adequate information is provided during the sale and purchase transaction (Hayes & Aue, 2016).

9. *5 Types of Due Diligence Services, and Benefits*

The author of this article provides 5 most used types of due diligence and theirs benefits (“5 types of due diligence”, n.d.).

- Financial due diligence identifies the companies’ assets and potential liabilities
- Operational and IT diligence is used to make sure operations and current technologies are operating efficiently and effectively
- People due diligence will focus on evaluating, in acquisition for example, the old organization structure and the new one. It also focuses on employment contracts
- Regulatory due diligence will review if the companies comply with regulatory requirements within its jurisdiction
- Environmental due diligence will ensure that companies are following environmental laws and policies

10. Due diligence in mergers and acquisitions April 15,2019 by Brandon Downs

This article is about the steps involved in due diligence and its importance in the process of mergers and acquisitions. Due diligence is important because, when properly implemented, it will lower the risk of unexpected legal and financial problems (Downs, 2019).

- Gather the team responsible for due diligence that include a team of legal and financial experts
- Gather important documents needed that includes details checklist to follow for an adequate implementation
- Information review to clarify possible concerns and request additional information if needed.
- Establish the purchase agreement

11. The benefits of effective financial due diligence, December 5th, 2018, by Moore and Smalley

This article is about the benefits a properly established financial due diligence. Financial due diligence will focus on the historical financial performance but also on the forecast financial performance for the company (Moore, 2018). It is important to do a financial due diligence review. The source of the information used for the review includes:

- Historical financial data
- Current financial data
- Forecast financial information

That review should provide the necessary information needed by the company to avoid costly consequences.

Background Related to the Problem

Insufficient due diligence or lack of due diligence in security is a costly issue and should be addressed in order to raise awareness in organization, about the impact it can have on the success of the company. At this point of the study, it appears clearly that insufficient due diligence or lack of due diligence is a considerable security problem.

That issue can have many repercussions for companies who take it lightly. The next step of this study will be to demonstrate the importance of due diligence and its benefits for the organization, the drivers of insufficient / lack of due diligence and possible solutions related to those issues.

Importance and Benefits of Due Diligence

As Rebecca Herold stated in her article *Multi-dimensional enterprise-wide security*: Due diligence, "due diligence should not only be a check box" (Herold, 2006). This sentence translates into the fact that top management should not limit their actions

by only writing and posting securities and privacy policies and procedures, but they should implement them, do follow ups and fix any gaps in the program.

Implementing due diligence in a company is a crucial step for the success and stability of the company. In fact, due diligence helps organizations understand the risks related to security and gives them a better understanding of their needs; therefore, they can avoid overspending and wasting resources.

Having Due diligence implemented in a company is also beneficial because it makes it easier to identify, security wise, who oversees key actions such as, incidence response procedures, encryptions and who is monitoring security on the client side and the provider side.

The list of benefits that a company can gain from implementing due diligence and practice it, is exorbitant (“Due diligence: from business”, 2014). However, below is a list of few of the benefits. Due diligence helps:

- Promote security
- A company to follow laws and regulations, compliance
- Identify the key information about clients or third party, shareholders beneficiaries and board members
- Cover risk assessment and risk management
- Provide proof of identity of different participants.

How to Properly Implement Due Diligence

Based on exciting research on due diligence, there are various ways of implementing it. However, some points are essential in implementing due diligence, and those steps are common in most studies. The steps that are presented in this part of the study, were retrieved from FreePint*, Due Diligence- from Business Burden to Business Benefit, and* are almost the same in other studies (“Due diligence: from business”, 2014). The proper way to implement due diligence is as follow:

1. Trial, test and benchmark proposed due diligence services to help determine how they complement or replace resources
2. Ensure due diligence services are scalable and flexible enough for you to implement and adapt to regulatory change
3. Assess the availability of management intelligence and audit data to help track and demonstrate robust compliance and ROI
4. Build in regular reviews with stakeholders to ensure due diligence processes align to changing business requirements
5. Build in regular reviews with due diligence service providers to reflect above and provision of new features and content.

Drivers of Insufficient/Lack of Due Diligence

The root causes of Insufficient/lack of due diligence in security are various. Insufficient due diligence can result from a mistake made or an action taken by the personal of the company, top level management or even a third-party contractor.

Security should be the main concern in all steps of the development plan in organization.

In fact, it is important to evaluate all parties involved in the development of the organization and know which part each of them is playing. Identifying key participants will make it easier to know where the issues are coming from and find adequate solutions. The list below reflects some drivers of insufficient due diligence and different explanation corresponding to each one of them.

Lack of attention

This happens when employees or key people in the organization do not pay attention to their actions. For example, those employees will leave passwords access cards or important information unattended or expose on computers or on the desk for everybody else to see it. Sensitive information should not be left in the open for anyone to have easy access to it.

Passwords for instance, should be stored in a secret file, for example, and not on the desktop or on sticky notes or lose pieces of paper that are left on the persons' desk. Those type of actions are mistakes that can affect the company's confidentiality, integrity and availability which can constitute a security issue and lead to loss of revenue and customers.

Lack of experience

Experience is a skill acquired because of practicing something for some time. Not having experience on how to operate a specific technology can be very dangerous for the company because of possible errors that can occur leading to possible losses or leakage of important data. Since getting experience on a topic comes from practicing that topic, employees should train more on how to operate different tools needed to complete their job.

The training should be done on a timeframe long enough so that the improvement of the employee can be seen over the time. There should be mentoring, or shadowing establish in the company so that new recruits can gain experience by working with the employees that have been in the company for a considerate amount of time. An employee that lack experience will always make errors until something is done to help gain experience.

Lack of identifying key employees

When a company doesn’t know who its key employees are, in other words, when the company cannot identify who is supposed to work on a specific technology or have clearance to access certain document, it can lead to security issues. In fact, if key employees are not identified, anyone can have access to sensitive information and consequently anyone can infiltrate the company and leak sensitive information.

In fact, distinction between each employee level of operation should be establish. For example, it is important to know who has clearance access the operations room,

where the servers are located and who can only have access to the common areas of the company. Establishing that distinction will make it easier to identify and narrow it down to find the culprit if there was to be a leak in the company.

Lack of communication about hidden projects

Communication is a very important tool in the success of any project. Lack of communication about hidden projects can constitute a danger to the company. When those hidden projects are not communicated to the IT technician, they cannot take adequate measures to ensure that security is update and protect the organization's data.

Even though some project need not to be revealed to the whole company until its completion, it is important to let the IT technician know about the project since the technician is the one that can put up firewalls and upgrade the security level to accommodate the new project. Lack of communication about hidden projects can prevent the technician to properly do the job required to protect the data.

Lack of knowledge

When a new product or service is created, there should be necessary actions taken to educate the personal on how to use it and how it works. Failing to do so will lead to a lack of knowledge of the product or service. When a new technology or tool is implemented, the proper training on how to use it or develop it, should also follow to avoid lack of knowledge.

Lack of knowledge happens when the people in charge of designing the project are unfamiliar with the actual technology they need, to develop the project. That is because there is no step by step on how to design the project, or there are new ways of designing it and the designer does not know about. Employees should be better educated on the technology they will have to use for the project they are working on.

Lack of resources

The organization might not have enough resources to properly conduct security check for its data and ensure that it is not stolen or tampered. Lack of resources can lead to a poor implementation of due diligence. It should be the company top priority to gather all necessary resources to increase or at least have the minimum-security level needed.

A company that lacks the necessary resources to ensure that the proper security is established, will have difficulties implementing due diligence, therefore will be at risk of facing insufficient due diligence or lack of due diligence in security. It will be wise to always make sure that the necessary resources are available to conduct the proper security checks to prevent loss of data and important information.

Weak policies

Organization should have strong security policies. Having weak policies can constitute a threat for the company. Top level management should up their security and policy standards. Security standards and policies should match the business level of the

organizations. This means that the policies in a fortune 500 company should not be the same as the one in a smaller company.

When the policies are established, standards should be implemented and used to reach policies objectives. There should be some mandatory controls and requirement for each level of the organization. For example, if a policy is established and there are no actual ways to control that policy, it become weak and therefore easy to bypass by employees. Mandatory controls and requirement should be used to strengthen the policies to avoid insufficient due diligence.

Third party technology

When using a third-party technology, it is often hard to evaluate the security level for that third party and ensure proper communication to meet customers' requirements. There is so much verification and control that an organization can do when requesting the service of a third party.

Also, most of the time the organization will assume that the third-party technology is already secure and that all necessary measures were taken to ensure that the technology meet security requirement. For instance, most businesses use third party technology to introduce a new product to their customers.

In some banks for example, a customer can use third party technology or application to quickly transfer money to another customer that has the same application. Even though the bank will be part of that transaction, the bank does not have complete

control of the security of that application. The use of third-party technology can create insufficient due diligence or lack of due diligence.

Lack of planning

Maintenance, updates and follow ups are necessary for any company using technology in the development of their business. It is important for an organization to plan, set aside specific times and resources to updates and general maintenance of software or any technology used. When the organization does not plan to do follow ups or schedule maintenance of the technology it can create security issues, because the technology will not be up to date and will not be able to fight against newer threats.

Technology is always evolving and with that, the security threats that goes with it ("What are the 12 biggest", 2016). Hackers are becoming more and more agile and can find a way to access almost anything. Consequently, organizations should also get ready to counterattack those attacks by planning regular updates and maintenance. Lack of planning from the organization will lead to an increase of security threats and will make it difficult to eradicate the problem of insufficient due diligence.

Poor management/lack of management involvement

Poor management can lead to security issue because, the managers will not take the appropriate measures to ensure the security. Management is supposed to give direction and oversee the evolution of the organization. That role also includes making sure that security protocol is followed by both the management team and the employees.

When management is not involved, there will just be delegation of tasks and not direct involvement in the development process (International Due Diligence Organization (IDDO), 2018). Management should be first in line to show the employees how it's done and be involved in the implementation of security procedures. Lack of management involvement can lead to insufficient due diligence.

Rush in decision making about security provider

Rushing into deciding is never a good idea. It lost of the time leads to poor or bad decision making. Not taking the time to conduct researches on the security provider the company wants to work with can lead to the organization taking fewer steps to ensure that the service they are using is safe for the company and potential customers.

Before choosing a security provider, the company should always conduct the appropriate evaluation, background check and reviews needed. The security provider should pass all the security tests and have all the features needed by the company to ensure the desired level of security; in the product they are offering.

Lack of familiarities with the security technology

Technology is always changing. Therefore, whenever a new security technology is introduced in the company, the employees should receive the proper trainings related to that new technology. The trainings will help them get familiar with the new technology. When, workers are not familiar with the technology they can make mistakes on how to use and how to secure the technology.

It is important for all members of the company to be familiar with the security technology to avoid unnecessary consequences. In fact, the best way to avoid insufficient due diligence will be know the tools that are being used to minimize mistakes and costly consequences for the organization.

Turnover of security policy makers, or enforcers (Experiential knowledge)

Experiential knowledge is only acquired through experience gained over time. Knowledge is not carried over to the newcomer in the company. Therefore, if the person that is specialized in a specific subject leaves the company, then the knowledge is gone with that person because experiential knowledge is not transferable.

For example, when a person who acquired experience in a technology used for data security, retires, quit or is fired, that person takes with them an important knowledge that cannot be thought in the short period of time dedicated to the turnover. That time frame can be a window of opportunity for hackers to attack the security system of the company. To avoid, insufficient due diligence in that case, measure should be taken to have a better turnover of security policy makers or enforcers.

Possible Solutions and Recommendations

Now that the root causes of insufficient/lack of due diligence have been identify, the next step will be to make some recommendations about possible solutions regarding the issue (Pandey, 2015). The recommendations and possible solutions presented in this part of the paper are based on the drivers of insufficient due diligence discussed above.

Based on the information collected, it appears that the issue is created by all participants in the organization. In fact, everyone from the highest level of management to the employees in their cubicles, plays a part in insufficient/ lack of due diligence. Consequently, the solutions should also start from the top of the company.

Possible recommendations that could solve the issue are as follow:

- Develop a training and awareness program. Through the training, employees will learn how to become more careful with sensitive information and know the different actions to take in case of an incidence occurring because of their lack of attention. The training will also help raise awareness among workers about possible security threats and learn about the use of new technologies to avoid mistakes or misuses.
- Implement a program that will focus only on educate about security, information privacy and compliance. This program will clarify the dos and don’ts of security and privacy and clarify possible grey areas regarding laws and regulations.
- Top level management should ensure that policies regarding security, compliance and ethics are reinforced. Those policies should not be written only for because they need to be written, but they should be put in practice; and that is the responsibility of top-level management. Management should always participate and show their support to those programs, to lead by example and encourage the employees to also participate and take it seriously. To do so, management should have a good understanding the policies and program themselves before implementing them.

- Highest management should implement Information Security Management System (ISMS) because it is an approach that, when implemented, demonstrate due diligence and therefore, gives credibility to the employees of the company, reassure the clients, and partners organizations. In addition, management should identify and know all keys employees, meaning who oversees what and when, and ensure that maintenance of the technology used is done frequently to minimize risk of threats.

Summary

Chapter two was to show that there are in fact existent research on lack of due diligence and insufficient due diligence topic. Those research show that insufficient due diligence can constitute a costly issue, however there are multiple solutions that can be applied to avoid such costs. The chapter also elaborated more on the background of the problem by demonstrating the importance of the issue and how to properly implement due diligence to avoid it being lacking in security. It was also important to identify the drivers of insufficient due diligence in security and propose some recommendations on how to solve it.

Chapter III: Methodology

Introduction

At this point of the paper, it is important to acknowledge that insufficient due diligence is an existing problem that need attention. The problem of insufficient due diligence has been properly analyzed and multiple solutions were provided for a proper implementation of due diligence. Those solutions provided do not always reflect how to properly use them for each one of the problems created by insufficient due diligence. The following part of this paper will elaborate on the proper method that should be followed to solve the problem mentioned in chapters 1 and 2.

Design of the Study

A qualitative approach will be followed for this next step of the paper. This approach was selected because it will allow to use a scientific method of observation to gather non-numerical data. This is the adequate type of research for this study because it will allow the use of meanings, definition, concepts and description of terms to emphasize how to reduce or completely avoid insufficient due diligence.

Also, to clearly identify the proper due diligence implementation, a taxonomy will be elaborated. The following taxonomy will show the classification of different types of due diligence and how to implement them. This taxonomy is to provide a clear understanding of the fact that due diligence exists, and it is a process to follow to minimize or eliminate insufficient due diligence.

In fact, during acquisitions and mergers for example, companies will be able to go down the list and make sure that all types of due diligence are examined during the establishment of their businesses. Companies will be able to know that they must evaluate all the third-party institutions and vendors from which they will need services to develop their businesses. Companies will be able to establish risks assessment internally, externally and even for remote security to ensure that transparency is present.

That risk assessment will be done by collecting and evaluating necessary documentation available in companies. Companies will need to go through those documentation thoroughly. Finally, at the end of each assessment, it is important for the companies to audit and review the information gathered to ensure that nothing was quickly overseen, so that companies can avoid hidden surprises and additional cost.

The taxonomy bellow shows the way to properly implement due diligence. When followed it will allow companies to reduce their costs and increase revenues. Companies will also be able to maintain integrity and a good reputation with their customers. This taxonomy is a map to success. In fact, this taxonomy is set up to provide a clear path for companies to follow to avoid or reduce insufficient due diligence. The first branch in the taxonomy show a list of different types of due diligence.

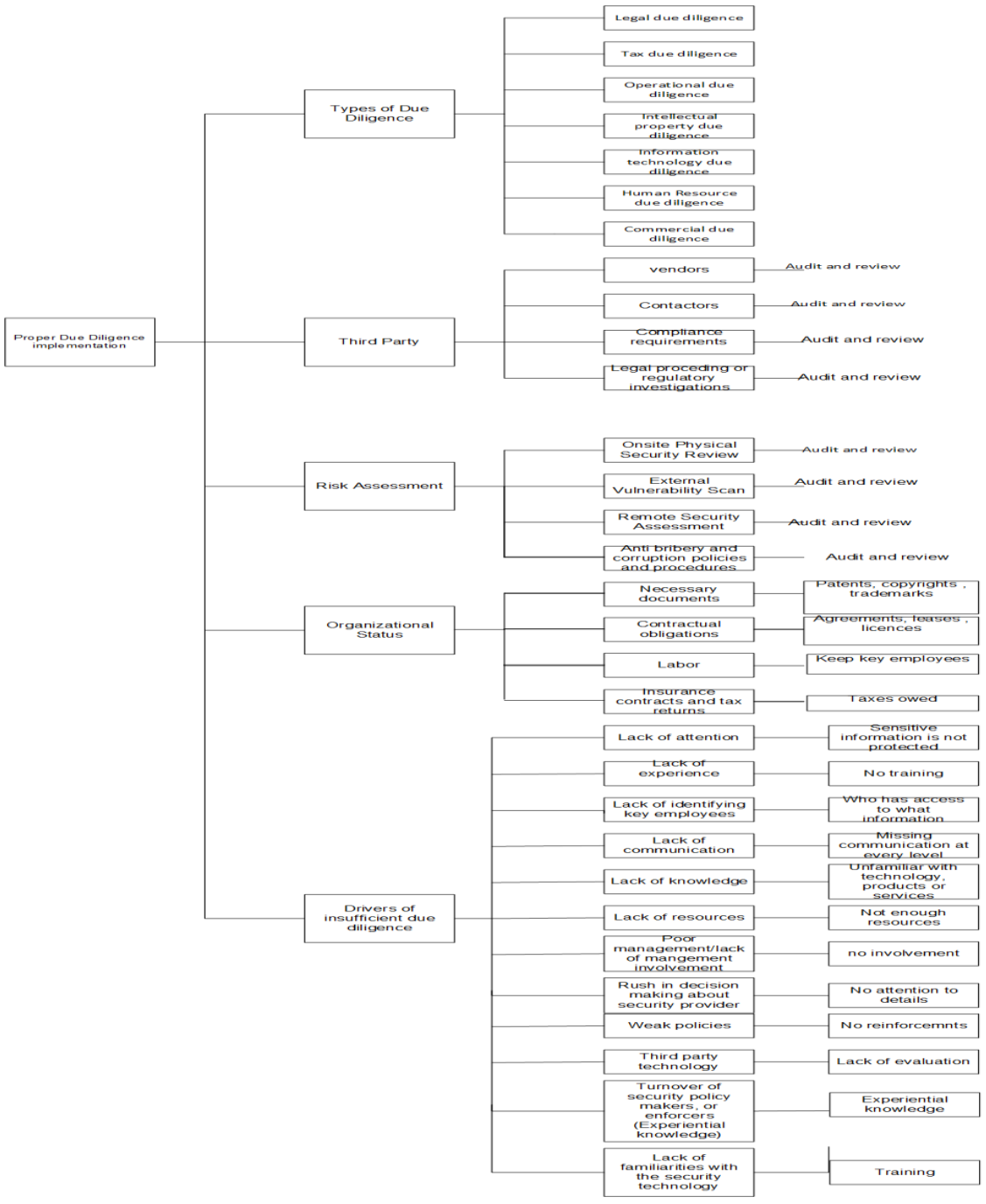
Listing the types of due diligence will help raise awareness among companies about the existence of more than just one type of due diligence. It is important to raise

awareness about the existence of more than just one type of due diligence, because most companies do not realize that there are different types of due diligence that exist. In fact, knowing the types of due diligence that need to be implemented will make it easier for leaders to know which direction to take to eliminate insufficient due diligence. It is always easier to have something to follow when going through implementation of due diligence. The taxonomy will be divided in section for better analysis of each part.

The goal of the taxonomy is to provide a support to leaders in their decision-making during acquisition and mergers. In fact, having a visual aid on the step-by-step actions to take will help reduce insufficient due diligence and can only be beneficial for leaders and their companies. Following the visual aid, will help companies minimize mistakes. Leaders will be able to go down the list to ensure that every due diligence step is followed and applied properly. Once that is done, insufficient due diligence will be eradicated from companies.

Figure 1

Taxonomy of proper due diligence



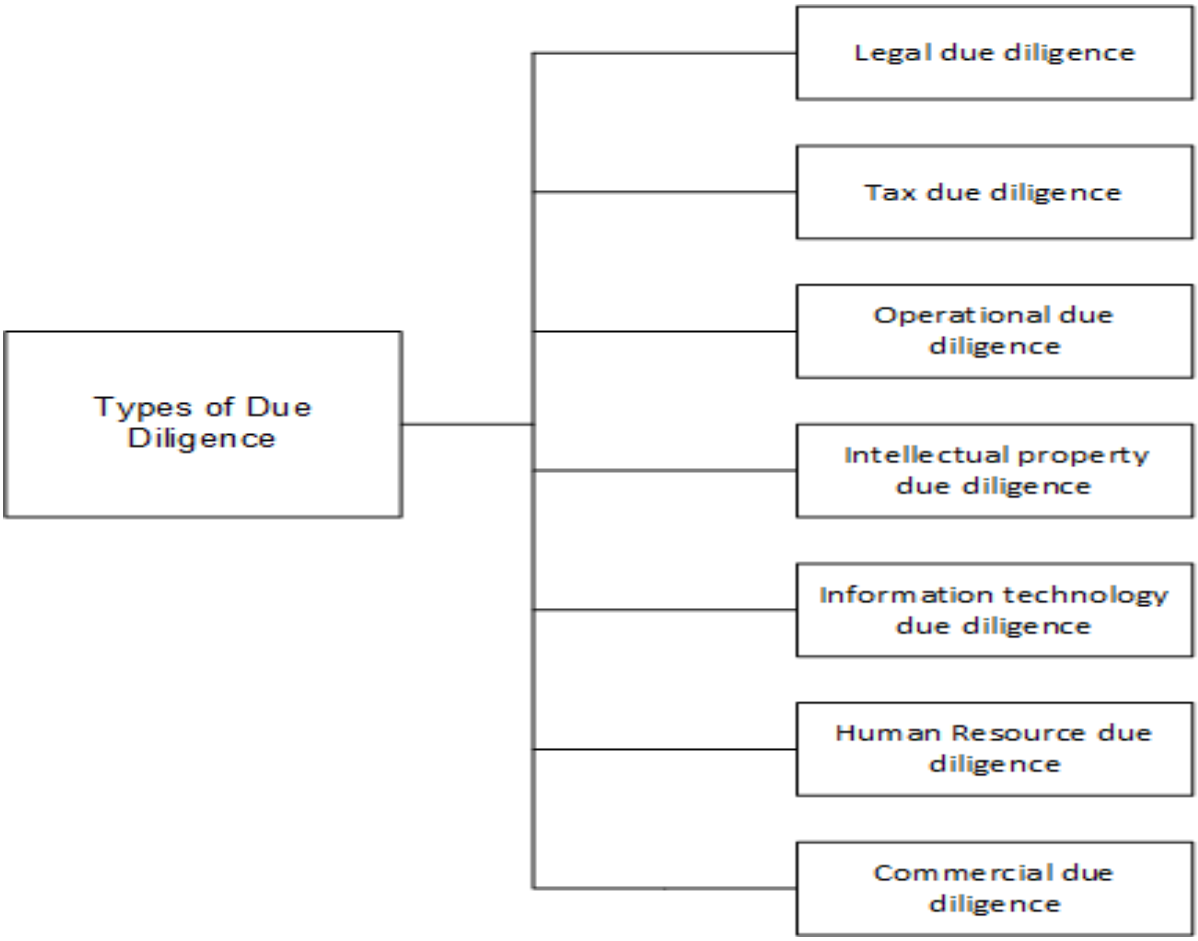
This taxonomy shows the different types of due diligence that should be implemented by companies. The overall taxonomy is divided into multiple layers. The layers of the taxonomy are then developed into different branches. The taxonomy starts with, the types of due diligence, followed by due diligence on third parties used during mergers and acquisitions.

The next branch on the taxonomy will be allocated to risk assessment due diligence, followed by organizational status due diligence. The last branch of the taxonomy will be about the drivers of due diligence. That branch will provide the reasons for which insufficient/lack of due diligence exist in companies. Due diligence should exist at every level of development and every aspect of the company.

It is important to know about the existence of those different types of due diligence to better understand them and take adequate measures to implement them. Ounce awareness is established about the existence of the different types of due diligence, it become easier to analyze them and apply them. Raising awareness about the existence of different types of due diligence will contribute to reduce or eliminate insufficient due/lack of due diligence in companies.

Figure 2

Taxonomy of types of due diligence



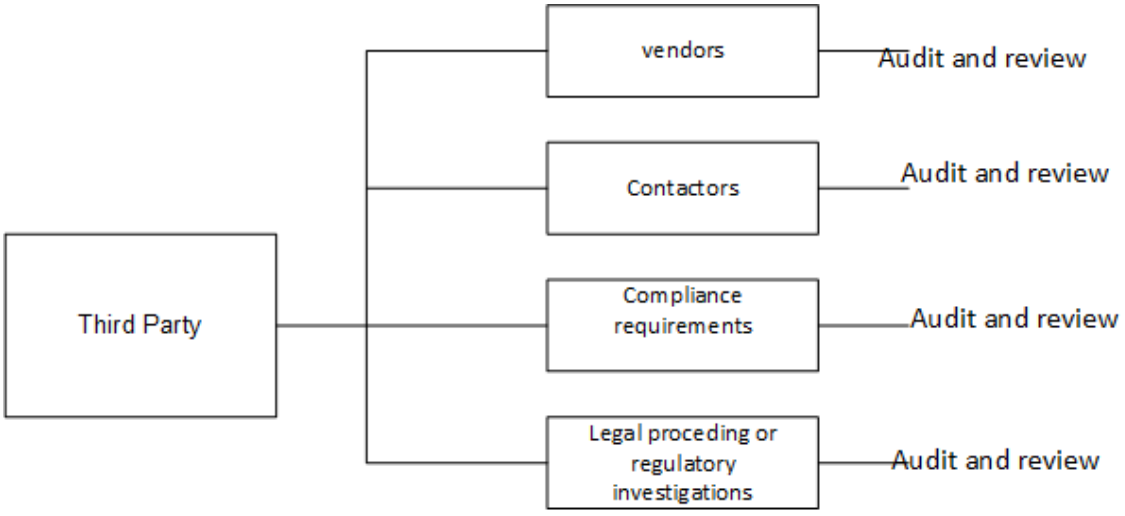
The next section of the taxonomy will focus on due diligence about third parties used by companies. The taxonomy about third party will provide deeper understanding of third parties that are involved in the company's development. In fact, before engaging into acquisitions and mergers, companies should ensure that they gather all the necessary information regarding vendors, the different contracts, make sure that compliance is met and finally ensure that all legal procedures are followed.

Vendors will have to be thoroughly evaluated to ensure that they are following due diligence. The different contracts that will have to be signed, need to be analyzed and reviewed to ensure there was no hidden clause. Companies will also need to ensure that the third parties they will be using are meeting compliance requirements and are compliant with rules or standards required to meet due diligence.

The last branch of this taxonomy will help companies ensure that legal proceeding or regulatory investigations are properly conducted and followed to meet due diligence. After conducting due diligence at each branch, it is also important to always conduct audit and review the information gathered at the end of each due diligence. Double checking the information by conducting audit and review will help reduce the margin of error.

Figure 3

Taxonomy of third party



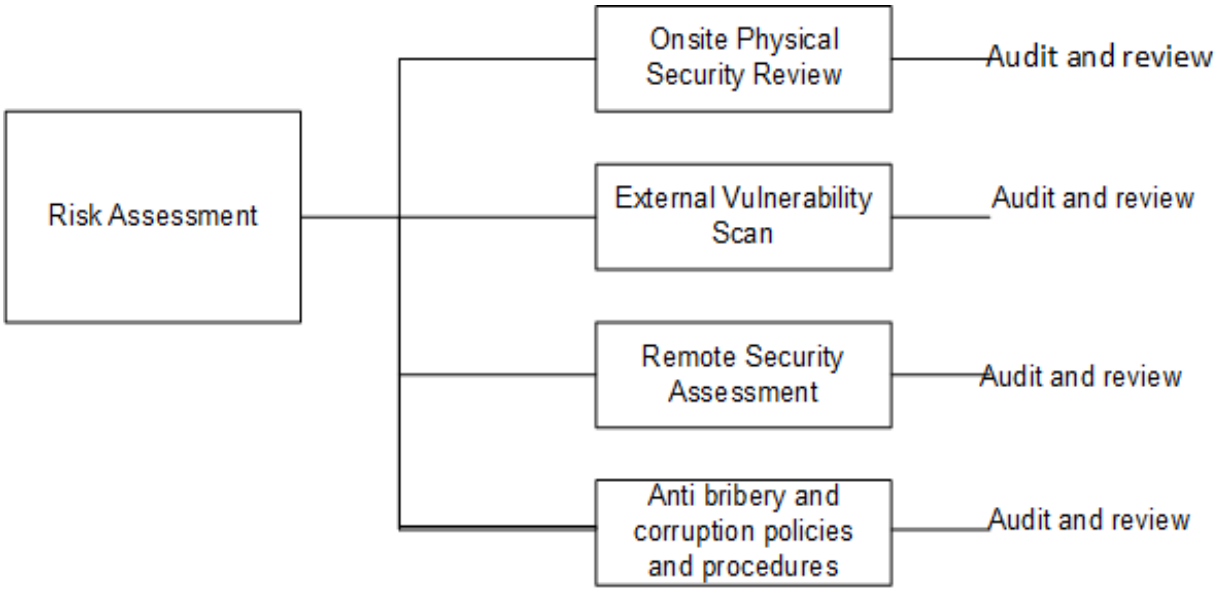
Every company should always evaluate risk during mergers and acquisitions. In fact, going into mergers and acquisition without conducting risk assessment can lead to costly consequences for companies. Risk assessment is a very important step in conducting due diligence because it will allow companies to be aware of potential risks and therefore take the required measures to resolve or prevent those risks.

The following taxonomy will help in evaluating risks by evaluating security and vulnerability of the environment. In fact, companies will need to conduct onsite physical security review to ensure that employees are safe and work areas are free of risk for employees and the company. Next, companies should conduct due diligence about external vulnerability by scanning all potential external factors that could constitute a vulnerability for companies. Most companies use third party to provide remote security, therefore it is important to conduct a remote security assessment to minimize risk.

Finally, companies will need to make sure that anti bribery and corruption procedures are already in place and are being executed. In fact, it can become costly for companies if proper due diligence is not implemented to prevent bribery and corruption from taking place. After each evaluation, audit and review should always be conducted to ensure that no information was overlooked and correct possible errors if needed.

Figure 4

Taxonomy of risk assessment



The following taxonomy will allow organizations to gather the necessary documents and contracts about the third-party organizations they desire to do business with. In fact, companies will need to access documents like patents, copyrights and trademarks to ensure that everything is up to date and meeting due diligence requirements. It is also important to review contractual obligations such as agreements, leases and licenses to make sure there is no hidden issues that could result to costly consequences for companies going into mergers and acquisitions.

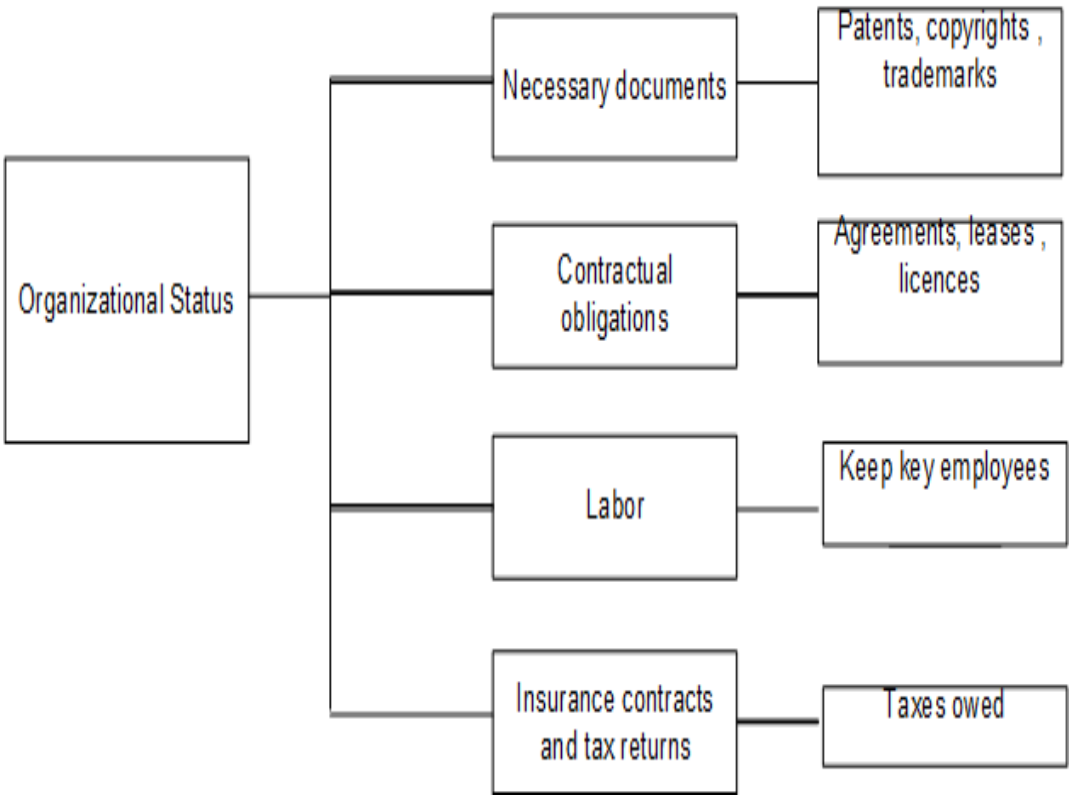
Conducting due diligence on companies' labor will help in identifying and retaining key employees. In fact, during acquisitions and mergers, companies will benefit in conducting proper due diligence about labor. That will help them maintain employees that are key to the success of the company. Keeping those employees will

help reduce error margins, cost of hiring and training new employees. Key employees already have more background knowledge about the company; therefore, it will be useful because it will allow companies to move faster during their development.

Finally, companies will need to conduct due diligence on insurance contracts and tax returns to verify that there were no taxes owed before going into acquisitions and mergers to avoid any possible surprises. After evaluation and assessments companies will know where to direct their focus to eliminate insufficient due diligence.

Figure 5

Taxonomy of organizational status



This part of the taxonomy is about the drivers of insufficient due diligence. A list of possible drivers was established to provide companies with an idea of possible drivers of insufficient due diligence and the possible causes linked to those insufficient due diligence. In fact, insufficient due diligence could result from lack of attention from employees or top management of companies, lack of attention could lead to sensitive information not being protected and therefore leading to costly consequences.

Lack of experience is another driver of insufficient due diligence. When employees do not have adequate experience and training about a subject or the job they are performing, it could lead to insufficient due diligence. The next driver will be lack of identifying key employees which could be caused by not knowing who has access to what information. Information flow and access should be closely monitor.

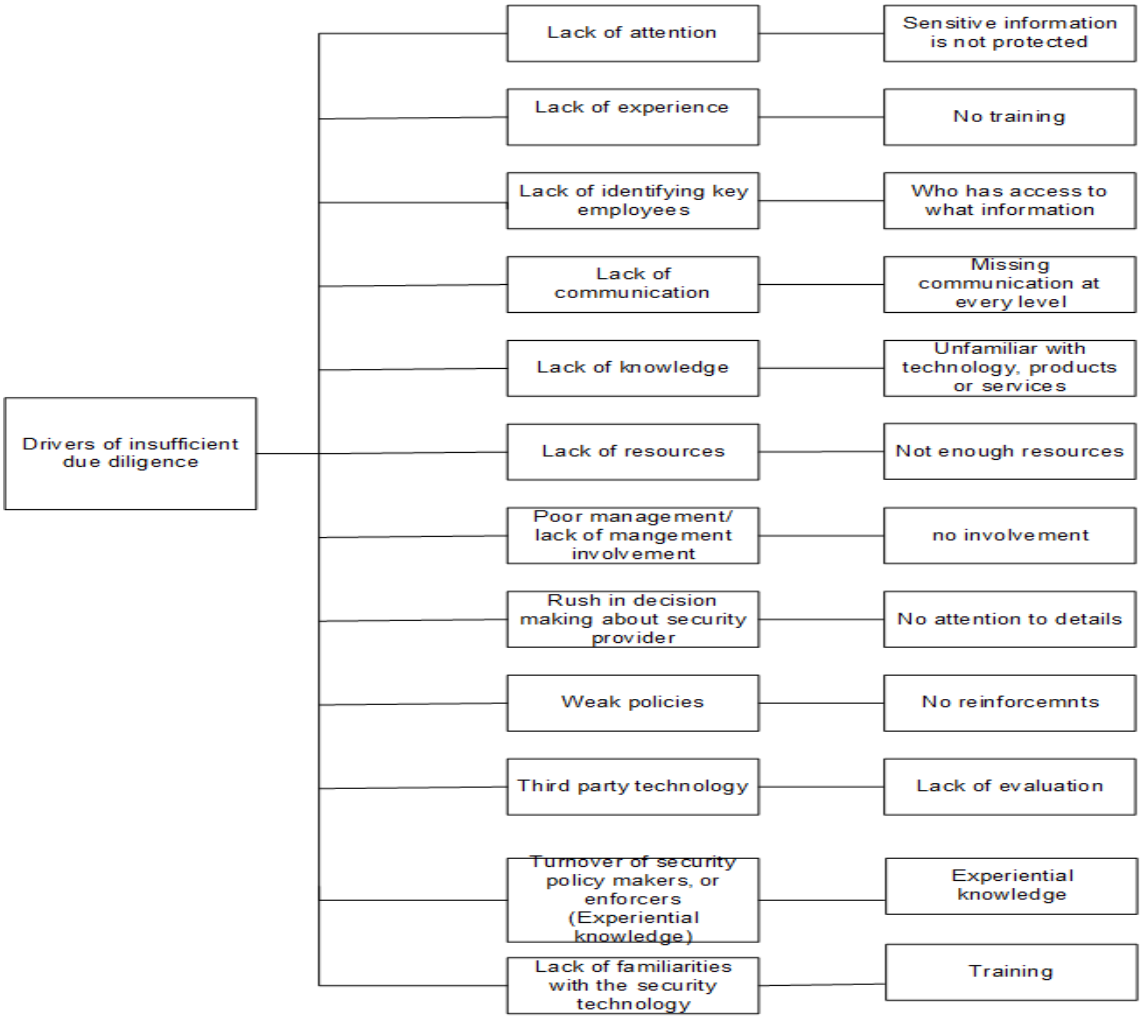
Lack of communication due to communication missing at every level and lack of knowledge, such as unfamiliarity with technology, products or services could cause insufficient due diligence. The lack of resources to properly train employees and lack of involvement from higher management are considered drivers of insufficient due diligence.

Companies rushing into decision making when considering which security provider to go with, could lead to insufficient due diligence. The cause of this lack of due diligence is when companies are not paying attention to details when selecting their security providers. Other drivers of insufficient due diligence are weak policies caused by lack of policies reinforcement, and third-party technology that are not reliable

because of lack of prior evaluation of those third-party technologies before using them. Another driver of insufficient due diligence will be a high turnover of security policy makers or enforcers which can cause loss of experiential knowledge. The last driver of insufficient due diligence on this taxonomy will be lack of familiarities with security technologies caused by not enough training available.

Figure 6

Taxonomy of drivers of insufficient due diligence



Data Presentation

The main purpose of this chapter is to establish a list of possible ways to raise awareness about insufficient due diligence. In fact, raising awareness about the existence of insufficient due diligence will help in resolving that issue. Companies will have to acknowledge that it is an existing issue, so that proper solutions could be established. That list will be in the form of a checklist that will provide the steps to follow to ensure due diligence is being followed or to correct insufficient due diligence.

The list below reflects the checklist to follow to prevent insufficient due diligence. The checklist will be divided in two categories. The first category will accentuate ways to raise awareness in organizations, the second one will focus on how to establish a security process to safeguard information and the last category will provide ways for due diligence implementation to stay constant.

Ways to Raise Awareness

Listed below is a succession of ways to raise awareness in organizations about the importance of due diligence (Hayes, 2016) which will help in reducing or eliminate insufficient due diligence.

- Seminars
- Quarterly meetings
- Mandatory compliance initiated by the company for the employees and management team
- Educational classes and training

- One on one review and evaluation
- End of year evaluations
- Available information resources
- Coaching and mentoring
- Educational games and activities

Definition of Terms and Goal of Practice

Seminars

A seminar can be defined as a conference, a meeting or a training with a purpose of education (“what is a seminar”, n.d.). It can be in the form of a class during which lectures, will be giving to employees by management. Those lectures will usually be about new changes in products, services and security that will have to be implemented and followed to meet certain requirement. The goal of seminars will be to provide better insight and understanding of a subject.

Quarterly meetings

Those meeting will take place usually every three (3) months. The main purpose of those quarterly meetings will be to go through statistics and review the results for the time that has passed. Those results will be used in the evaluation of employees' performances, to ensure that everyone is meeting the required set goals to meet due diligence (Wick, 2012). Finally, during quarterly meetings, it will be a good time to educate on new ideas that could be used to reduce insufficient due diligence and to set the tone and expectations for next quarter

Mandatory compliance

Mandatory compliance will be initiated by the company for the employees and management team. Compliance is the fact of complying with set of rules or command with the goal of limiting or avoiding security issues. Mandatory compliance will have for goal to ensure that rules are followed to avoid insufficient due diligence.

Educational classes and training

This method will be used to educate and train employees on updated due diligence that should be followed to minimize or avoid errors. The goal here will be to ensure that everyone is aware of changes and in trained on how to implement those changes. Providing educational classes and training will be the best practice to fill in employees with the knowledge needed for them to practice adequate due diligence and by the same mean avoid insufficient due diligence.

One on one review and evaluation

Conducting a one-on-one review and evaluation will be very beneficial for employees and the management team. In fact, this allocated time with each employee will be a good opportunity to evaluate their monthly progress, their adherence to due diligence and make necessary constructive critics and adjustments to reduce and eliminate insufficient due diligence.

End of year evaluations

This evaluation is mostly to draw a summary of the yearlong progress. It will be the time to reflect on the good and bad decisions taken during the year. The idea here will be to make a comparison between actions that contributed to a good implementation of due diligence on one side and on the other side on those that led to insufficient due diligence. That evaluation will also be used to improve performance for the years to come.

Available information resources

One key solution to avoid insufficient due diligence is to ensure that when there is an update regarding a product or service, that information is made available as soon as it is updated. Making the resources available to employees will reduce the error margin. Employees will be able to refer to the information available to them to be able to follow due diligence. When resources are made available, there should not be a raison why they would not be used to avoid insufficient due diligence.

Coaching and mentoring

Due diligence should be introduced from the very beginning. In fact, new employees coming in the company should go through some mentoring and coaching session right from the beginning. Also, the people in charge of coaching and mentoring should be able to communicate correct information to the new coming. It is basically the foundation for a good implementation of due diligence.

Educational games and activities

Learning is always easier when it is in a form of games and activities. Those games and activities will allow employees to interact with each other but also to learn about new products, services. The goal is to educate on due diligence while making the process bearable by using games and activities. The information delivery will flow easily, and it will be easier for employees to retain it.

Security Process to Safeguard Information

To safeguards information, there a few steps to take. Those steps will be illustrated in two different figures that will be used to explain how information could be safeguarded. It is important to know who has access to what information and know how access to information is granted.

- Know who has access to what information

It is important to ensure that information is accessed by the correct person. In fact, a system should be established to identify who has clearance to access sensitive information and who does not. This system will be beneficial because it will allow to easily trace down possible culprit in case of data breach for example. It will also prevent data tempering or unauthorized access to data. In fact, some access to data will be restricted to only certain employees. Employees with preset clearance will be able to access the information.

- How access to information is granted

Figure 7 illustrates the process by which an employee goes through the process of accessing information. Generally, employees will be given a tool, either a badge, access cards or codes, to be able to enter certain area at work or access information. That tool will be set up so that it only gives access to the employee to only certain areas at work. That is a due diligence practice, ensuring that access to information is controlled.

In this scenario, the employee has an access card that will be scanned to access the employee database. The person will then have to enter their credentials, which must be a match with the one contained in the company database. Once the match is established, the employee will then be able to access the information requested.

Figure 7

Process by Which Information is Accessed

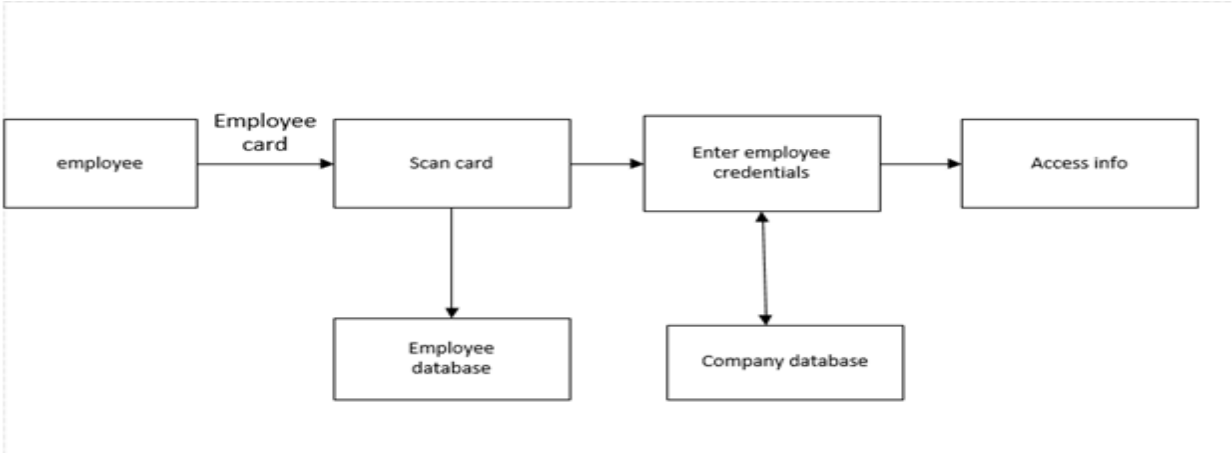
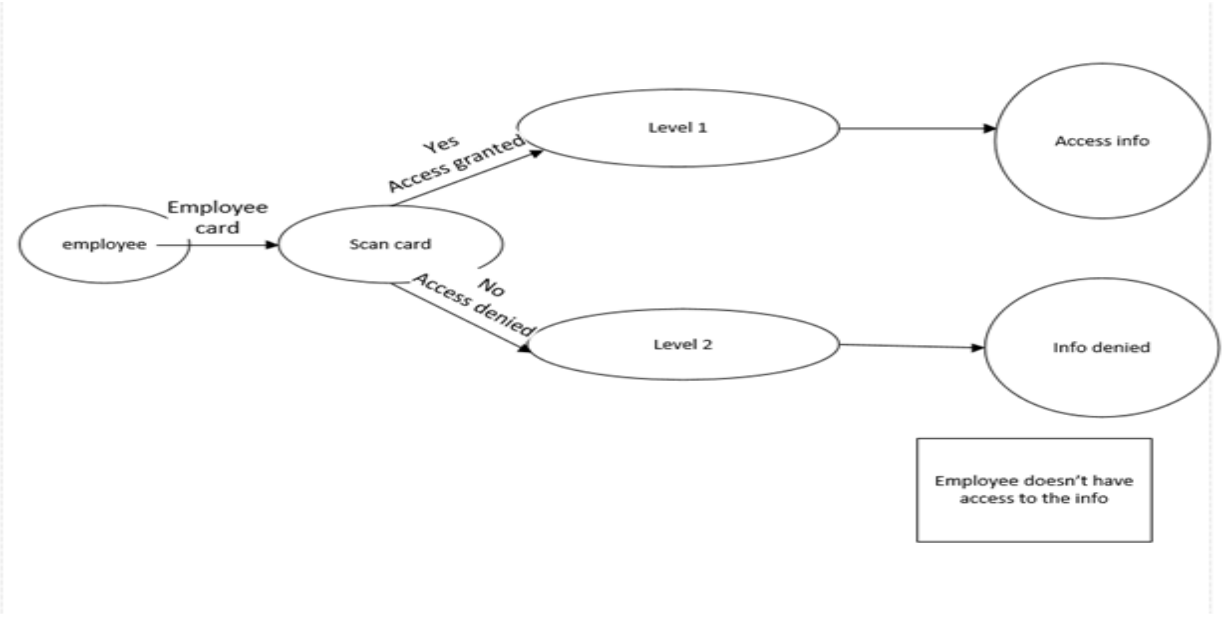


Figure 8 will be used to illustrate how information access is granted based on levels of security. In this case, employees will still have an access card; however, the level of information that can be access will be different. In fact, in one hand, when the employee that is set up to access information at level one swipes the card, the access will be granted, and that employee will be able to access the information.

In the other hand, when an employee that is part of a different level, level two of security for example, scans the card, the access to information will be denied because the employee does not meet the requirements to access that type of information. This system is established to reduce or eliminate insufficient due diligence or lack of due diligence in companies.

Figure 8

Process by which information is granted



Those established levels of security will make it easier to monitor and control data flow and access. It is beneficial because it will help reduce data tempering, data loss and will also help maintain data integrity. Also, in the case of incidents, it will be easier to identify the source because leaders will know who had access to which information from the beginning. Implementing this process will help promote due diligence in companies.

Constant Due Diligence

Due diligence should be implemented on an everyday basis to avoid insufficient due diligence. In fact, practicing due diligence in everyday tasks and at every level of the company, will reduce the risk of errors and mistakes which will be beneficial for companies in the long run. Below are few ways to help maintain a constant due diligence.

- **Monitor and remind**

This simply consist of making sure that due diligence is observed by having a monitoring system in place. The objective of Monitoring will be to ensure that employees are following security guidelines. It is also important to remind employees when needed to comply with due diligence. Employees could be reminded through personal or general communication. Monitor and remind will have for goal to reduce the percentage of margin of error and therefore promote due diligence practices in companies.

- **Lock electronic devices**

It is important to always lock electronic devices such as computes or tablets that are used by employees to complete their tasks at work. Locking devices will ensure that no data are access or copied by individual that are usually not granted access to certain information. Information must be guarded and protected at every level and locking electronic devices is a preventive measure to reduce or eliminate insufficient due diligence.

- **Correctives measures**

In cases where the rules established to comply to due diligence are not followed, correctives measures should be implemented when needed. In fact, correctives measures will be in place not to punish employees for their mistakes but to remind them that there are consequences for not complying with due diligence. Therefore, people will be more careful and insufficient due diligence will be avoided. Corrective measures should be set up so that they don’t appear as aggressive and scary, but they should rather be perceived as a way to learn, encourage and apply due diligence.

- **Desks must be cleared of important information**

Workspaces should always be free of notes and personal information. Desks and public spaces at work should be free of important information. It should be established, as a requirement that employees at the end of their shift, take the time to put away any documents that was used during their working hours. Important documents left in the open constitute a risk.

In fact, those documents could become easily accessible by anyone outside of the company. There should not be any notes with customers' information, companies' financial account information, for example, left on the desk. This would constitute a high risk for information being stolen, and therefore contribute to the increase of insufficient due diligence.

- **Prohibited use of personal electronic devices**

It is easy to capture and share data in a single click, with small electronic devices. Therefore, the use of cell phones or personal electronic devices should be prohibited in certain areas at the office. Prohibiting the use of personal electronic devices is a preventive measure to protect information. This will help reduce insufficient due diligence and improve productivity, since distraction will be minimized.

Incentives and Rewards

It is important to establish rules and requirements with the goal of reducing or eliminating insufficient due diligence. However, those rules should not feel like a burden to employees. Employees should not feel fear or pressure when coming to work. Therefore, to better implement due diligence, incentives and reward should be also implemented to recognize employees, effort, dedication to the job, and meeting due diligence. Those rewards and incentives could be in the form of:

- Points for meeting compliance: Each employee could receive a certain number of points for practicing due diligence. Accumulated points could be exchange for work gadgets, gift cards, gifts or even personal days off.

- Reward for following due diligence: Employees that meet the requirements for due diligence could receive rewards and recognition for the good job they did. Having rewards in place will also motivate employees to always to their best and meet due diligence.
- Opportunity to move up the ladder: When goals and due diligence are met, it becomes easier for employees to meet the rest of the requirements needed to move up the ladder in the company. An employee that is promoting due diligence in their work is more likely to move faster up the ladder.

Elaborated Checklists

These elaborated checklists could be followed to ensure that due diligence is met. The checklists will provide the actions to implement to reduce or eliminate insufficient due diligence. The checklists will be presented in a format of tables. Table number one (1), in one hand, provides a checklist that could be followed within the company. In fact, by following the checklist, leaders will be able to reduce insufficient due diligence.

The checklist in table1 is set up to provide a clear pathway to ensure that insufficient due diligence is eliminated. In the category of education and learning for example, the actions that need to be implemented to reduce insufficient due diligence will be seminars, mandatory compliance, educational classes and training.

Implementing those actions, will help solve the issue of insufficient due diligence by increasing knowledge and best practices. Leaders will be able to separate the issue

of insufficient due diligence by categories and follow the actions that need to be implemented to resolve the issue.

Table 1

Checklist to Follow Within the Company

Categories	Action implemented	Issue solved
Education and learning	• Seminars • Quarterly meetings • Mandatory compliance • Educational classes and training • One on one review and evaluation • End of year evaluations • Available information resources • Coaching and mentoring • Educational games and activities	Increase knowledge and best practices
Security and fail-safe	• Monitor and remind • Lock electronic devices • Corrective measures • Clear desks • Prohibited use of personal	Reduce and eliminate mistakes

Table 1 continued

	electronic devices	
Reward	• Incentives • rewards	Motivate and encourage the implementation of due diligence

In the other hand, the elaborated checklist presented in table 2 is a checklist that should be followed outside of the company. In fact, companies should use that checklist to evaluate third parties for example. During acquisitions and mergers, companies should make sure that third parties meet the requirements for due diligence before starting a business with them.

The due diligence checklist, if followed, will allow companies to eliminate insufficient due diligence during acquisitions and mergers. In fact, one of the categories to be examined will be the category of transparency of services or products. In this category, the actions to be implemented will be to ensure services and products meet due diligence, know what due diligence needs to be followed to provide better prices and services, require that forms and documents be updated. When those actions are followed and properly implemented, companies will be able to maintain integrity and reduce margin error.

Table 2

Checklist to Follow Outside of the Company

Categories	Actions implemented	Issue solved
Transparency of services or products	• Ensure services and products meet due diligence • Know what due diligence needs to be followed to provide better prices and services • Require that forms and documents are updated • No hidden parts deliver what is expected	• Maintain integrity • Maintain availability • Reduce margin error
Evaluation and examination of stakeholders	• Ensure stakeholders (management, employees, service providers) follow due diligence • Evaluate performance • Examination of products and services •	• Maintain reputation • Provide better products and services
Government regulations	• Follow regulations • Submit necessary legal forms and applications Maintain up to date administrative documents	• Less paperwork to go through • Faster processing of requests, saving time and money Less control and inspection Requirements are met

The checklists were elaborated to provide a step-by-step tool for companies to follow to reduce or eliminate insufficient due diligence. The checklists were divided in categories to guide companies and to make it easier to utilize them. Each of the categories includes a list of actions that should be implemented to meet due diligence. Finally, when those actions are correctly implemented, they should help solve common issues related to insufficient due diligence and therefore allowing companies to implement proper due diligence.

Summary

Chapter III covered possible ways to raise awareness about insufficient due diligence among members of the management team and employees of companies. This chapter also accentuated the fact that to eliminate insufficient due diligence, there must a certain type of control over information access and flow. Also, a checklist, against which companies can compare to ensure that they are following due diligence was established. Moving forward, the next step will be to demonstrate the consequences that insufficient due diligence can have on the companies.

Chapter IV: Data Presentation and Analysis

Introduction

Insufficient due diligence or lack of due diligence can have consequences that could be costly for companies at different levels. Companies can face consequences at the financial aspect, legal aspect and their culture and integrity could also be impacted. This chapter will focus mainly on underlining the impact insufficient due diligence can have and the costly consequences that it can constitute for the development of companies.

The focus of this section of the paper will be on data presentation and analysis. The issue of insufficient due diligence or lack of due diligence is not well represented in research. In fact, there are not enough studies about the issue, in terms of numbers, and statistics on the impact of insufficient due diligence in companies. Therefore, this part of the paper will focus on qualitative data rather than quantitative data.

Data Analysis

Insufficient due diligence can lead to costly consequences for companies. Those consequences can be organized in different categories. The categories that will be detailed in this part of the paper will be the financial consequences, legal consequences, integrity consequences and finally the workforce level consequences. The data analysis will provide a clear understanding of the consequences that insufficient due diligence or lack of due diligence could generate in companies.

Financial consequences

Every time due diligence is not implemented, it can generate financial consequences for companies. In fact, whenever due diligence is missing from the composition of a product or services, it will take more resources to correct the mistakes generated by insufficient due diligence (“When due diligence fails”: 2017). More labor will be needed to correct the mistakes which will generate more cost for companies. Consequently, cost will increase leading to decrease of revenue, which will not be beneficial for companies. In fact, the objectives of companies should be to reduce cost and increase revenue, but not the other way around. Other costs that could be generated by lack or insufficient due diligence, could be financial loss through fraud.

When data is not protected, for example, it can be tempered and stolen. Correcting that mistake due to insufficient due diligence will be costly for companies. Another financial cost could be coming from fines that are generated because of breaches of regulations for misuse.

Legal consequences

In some cases, insufficient due diligence and failure to implement due diligence, could be considered as a criminal act and will be punishable by law. There have been cases that lead to civil lawsuit due to breach of fiduciary duties. Not complying with due diligence will mean going through long period of time spent in courts, for companies, trying to find a resolution that will not be too costly for them.

Integrity consequences

Companies' integrity in their services and products is very important. It is that integrity that will motivate the customer to come back to the service or product. The customers should be able to trust the products and services that are offered to them by companies. Insufficient due diligence will damage company's reputation.

In fact, not implementing due diligence can lead to loss or transfer of data, which will make the customer feel insecure about using their products or services. Also, there could be loss from theft of intellectual property. Implementation of due diligence is very important to maintain integrity and avoid unnecessary costs.

Workforce level

Insufficient due diligence can lead to a reduction in workforce. There have been cases where employees were fired for not complying with due diligence. That will constitute another cost for the companies. In fact, letting go some of the workforce will imply going through the process of hiring new people and investing in training and getting the new employees ready to take over the one leaving for not following due diligence. Therefore, it will be a smart move for companies to establish due diligence from the beginning with the workforce.

Summary

The focus of this chapter was on consequences generated by insufficient due diligence. In fact, insufficient due diligence can create costly consequences for companies. Lack of due diligence can be very costly for companies at different levels. The consequences could range from losing customers and intellectual property to facing legal problems such as civil lawsuit.

This chapter proved once more that there are no benefits for companies that are not following due diligence, only costly consequences. A load of information was provided during the development of this paper. The following chapter will summarize what has been discussed, the results found so far, draw necessary conclusions and finally make some recommendations.

Chapter V: Results, Conclusion, and Recommendations

Introduction

This chapter constitute the last part of the paper. This paper was elaborate to raise awareness of the existence of insufficient or lack of due diligence. In fact, in one hand, the paper provided elaborated information to confirm that insufficient due diligence constitutes a security and privacy issue and point out its costly consequences.

In the other hand however, possible recommendations were made on how to resolve the issue of insufficient due diligence or lack of due diligence. The paper provides a literature review that provides a background of insufficient due diligence, shows the existence of the problem but also possible ways to eradicate the problem when due diligence is properly implemented.

Results

The overall methodology and study of the paper provided the steps to follow to properly implement due diligence and therefore eliminate the existence of insufficient due diligence in companies. In the development of the paper, steps to follow in order to properly implement due diligence, were provided. These steps were presented on different levels, which are: steps within the company and with third parties outside of the company.

The results obtained from the study reflect that, the solution to insufficient due diligence or lack of due diligence is for companies to properly implement due diligence

by following the required steps that were elaborated. Instead of rushing into decision making, companies should invest the time and effort into analyzing and evaluating the business they are getting into, to uncover possible hidden problems.

The study questions that were raised during the elaboration of the paper are as follow: what, why, where, who, when and how?

- **What:** what is insufficient due diligence?

This question was answered in the study by providing a definition of insufficient due diligence or lack of due diligence.

- **Why:** Why insufficient due diligence happens.

The main reason insufficient due diligence is still present is because companies do not take the time to conduct a proper due diligence. companies will rush through decisions making and might miss important steps.

- **Where:** where insufficient due diligence happens?

Insufficient due diligence can happen at every level of a company's development process and in different department. It can be found from the financial department through the human resource department.

- **Who:** Who is responsible for insufficient due diligence?

The answer to this question will be everybody that is part of the organization can be responsible for insufficient due diligence, starting from the top management to the employees, passing by third parties used in the company's development. In fact, an established security starts with everybody's input.

- **When:** When does insufficient due diligence happens?

There is not specific answer to that question, timeframe wise, because insufficient due diligence could happen at any time and moment in the company's evolution and development.

- **How:** How to eliminate insufficient due diligence?

The best way to eliminate insufficient due diligence is to use a checklist to conduct a proper due diligence. The checklist will be used as a support to follow to verify that due diligence is met a every single step and for every components of the organization. Constant monitoring, review and audit should also be established at the beginning, mid-year and end of year, to ensure that no actions or transactions is being quickly overseen.

Conclusion

The study presented here was about insufficient due diligence or lack of due diligence as a security and privacy issue for companies. Throughout the paper, it was demonstrated that insufficient due diligence is an existing problem that need attention. Companies will most of the time not pay adequate attention to the problem, which will lead to costly consequences for them.

In fact, insufficient due diligence can have important consequences that could be irreversible sometimes. It can affect the company's reputation, and brand image. Insufficient due diligence generates cost for companies and those cost could have been avoided by simply implemented a proper due diligence. Insufficient due diligence was proven to have financial consequences for companies.

During the study, solutions were provided on how to resolve the issue of insufficient due diligence. The main solution that was provided in this paper was for companies to take the time to establish a proper due diligence. Implementing due diligence will resolve the issue from the root and therefore there will not any reasons to invest money, time and capital on trying to resolve the issue.

Finally, the paper provides ways to implement proper due diligence. In fact, a taxonomy was established that provide a list of different due diligence that should be done by companies. Checklists were elaborated also to provide a support that can be used by companies to avoid insufficient due diligence and implement proper due diligence.

In conclusion, this document was to help the students in the Information Assurance program with their final Thesis/Starred report. The content of the report was presented in its entirety.

Future work

The recommendations that could be provided for future work could be more quantitative research on the consequences related to insufficient due diligence and possible tools that could be used by companies to implement due diligence other that a checklist. There should also be more positive results of a good due diligence being implement.

References

Herold, R. (2006). *Multi-dimensional enterprise-wide security*: Due diligence. Search Security TechTarget. Retrieved from: https://searchsecurity.techtarget.com/feature/Multi-dimensional-enterprise-wide-security-Due-diligence.

Cloud Security Alliance (CSA). *The notorious nine: Cloud Computing Top Threats in 2013.* Retrieved from: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Olcott, J. (August 2016). Security Breaches in Healthcare: How these 7 recent cases happened. Retrieved from: https://www.bitsighttech.com/blog/security-breaches-healthcare

Eitc and other refundable credits. *Consequences of not meeting your due diligence requirements.* Retrieved from: https://www.eitc.irs.gov/tax-preparer-toolkit/preparer-due-diligence/consequences-of-failing-to-meet-your-due-diligence

Burke, L. (2015): *Due diligence Failure*. Retrieved from: http://www.interfima.org/publications/due-diligence-failures/

International Due Diligence Organization. (2018). *BNP Paribas; the success of due diligence and failure of management*. Retrieved from: https://www.international-due-diligence.org/bnp-paribas-success-due-diligence-failure-management/

IT Governance. (2016). *9 reasons to implement Information Security Management System (ISMS)*Retrieved from https://www.itgovernanceusa.com/blog/9-reasons-to-implement-an-information-security-management-system-isms/

Freepint. (2014). *Due diligence: from business burden to business benefit.* Retrieved from https://www.lexisnexis.de/whitepaper/due-diligence-overview.pdf

Centry Blog. (2017). *When Due Diligence Fails.* Retrieved from: https://centry.blog/2017/04/27/when-due-diligence-fails/

IBM, Cloud Computing News. (2016). *What are the 12 biggest cloud computing security threats?* Retrieved from: https://www.ibm.com/blogs/cloud-computing/2016/04/12-biggest-cloud-computing-security-threats/

Pandey, S. & Farik, M. (2015). Cloud Computing Security: latest issues and countermeasures. Retrieved from http://www.ijstr.org/final-print/nov2015/Cloud-Computing-Security-Latest-Issues-Countermeasures.pdf

D. A. Wick. (October 17, 2012). *Four purposes for quarterly meetings.* Retrieved from: https://strategicdiscipline.positioningsystems.com/bid/83318/Four-Purposes-for-Quarterly-Meetings

what is a seminar, retrieved from : https://evenues.com/event-planning-guide/what-is-a-seminar

Z. Anjum. (2019, October 20). *The consequences of inadequate due diligence.*Retrieved from: https://www.linkedin.com/pulse/consequences-inadequate-due-diligence-zafar

Bukh, A. *Failure to perform due diligence.* Retrieved from: https://www.nyccriminallawyer.com/fraud-charge/investment-fraud/failure-to-perform-due-diligence/

Startup guide powered by 1&1 IONOS. (2019, July 31). *Due diligence: definition and history of precautionary risk assessment.* Retrieved from: https://www.ionos.com/startupguide/get-started/due-diligence-procedure/

Rsm insight. *(2017 September 15). How integrity due diligence can protect your company from risk.* Retrieved from:https://rsmus.com/what-we-do/services/financial-advisory/how-integrity-due-diligence-can-protect-your-company-from-a-worl.html

Stephenson, D. (2013, March 7). *The top 10 due diligence disasters,* retrieved from: https://www.firmex.com/resources/uncategorized/top-10-due-diligence-disasters/

W.B.E. Davis. (2009). *The Importance of Due Diligence Investigations: Failed Mergers and Acquisitions of the United States' Companies* retrieved from: http://www.ankarabarosu.org.tr/siteler/AnkaraBarReview/tekmakale/2009-1/1.pdf

Dicentra safety, quality, compliance. (2018, august 8). Seven *(7) Consequences of Improper Regulatory Due Diligence.* Retrieved from:

https://dicentra.com/blog/regulatory-due-diligence-category/regulatory-due-diligence-consequences

iCorps. (2014, November 11). *Lack of Due Diligence: How It Can Hurt Your Company.* Retrieved from : https://blog.icorps.com/bid/185776/why-the-lack-of-due-diligence-can-hurt-your-company

M. and L. Ritter. (2017, December 4). *Warning: Be sure your due diligence is thorough.* Retrieved from: https://www.mlrpc.com/articles/warning-sure-due-diligence-thorough/

Startup guide powered by 1&1 IONOS. (2019, July 31). *Due diligence: definition and history of precautionary risk assessment.* Retrieved from: https://www.ionos.com/startupguide/get-started/due-diligence-procedure/

Ankara. (2009). *The Importance of Due Diligence Investigations: Failed Mergers and Acquisitions of the United States' Companies.* Retrieved from:http://www.ankarabarosu.org.tr/siteler/AnkaraBarReview/tekmakale/2009-1/1.pdf

Hayes, S. & Aue, D. (2016, May 31). *Understanding the Importance of Due Diligence. Retrieved from:* https://www.rsm.global/newzealand/news/understanding-importance-due-diligence

Wikiaccounting blog. (n.d). *5 Types of Due Diligence Services, and Benefits*. Retrieved from : https://www.wikiaccounting.com/concept-due-diligence/

Downs, B. (2019, April 15). *Due diligence in mergers and acquisitions.* Retrieved form: https://www.bbgbroker.com/due-diligence-in-mergers-and-acquisitions/

Moore and Smalley. (2018, December 5). *The benefits of effective financial due diligence.* Retrieved from: https://mooreandsmalley.co.uk/insights/knowledge-post/the-benefits-of-effective-financial-due-diligence/