MASTER THESIS

Course code: BE304E

Candidate names: Runar Horn and Christ-Amour Ignoumba

A digitalized society in front of the cyberwar - are we prepared?

A case study of four Norwegian organizations

Date: 22.05.2017

Total number of pages: 102

NORD University

www.nord.no

Abstract:

The purpose of this study is to investigate how Norwegian companies respond to the continuously growing threat from cybercrime. We live in a society that becomes more digitalized every day that goes by, which makes us more vulnerable and exposed to the cyber threat. Our problem statement and research questions will investigate specifically at how the internal control system of our respondents are affected by this threat. In addition, we will take a close look at the different type of frauds that are out there, and how companies today are affected by institutional forces. In order to do this research we have chosen to cooperate with four different Norwegian firms; Company A, Y, B and X. Company X and B are operating in the health sector, Company A in the finance industry whereas Company Y in the automotive industry. However, all of them wanted to stay anonymous.

Doing research towards this area, in which we applied the institutional theory, have been to great interest for us and have provided some exciting findings. We experience that the subject has become even more important than when we started our research, based on media and articles we have seen in the news. Our findings show that the most common type of fraudulent activity today is hacking, phishing, CEO fraud and identity theft. Based on our findings, working towards having the right organizational culture and attitudes of employees is the most important measures to fight cybercrime. In addition, having satisfactory security systems in place (e.g. antivirus, firewall, backup system) is important, but more importantly, the employees needs to know how to use them. The companies we have worked with are all regulated by laws, but according to our respondents it was a common agreement that only complying with laws and regulations is not enough to stay satisfactory protected against cybercrime. At the end we summarized our discussion by comparing virus theory to cybercrime as a metaphor. Our findings in this investigation show that dealing with a continuously growing cyber threat demand a great amount of resources and attention, and in that way clearly impacts the internal control system.

Keywords: Cybercrime, fraud, internal control systems, institutional theory

FOREWORD

This research paper is our master thesis in Business Administration, at Bodø Nord University, Norway. Through this work we gained knowledge in the concept of IT related frauds and internal control systems in four Norwegian companies and insight into how useful these systems measures are in contrast with IT development.

First and foremost we would like thank and express our appreciation to our thesis supervisor, Mr. Anatoli Bourmistrov for his great supports, help, inspiration, advice, encouragement and guidance during our research work. He has always been working in a professional manner with very rapid replies and has offered us great timely advices.

Furthermore, we would like to thank all the representatives in companies such as Company A, Company X, Company Y and Company B that have accepted working with us knowing full well the sensitive nature of our problem statement. Additionally, we would like to send our special gratitude to Kristian Thaysen - partner BDO, compliance and investigation and Arne Helme - KPMG Partner and advisor in the development of complex IT systems and solutions for their supports and great answers.

Finally, we would like to show our gratefulness to our respective families with their unlimited love and assistance. Also a big thank you to all of our friends, colleagues and most importantly each other, as without each other, this work would not have been possible.

Bodø, Mai 2017
Runar Horn A. and Christ A. Ignoumba

ACRONYMS

ACFE: Association of Fraud Examiners

CEO: Chief Executive Officer

CFO: Chief Financial Officer

CGMA: Chartered Global Management Accountant

COBIT: Control Objectives for Information Technology

COSO: Committee of Sponsoring Organization

CRM: Customer Relationship Management

DDoS: Distributed denial of service

EFT: Electronic Funds Transfer

ERM: Enterprise Risk Management

IA: Internal Audit

IC: Internal Control

ICT: Information and Communication Technology

ID: Identification

ISACA: Information System Audit and Control Association

ISO: International Organization for standardization

IT: Information Technology

NSM: Norsk sikkerhetsmyndighet

NSD: Norsk senter for forskningsdata

SOX: Sarbanes-Oxley Act

Contents

FIGURES

TABLES

1 INTRODUCTION

1.0 Introduction

For the introduction of this assignment we will present the reasons (motivation and purpose) why we chose our topic of research. Additionally, we will outline our reflection on methodology (collection of data) and give an insight about the chosen theory we have decided to focus on.

1.1 Motivation

The development of Information technology communication (ITC) has become the key element in many organizations today. Elements such as information systems and electronic documents are becoming more common for companies. Having those elements increases the accuracy and speed of transaction processing, which can lead to competitive advantages for many organizations in terms of operational efficiency, cost savings and reduction of human errors. According to ITIF (information technology and innovation foundation, P2-4) research report, IT related jobs increased by 22.2% between the years of 2001 to 2011. Companies that invested in more IT expanded their workforces by 14% between 2006-2010 and the growth rate of e-business from 2000 to 2014 was 25%. However, although increased use of information technology contributes to opportunities of growth and development, it also represent threats.

Sieber (1986, P15), predicted how the growth of IT would lead to the increase of computer crime. He stated that "Increasing computerization, particularly in the administration of deposit money, in the balancing of accounts and stock-keeping, in the field of electronic funds transfer systems, and in the private sector, as well as new computer applications such as electronic home banking, electronic mail systems, and other interactive videotext systems will lead to increase in the number of offences and losses". Sieber (1986), prediction has proven to be quite accurate two decades later. According to Association of Certified Fraud Examiners (ACFE, 2014, P4) study, the average organization typically loses approximately 5% of its revenue due to fraud every year which translate into the losses of approximately $3,7 trillion. PwC (Global Economic Crime Survey, P2) statics shows that cybercrime is the second most reported (still rising) economic crime in 2016, affecting 32% of organizations and only 37% of them have a cyber incident response plan. Kaspersky Lab report (2016, P5) reported that companies main direct loss of funds today is due to cybercrime and is seen as complex and difficult to prevent.

Moreover the cyber-attack dubbed "Wannacry" is a ransomware that blocks access to files unless victims pays off the hackers. The attack are one of the most serious incidents ever seen, affecting more than 150 countries. Chinese universities, Russia's interior ministry and Britain's National Health Service (NHS) all saw their computer systems taken hostage in the attack (*see appendix 3*). According to the Internet Security Threat Report, the varieties of ransomware have more than tripled since 2014. Cryptowall a variety of ransomware netted approximately 18 million dollars for hackers in 2015. The average price of ransomware has gone up from 373 dollars per victim in 2014 to 1077 dollars per victim in 2016 (the Economist, 2017).

Based on what is said above, we have outlined how the evolution of ICT that can be perceived by many as opportunities, can also be perceived as threats. Researching and discovering the dark side of increased use of IT is our main motivation for choosing this subject. We believe this is a topic that is relevant in today's society as the application of IT is only increasing, and so is the criminal activity through cybercrime. According to what we see in the media, it is not only companies that are victims of cybercrime, but lately also politicians are getting attacked. We also have the impression that Norway is an attractive target since we are one of the first to take advantage of new technology, in combination with the reputation for being wealthy and naive. In addition to this, we believe this certain subject has not been researched as much as many other subjects within the accounting sector. That gives us the motivation that we might discover new findings and trends that has not been found before.

1.2 Problem statement and Research question

In order to analyze, examine and accomplish the objectives of our study it is important to get a historical overview of how the development of IT based frauds have been. With this we mean what types of fraud, how frequently those fraud are incurring and the complexity of such fraud. The complexity of a fraud is the way it is put together, which is determined by the size of it, number of individuals involved and the strategy that is used to actually accomplish the fraud. In addition, when looking at the historical perspective, we need to take a look at the internal control practices that has actually been used to deal with frauds related to IT. This means the certain types of controls, amount of controls and how these have developed over time. A third area we need to do background research on is the external parties that plays a role in defining the internal controls that exist within a company. We all know that business is

regulated by law and order, and the internal control is no exception. Based on what is mentioned, we came up with this problem statement:

How have internal control systems developed to respond to growth in IT, and a need to prevent and detect fraud?

In order to have a better understanding of our problem statement, the three following research questions are explored:

- How IT based fraud instances experienced by companies have changed over time?
- How have internal control practices companies use to prevent the IT based fraud developed?
- What kinds of institutional forces dominate in designing internal control practices?

1.3 Reflection over methodology and theory choices

For our study, we will use the qualitative approach for researching and collection of information. The reason we have chosen qualitative approach is because it will help us gain a deeper insight of our research questions. Primary and secondary data will both be used. Primary, because it is mandatory for our study to conduct interviews to collect data, while secondary which is already presented in the literature framework focus mainly on data being collected through other parties such as: articles, study report statistics, books and information made public by companies.

In order to have a better understanding about the growth of IT fraud, it was important for us to explain the concept of internal control. Many organizations today that are victim of fraudulent activities whether internally or externally, so having adequate internal control systems can help companies prevent and detect fraud but also protect their resources. Internal control system of an entity is a structure laid down by executive managers for effective control of an organization activities. It is linked to corporate governance. Due to institutional changes, the Sarbanes Oxley Act, that was introduced in the USA in 2002 required management to reinforce their (IT) internal control and supply assessment of its effectiveness. Most regulatory authorities are adopting this law today in order to prevent the repeat of the corporate scandals (Enron and WorldCom) that happened in early 2000s. Poor internal control system often lead to losses, failures and can damage the reputation of a company. Different control models such as COSO, COBIT and ERM have impacted the practice of internal

control in organizations. Internal audit is also a part of internal control system, that is put in place in order to help management.

A purpose of our study is to gain knowledge on how the growth of IT have led to the increase of fraud within companies. With all the changes (internal and external) companies occurred over the years, due to the implementation of IT, change in laws and regulations (*see appendix 2*) and different applications of internal control models, we found it necessary to use institutional theory as our theoretical choice. We chose the institutional approach because of its specific concern with the relationships among individual beliefs and actions, the entities within which they occur and the collective social structures in which norms, rules and beliefs are attached. Beyond that we also shed light on the different forces that can affect an organization internally and externally: coercive, mimetic and normative isomorphism.

2 THEORETICAL FRAMEWORK

2.0 Introduction

This chapter is devoted to explain and explore the literature that focuses on our research questions. We start by reviewing the concept of fraud and IT fraud (e-business fraud) in organizations. Then define the concept of internal control in order to examine different internal control models (COSO, COBIT, ERM) for organizations effectiveness. Different aspects of Institutional theory are explained thoroughly, such as legitimacy, institutional pressures and the action and norm model.

2.1 Fraud Overview

Fraud is a deception that affects all types of organizations regardless of the sector, size, country, public or private. There are many definitions of fraud and fraudulent activities. According to the association of certified fraud examiners (ACFE, 2014, P6), fraud is “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources of assets”. Alexopoulos et al (2007) stresses that the main reason behind committing fraudulent activities is to achieve gain on false ground by an illegal means. Which has an impact on the economy, organization welfare, law and moral values. (Abdallah et al, 2016)

Bologna and Lindquist (1995) classify fraud between internal versus external fraud. In external fraud, fraudulent activities are carried out by vendors, suppliers or contractors

whereas in internal, they are carried out by employees stealing from the company or managers cooking the books. A combination of both internal and external fraud can also occur, for example an employee might collaborate with a supplier in order to deprive the company. (Jans, Lybaert, Vanhoof, 2009)

2.1.1 Types of fraud.

ACFE definition of fraud comprehend a considerable range of conduct by employees, managers, executives and principals of organizations. According to Wells (2005), those fraudulent activities varies from asset misappropriation, fraudulent statements and corruption by using companies property for personal gain.

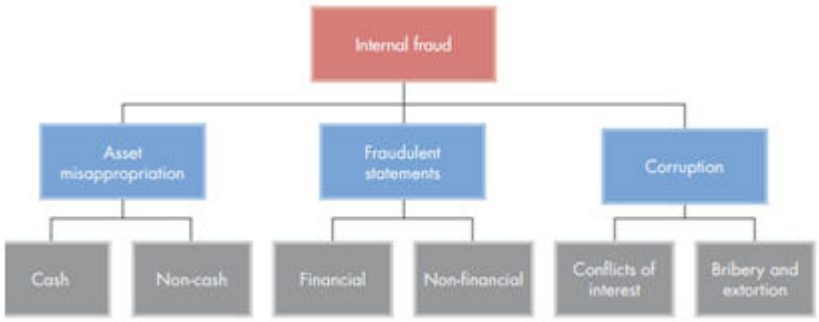


Figure 1: types of internal fraud *(CGMA, Fraud Risk Management, P4)*

- **Asset misappropriation,** involves employees or managers abusing their position to steal (assets) from a company through fraudulent activities. It is the fraudulent activity that is the most common because it occurs most often. According to the statistics data of ACFE, asset misappropriation happens in over 83% of fraud schemes, but the statistics also show that it is the least expensive fraud on a per-fraud basis. Asset misappropriation fraud include: check forgery, theft of money, inventory theft, payroll fraud or theft of services. (ACFE, 2016, P12)

- **Fraudulent statements,** is the manipulation of financial statements in order to create financial opportunities for an individual or an organization. Based on ACFE statistics, fraudulent statements occurs least frequently, it happens only in 10% of all cases and is easily the most expensive fraud on a per-fraud basis. Some examples include: manipulation of stock price, favorable loan terms or increased year-end bonuses.

- **Corruption**, is the second most frequently occurred fraud scheme after asset misappropriation according to ACFE. It is about 35% of all fraud that is uncovered. It includes schemes such as: accepting bribes or inappropriate gifts and shell company schemes. (ACFE, 2026, P16)

2.1.2 The fraud triangle

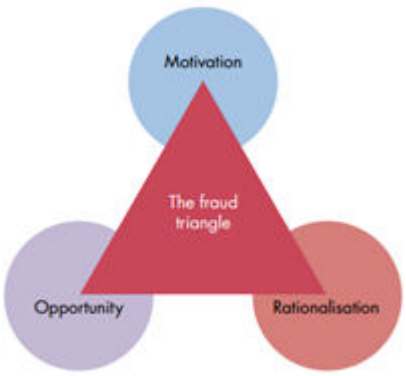


Figure 2: The fraud triangles (*CGMA, Fraud Risk Management, P5)*

Sutherland (1949) was the first to identified the three elements of the fraud triangle; motivation/pressures, opportunity and attitudes/rationalizations. Later, Cressey (1953) utilized those elements to develop the fraud triangle to investigate frauds. (Sandhu, 2016)

Motivation/pressures, motivates an individual to behave illegally, Cressey (1953) hypothesized that an individual commit fraud because of non-sharable financial pressure. Those financial pressure are the financial problems experienced by individuals, which they do not intend to share with others. The pressure to carry out fraud can be divided into two category: financial fraud and non-financial fraud. According to the KPMG (2013, P7) survey study the fundamental motive for fraudster is mostly related to greed, financial gain and financial difficulty.

Opportunity to commit fraud, according to Cressey (1953) emerges when an individual in a position of trust violates that trust to address a non-sharable financial pressure. In accounting, opportunity has been examined within the context of weak internal controls which according to KPMG survey reports, is a major factor attributable to fraud. Coenen (2008) claim that an opportunity emerges when the individual has the technical skills and knowledge of "assets, people, information and computer systems that enables him or her not only to commit the

fraud but to conceal it". The opportunity to carry out fraudulent activities increase when the company control structure are weak, its corporate governance becomes less effective and its audits function quality deteriorate. (Lokanan, 2015)

Attitudes/rationalization, Dellaportas (2013) stresses that rationalization is the lack of feelings and indifference expressed by offenders to rationalize any guilt emerging from their misbehavior. Coenen (2008), claim that an employee rationalize their fraudulent behavior by assuring themselves that it is acceptable to commit fraud (Lokanan, 2015). According to KPMG global study survey, rationalization is seen as an emotional motivator, such as fear, anger or the sense of superiority. The sense of superiority accounted for 36 percent of fraud scandals, making it the most important emotion of rationalization. Fraudsters with such emotion are often managers/directors of organizations (KPMG, 2013, P8).

2.1.3 Detection Of Fraud Schemes

Based on ACFE study research, the best way to uncover fraud is through tips (39,1%), internal audit (16.5%) and management review (13.4%). In an organization, employees are seen as a valuable source for detecting potential fraud. ACFE surveys report shows that almost half all the tips that led to the detection of fraud came from employees (51.5%). Other source of tips came from customers (17.8%), anonymous tips (14%), vendor (9.9%), other (12.6%), shareholder (2.7%) and competitor (1,6%). (ACFE, 2016, P21-26)

2.1.4 IT Fraud (Electronic Fraud)

The evolution and development of information technology has had beneficial effects on electronic businesses. According to Clinton, (2000) E-business is based on the electronic text, sound and video. It includes many diverse activities such as electronic trading of goods and services, online delivery of digital content, electronic fund transfers, electronic shares trading, electronic bills of lading, commercial auctions, collaborative design and engineering online sourcing, public procurement, direct consumer marketing and after sales services. It involves both products (consumer goods, specialized medical equipment) and services (information services, financial and legal services). (Kareem et al, 2014)

Clarke (1999) developed the acronym CRAVED to explain different aspects that make certain customer products more vulnerable to theft. He designated "hot products" by characterizing product patterns that made theft feasible, desirable and enticing. CRAVED attributes includes : Concealable, Removable, Available, Enjoyable, and Disposable. Newman and Clarke

(2003,), later used the "hot products" point of view to highlight the internet knowledge that make e-business feasible. They identified the components in IT that make commission of crime feasible. Hence came up with the SCAREM acronym: Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity. *Stealth*, is referred as a convenience provided to all who utilize the internet. It is one of the main problems in tracing fraudsters across the web because of how developed their hacking skills are, vulnerabilities in IT security systems and lack of IT professionals in law enforcement. *Challenge*, is referred as the internet fraudster's motivation trying to beat the computing system. *Anonymity,* is referred as being problematic to track the location and identity of the fraudsters, due to there being many ways to avoid IP address tracking. It also allows hackers to spend longer period in order to attempt to gain illegal entry into a target IT system. *Reconnaissance,* refers to the process online fraudster take to look for holes or gaps in an IT security system before carrying out their attack. *Escape,* gives an advantage to online fraudster over law enforcement, more than often their crimes goes undetected. *Multiplicity,* refers to how online fraud can be multiplied exponentially. (Newman and Clarke 2003, 61-63)

2.1.5 Major IT Fraud Areas

Function	Description
Hacking	unauthorized intrusion into a computer or a network.
Electronic funds transfer fraud	Prime target: information system and intelligence database of banks.
Credit card fraud	The use of a credit card account through the theft of the account holder's card number, card detail and personal information.
Money laundering	Infiltration of banking system by organized crime, use of electronic non-bank transfer and cyber-banking, and many other sophisticated techniques
Investment fraud	illegal activity of supplying false information to someone so that they will invest in something
Telemarketing fraud	The major telemarketing frauds are: credit card sales, advance fee loans, telephone slamming, credit card loss protection, telephone cramming and magazine sales.

Identity theft	When a fraudster access enough information about someone's identity (name, date of birth, account number) to commit identity fraud

Table 1. major IT fraud areas (*Newman and Clarke 2003, P54*)

2.2 Internal Control systems

Kaplan (2008), define internal control as a process designed and effected by those in charge with governance (board of directors), management and other personnel to provide reasonable assurance regarding the achievement of an organization's objectives in the effectiveness and efficiency of operations, reliability of financial and management reporting, compliance with applicable laws and regulations and protect its reputation. Cunningham (2004), argue that internal control systems (ICS) start as internal processes with positive goals to help an organization meet its set of objectives, which is primarily provided by management. Lawson et al (2006), noted that weakness in the internal control systems can result to failure of a company. (Samuel and Wakogi, 2014)

2.2.1 Committee of the Sponsoring Organization (COSO)

COSO's internal control integrated framework states that internal control can be judge to be effective when "the boards of directors and management have reasonable assurances that they understand the extent to which the entity's operational objectives are being achieved, the published financial statements are being prepared reliably, and the applicable laws and regulations are being complied with."

The Committee of Sponsoring Organizations (COSO) identifies five main components of internal control: Control environment, Risk assessment, control activities, information and communication and monitoring. Control environment component defines the ethos (set of values or operating principles) of an organization and the way it operates. Risk assessment component refers to the process of identifying and analyzing risks that pose a threat to achieving the firm's objectives. Control activities component refers to the procedures, practices and policies that assure management that objectives of an organization are achieved and that strategies about risk mitigation are carried out effectively. In Information and Communication, information should be identified, captured and communicated to all stakeholders such as board of directors, management and employees in order to carry out their responsibilities effectively. Monitoring component is referred as a process of assessing the

quality of the system's performance over time, which includes monitoring activities and separate evaluations. (COSO, 2004)

2.2.2 Control Objectives for Information and Related Technology (COBIT)

Colbert and Bowen (1996) assert that internal control based on COSO does not identify control objectives at a level of specificity sufficient to design detailed audit tests. They further observe that the COSO framework does not address the complexity and risks inherent in IT. Most organizations rely on technology which mean they need a framework to address how technology function in today's audit environment. These reasons are why most companies and auditors in computerized environments are adopting different specialized frameworks, such as COBIT in order to supplement COSO. (Tuttle and Vandervelde, 2007)

Control objectives for information and related technology (COBIT) was developed by the information systems audit and control association (ISACA) and the IT governance built in part upon the COSO evaluation framework (Lin et al, 2010). Its main objectives is to bridge a gap that exists between business control models and the more focus control models of IT. (Curtis et al, 2000)

The COBIT framework relies on a process model that is organized and contains four primary domains: planning and organization, acquisition and implementation, delivery and support and monitoring and evaluation. Each domain consist of specific processes that a company should address to carry out detailed and specific IT related control objectives (Tuttle and Vandervelde, 2007). The COBIT framework has 34 processes which can be identified within the four domains. (Lin et al, 2010)

2.2.3 Enterprise Risk Management (ERM) System

Mike (2005) and Power (2007), observe that the interest of ERM has grown rapidly during the past 15 years, with regulators, professional associations and rating firms wanting to adopt the system. Following this demand, more and more organizations are embracing enterprise risk management, but its implementation remains poorly integrated. The evolution of ERM started in the late 1990s and its main goal is to holistically manage all risks faced by an organization (Elliot, 2013). Due to the struggle many companies are facing with the implementation of ERM, COSO introduced the COSO ERM (expansion of the COSO framework) framework in 2004 to support managers at all levels of decision making and planning but also to provide a

precise guide for its design and implementation. (Arena et al, 2010), (Bharathy & McShane, 2014)

As shown in the figure below, ERM constitute a three-dimensional matrix of eight elements which are essential to achieve strategic, operational, reporting and compliance goals. Strategic refers to high level goals that should be aligned with supporting the organization's mission.; operational, effectiveness and efficiency use of resources; reporting, refers to the reliability of reporting and compliance, refers to compliance with regulations and law.

Figure.3. COSO's enterprise risk management cube *(reproduced from COSO, 2004, p. 7).*

2.2.4 Corporate Governance

Corporate governance is the mechanism by which a corporation is managed and monitored. Rezaee (2004) states that it determines a power sharing relationship between corporation executives and investors by administering structure through which: the objectives are defined; Policies and procedures are established to ensure achievement of these objectives; and activities, affairs, and performance are monitored. Corporate governance specifies the distribution of rights and responsibilities of different participants in a corporation. The governance structure consist of both internal mechanism (the roles of the board of directors and management) and external mechanism (the market-based monitoring and the legal/regulatory system). (Rezaee, 2004)

Standard and Poor's (2002) define corporate governance as "encompassing the interactions between a company's management, its board of directors, and its financial stakeholders."

Shleifer and Vishny (1997) explain, "Corporate governance deals with the ways in which suppliers of finance to corporations assure themselves of getting a return on their investment."

Corporate governance functions consist of :

Function	Description
Oversight function	The board of directors participates in strategic decision making, provide strategic advice to management and oversee managerial plans, decisions and actions, yet avoid micromanaging.
Board of directors	delegates its authorities to management, who makes decision on behalf of the shareholders.
Audit committees	have oversight responsibility over corporate governance and the financial reporting process, internal control, structure and audit functions.
Managerial function	the effectiveness of this function depends on the alignment of management in achieving the goal of creating shareholder value.
Audit function	Auditors are an integral part of corporate governance, their expertise in internal control ensure the integrity and reliability of financial statements.
Legal and financial advisory functions	Professional advisors give legal advise and assist the company, its directors and employees in complying with applicable laws and fiduciary obligations.
Monitoring function	Direct participation of investors in the business and financial affairs of corporations.
Compliance function	The rules and regulations established by governing bodies and regulators to create a compliance framework for public organizations to achieve their goals.

Table 2. corporate governance functions (Rezaee, 2004).

2.2.5 IT Governance.

After many corporate scandals (Enron, WorldCom, Tyco, Adelphia) resulting to the loss of billions of dollars, the U.S. Congress executed a new law to prevent financial fraud which was signed by president Bush in July 30 2002. This law required CEO's to reinforce IT related internal control and corporate governance because the data used in financial reporting are stored, captured and reported by computer based system. IT governance was established in 1998 but its development began in early 2000s due to the SOX law. (Thapa et al, 2007)

According to Ko and Fink (2010) IT governance defines that part of corporate governance that deals with the management of the IT systems of an organization. IT governance particularly focus on IT risk management and the alignment of corporate system to purposes of business. Bhattacharjya and Chang (2007) state that IT governance became important over years because it was recognized that information systems and their technology influence every aspect of an organization's activities which also create organizational value.(Rubino et al, 2014)

Van Grembergen & De Haes (2009) define IT governance as "processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments." Bowen et al (2007) explain that structures refer to committees and councils, along with formal positions and roles for IT-related decision-making. Processes focus on the implementation of IT management techniques and procedures in compliance with establishing IT strategies and policies. Peterson (2004) state that relational mechanisms refer to the active participation and collaboration between IT management, corporate executives and business management. (Heroux and Fortin, 2014)

Neirotti and Paolucci (2007) with their study prove that organizations show a successful return on IT investment, have better IT management practices that give them the opportunity to adapt their organizational routines to meet business needs. In addition, Lunardi et al (2012) study of more than 400 Brazilian companies showed that companies that adopt IT governance mechanism have an improvement in their financial performance, mainly in relation to profitability.

2.2.6 Internal Audit Function

Internal audit (IA) is defined by the institute of internal auditors, as an independent and objective activity that provides a company assurance regarding its operations which it guides towards improvement and contribution by bringing added value. IA evaluate the management

process, the governance and controlling process and the risks an organization is exposed to. They also offers solutions to improve efficiency and cover deficiency (IIA, 2009, P3). In respect of governance, the objectives of IA includes promoting appropriate ethics and values, ensuring effective organizational performance management and accountability, communicating risk and control information to relevant areas of management and coordinating the activities of, and communicating information among the board of directors, external and internal auditors and management (IIA, 2012, P11). In other words, as stated by Reid and Ashelby (2002) IA objectives is to provide management with re-assurance that their internal control system are adequate for the need of the company and are operating satisfactorily.

IA is an integral part of the internal control system set up by management of an organization to analyze, evaluate and report operations of accounting and other controls. Therefore, the quality and effectiveness of internal audit procedures are fundamental since the work of internal auditors cover a broad variety of assignments in an organization. (Belfo and Trigo, 2013)

GhiĠăet. al (2005) and BoĠa-Avram (2009) discuss about the distinction and separation of internal audit and external audit. According to them, internal audit in many cases is a direct employee of an organization which still has great independence within the organization, whereas external audit is completely independent outsourced. This separation is due to the SOX law which states that a company cannot use the same audit company for both external audit services and internal audit consultancy. (Silviu, 2014)

2.3 Institutional Theory

According to Hoffman (1999, P351), institution from organization aspect are " rules, norms, and beliefs that describe reality for the organization, explaining what is and what is not, what can be acted upon and what cannot". He then states that institutional theory asks questions about how social choices are shaped, mediated, and channeled by the institutional environment. Pfeffer & Salancik (2003) stress that in order to understand an organization, one should understand the environment (surrounding). Institutional theory deals with how organizations are affected by internal and external forces which are located beyond its control. This theory can be used to explain the changes in social values, technological advancements,

and regulations which affect the decisions concerning continuous activities and environmental management. (Hoffman, 1999)

Greenwood and Hinings (1996) observe that institutional theory connects to a wider perspective of homo economics instead of considering rationality. Which helps one look beyond market pressures to examine behavior and addresses institutional pressure as a dimension of behavioral analysis. Hoffman (1999)

2.3.1 Legitimacy

Barley and Tolbert (1997, P93), state that in the institutional perspective "organizations are suspended in a web of values, norms, beliefs, and taken-for-granted assumptions that guide and constrain their actions over time". Scott (2008) notes that an institution is a social structure that gives organizations and individuals orientations but at the same time controls and constraints them. (Mignard and Rivard, 2009)

According to Meyer and Rowan (1977), the underlying assumption of institutional theory is that organizations and organizational actors seek to gain legitimacy in their environments to be accepted and therefore assure their long term survival. Legitimacy is considered the core concept in institutional theory (Barley, 2008, P506). Institutional theorist often use the term "institutional field" when they refer to the environment within which legitimacy must be gained, repaired, or maintained (Suchman, 1995). (DiMaggio and Powell, 1983, P148) define legitimacy related to the organizational level as "those organizations that, in the aggregate, constitute a recognized area of institutional life: key suppliers, resource and product consumers, regulatory agencies, and other organizations that produce similar services or products". (Mignard and Rivard, 2009)

An organization within its institutional field can be seen as connected to or similar to other organizations (Scott, 2008). (DiMaggio and Powell, 1983), explain that the term "connect" refers to the relations and communications that exist between organizations. Scott (2008), later adds that organizations tend to be more influenced by organizations with similar behavior or by those it has contact with. (Mignard and Rivard, 2009)

2.3.2 Institutional Pressures and Isomorphism

Meyer and Rowan (1977, P340) defined isomorphism as "organizations are driven to incorporate the practices and procedures defined by prevailing rationalized concepts of organizational work and institutionalized society. Organizations that do so increase their legitimacy and their survival prospects, independent of the immediate efficacy of the acquired practices and procedures".

DiMaggio and Powell (1983) further developed that definition by linking it to organizational and sociological theory. They asked Questions on why organizations are so similar and concluded with the similarity being a result of organizations seeking to gain legitimacy within their large environments. Therefore in order to describe the process of institutional pressures DiMaggio and Powell adopted the concept of isomorphism. They defined isomorphism as "a constraining process that forces one unit in a population to resemble other units that face the same set of institutional conditions". (DiMaggio and Powell, 1983, P149)

DiMaggio and Powell (1983), propose three mechanism through which institutional isomorphic change occurs: coercive isomorphism, that stems from political influence and the problem of legitimacy; mimetic isomorphism, which results to standard responses to uncertainty and normative isomorphism, which is associated with professional values.

Coercive isomorphism/pressure, is illustrated through both formal and informal pressures that are exerted on organizations by other organizations which depend on and are informed by cultural expectations in the society within which they operate (DiMaggio and Powell 1983). Those kinds of pressures can be felt as force, persuasion or as invitations to join the collusion. According to Pfeffer and Salancik (1978), Coercive isomorphism is similar to the resource dependence model, meaning that organizations are viewed as constrained by those they depend on for resources. Those constraints include pressures in order to bring an organization's structure in line with the demands of powerful actors (Pfeffer and Salancik 1978). Recent regulations imposed on organizations such as the Sarbanes–Oxley (SOX) Act and Information Security Management Act are examples of coercive pressure that organizations face. These regulations demand compliance with their requirements. Meyer and Rowan (1977, P150), have pointed out that as rationalized states and other large rational organizations enlarge their control over parts of social life organizational structures increasingly come to reflect rules institutionalized and legitimated by and within the state.

Which results in organization being increasingly similar in a given domains and increasingly organized around rituals of conformity to wider institutions. (DiMaggio and Powell 1983)

Mimetic isomorphism/pressure, results from the organizational response to uncertainty, in which they behave or imitate successful peers as a safe strategy (DiMaggio and Powell, 1983). According to DiMaggio and Powell (1983, P152), "when organizational technologies are poorly understood, when goals are ambiguous, or when the environment creates symbolic uncertainty, organizations may model themselves on other organizations in the organizational field", which are perceived to be successful and legitimate. Meaning that, organizations imitate the behavior of other organization in the environment, especially the ones that are similar and have higher status, success and prestige. For example, if an organization decide to adopt or have adopted new technologies that are successful, this will exert mimetic isomorphism on other organizations to do the same, due to the belief that successful actions is more likely to yield beneficial outcomes. The advantages of mimetic behavior are substantial, when an organization have difficulty with ambiguous causes or unclear solutions adopting another organization's practice may yield a viable solution with little expense (Cyert and March, 1963). Additionally, DiMaggio and Powell (1983) argued that industry associations disseminate organizational practices and help companies imitate each other. (DiMaggio and Powell 1983)

Normative isomorphism/pressure, is a result of professionalization, where workers strive to define their role. It is often interpreted as "the collective struggle of members of an occupation to define conditions and methods of their work, to control the production of producers, and to establish a cognitive base and legitimacy for their occupational autonomy" (DiMaggio and Powell, 1983, P152). The degree of professionalization of employees affects the nature of the management control system (DiMaggio and Powell, 1983). The different norms and values that professionals develop through formal education and professional networks increase the similarity of the skills and knowledge of the total workforce in an organizational environment (Boon et al, 2009). DiMaggio and Powell (1983) state that two aspects of professionalization are important sources of isomorphism: the first one consist of members of professions receiving the same training (e.g. physicians and university professors) so they can have similar views. The second one consist of professions members or business partners interacting through professional and trade associations. That is because organizations that are in the same environment usually share the same goals and they are

subject to normative isomorphism originating from other members of its field. For example, an organization that want to adopt new technologies and organizational practices is generally influenced by how its business partners take action concerning those technologies and practices.(Teo et al, 2003)

Moreover, Scott (2001; 2008) denoted institutions as "multifaceted systems incorporating symbolic systems-cognitive constructions and normative rules- and regulative processes carried out trough and shaping social behavior". Furthermore, he categorized between institution theory between three pillars: the regulative, normative and cognitive pillar. The table under show the contrast between Scott's (2008) three pillars of institutions and DiMaggio and Powell (1983) institutional forces.

	Regulative	**Normative**	**Cognitive**
Basis of compliance	Expediency	Social obligation	Shared understanding
Basis of order	Regulatives rules	Expectations	Constitutive schema
Mechanism	Coercive	Normative	Mimetic
Indicators	Law;Rules, Sanctions	Certification, professionalization	Common goal, beleifs
Basis of legitimacy	Legally sanctioned	Morally governed	Recognisable, Comprehensible

Table 3: Scott's (2008) institutional pressures

As it can be seen in the table above, the regulative pillar is very much comparable to DiMaggio and Powell (1983) coercive isomorphism, whereas normative pillar to normative isomorphism and cognitive to mimetic isomorphism.

2.3.3 Institutional isomorphism and Public Sector Organizations

According to Frumkin and Galaskiewicz (2004), even though the public sector organizations is seen as driving the institutionalization of corporations and nonprofit organizations, it hasn't really been studied in relation to institutional pressures. Their study analyzed whether public sector organizations in comparison with organizations in the business and nonprofit sectors are affected more or less to institutional theory three mechanisms (coercive, mimetic and normative).

Frumkin and Galaskiewicz (2004) findings were divided into two different hypothesis. The first one, "institutional pressures do not affect all organizations the same" stated that institutional pressure was weaker profits oriented organizations than for nonprofits and government establishment because the former have owners who monitor performance and assert claims over residual earning, while the latter do not (Frumkin and Galaskiewicz, 2004, P302). The second hypothesis pointed out that profits oriented organizations, nonprofits and government establishment have distinctive levels of external control. Furthermore, they added that coercive and normative pressures transformed government organizations from traditional bureaucracies to be more like profits and nonprofits oriented organizations. Whereas mimetic pressure made government organizations more like traditional bureaucracies (Frumkin and Galaskiewicz, 2004, P303)

2.3.4 Institutional model of accounting

In their study about institutionalization, Bergevärn et al (1995) investigated on a comparative study between two different countries. It focused on how accounting system was becoming institutionalized in Sweden and Norway. The interpretation of their study reflected Hopwood's (1987) belief that accounting was changing regularly and consequently stated that a complete new accounting term must, besides accounting practices, also incorporate accounting norms and the use of accounting. Bergevärn et al (1995), stressed that in order to understand their study, it was imperative to distinguish between the accounting action system and the accounting norm system.

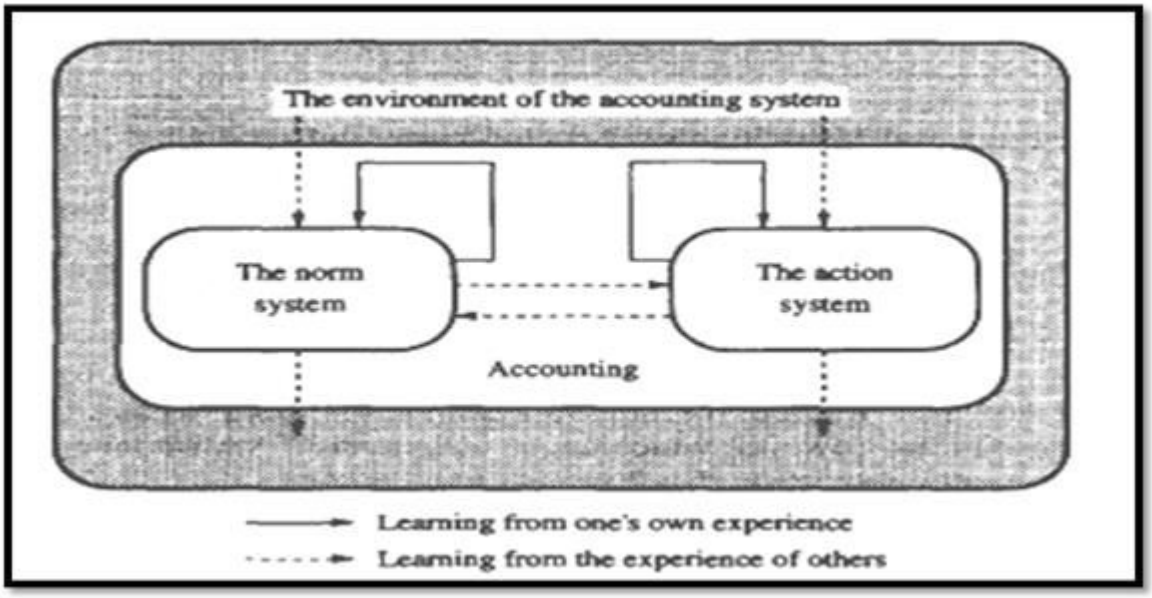


Figure 4, Norm and Action system *(Reproduced from Bergevärn et al (1995, P29)*

According to them, the accounting action system constitute the instrumental accounting activities which operates within single organizations and can be divided into separate but interrelated activities. In other words, the accounting action system represent the internal environment of an organization (for examples, culture and traditions). The accounting norm system comprises of the institutional environment of the accounting action system, meaning that it is characterized by rules and requirements that organizations must follow if they want to receive support and legitimacy from the environment. In other words, it is based on the external environment of an organization. The norm system outlines how things are supposed to be, whereas the action system outlines how things really are, Which mean respectively how accounting is practice and how it is used. Bergevärn et al (1995), adopted DiMaggio and Powell's (1983) theory to explain the three ways in which an organization can learn from the experience of another organization: coercive, mimetic and normative.

Based on the figure above, accounting norm is seen as a system capable of learning from other's experience (for example, learning from the experiences in the system environment, its own experience or in the action system). However, Bergevärn et al (1995) stated that the norm system learning modes also applies when discussing the action system. They observed that the environment can also learn from the norm and action system, which means that "the theoretical level several relations may occur in the institutionalization of accounting" (Bergevärn et al, 1995, P29), despite the institutional argument that says that the norm system

only learns from the experience of the environment and that the action system only learns from the experience of the norm system.

The results of their study showed that the norm system influenced the action system more strongly in Norway than in Sweden. They also observed that the accounting system between Norway and Sweden were alike because the norms did not control the substance of any action in any of the cases they studied, despite the fact that formal control being more coercive in Norway. However, Bergevärn et al (1995) found out that the institutionalization process in the case study was different which they found surprising since they were expecting it to be more alike.

2.4 Summary

We have presented and outlined different theories that can help us answer our problem statement effectively. We started first by explaining the concept of "fraud", then the different types of fraud that exist and the reasons individuals are so tempted to carry out those activities. Since our research question is based on IT growth and fraud, we outlined the major area IT fraud occurs the most. In order to prevent and detect those fraudulent activities, we shed light on internal control systems and its models for the effectiveness of any organization. Our theory of choice presented was institutional theory. Based on institutional approach we explained organizational legitimacy and the different institutional forces. Lastly, we presented the norm and action system model we feel could help us analyze and examine the empirical part of our study.

3 METHODOLOGY

3.0 Introduction

Gripsrud et al (2010) stated methodology as a systematic procedure which is about how we proceed to collect, analyze and interpret various kind of information in order to give meaning and explain a problem statement the best way possible. In this chapter we will describe our data collection methods (how we proceeded to collect data, which method is used and how these are conducted) and the reasons we chose them to help us answer our research questions. Additionally, the notions of validity and reliability will be touched upon.

3.1 Scientific Theory Approach

Johnson and Cassell (2011) denote that The philosophy of science is about having a reflexive approach to science as a phenomenon and concept. Easterby-Smith et al (2004) argued that it was important to understand how philosophical factors impact research because it allow us to administer better answers to research questions. Those Philosophical factors and assumptions made will:

- Influence what type of data can be collected in a research projects
- influence how to interpret the collected data.

For our thesis it was important that we understand the philosophical issues because the knowledge of philosophy of science helped us in explaining the research design.

The methodology and research techniques used in a research projects depends on the assumptions made regarding ontology and epistemology. According to Easterby-Smith et al (2004, p31) Ontology is related to the nature of truth in world, it can be subjective or objective and therefore explained as assumptions that we make the nature of reality. In other words, Ontology says something about a researcher's perception of what is real and true, its nature or being ,and often answers the question "what".

Easterby-Smith et al (2004, p31) state that Epistemology is related to the way we see the nature of reality in world and that each individual look at social world issues from different perspective each gained through their background, education, personal and professional experiences. In other words epistemology is about the theory of knowledge, in which we know something exists and often answer the questions “how” and “what”. There are three major epistemological view on how social science research should be conducted: positivism, relativism and social constructionism.

- Positivism argues that only facts derived from the scientific method can make legitimate knowledge claims and that the researcher is separate from and not affecting the outcomes of research. positivist epistemology has the following characteristics: Independence (the observer is independent of what is being observed); Value-free and scientific (the topic of choice and method can be made objectively); Large samples; Empirical operationalisation (usually quantitative); Generalization (enough samples should be selected in order to generalize to a population. Easterby-Smith et al (2004)
- Relativism argues that knowledge is relative to time, place, society and culture. Easterby-Smith et al (2004, p42) denote that relativism accepts the value of multiple data sources, by granting greater efficiency which include outsourcing materials and opinions. There are strengths and weaknesses when it comes to relativist perspective: the strong points include that it recognizes the value of using multiple sources of data and perspectives whereas the weak points include the requirement of large samples which might be costly.

Social constructionism (Interpretivism) starts from data instead of a literature based theory or hypotheses to be tested out, its approach mainly takes on an open minded approach. In social constructionism researchers generally look at companies in depth and mostly appoints to lengthy conversations, observations and secondary data (Easterby-Smith et al 2004,p40). Interpretivism look for a deeper understanding of meaning in data analysis rather than to focus on the generalization of things. This approach is often employed while doing qualitative research which involves observations, in depth interviews and analysis of text.
For our thesis, we will gather knowledge that will be communicated to us by our informants, by doing so we will try to obtain their various perspective and understanding concerning our research questions. Thereby social constructionism is best suited for our research and also because we are doing a qualitative case study.

3.2 Research design

According to Johannessen et.al (2011) it is important when selecting a method to find out which method is best suited to answer a problem statement. For our thesis, we have chosen to do a case study with a qualitative research design. Johannessen et.al (2011) denote that qualitative methods are much more appropriate when one don't know much about a subject or topic of choice beforehand. Mark & Philip (2009) states that qualitative research methods are

seen as the most applicable technique when it comes to researchers need to profoundly understand about perceptions or feeling of the respondents. Mehmetoglu (2004), argues that qualitative methods are more useful and advantageous because it helps researchers be able to extensively gain answers to questions such as “Why?”, “What?” and “How?” in their research questions.

When it comes to research designs, Mark & Philip (2009) proposed that there are seven of them, which are: experimental, survey, case study, action research, grounded theory, ethnography and archival research design.

Since we decided to do a case study for our thesis, we will shed light as to why we think this design is suitable for our research. Mark & Philip (2009, p146) define a case study design as “a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence”. In other words case study design includes in-depth, contextual investigations of matters of a phenomenon. Based on Yin (2009) point of view we know that there are some important statements about choosing a case design:

- Researchers should have theoretical assumptions that underlie the future study.
- The theoretical findings could be interpreted with already existing theory on the subject.

Case study design is widely recommended by scholars if researchers desire to acquire a rich knowledge of the research context.

There are various categories of case study, Yin (2009) notes three categories, namely exploratory, descriptive and explanatory case studies. Descriptive case studies describe the methods, strategies and techniques that is practiced in different organizations. Explanatory case studies examine data closely so it can explain the phenomena in the data. In other words, this study look at theories that give good explanation on a case without there being any generalizations. Exploratory case studies explore the phenomenon in the data which serves as a point of interest to the researcher. In other words, this study may address why organizations uses certain strategies or methods to research phenomenon that are less known.

In our thesis, we will do both an explorative and explanatory case study. Explanatory design because it involves in-depth, contextual investigations of our topic and is important in

answering the "how" kind of questions. The use of this design helps us clarify any perceived problems we may encounter. Explorative case study because even though our topic is relevant in today's society, we believe that it has not been research as much as many other subjects. This help us discover new findings and trends that has not been found before. Also it was important for us to understand the context of what we were writing, we wanted to explore and then explain our findings.

3.3 data collection method

According to Bogdan and Biklen (2007, p 117) "the term data refers to the rough materials researcher collects from the world he or she is studying; data are the particulars that form the basis of analysis." Johannessen et.al. (2011) denote that there exist two predominant techniques of case study design to collect data; quantitative and qualitative and that there's a clear difference between them. Since we are employing both explanatory and exploratory case study design, we chose qualitative research method to collect our data. First because it is seemly more in use than quantitative method in this type of research design; second because it is suitable for gaining insight into our informants own experiences, thoughts and feelings. We find this method convenient in order to gain deeper insight in organizations (our cases) internal control because there are so many things to learn which in return will help us operationalize our study. Furthermore, we can employ alternatives such as interviews, observation, documentary analysis and questionnaires to reach the in depth view towards our cases. After considering all the alternatives, we concluded that the most productive approach for our thesis would be to do interviews.

3.3.1 Primary and secondary data

Both primary and secondary data are used in our study. Primary data is the data that is collected directly from first- hand experience, in our case it is the data that is collected through qualitative in depth interviews with our respondents and because we wanted to have firsthand knowledge from our informants. We wanted them to accentuate their feelings regarding IT related fraud and internal control systems so we could understand it better. Secondary data, is the data that is published and collected by other parties. According to Saunders and Lewis (2009) definition, secondary data "is information gathered by someone other than the researcher conducting the current study". This data focuses mainly on our literature review framework and empirical findings chapter where we outlined different

theories of our study and our cases information. In order to do so, we used articles, books, study statistics reports and published surveys.

3.3.2 Interview

An interview method is a primary data collection technique, based on Donald and Pamela (2014,p 142) definition " an interview is the best method for researchers if the study is on the exploratory stages of research", this means that the use of interview enable researchers to gain valid, reliable and updated data in order to answers research questions. Furthermore, Donald and Pamela argue that there are three main ways of doing an interview, those methods are: unstructured interview; semi-structured interview and structured interview.

- Unstructured interview, sometimes referred as discovery or informal interview has no specific question or order topic to discussed. Brewerton et al (2001, p 77) state that, this method allow researchers carte blanche (free rein) to address any or all given number of topics which may be of interest to the researcher. Questions are not fixed or established but are allowed to evolve during the interview process. Here, comparability, ease of analysis and quantification are secondary to acquiring rich and important data from individuals using open ended instead of forced choice questions.
- Semi-structured interview, the questions in the interview guide would be would be predetermined in advance to acquire relevant information and the rest should be open ended in order to investigate other responses further. Brewerton et al (2001, p 78) denote that semi-structured interview is in most cases easy to analyze, quantify and compare however it allows interviewees clarify/explain their responses and to administer more in depth information where necessary. It is often referred as "qualitative research interview"
- Structured interview, often referred as quantitative research interview, because they're most often used to collect quantifiable data. According to Brewerton et al (2001, p 77), this type of interview include a recommended set of questions which the researcher ask in fixed order and which mainly require the interviewee to respond by a selection of one or many fixed alternatives.

For our research, we have chosen the application of a semi-structured interview form because, as explained above, it focuses on the interview experience of a subject and on the questions we need answers to. The advantage of this structured approach is that most of the responses

we will get from our representatives will be comparable and because all informants will respond to questions based on our topic. By using this method, it was substantial that the questions we asked were open ended so that the interviewees could respond as freely as possible. Along the way, based on our respondents answers we had the opportunity to ask further questions that were not initially listed in our interview guide. Dalen (2004) states in his book that when interviewing an informant he or she should not feel as you are interrogating them, that's why we started by asking our informants simple questions even though those questions had little relevance for our thesis. As a conclusion, we employed semi-structured interview in hope of gaining the most valid and reliable information about our problem statement.

3.3.3 Interview implementation

Before we contacted any firms, we had to come up with an interview guide. We did that for two different reasons; the first one was about familiarity, the interview guide was sent to our informants prior to the interviews in order for them to be familiarized with our topic of choice (questions) so when it would come time for an interview they would relax because they'd have an idea about what is coming. The second one was about us not being completely off topic we thought that it was important and necessary to have a trial interview, the purpose of it was to test out the questions in the interview guide. So we contacted one of our informants Arne Helme (KPMG, partner and advisory in the development of complex IT systems and solutions) whom helped us shed light on what to focus on when interviewing different companies. Since we made three research questions (fraud instances, internal control and institution instances) in order to answer our problem statement, we had those in mind when designing our interview guide. What we found out was that we were completely off topic when it came to questions based on internal control, most of the questions asked did not answer our research question, moreover we also needed to make those questions more understandable and relatable. As Dalen (2004) argued a trial interview should be conducted because it can give us positive feedback on whether or not your interview guide works.

Since we are writing our thesis in Norway and the case studies are about Norwegian companies, it was easy for us to arrange a face to face interviewing session with the various company's representatives. After contacting the right representatives by calls and emails we received the participating agreement from four different firms: Company X, Company A, Company B, Company Y and Kristian Thaysen (BDO, partner). However based on our

respondents' busy schedule, the interviews were conducted when and where it best suited them. Before each interview we talked a little bit about ourselves, the purpose of the research and asked if it was okay to use a voice recorder just to make sure that we got all the necessary data.

After finishing with our research interviews (collecting data), we used a method known as word-for-word transcription. This was for the most part to get all the data on paper so we could examine, interpret and categorize them. Which was quite challenging for us due to the fact that we needed to determine which data could lead to acquiring insight of our topic but also to generalize the most essential findings. As Christoffersen et al (2010) stated the importance of organizing data is to find coherences, patterns and to get an overview of the data collected. Our interview guide categorization process was divided into different phases of our research questions. This was due to the fact that we find it easier to categorize our collected data and to be able to link our interview responses to chapter 2 (theory framework). After the transcription we had to send copies to our informants, first because we wanted to make sure we had no misunderstandings. Second, because we wanted them to be sure that there was not any information they didn't want us to use, in case something could affect them in a bad way, or be taken as an advantage by competitors or fraudsters. However, after reading the transcripts, all of our representatives asked us for anonymity, which we gave them of course.

3.3.4 Presentation of informants

According to Dalland (2007) it is important when it comes to informants to find people who are relevant to your topic. For us this meant we needed to make a strategic choice to find firms and representatives that had good knowledge about this subject. Since our problem statement involves the development of IT, internal control and fraud, we thought that it was necessary to contact organizations that are dependent on ICT. The first thing that came into our minds was the banking industry, so we sent emails and called different Norwegian located banks. Most were none too happy disclosing any information due to the sensitive nature of our problem statement. However, Respondent 2 (IT and Risk Management director) from Company A accepted our request. Since our goal is to make a differentiation between firms in different industry, we thought that it was important to find another firm that was not in the banking industry. After our meeting with Arne Helme, we thought that it would be

appropriate to cooperate with a company in a healthcare industry, the reason for it is due to the fact that, as he told us:

"*the healthcare industry is much less prepared to cybercrime than many other industries and that the value in health data and personal information should not be underestimated"*

Hence we contacted Company B and Company X. Company Y was the least challenging company to agree to have an interview with us, we called and Respondent 1 (economy chief) right away accepted our request. We also tried to contact small and medium firms, because we wanted to see the contrast between big and small companies regarding their respective internal control system, type of frauds and the amount of resources they put in their systems to combat against fraud. However, we didn't get any luck with such firms, we contacted at least 20 S&M companies (most of them were private) but got rejected.

With Respondent 8, we wanted some kind of confirmation of our empirical findings. We had our interview with Thaysen from BDO after we already collected the data from the companies we used as our cases. Since confirmation is what we were looking for, we made sure to ask the same questions as others but also some additional questions because we as researchers wanted to take advantage of the fact that we were interviewing somebody that knew a lot about our problem statement but also has worked with lots of different firms, meaning that his answers to our questions would be diversified. From big to small companies, private or public sector and different industries.

Informant	**Company**	**Position**	**Location**
Respondent 1 (R1)	Company Y	Economy chief	Norway
Respondent 2 (R2)	Company A	IT and risk management director	Norway
Respondent 3 (R3)	Company A	Head of security	Norway
Respondent 4 (R4)	Company A	-	Norway
Respondent 5 (R5)	Company X	Compliance manager	Norway

Respondent 6 (R6)	Company X	IT manager	Norway
Respondent 7 (R7)	KPMG	Partner, advisory	Norway
Respondent 8 (R8)	BDO	Partner, compliance	Norway
Respondent 9 (R9)	Company B	Economy chief	Norway
Respondent 10 (R10)	Company B	IT chief	Norway

Table 4. Presentation of respondents

The table above shows all the representatives we used in our study research to gather data. Our informants consist of Norwegian managers in the economy and IT department and most of them have been in their respective positions for more than 10 years. Experience was key for us, we wanted our respondents to have knowledge about our problem statement in order for them to share with us based on their experience whether or not the development of IT has led to more fraudulent activities and the different measures they are taking to prevent and detect those activities.

Moreover, due to sensitive nature of our problem statement, we made sure to have an approval/agreement with NSD (Norwegian centre for research data) so that any sensitive information we used in our research paper would be properly treated (*see appendix 4*). In that case we filled an application to NSD to check if our project had to be signed up and treated under their supervision, in which it had to. Thereby we received instructions from NSD about how to treat our collected and stored data, but also several instructions regarding communication to our respondents.

3.4 Validity and reliability

Mark and Philip (2009, p 156) state that "all researchers are eager to reduce the possibility of getting wrong answers, in order to avoid it they have to pay high attentions according to what research design should be chosen and used. The type of research design being selected would impact immensely on reliability and validity of the research".

3.4.1 Validity

Easterby-Smith et al (2004) define validity as "a concerned with whether the findings are really about what they appear to be about". In other words, validity relates and measures the truthfulness or accuracy of the research findings. Validity is a major component in doing research considering the fact that any research could be influenced by different outside factors which can discredit the research results. Easterby-Smith et al (2004) argue that in social constructionist research literature, there are many criteria for assessing the validity of the data collected during a research process, those are mainly: authenticity, plausibility and criticality.

Authenticity, implies convincing the reader that the researcher has acquired a deep understanding of the topic at hand. Plausibility requires the research to link into some ongoing interest among other researchers and criticality encourages readers to question their taken-for-granted assumptions, and thus offer something genuinely novel.

According to Yin (2009), there are three form of validity; construct, internal and external validity. Construct validity implies that researchers should use correct labels to enhance the quality of their research. In order to do so, one should use diversified sources of evidence, discuss the theme with experts and have the most essential informants read through a draft of the research at hand. In our case, we've worked closely with our supervisors who've helped us during the whole process of the research project. We've also worked closely with some key informants to foresee what we have done so far.

Internal validity, also known as credibility is the truth about deductions regarding cause-effect or causal relationships. Therefore, internal validity is only applicable in studies that try to enact a causal relationship. To improve internal validity, researchers should look for alternatives explanations by asking questions such as: can we conclude that the changes in the independent variable caused the observed changes in the dependent variable? Or, is the evidence for such conclusion good or poor?

External validity, also known as transferability refers to the degree to which the results of an empirical investigation can be generalized to or across individuals, settings and times. In other words, it refers to things that happen outside of the investigation and could affect whether the findings are representatives and can generalized.

In order to eliminate threats for validity in our research project, we assembled reliable information from two data collection techniques: primary, based on the in depth interviews and secondary, based on the respective companies websites, forums and annual reports. Primary method is the main threat for validity in our project because of the respondents, namely the information they disclosed to us during the interviews. There are always risks of interviewees telling the researcher what they want to hear, that's why building trust with our informants was crucial. Especially due to the nature of our problem statement, our topic relates to fraud and internal control which is quite a sensitive subject for many organizations because most firms would not like to talk about their security breaches or how they are being violated. An informant might disclose false information to the researcher in order for the project to be looked at in a better light. Another risk is the informant giving the researcher false information in fear that their competitors might use that information against them. The only way to prevent this is to guarantee the informants confidentiality and anonymity. Which we have done, after we sent the transcribed interview to our representatives, they asked us to give them full anonymity.

3.4.2 Reliability

Reliability, also known as dependability is according to Easterby-Smith et al (2004) a concern with the transparency in research projects, how the respondents are selected, how data is created, summarized and transformed into ideas and explanations. Mark and Philip (2009) denote that reliability refers to the extent to which the techniques of data collection and analysis process will be consistent findings. In other words, reliability is about the quality and the consistency of a research study, if findings from a research are replicated consistently they are reliable. One can intermittently notice reliability in qualitative research considering that qualitative research tends to include consistency. Since our thesis is based on qualitative research, high considerations in relation to reliability is paid (focused on).

Mark and Philip (2009) argue that there are four threats to reliability, those are: participant error, participant bias, observer error and observer bias. Those threats mainly come from human error or human bias, either from researchers or informants.

We did our best to reduce threats of human error and bias in our research to get the most reliable results. We increased reliability in our research study by being open and transparent concerning the methodological techniques we used. Each step taken in relation to the procedures of how the respondents were selected, how the interviews and data collection were

performed so that the reader could gain a deep understanding of how this affected our study. As mentioned before we used semi-structured interview method to collect data, in order for our respondents to feel free or relax when expressing their feeling and views during the interview process. A transparent and open approach enhance the quality of a research study and other researchers will find it easier to duplicate that kind of study (our study).

3.5 Summary

In this chapter, we have presented and interpreted our methodology choice or technique. We chose to do an explorative and explanatory case study of four different Norwegian companies (Company A, Company X, Company B and Company Y). We outlined the various ways we want to collect our data, we went for qualitative method, by using in depth interview that were semi-structured. Furthermore, we've also analyzed the difference between primary and secondary data and which of the two methods we thought was best suited for our research. The introduction of the informants was presented and as a conclusion we distinguished the difference between validity and reliability.

4. EMPIRICAL FINDINGS

4.0 Introduction

In this chapter we will present our empirical findings, from our interviews with Company A, Company X, Company B and Company Y. First we will state how the current situation is in Norway regarding cybercrime, and go through different examples of fraud that cybercrime consist of. Based on the answers from our respondents and experts we have worked with, we will categorize the different fraud types into three groups: common, critical and other. For each category we will go through the frauds that was discussed with our informants and present them under one of these categories. Then we will look closer on how the internal control system of our respondents are affected by the evolving picture of threat that cybercrime consist of. This means looking closer into ICT development, control processes, risk management and security measures. When doing this we will present findings from our respondents in two different parts. Each part will consist of companies that are affected by a certain context. The third part will focus on the external pressure from legal authorities. This means how institutional forces are affecting our respondents, and how important external pressure, in terms of laws and regulations, is as a driver to work with internal control.

4.1.1 Cybercrime in Norway

Computer related crime over the internet is an activity that has been growing rapidly in recent years, and it is still growing. Unfortunately, Norway is one of the most attractive countries as victims of cybercrime. This is because we are one of the leading countries in taking in use new technology, we are a wealthy country and we are having a reputation for being naive. According to one of our respondents there was 22000 registered attacks against Norwegian companies in 2016. The list of registered attacks is growing, but the unregistered numbers are also big, since many companies do not want to report the incidents of various reasons, says R3 from Company A. According to Mørketallsundersøkelsen 2016, which is a report of unregistered attacks from Næringslivets Sikkerhetsråd, 412/1500 (27%) of the interviewed companies (a random selection of companies that have five employees or more) said that they had experienced unwanted cyber attacks in 2016.

One of the very latest trends we have seen regarding this is that not only regular businesses or institutions is exposed for this threat, but also politicians. That fraudsters want to impact the political agenda is now more common, and there are rumors that both the presidential election in USA and Brexit was affected by foreign hackers. A couple of our respondents said that they often see organized attempts of hacking that start and stops at the same time each day. Since the attempts can be connected to normal working hours from other time zones (e.g. Russia) it is not unreasonable to say that this is most likely hacking attempts from governmental level. One of our respondents was not in doubt regarding this "*There are people who are publicly employed to attack, and we are in a cyber war*". 13th of February this year VG reported that 727 persons on governmental level had gotten their emails hacked, in which former prime minister Jens Stoltenberg was one of them. Respondent 3, head of security, from Company A is curious to observe what will be done to deal with this in the future:

"It will be very exciting to watch what is happening in the time to come when we see massive attacks towards the environment that are on the top in Norway. Both when it comes to industry and politics."

4.1.2 Common fraud types

What we have seen that stand out as the most frequent fraud hitting businesses is fictitious emails, or phishing. The term "phishing" is describing the act of searching or fishing for sensitive information like passwords or credit card information for malicious purposes.

Ransomware is the type of phishing that stands out as the clearly most popular, and all of our respondents mentioned that they have received this type of email, some more than others. This kind of fraud works in the way that the fraudster send an email that looks like it comes from a normal Norwegian organization, and want you to click on a link that leads you to open up and release a virus into your computer. Once the virus is released in your system it will immediately encrypt all files and systems, and the computer is then out of use. After the files are encrypted or the systems are taken down, the criminal usually demand an amount of money for a key that will decrypt everything again. It is strongly advised against paying the money they demand, to prevent motivating and financing this kind of activity. At the same time, when the files and systems are encrypted it is impossible to get them back, unless there is a backup solution to recover. Therefore, if the price for the decryption key is not too high, or the information is so valuable that the company cannot afford to lose it, many companies have ended up paying. The reason these attacks has been successful in Norway is that the fictitious email looks convincing with both good layout and written Norwegian language.

One example mentioned by two of our respondents was an email that looked like it came from Telenor, but was actually sent from hackers, with a fictitious invoice in it. One of our respondents said that this Telenor-campaign was the biggest he had ever seen, and Company A said that 600 of their employees received this. Of those 600, there was several who actually got baited, who needed to have their computer cleaned up and then reinstall all programs and software.

Another example regarding this, mentioned by Company A, is fictitious emails looking like they come from Posten. This is especially popular before Christmas when many people order gifts over the internet, and then are expecting something from Posten. These kinds of fictitious emails are sent out to huge amounts of receivers, and when expecting something from Posten it is easy to get baited by this kind of fraud.

Both Company X and Company A said that they see a trend where fraudsters are aware of when their targets are low on staff, and using this weakness as a time to attack. This can either be at certain hours of the day or in periods when companies are low on staff, such as long weekends or vacations. At these periods the full time employees are absent, and substitutes are in place who do not have the same level of confidence. Fictitious invoices, from a company that they have never heard of, comes in every summer requesting transfer of with

quite big amounts. They stressed that it is a great cost for them to have enough competence and capacity to defend themselves 365 days every year.

Another fraud that has been popular lately is CEO fraud, and three of our respondents told us that they had experienced this. This kind of fraud works in the way that fraudsters collect information about the company they want to attack. This involves mapping information about economy chiefs or employees with authorities to perform transactions. Then, the attack starts when an email is sent to the subordinates of a CEO or CFO, requesting a transfer to a foreign bank account. The email looks like it comes from the economy chief or CEO and typically the fraudster say that the transaction should happen quickly. The reason this fraud has become popular in the latest years is both because the fraudsters are being creative and finding new ways of perpetrating fraud, but also because, in today's society, it is easy to gather information through social channels such as Facebook, Instagram and LinkedIn.

A third popular fraud towards bigger companies is hacking. All of our respondents except Company Y told us that attempts of hacking into their systems was something they registered daily. None of them had experienced any successful attempts regarding this, since they all have good security systems to protect the sensitive information that is stored in their databases.

What we was surprised to see was that none of the companies we interviewed mentioned that they had experienced identity theft fraud. The auditor we interviewed from BDO was very clear about identity theft as one of the most common fraud types of6 our time. He explained that when leaders quit their job, it is not unusual to see them start a new company as a competitor to the one they just left. The leaders then bring sensitive information and business secrets from their previous company, to the new company. These business secrets can be documents such as strategies, price lists or customer lists. He further pointed out that this comes as a consequence of increased digitization in later years, since the information is both easier to access and bring to the new company.

4.1.3 Critical fraud types

What kind of fraud that is critical and which one is not, is depending on what type of business it is and what context they are operating in. What we found from our interviews is that it is a common understanding for businesses that are storing sensitive information that they have to

protect this at all costs. Company A, Company X and Company B all said that it would be a disaster if someone managed to hack into their systems and cause a leak of information about employees, patients or customers. It would not only be very critical for those who are inflicted, but also the reputation of the company itself would take a huge hit. All kinds of threats that could harm the trust between a company and their stakeholders, is seen as a very serious type of threat that has to be dealt with. A leak of information do not only have reputational consequences, but also monetary, just imagine the amount of money a fraudster could demand by blackmailing a health institution if he had sensitive information about patients as hostage.

Company A talked about how the picture of the threat have evolved for them in the latest years. The traditional picture of threat for a bank have in many years contained threats such as bank robbery, burglary or sabotage. If we were to ask them a few years back they would maybe have considered these threats as critical. Today, even if a robbery actually occur, the bank will not lose much since the amount of money that are stored in the banks have decreased to a very low level. Respondent 3 explained this shift like this:

"*The reason for this shift is that banks have quitted regular cashier services, but also the potential to get more value through cybercrime is a lot bigger, the chance of getting caught is a lot smaller, and the punishment is also different. The criminals are professionals, and they choose what gives them the best outcome combined with the smallest chance of getting caught.*"

They could further confirm that their biggest concern today is to protect the sensitive information they have in their databases, since that is what they live on. Respondent 2 pointed out that banks today rely greatly on trust, both when it comes to managing money, that the money customers are saving is safe, but also managing information. He emphasized not only are the information sensitive, but there is such huge amounts of data, which also increase the potential consequences of a leak. Not surprisingly was their biggest challenge in the future to secure this information, and protect the trust from their stakeholders, especially customers. Regarding this they said that it is hard to keep a balance between making sure new products are secure from hackers, and at the same time make them easy to use, since too much security can be experienced as a struggle for customers. Company X shared the same opinion

regarding the importance of protecting the trust between them and the customers, and said that worst case scenario was to inflict their customers and hurt them.

Regarding more regular businesses, in our case Company Y, the major concern seems to be more monetary. Since they are not protecting sensitive information about customers, the respondent was talking more about internal control routines to prevent fraud like theft, both externally and internally. Despite that it is not the major concern, reputational harm and bad marketing was still mentioned by Company Y as threats they need to pay attention to. Based on information we have collected from the experts we have talked to from KPMG and BDO we can say that smaller and more regular businesses are not that aware of the threat from cybercrime and its consequences. Unfortunately, they are not any less exposed to cybercrime as the fraudsters see them as less prepared to protect themselves, which makes them easier targets. This explains why the economy chief at Company Y couldn't give us very much information about threats from cybercrime, but rather talked about more traditional types of fraud like theft.

Phishing, or basically ransomware, was mentioned under the headline "common fraud types" but it has the potential to be one of the most critical types of fraud as well. What is deciding if it becomes critical or not is the type of information or systems that are encrypted, and also if the victim have backup solutions to recover and the quality of these. A worst case scenario regarding this is that the fraudster have managed to encrypt your most sensitive files or taken down the most central systems, and there is no backup solution to recover, then your fate is basically in the hands of the fraudster. When the files are encrypted, it is as mentioned above, impossible to decrypt them again. Then, if you are very dependent on that information, and the fraudster know this, he can require a very high amount of money to help you out. The solution is either to have backup recovery systems, pay the fraudster and hope he gives you the decryption key or catch the fraudster. In most cases, the police do not have capacity to deal with these kind of frauds, especially if the fraudster have no ties to Norway. Besides contacting the police, you can contact your IT-supplier, because sometimes there are backups in your computer system that you don't know of, but this is not certain.

Another type of fraud that can be critical in the right context is DDoS attack. None of our respondents was concerned about this as they did not consider it critical in their industry, but both Company A and Company X stressed that this type of fraud could be very critical in

other industries. DDoS (distributed-denial-of-service) attacks are an attack where you deny someone or something to access information or resources they need access to, often towards websites. A successful attack can for example take down a website so that it will not be available for employees, customers or other stakeholders. There was only one of our respondent that told us they have experienced this towards themselves and their internet supplier. The last time was a couple years ago, and they confirmed that all of their services was unavailable, both internally and externally for about 15-30 minutes. Further they said that they are not very dependent on having internet access 24/7 since the employees can still do their job in cases like this, and they do not sell any products or host any critical services through their website.

However, some of our respondents emphasized that this can be a very critical type of fraud in other industries where companies are depending on online booking systems or online sale. Examples that was mentioned in our interviews was the hotel and aircraft industry, since they are depending on having a website up and running 24/7. Big companies like Norwegian, SAS and Thon Hotels can lose millions if their website is down for only an hour, since customers cannot access their online booking system and then order from their competitors instead. Also companies that are depending greatly on internet shopping is very exposed for this kind of threat. Besides the consequence of not selling tickets or products, this kind of incident can also create panic when the employees cannot access information that is stored in online systems. This can be information like how much is left in stock or information about existing orders.

4.1.4 Other fraud types

So far we have presented the most common and critical frauds regarding cybercrime, but there is still a few that was a topic in our interviews. These frauds are not one those frauds that occur the most often, and despite that every type of fraud can be critical, these types of fraud is not seen as the most critical ones. The first fraud under this category that we want to shed light on is a technique to launder money, called money mules. A money mule is a person who receives and transfer illegally obtained money from criminals, and are also assisting them withdrawing the money. These money mules makes it much harder for investigators to follow the trace. Company A told us they have experiences with these accounts, and they have a list where they register every mule account that they know. If anyone is trying to use one of the those accounts that are on the list, then an alarm goes off. Investigation notifications or

actually successful use of these mules is how Company A get their information about them and can register them in their system.

A couple other fraud types related to banks are credit card fraud and accessing big payment centrals. Company A said that they experience credit card fraud all the time, while they pointed out that this is a calculated risk where the revenues are exceeding the small losses they have regarding credit cards, so this was not a concern for them. Maybe the most critical way of doing credit card fraud is illegal access of big payment centrals. These centrals have stored hundreds of thousands credit card numbers. Respondent 3 explained how it is done:

"*For example one big store that has a certain payment motor that every payment goes through, then you can access this motor and take all the credit card numbers*"

Company A often get notifications that credit cards have been stolen or copied, then they contact those who are inflicted and tell them to destroy their card and that they will receive new.

The last type of fraud we are going to mention under this category is domain registration fraud, which was mentioned by Company X. They had experienced this themselves and they almost got baited by it one time. This fraud works in the way that someone, typically eastern (like China or Japan), contacts you and ask if you own the website "www.CompanyX.no" or "www.CompanyX.com" which you often do if you are Company X. Then they tell you that there is someone else that want to register a similar domain name like "www.CompanyX.com.cn", but they wanted to ask if you wanted to buy it first, since this domain is so similar to your brand and website. They tell you that you are first in line, and if you want to buy it you can have it. One of our respondents at Company X described their interaction with the fraudsters like this

"*There was a lot of documents back and forth, and they were quite targeted and hard to detect".*

Company X didn't get baited on this, since they stopped up, took a step back and looked at what was going on. Further they pointed out the importance of being aware in a busy daily life, but often a Google search is enough to bust someone.

4.1.5 Visual summary of fraud types

In the table under we present a visual display of our various fraud types findings we discussed above.

Fraud	Category	Experienced by
Phishing (ransomware)	Common, critical	Company A, Company X, Company B, Company Y
CEO fraud	Common	Company A, Company X, Company B
Hacking attempts	Common/ critical	Company A, Company X, Company B
Identity theft	Common	-
DDoS attack	Critical	Company X, Company A
Money mules	Other	Company A
Credit card fraud	Other	Company A
Domain registration fraud	Other	Company X

Table 5: visual summary of fraud types

4.2 Measures against cybercrime

In this subchapter, we are going to take a closer look at how our case companies deal with the threat of cybercrime. First, we will shed light on the various control systems and measures each firm applies, and then explain why and how they combat cybercrime. Since the cyber threat can vary with the context surrounding a company, we will present findings from our respondents separately, depending on what is their main concern towards cyber security. First, we will present empirical information about companies concerned about sensitive information and information security. The second part will be presenting findings about Company Y, who is more concerned about monetary losses from cybercrime like most companies in Norway.

4.2.1 Companies with focus on information security - Internal control systems

When it comes to internal control systems, we found that Company A, Company X and Company B uses different systems. Company A employs the framework of the committee of sponsoring organizations of the treadway commissions (COSO) and the framework of the control objectives for information and related technology (COBIT) (two internationally recognized intern control systems) as a basis for their principle for internal control. The company uses all five levels of the COSO framework; control environment; risk management; control activities; information and communication and monitoring, in order to help them achieve their goals of efficient operations, reliable financial reporting, compliance with laws and regulations and COBIT for the evaluation of ICT.

Company X on the other hand uses ISO 20001 and 20002 (two international standards), where the main reason is information security. They use this first of all because they are a business that stores personal information about their employees, but also because they are an organization that provide managed IT services for the health sector. There is a model called BSIMM (international maturity measurement) regarding information security and measurement of maturity that the company is using in order to see how mature they are. They use the same model to do a systematic review of checklists that are very comprehensive for both Company X and the products they offer. The company also look at ISO 27000 and 27001 standards for the quality of management system.

Whereas, Company B is a part of HelseCERT, which mean they have Norsk Helsenett as their supplier for internal control, mainly computer network. Since Norsk Helsenett is their supplier, they also have the infrastructure in place to monitor the network system. Moreover, the organization have a regional cooperation towards the ICT-infrastructure in Helse Midt-Norge, where HEMIT (The Central Norway Regional Health IT, an internal administrator and provider of IT systems) is their outsourcing provider. HEMIT has resources regarding taking care of the drift network and also computer security and monitoring. Furthermore, the company has the mercantile part, where employees are responsible for computer security both at HEMIT and at the individual health entities. Those employees form a group called regional security forum, where they make plans for how they can manage, handle and protect all the sorted data. The company is using ISO 9000:2000 standard for their quality system.

4.2.2 Security measures and Risk management

For all of our representatives having the best security measures is a pivotal factor to combat fraud. Most of our informants emphasized that, in order to avoid threats from cybercrime one should look at the organization culture and systems. The security of Company A is based on 80 percent attitude and 20 percent systems, which they denoted was a well known 80/20-rule regarding security. They further stressed that attitude and knowledge was the absolute most important defence there was. In order to succeed, the company is using lots of resources and are going to use even more in the future to inform and train their employees. This means make them aware of what is happening so they can be capable to avoid and detect any types of fraudulent activities against the company, instead of having only technical solutions which are in itself not good enough. Company A is using a training program they call "passopp" that focuses on higher understanding and readiness for fraudulent threats, and are something they are working continuously with by updating their employees.

When it came to the organization culture, balance was the key word our Company A informants used, they argued that one has to have culture and understanding but also to never shy away from failure. Instead, when it happens one should talk about it. In a worst case scenario, an employee might make a mistake by actually clicking on something and get their computer infected. They know they have done something wrong but at the same time do not tell the managers what's happened because of fear of receiving the wrong consequences and it becomes a culture of fear.
According to Respondent 2, Company A has worked in two ways the latest years, he underlined that:

"One of the ways is structured documents, what is written and what is needed to deal with the framework regarding steering and control. And the other way is culture, and especially the password programs we are training all our employees towards."

The company has been using, for the past year, an e-learning program called Nanolearning, which focuses on organizational culture oriented work on information security. That is because information security is their biggest threat. Moreover, to avoid any types of threats, they are also working towards the company leadership level so they can build a strong security system at the top that can work with crisis readiness just in case something happens.

Just like Company A, Company X also share similar views when it comes to important measures against threats. They accentuated that training employees and working with culture and attitudes are important. They argued that, the company can produce as many security systems as they want but if an employee is not up to date hackers and fraudsters are always going to be in front. That is why they depend on that their employees know the kind of areas they belong to, and how to think critically and use their own sense to detect fraud. Considering that it would be dangerous if the employees was only relying on the company security barriers alone. So they have to show expectations that everyone is contributing to a good culture of security, do not take things for granted and that the environment they operate in is safe. That feeling was shared by our informant from BDO, he said that tests were done to see if employees training was effective. However, in his opinion, those tests usually don't have a very good score, but pointed out that:

"It is important to create a good culture of security and internal control around it, and you also need exercises related to the different topics."

In order to create a successful culture, Company X stressed that it takes time and one has to be prepared. They conduct business meeting ends 2-3 times a year, where they try to take some time to present the picture of threat and use information from NSM (Nasjonal sikkerhetsmyndighet). They show examples of things that have happened to them and give information about new security systems. This is something the company has been doing for years, as one of our respondent pointed out that during those business meetings they have talked about the times when Telenor and Statoil were hacked First, because the companies were open about their situations, but also because they wanted to know how it was done.

Another relevant security system that Company X has been implementing and are considering of using is the cloud-based equipment and services. Cloud-based equipments are shared online, which means software and other utilities can be accessed electronically by whoever have access and a demand for it. They emphasized that the benefit of using such system as an internal type of equipment is because these equipments are being updated all the time, and also practically very easy for their employees to use. However, there are also threats with using this system because there is someone else who have made the security system for these equipments, meaning that they will have to trust an external third party and then be even more aware of what they use these cloud-based equipments for and what they save there.

If they ever decide to use cloud-based, our respondents pointed out that, they are going to have explicit guidelines that each employee has to follow tied to the equipment. These guidelines will then be a part of the company quality system, where each employee have to confirm that they have read it. Just like Company X's current quality system, the new system will have a function to register confirmations. Employees won't get access to this equipment before they have confirmed that they actually have read these guidelines. As Respondent 6 stated:

"These guidelines are typical in the way that they demand own considerations and attitudes while they use the system, because we cannot divide what is trustable and what is not trustable information to be posted on these cloud-based services. We are depending on our employees to show good attitude and that they actually also are personally aware that there are expectations regarding this."

Based on technical solutions, our informants from Company X stated that the most important security barrier is a project they started working with in 2015. This was a system for monitoring and active blocking of threats on the firewall side, which is a firewall solution with a lot of different modules that can easily stop threats, based on known vulnerabilities and threats. Something they have used a lot of time working with. The security barrier also have end-point security, which is about threats that are detected on the client side, which are existing outside the company's network so it can be easier for them to help them. However, there are vulnerabilities that they are concerned about, which are personal devices used by employees or customers outside of their security system. Which they exemplify by saying that; "*it can be employees that are helping a customer on a mobile device or out traveling on a airport or a hotel, something they do not have control over"*.

Company A also share the same concern as Company X when it comes to clients security. They feel that the technical solutions systems the company is using is solid and good. However, they fear that despite having an internet bank that is 100 percent safe, their customers are using this bank through ipads, iphones and other devices that are unsafe. So if those devices have viruses then hackers can easily get into the internet bank. In order to avoid those situations, Company A want to simulate the work they have done internally (by training,

updating and creating a safe environment for their employees) to their customers, so they can understand the usage of their services and use it in the right way.

When it comes to security measures, Company B relies on their suppliers. They stressed that the picture of threat is increasing, which means that their suppliers need to be aware and responsible for ensuring that their products are good enough to meet these threats. In respect to the picture of threat, they denoted that there were two factors; one is their infrastructure, that it is safe and keep attacks outside, and the second is that the systems that exist and software that are going to be used have authentication mechanisms which secures their data. They emphasized not wanting to develop any new systems but buying something that is in the shelf already, which is about buying a program that is internationally recognized, so that the necessary security measures are in place and working, which of course will be checked.

Company B is not the only company that relies on suppliers. Company A also relies on a third party, in which they point out are extending the picture of threat. As they underlined, the company is doing a lot developing (IT systems) where they engage third party suppliers which can be used as a link by hackers to reach out to their customers or themselves. One of the respondents implied that if a supplier is making a product that are delivered to one of their customers, but don't have the same level of security as them, then hackers can use that supplier as a loophole to catch information about customers. That is why it is essential for their partners to have good security as well. Additionally, Company A is working on risk management analyses continuously. They are building their own control and report system as a supplier, which they denoted consist of elements such as how the company report incidents and how they are working on improvements.

In order to avoid the cyber threat, Company B argues that, in the last two years they have had an agreement with experts at Norsk Helsenett that have engaged people to try to penetrate and get into their databases to hopefully find some weaknesses so they can start and develop some measures. Moreover, they have an information security advisor who is in dialogue with Norsk Helsenett to find solutions of how they are going to perform this approach. Something they've tried both internally and externally. As respondent 9 stated:

"I can say that, and I have been here for 12 years, and we have not had any extern burglaries into our data, but we have had incidents where our own employees have snooped in the

system, they have accessed confidential files about patients that they actually didn't have access to."

When it comes to attacks against the health sector, our informants highlighted that the sector is quite rigid and have norms for information security that they have to follow carefully. Furthermore, they added that there are rules for authentication routines. Sometimes the company deviate from those authentications routines and use alternative solutions that are not a part of the original routines. In those cases they have to do careful risk considering on the new solution, and accept that one-time solutions will be used for a while. However, R10 emphasized that in these situations it is important to have a plan for when they are going back to solutions that are a part of their routines. As one of our respondents accentuated in an exemplification:

"For example now, we have a solution where employees can log into working platforms through a private device, using a private password and an SMS code to get in. This is for a three month period and then they go to ID-porten where they use bank ID and that kind of authentication."

4.2.3 Common measures

When it comes to security and systems all of our informants believe that it is best to make common systems, since everyone is under the same threat. Our Company A respondents emphasized that if they make something regarding security, they'll share with others. However, they'll also need to be careful because there are certain subjects that might only be necessary for them. In 2014 Company A established FinansCERT in order to have resources and ways that can help them prevent threats of fraud. Every Norwegian bank are in on it and financing it together and based on what one of our respondent told us:

"There is a close cooperation between FinansCERT, the police and everyone that are monitoring this traffic. There are exchange of information when we have a picture of threat that are growing, and then we discuss it."

Moreover, for the prevention of internal threats, they argued that in FinansCERT they make best practical solutions to avoid recruiting unwanted people. First, they need to know that the person applying for a job is actually that exact person, and not someone else. So when it

comes to internal threats, they've made common procedure regarding recruitment that are the best practice solution for the banking industry. Further they denoted that they can have all the best systems in the world, but if there is someone on the inside committing fraudulent activities, the security systems won't matter, as they will have access to everything.

The health sector (Company X and Company B) have a cooperation with Norsk Helsenett, department HelseCERT, where they exchange information about threats. They look at the various threats and make considerations. One of our Company X respondents stated that they work a lot with HelseCERT. They have continuous contact and are member of Norwegian information security forum. Furthermore they stressed that Norsk Helsenett was auditing them, on their internal control routines. They believed that it was very important for the company and the health sector in Norway to have a function like that, because it causes a close cooperation between everyone in the health sector.

Our respondent from BDO also added that although in Norway many organizations are not fully prepared for the new picture of threat, there exist FinansCERT, HelseCERT and KraftCERT for the respective companies in the bank, healthcare and power sector. Those can help industries take cybercrime more seriously, and help to prevent any attempt of fraudulent activities. Moreover, he posits that the challenge for these CERT's are that they are dealing with only the tip of the iceberg, but do not have the capacity to do anything more.

4.2.4 ICT Development and Internal Control process

Based on the data collected, our respondents felt that there are pros and cons when it comes to the development of ICT. Company X admits being worried with ICT development because of how the picture of threat is evolving and they sometimes feel vulnerable, meaning that it has made their jobs more challenging since they have quite a big system and Norway don't have good enough level of education to deal with how rapidly IT is developing. They additionally underlined that Norway and the rest of the world should be self critical about the evolution of IT. Moreover, Norway is way ahead in using new technology both mobile devices and also technology software which they are drivers of in relation to the world. That is why our respondents pointed out that it is important not to be naive when it comes to new technology and that one should always be prepared. However, our BDO respondent emphasized that Norway has a reputation of being very naive regarding new technology and that makes us more exposed to cybercrime.

Company A feels that IT has given them new opportunities, in that they can access a lot of data, can have analytic approaches and can make new system controls, meaning that the development of IT has open up for making the control side more effective. Respondent 2 emphasized that the development of IT has had a positive effect of his job, the reason for it being that, as he stated:

"We are working with robots (computer programs) who are doing repeating tasks with also with high quality. They rarely make mistakes, working 24/7 and are following all orders. If 200 employees did the same there would be more mistakes."

Respondent 3, later added that:

"For me, IT has made it easier to educate employees through e-learning programs, so you can deliver it to them electronically. Compared to earlier when you had to travel around and make evening sessions, this is a huge benefit. You can also communicate more often and better (Skype etc),measure it and have good overview."

Respondent 6 explained that with ICT development, Company X has acquired quite big systems which in return make their job more challenging. He highlighted that Norway don't have a good enough education to deal with digitalization and that there is not a specific university to deal with the problem that is emerging. However, he stated that the University of Gjøvik have a information security engineer program which has a good reputation.

As a result of IT development and digitalization, the representative from BDO accentuated that the picture of threat has increased dramatically and there will always be chances of fraudulent activities committed internally or externally. Moreover, he pointed out that there are many companies who are outsourcing services and then there are third parties that have access to company databases, which can be problematic because lots of things can happen. Examples of that can be sabotage by people who have access to different accounts and systems, changing of bank account information or changes in the master file in the accounting system. Furthermore, he said:

"The reason the picture have been extended is because the amount of information that is stored is huge and are escalating all the time."

According to Respondent 4, Company A's framework, leading strategy and standards are the most important control process the company has because it tells them how to work. Those processes consist of; first their technical system, in which they have created an intranet solution where one can do Google similar search and hit. The second is how they work with incidents that happen, how they report it, work with measures and learn from their mistakes. Moreover, R4 continuously added that those reports goes to the leaders of the company so they can work on measures. The third and last thing is how leadership have to secure that the company is moving towards the right direction and once a year they have to evaluate the internal control of the firm and confirm that everything is okay.

When it comes to internal control process, our informants explained that one cannot look at internal control as an individual process, because it should be seen as an integrated system. Many processes are working towards a common goal, and if one fails then the others might not be as effective. They reiterated that one can have very good routines and guidelines, but if no one knows where they are or read them then they are gone. Internal control should be looked as a whole, then build up its weak areas and try to improve all the time.

4.2.5 Reputational risk

According to R2, the most important to have in mind today for the banking industry is that they rely greatly on trust, both when it comes to managing money and managing information. He accentuated that the biggest risk or threat Company A has is information, because the company is sitting on a lot of information about customers. R2 also added that managing all of those customer economic information is a task that has to be taken serious, because this has to do with reputation risk, which also is the biggest risk.

On the other side, R8 claimed that most business today are overrating reputation risk when it comes to critical incidents. He underlined that organizations today are too worried about reputation in cases like this:

"*I do not say that is not important, and the reputation can easily take a hit, but my experience is that this is just for a little time and then people quickly forget. What was written in the*

newspaper yesterday is forgotten today. My point is not that this is not important, but I think most of companies exaggerate. For example DNB didn't take a huge hit from the Panama papers case."

4.2.6 Corporate Governance

In order to reduce risk factors, such as reputation damage, loss of confidence from employees or clients, each company has put in place management and governance systems that can help them establish and secure the institution reasonably.

Company A and Company X have a classical organization design, each firm has an internal organization that provides a clear division of roles and clear lines of responsibility. The line organization handle all the personnel-related, technical and administrative matters. As stated by Company X, when it comes to the fonctionnement of the company, everything takes place largely in the form of projects in accordance with their established methodology. All projects has to be estimated and monitored with regular reporting. As R5 noted, Company X is now working with a big audit for their security guidelines, something they are building up from the start again. A few years ago the company built up what they called the third generation security guideline which they are taking a huge audit on. They stressed about working out a report and get it to the leadership. Furthermore, they added that, it is up to the top management to make the last decision regarding implementation of the security guidelines.

Moreover, our representatives accentuated that to achieve efficient operation, it is very important that all the positions and roles are filled by competent and motivated employees.

During the interview with Company A, our informants informed us that apply a control model with three lines of defense: The first and most important defense is about how employees are trained and educated (day to day risk management), here the CEO is responsible for the group's management being followed up within the framework adopted by the board of directors. The second line is about how managers, risk management and compliance management are helping and monitoring (overall risk reporting and follow up), and the third line consist of internal auditing, which is about how internal auditors monitor that the risk management processes are targeted, effective and function as intended. Ernst & Young are responsible for providing their services to Company A when it comes to internal audit.

Internal audit reports to the board of directors and their recommendations for improvements in each company's risk management are continuously reviewed.

4.2.7 Company Y - focus on monetary losses. Internal control system and security measures

As explained above, this part will solely focus on Company Y's control systems and security measures. When it comes to the way the company avoid any types of threats, our respondent stated that they have good routines on money, for example their employees cannot release a product before confirming in the bank that they have received their money. Moreover, they need to have good routines in the accounting department meaning that they have to have two people on every invoice. He further underlined that the company has internal auditing in the consolidation, in which they receive internal auditing reports. Based on those reports they set up routines that comply with requirements from the reports.

Regarding the security system, Company Y depends a lot on another company they cooperate with, who owns 50% of the company, so the sensitive business IT-systems are drifted by them. When it comes to other kind of systems Company Y is using, they stressed that they are using a very old system and that they are not keeping up with ICT development. Moreover, the company is waiting to expand their CRM (Customer relationship management) system, so the new things that should have been implemented are still being hampered by the old system. According to our Company Y informant, the best way to avoid any fraudulent activities in a business like theirs, is as he described:

"I think it is important with openness, that the departments are transparent, and that there is at least two people sitting on accounting and transactions, for example acceptance of invoices or other transactions."

Our respondent also emphasized that their motivation for having good controls is because they don't want to lose money, but keeping a good reputation of the company and taking care of the employees was also important. As he explained:

"There can be employees with gambling problems or alcoholic problems and if the temptation to take something is too big, then they will fall for it. So we have a responsibility to

not offer any temptations to the employees. But also reputation, fraud towards us would not be good marketing. So these are the motivations to have good controls."

4.2.8 Visual summary of internal control systems

In the table under we present a visual display of our internal control systems, key measures and other findings we discussed above.

Internal control systems	Important Security measures	Common measures	Company
COSO and COBIT	- Culture and attitude - Employees training - Passopp and Nanolearning programs - Monitoring - Technical systems	FinansCERT	Company A
ISO 20001 and 20002 BSIMM ISO 27000, 27002 and ISO 9001	- Culture and attitude - Employees training - Cloud-based equipment and services - Monitoring - Technical systems	HelseCERT	Company X
ISO 9001:2000 Hemit Norsk Helsenett	- Rely on suppliers - Authentication routines - Technical systems	HelseCERT	Company B
COSO	- Employees training - Good routines on money - Monitoring - Focus on accounting and transactions		Company Y

Table 6: types of internal control systems

4.3 External pressure from legal authorities

In our study we wanted to look closer into what drives the respective companies to work with, maintain and update their internal control systems to deal with cybercrime. In this subchapter we are going to focus on the external pressure from legal authorities through laws and regulations, containing requirements of measures that the various companies need to have in place to deal with cybercrime.

4.3.1 Laws and regulations as a driver for internal control

During our interviews when we talked about drivers for internal control, we wanted to shed light upon how important pressure from legal authorities was as a driver. A finding in our interviews was that our respondents that are concerned with information security are more strict regulated by laws than regular businesses like Company Y. This came clear when we asked a question about what drives the internal control, where both Company X and Company A had a lot to say about laws and regulations, but Company Y barely talked about it at all. However, Company A pointed out that this was not the main driver for them, of various reasons. They emphasized the importance of being internally motivated instead of externally, as they said that you shouldn't hide behind a regulatory framework, since then you won't get the internal motivation to work with internal control. They continued talking about the importance of protecting sensitive information, and even though laws and regulations are very strict, they are just minimum requirements for them. As they said, it would not be enough if they only implemented what is required by law, and therefore laws and regulations only becomes the cornerstones in their internal control system. When we asked if they thought they were more updated than those who are deciding the laws, then Respondent 3 had this to say:

"We are the ones that are out in the frontline of the war, so we get experiences of what is the actual challenges"

4.3.2 Impact from legal authorities

Company X gave us the impression that they were even more strict regulated by laws than Company A, as they elaborated more about this and how they worked towards external requirements. They pointed out that since they deliver a product to the health sector, which are very strict regulated, then they are responsible for this product living up to those requirements. Besides this, they made it clear that there are responsibilities for them regarding laws, when they work with other companies outside the health sector as well.

Every organization in the health sector associated with Norsk Helsenett, in our case Company X and Company B, are contractually bound to comply with a directive called Normen. Normen covers all aspects of information security as regulated by Norwegian law and ensures a secure interoperability for all companies that comply with its rules and regulation (ehelse, 2016, p3-10). According to ehelse.no, Normen is the first of its kind in Europe, no other overall standards on information security in the health sector are yet developed in any of EU/ EEZ countries.

Failing to meet the information security standards may lead to the exclusion of the contract-breaching entity. Our informants from Company X said that failing to meet law requirements could lead to sanctions, but they could not give any specifics about this, as that was up to the judges. However, they pointed out that the Computer Supervision can give fines, and that there will come a new directive for privacy in 2018 where huge fines can be given if requirements from laws are not met.

According to one of the respondents at Company X, they are most affected by the ISO standards which was presented in an earlier chapter. Even though they are not mandatory to follow, the respondent pointed out that these standards are necessary for them being in the market and are raising strict and clear guidelines of having good internal control. The guidelines are meant to work as an ensurement and safety factor for the customers, but besides affecting the product, they are also meant to deal with sensitive information that is stored locally about own employees. ISO 27000, 27001, 27002 and 9001 are the most relevant standards, where 27001 are raising requirements of having a quality management system and 27002 are going into detail about this.

A third law they are affected by is the Personal Data Law which is regulating when and how personal information can be used. The Computer Supervision is behind this law, and according to them you shall classify your IT-systems with respect to criticalness and sensitivity. There are law requirements that you shall have goals, strategies and politics for information security. Further, this law also contain guidelines that have to be followed, in which they said they was inspired by others:

"*There are also requirements for guidelines, and then we have looked at other businesses guidelines where they are open about this, and collected much inspiration to build up our own guidelines."*

While Company X mostly focused on how they work with laws regulating their business with customers, Company B told us they were most affected by laws regulating how information flows internally. They said that recent development in technology has opened up for new ways of exchanging information in effective ways, but they cannot fully take advantage of this because they have to think of security first. They didn't give any exact references to laws about this, but pointed out that technology provides different ways to share data internally, which is very strict regulated by law. They made it clear that since their security systems are outsourced, internal regulations are affecting them more than laws regulating how they have to protect themselves from the world around them.

Company A pointed out laws regarding reporting to the Finance Supervision as a very strict part of the law that is affecting them. They said that when an incident occurs they have to state in a report what was done to deal with the incident, and what kind of measures that was used. Every quarter the risk management department deliver a report to the board where they explain relevant threats, incidents and measures. We continued by asking if their work towards legal authorities was affected by laws and regulations from abroad, to which R2 answered:

"*yes, we are a part of an EØS-system, and Norway have committed to implement all laws and regulations that are coming from EU. Often when Norwegian authorities are translating these laws to Norwegian they are translating them more strict. The regime in Norway is more strict than abroad".*

R3 told us that laws regulating money laundering is another area that are strict regulated in Norway. Money laundering laws, which are given by the Ministry of Finance, are one of the areas they spend most resources and time on. He said that there will soon come a new money laundering directive from EU, which will be treated very strict in Norway. The Finance Supervision is the entity who are ensuring that Norwegian companies are following laws and regulations regarding money laundering.

Despite that Company A is more than happy to implement new laws and regulations from the authorities, some of them can lead to problems. The Finance Supervision in Norway are today demanding that banks should have their own cash depot so that they can provide their customers with cash in case there is a crisis, like for example if the infrastructure in Norway is shut down completely. Company A do not have the systems and facilities to meet that demand, so R3 told us that they try to convince the Finance Supervision that they have backup solutions for a potential crisis, but so far they have not come to an agreement.

Company Y is not very affected by laws and regulations regarding internal control since they are depending on company B when it comes to this. However, when we asked if they look abroad for inspiration to deal with cybercrime, they told us that they implement and adjust to those laws that are taken in use by the Norwegian government. At last, Company A claimed that the authorities in Norway have become better when it comes to making risk management modules which now are a form of best-practice solution. They collect the best from both abroad and Norwegian practices and adding it together to Norwegian relations.

4.3.3 Visual summary of impact from legal authorities

In the table under we present a visual display of how our respondents are affected by laws and regulations, as we discussed above.

Company	Impact from legal authorities
Company A	• The Financial Supervision • The Ministry of Finance • Sarbanes-Oxley Act
Company X	• Normen • ISO Standards • The Computer Supervision
Company B	• Normen • ISO Standards • The Computer Supervision

Company Y	•

Table 7:impact from legal authorities

4.4 Summary

Our findings stipulated that there are some types of fraud from the model by Newman and Clarke that are getting weaker and more outdated, while others are still popular today. Hacking and identity theft is fraud types that was considered as major IT fraud areas in 2003, and are still widely used today. Fraud types like telemarketing fraud, credit card fraud and investment fraud are major IT fraud areas from 2003 that play a smaller role in today's picture of threat. New and innovative types of fraud like CEO fraud and phishing have replaced the outdated fraud types. Furthermore, our findings showed that COSO, COBIT and ISO standards are the control systems that our representatives are using. According to our informants, the most important part of the internal control is to work towards the employees having sufficient knowledge and training about how to use systems applied to protect against cybercrime. Along with that, having the right organizational culture in place was also stressed as very important. At last, our findings demonstrate that companies operating in the health and finance sector is strict regulated by the authorities. This is to ensure that sensitive economic and patient information is being protected against cybercrime. The Ministry of Finance and the Finance Supervision is regulating the finance sector, while Normen and the Computer Supervision are having their eyes on the health sector.

5 ANALYSIS AND DISCUSSION

5.0 Introduction

To analyse the data collected through interview methods, this chapter will discuss the findings connected to three investigative questions. Which will be analyzed and discussed based on our opinion and knowledge. The objective of this analysis is to compare the theory behind fraud, internal control and institutional theory with the actual reality and practical processes firms employ. Our attention will be directed at where our findings are in line with the theory but also where they diverge from it. This might lead to the detection of some possible failure- or suggestion points, and potential solutions.

Based on information we have gathered from our interviews, we have seen that relationships exists between essential components of the subject cybercrime. These components are institutional pressures, change in fraud instances, development of internal control systems and growth in IT which we have tried to illustrate in figure 5 below. What we have seen, and will discuss later in this chapter, is that a more digitalized society is affecting the institutional forces which again is putting pressure on the development of internal control systems of companies. In addition to that, the digitization is causing a change in fraud instances as some fraud types becomes outdated, while other more innovative fraud types are developing. This is also having an impact on institutional pressures and development of internal control practices, as shown in the figure below:

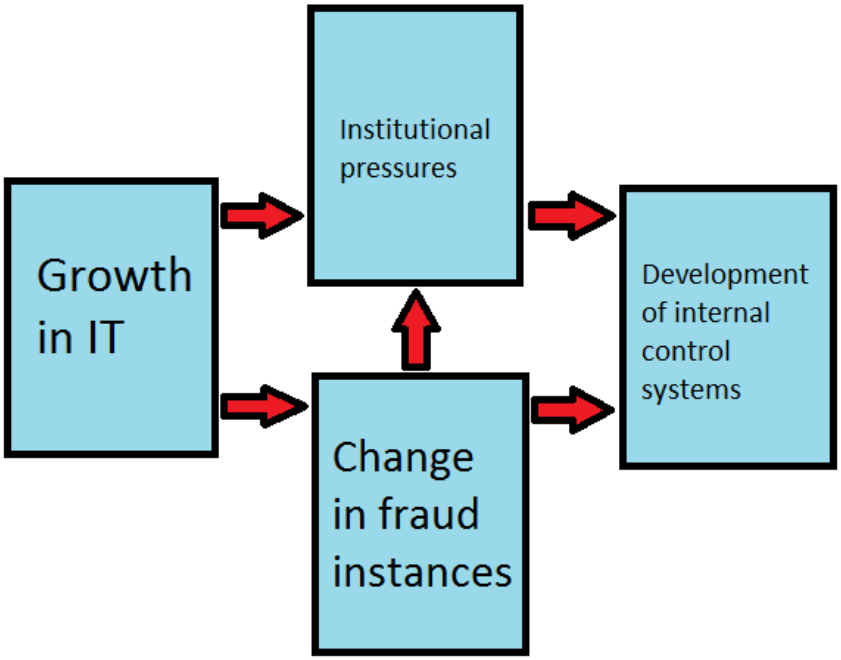


Figure 5, relationships between components of cybercrime

5.1.1 Outdated and weaker types of fraud

Our first research question is concerning the fraud area, and are trying to answer how fraud related to cybercrime have evolved. In the following part we will discuss and answer our first research question by explaining how IT related fraud have changed since Newman and Clarke made their model in 2003.

Credit card fraud and investment fraud is both types of fraud that is mainly a concern in the finance industry. In the model by Newman and Clarke both of them are described as major IT fraud areas, which means they was one of the most popular or critical types of fraud. Investment fraud is done by making someone do a bad investment by supplying them with false information. From our data collection we have seen a change in the picture of threat, that this type of fraud is going down. It was barely mentioned during the interviews with our informants, which is also the reason we didn't present it in chapter four. Only one of our respondents talked about investment fraud, and that was because we specifically asked about it. They confirmed that this kind of fraud was more popular several years back, but have been significantly decreased lately. The investment industry has been strict regulated through laws in recent years, which are killing the motivation for fraudsters to engage in this type of crime.

Credit card fraud on the other hand is still very popular today, and fraudsters are continuously finding new ways of doing this. What have changed regarding credit card fraud in recent years is that the criticalness of this type of fraud has been a lot smaller compared to other more dangerous type of fraud.. There are many reasons for this, on one side cybercrime as a whole has, as explained earlier, become more complex and a bigger problem today. On the other side, the activity of fraud related to credit cards has become predictable from year to year, and is now a calculated risk for banks. Along with this, credit card fraud is today easier to manage through better technology and solutions. Lost credit cards or copied information can now be handled by blocking the card or using geographical restrictions on the card. On the basis of what mentioned above, Company A told us that credit card fraud is just a minor concern for them. They can’t avoid it, so there is an anticipated cost related to this, but today there are other types of fraud that is far more dangerous.

Another type of crime that is classified as a major IT fraud area by Newman and Clarke is telemarketing fraud, which is fraudulent selling by using a telephone. Telemarketing fraud was not presented in the empirical chapter because it play a very small role in today’s picture

of cyber threats. Despite that the usage of cell phones has exploded since 2003, technology has also opened up other, more effective and attractive, ways of perpetrating fraud. This type of fraud is not eliminated, and will probably always exist, but it cannot be categorized as one of the major IT fraud areas today.

5.1.2 Still going strong

Identity theft, which is illegally use of another person's identity, was both presented as a major IT fraud area in the model from 2003, and described by our informant from BDO as one of the most common today. To our surprise, this type of fraud was not mentioned by any of our informants as an incident they had experienced. A reason for this is that ID-theft is not a main concern in the industry where our four informants operate. R8 from BDO was speaking for Norwegian companies as a whole, where this type of fraud is a bigger problem. Even though they didn't mention any incidents, Company A gave us the impression that they take this kind of fraud seriously as they pointed out that they were making their employees aware of the threat from identity theft through their Nanolearning sessions.

Due to the fact that cybercrime activity has increased since the model by Newman and Clarke was made, the necessity of money laundering has also increased. Money laundering is a type of crime most people think of as the act of white washing dirty physical money, but even though the money is stolen electronically, the money needs treated right in order to be usable. On the basis of that, money laundering will always exist as long as fraudsters are engaging in cybercrime. When the illegal money is obtained it has to be transferred fast within the financial system, to avoid getting caught. The techniques of doing money laundering is under continuous development, today, using offshore accounts, shell accounts and money mules are the most common techniques. This being said, there are crimes done over a computer with internet that concerns companies today even more.

5.1.3 Dominating today

According to our informants hacking is the clearly most frequently seen fraud today from those included in the model from Newman and Clarke. Three of our four informants said that they experience a lot of hacking activity per day. Further they emphasized that the reason hacktivism is still very popular is that the chance of getting caught is very low. On one side new technology can improve the efficiency of a company, but on the other side, fraudsters can

take advantage of it to stay hidden and attack from the dark. One of our respondents put it like this:

"*You can sit in Spain, make it look like you sit in Russia, attack in Norway and use equipment from Australia"*

The financial gain may be higher in other types of cybercrime, but when you attack from your own computer, in your own home, using the latest techniques to hide your traces, then the risk of getting caught is very low. In addition, hacking is something that can be done by almost everyone as long as you have a computer, internet and the knowledge necessary. Based on low detection risk and good availability, engaging in cybercrime through hacking is a very attractive and easy way for criminals to perform cybercrime. Hacking, along with CEO fraud and phishing, is the types of fraud that require the most resources and attention for companies today. They are also the main types that have replaced the outdated and weaker IT fraud areas.

The last major IT fraud area in the model from Newman and Clarke that we have not discussed yet is electronic funds transfer (EFT) fraud. EFT fraud is an electronic transfer of funds from one bank account to another, and is also the core idea behind CEO fraud, which was presented in chapter four. At the time when the model was made in 2003, the prime target of the ones performing EFT fraud was information systems and intelligence databases of banks. The main difference between now and then, is that today the prime target is leaders or CEOs, where the idea is to make an employee do a wrongful transfer of money through social manipulation. The old way of doing EFT fraud was, on the other hand, the fraudsters themselves who made the illegal transfer of money. This can still be seen today, but then often from the inside of an organization if employees are turning on their own company. Hacking into companies systems with a goal to steal money is rarely seen today, the trend is going towards making employees make mistakes themselves. One way of doing that is CEO fraud, another one is phishing.

Based on the information gathered from our respondents, the type of fraud that is seen most frequently among businesses today, is phishing. This type of fraud was not mentioned in the model by Newman and Clarke, which means it was not considered as a major IT fraud area in 2003. However, phishing can be seen as an subcategory of hacking, which was presented in

the model. Even though you classify it as hacking or not, it is treated as an own category today due to its high popularity. This crime is done almost solely through email, and with increased use of electronic communication, including use of email, the potential victims is also increasing for a crime like this. Emails with fraudulent content is usually sent to hundreds of thousands receivers, and knowing that you can reach out to a huge number of targets makes phishing more attractive than ever before.

Below we have presented a figure that are visualizing the change we have seen in the IT fraud area. The first square contains the major IT fraud areas presented by Newman and Clarke in 2003, while the next square are illustrating that one of the dominating fraud types today barely existed back then. In addition to that, it is important to note that CEO fraud is not presented at all in the first graph because it didn't exist back then. In the second graph, which is presenting the situation today, we have illustrated the division of fraud like we have discussed above. Only change is that credit card fraud is presented under the "still going strong" category because the activity of credit card fraud is still quite high, even though the banks are having good control over this type of fraud.

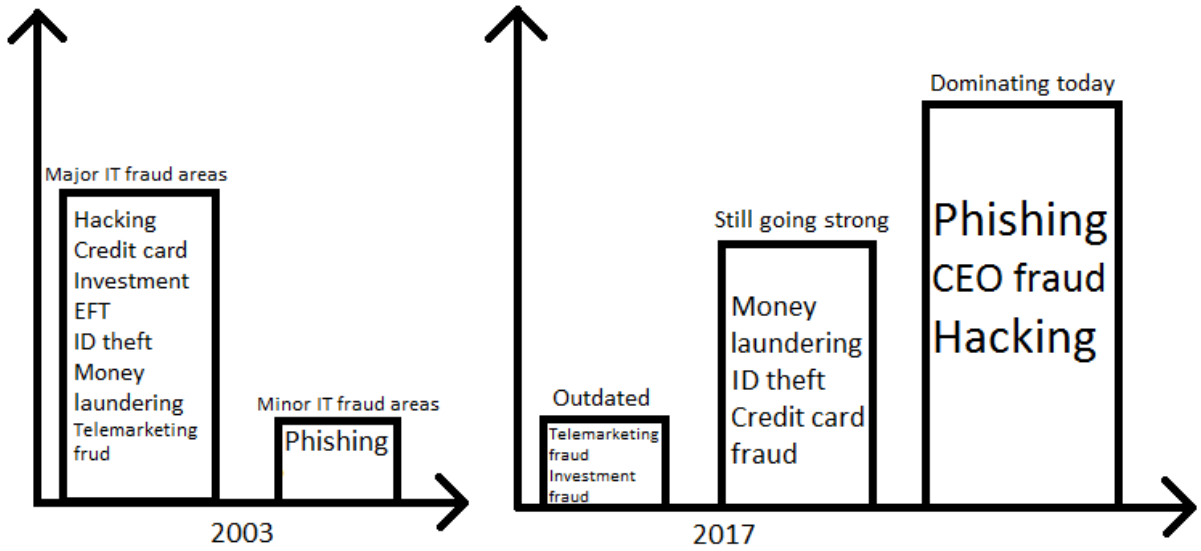


Figure 6, Change in major IT fraud areas

5.1.4 Change in the picture of threat

In our research we are contributing to the literature by explaining a change in the picture of threat, but also why the change is happening. Above we have mentioned both outdated types of fraud and new and innovative types of fraud, but what is causing this change? Both phishing and CEO fraud is mainly done by email, where phishing is a way of hacking into computer systems through other people's mistakes, and CEO fraud is a method of doing social manipulation. On the other side, both telemarketing fraud and investment fraud require the fraudster to interact directly with other people, and would normally deal with one person at a time. Based on this, we can see that the type of frauds that are popular today are fraudulent activities where the fraudster do not have to interact directly with other people, except by email. There can be different factors explaining this, where risk of getting caught and potential financial gain is taken into consideration. Fraudsters might consider direct contact with other people as an increased chance of being busted, while at the same time finding the latest technology attractive in terms of staying anonymous in their criminal acts. Regarding financial gain, fraudsters see a better potential in phishing and CEO fraud. As for phishing, there is a possibility of reaching out to an almost unlimited wide range of targets, while investment fraud and telemarketing fraud is normally focusing one target at a time. CEO fraud is also usually focusing one target at a time, but the potential financial gain from a successful CEO fraud is huge.

Another important factor of explaining the change in the picture of cyber threat is that the security measures are improving. Companies and organizations are learning from own incidents and experiences, meaning that measures are being implemented to stop the same attacks from happening again. This is forcing the fraudsters to thing new and innovative in order to be successful in their criminal acts. The outdated mentioned types of fraud are all actions that are rooted back to 2003, since they were considered major IT fraud areas back then. However, there is no surprise that companies today now have learned how they work, and how to protect themselves against them by working with necessary security measures that we will discuss in the next part of this chapter.

5.1.5 Internal versus external fraud

Bologna and Lindquist (1995) point out how fraud can be categorized as either internal or external. Internal fraud is described as managers cooking the books or employees turning on their own company, while external fraud is perpetrated by suppliers, vendors or contractors.

Based on our findings we see a change that today most of fraud connected to cybercrime is done externally. It is important to add independent civilians and governments as potential offenders, since today most of IT frauds are done by those two groups, and not by suppliers, contractors or vendors as the old theory point out.

5.1.6 Fraud triangle

The fraud triangle is a very famous model of theory when it comes to fraud, and it can of course be connected to IT based fraud. The question is, do all of its components stay relevant when it comes to cybercrime, and is there any difference between external and internal fraud? The idea of the model is that all of the three explanatory factors motivation, pressure and rationalization must exist for a person to act unethically.

Motivation or pressure tries to explain why the fraudster is pushed towards performing their acts, examples of this can be money problems like gambling. When connecting the fraud triangle to cybercrime, it is important to point out that the fraud triangle focuses more on fraud from the inside, while cybercrime is mainly done as an external fraud. This is leading to a change in the fraud triangle, since committing fraud against your own company require much more pressure or motivation from an individual, than to attack a foreign company from outside. Therefore, the motivation/ pressure component is decreased and play a smaller role in explaining the criminal acts of fraudsters engaging in cybercrime. This component is still not irrelevant, and our informants claimed that the main motivation behind cybercrime is financial greed, sabotage or influencing political events.

Rationalization, which is the second component of the fraud triangle, is the mindset of a person and how he justify the criminal acts. When connecting this component to cybercrime, it is important to have in mind that cybercrime is almost always done towards people that the fraudster have never seen or do not know. This is greatly decreasing the need to rationalize compared to when a fraudster committing fraud against his or her own company, where they have a relationship to their boss, coworkers and the company itself. A person might feel bad for the crime, but with no relationship to the victims the act itself is easier to rationalize. Based on this, when applying the fraud triangle to cybercrime in today's society the rationalization component has changed to be less important.

The last component of the fraud triangle is opportunity, which has to be in place for the criminal act to be feasible. Unlike the two previously mentioned components, opportunity is a component that is bigger and more important when connecting the fraud triangle to cybercrime. In the traditional model, the opportunity component is achieved by gaining position and trust in a company. On the other hand, if a person want to perform cybercrime, the only thing needed is a computer with network, and the skills to use it. Knowing that knowledge about how to perform cybercrime is available for everyone on websites like Google and YouTube, the opportunity is there for basically everyone. As shown in the figure below, the opportunity component is significantly increased when applying the fraud triangle to cybercrime in today's society. Another important factor of explaining why the opportunity component is increasing is that the society is becoming more digitalized, which means the potential victims are increasing.

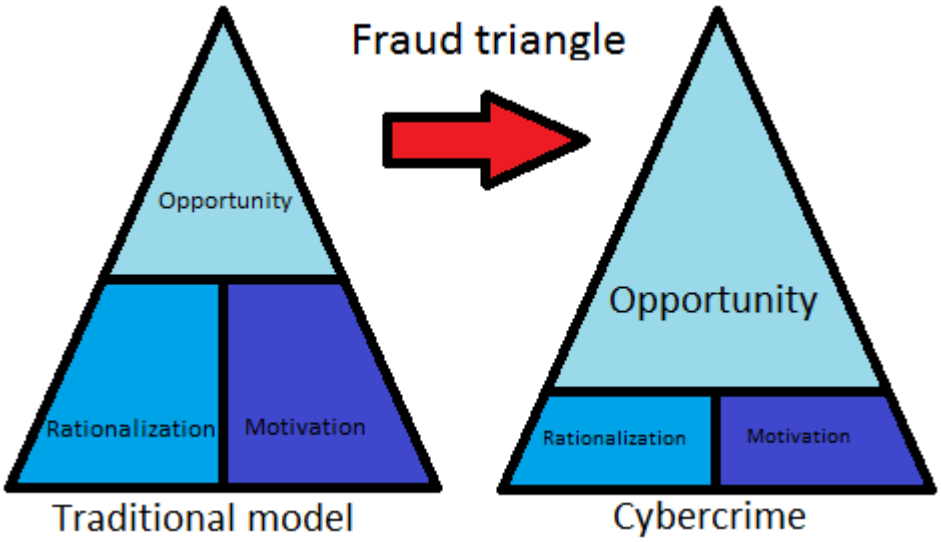


Figure 7, fraud triangle change

5.2 Development of internal control system

To tackle our problem statement, the second investigative question needs to be answered in order to find out how internal control practices companies use to prevent the IT based fraud have developed. Based on our findings it seems that companies that depend the most on IT (Company A, Company Y and Company B) are those that are most vulnerable to fraudulent activities. In order for those companies to prevent and detect those activities they rely heavily on IT systems and their development. Due to the corporate scandals that occurred in early

2000's in the United States, SOX law was created. It mainly stated that companies needed to reinforce their internal control and that it needed to be more based on IT. Our findings illustrated that Company A, although being a Norwegian company employ both COSO and COBIT, two international recognized internal control systems which are required by the SOX law. According to the observation made by Colbert and Bowen (1996), the COSO framework does not identify control objectives at a level of specificity sufficient to design detailed audit tests and does not address the complexity and risks inherent in IT, which is why COBIT a more IT friendly system was created. Whereas, Company X and Company B both employ ISO standards, which also rely heavily on IT. Company Y on the other hand uses only COSO as its internal control system. Based on the theory and our findings, we can see that internal control systems has developed to become a more IT based control system. The main reason for this is the SOX law, which not only affected American companies but international companies as well. As Bhattacharjya and Chang (2007) stated, IT systems became important over the years because it was recognized that information systems and their technology influence every aspect of an organization's activities which also create organizational value. Company Y is the only one based on our findings not affected by SOX, because COSO existed long before, it was formed in 1985. We can also see that based on the illustration of our findings, our company cases look abroad when it comes to implementing new control systems.

Some questions can arise as to why they do so, is it because Norway don't have the necessary equipment? Meaning that their control system is not as developed as others, or is it because of the reputation that those international control systems have? Our findings show that reputation of the systems our representatives are using are one of the key elements as to why our they have the best control systems in place. By having a system that has a good reputation and has been in place for a long time motivate our informants to administer those systems. Our results also show that none of our company cases uses ERM system, an expansion of COSO, the reason for it can be that the model don't have a good reputation when it comes to implementation. The theory suggest that even though more firms are embracing it, its implementation remains poorly integrated. Whereas our representatives focus is mainly on systems they trust and know.

5.2.1 Effectiveness of internal control system

In order for any firm to have a effective control system, various system functions have to be in place and be well managed by an organization. ISO standards (namely 20001, 20002, 27000, 27002 and 9001), COSO and COBIT are the main systems our representatives use to prevent and detect fraud. The theory shows that COSO identifies five main functions: control environment, risk assessment, control activities, information and communication and monitoring. Our findings demonstrate that all of those components are closely followed by Company A and Company Y. As presented in chapter four, two of our respondents also follow each step of the ISO standards closely. Furthermore, an effective internal control system consist of two important elements; the technical system, which are already mentioned, and the culture/ attitudes system.

5.2.2 Technical and culture system

The findings highlight that the technical system is not the most important part of internal control systems, but employee training is. As our informants from Company A and Company X depicted, a well managed security system should be based on 80 percent attitudes and 20 percent system. Because knowledge and attitude is the most important defense there is. Furthermore, they explained that companies can produce as many security systems as they want but if an employee is not up to date hackers and fraudsters are always going to be in front. All of this falls into the COSO elements, namely information and communication, monitoring and control activities components. Even though Company X and Company B don't use COSO, their control systems in a way mirror each other. Internal control systems has developed to be a more IT based system today. However, those systems can be quite complex to understand, therefore it is necessary to have the right resources in place, and educate employees in using those systems. Our findings show that the technical system is not enough when it comes to implementation success of internal control, one should focus more on the employees. Training allow our company cases to develop and promote their own culture. That is why Company A is using training programs such as "passopp" to update and inform their employees about the threats that are surrounding them.

Our findings also show, particularly Company A and Company X a concern when it comes to client security (risk management). Even though they have solid systems in place, they worry about the items their clients utilize to access their information such as iphones and ipads. Many fraudsters know that clients don't have the same amount of protection and knowledge

when it comes to security which make them easy targets. That is why our informants want to simulate employees training to clients training so that all parties involved can be ready. Those findings falls mainly into the risk assessment and monitoring components of COSO but also on IT governance, which according to Ko and Fink (2010) focus on IT risk management and the alignment of corporate system to purpose of businesses.

5.2.3 Organization structure and Information flow

Rezaee (2004) argues that corporate governance determines a power sharing relationship between corporation executives and investors by administering structure through which: the objectives are defined; policies and procedures are established to ensure achievement of these objectives; and activities, affairs, and performance are monitored. It also specifies the distribution of rights and responsibilities of different participants in a corporation. The findings demonstrate that when it comes to corporate governance, our representatives have a hierarchical and classical structure. For example, our respondents from Company X stipulated that they have been working on big audit for their security guidelines but in order to apply it they have to report everything to the company managers, they makes the final decision. Here we can see the structure and the hierarchy of the firm, there's a clear distribution of roles and each employee's have their own responsibility. Based on the findings we can posit that, our informants responsibilities are to build the security system of the organization while managers make the final decisions. Rezaee (2004) further stated that the functions of corporate governance should consist a managerial function, audit function, audit committees, board of directors and an oversight function. Our findings also show that, Company A and to an extent Company X, Y and B have those functions, we used the word extent to describe other firms because of the audit function. We can assume that all of our company cases have an external audit function in place, however when it comes to internal audit we are sure that Company A comprises of one due to the fact they have to follow the SOX law requirements. Which states that internal and external audit should be separate because a company cannot use the same audit company for both external audit services and internal audit consultancy. As a result Company A, comprise of an audit committee in their management system that is independent of the board and executive management. Our findings also show that having the proper structure in an organization help with the effectiveness of internal control.

The fourth component of the COSO framework, communication and information, state that in an organization, information should be identified, captured and communicated to all

stakeholders such as board of directors, management and employees in order to carry out their responsibilities effectively. Communication between employees and management in our findings seems to be well managed, our informants from Company A and Company X stipulated about their company's line of defense which are primarily based on the information flow between management and employees (how employees are trained, educated and monitored). Our findings also show that each company's structure is comprised of the board of directors making all the decisions and those decisions are in return communicated to the CEO who then make sure that those directives are followed properly in the company.

5.2.4 Common goal! let's work together

Cunningham (2004), argue that ICS start as internal processes with positive goals to help an organization meet its set of objectives, which is primarily provided by management. Although most theories concerning internal control systems are seen as individual systems for organizations, our findings show that three of our case companies (Company A, Company X and Company B) would rather have common system measures. Our representatives argued that it was best to make common system, share information with others in their respective industries because of the threats they are all under. Company A accentuated that they participate in FinansCERT and that all Norwegian banks are participating on it. Whereas Company X and Company B participates in HelseCERT. They highlighted that having a common system will help them fight and keep them updated towards cybercrime.

5.3 What kinds of institutional forces dominate in designing internal control practices?

Our last research question is trying to answer how the internal control systems of companies is affected by institutional forces. In this part we will analyse and compare institutional theory with the data we have collected to answer this research question. Breaking down institutional theory we have three types of isomorphism which are coercive, mimetic and normative. We will divide this subchapter in three parts where we analyse and discuss how companies respond to the three types of pressures mentioned above.

5.3.1 Company responses to coercive pressures

The first type of isomorphism that we are going to take a closer look at is the coercive pressures. Coercive isomorphism is external pressures that can be perceived as force, persuasion or invitation to change, which are derived from expectations in the society. A typical coercive pressure is governmental laws that are regulating the industry in which a

company operates. In part three in the empirical part we made a table at the end as a summary of how our respondents is affected by laws and regulations.

Based on our findings it is reasonable to state that the coercive pressures are stronger on our respondents who are concerned with information security. The importance of securing sensitive patient information and economic information is strictly regulated in Norway, which are causing coercive pressures. The main sources of coercive pressures in the finance industry is the Finance Supervision and the Ministry of Finance, while Normen and the Computer Supervision is the most important actors in the health sector. DiMaggio and Powell stated in their theory from 1983 that coercive pressures is also an invitation to change, which can be said about the ISO standards. These standards are voluntary to follow, but since widely used, they have become a coercive pressure through cultural expectations (public opinion), and the expectation of having a good security information system. R5 said in the interview that the ISO standards have become necessary for being in the market, since they are ensuring that the health systems delivered by Company X is safe, and their customers will only buy the systems that are safe. Moreover, seeking external legitimacy is also an important factor for our respondents, Meyer and Rowan (1977) stipulated that in institutional theory companies enhance their legitimacy by conforming to public opinion, and institutionalised rules and procedures.

5.3.2 Company responses to mimetic pressures

According to DiMaggio and Powell (1983) mimetic pressure is a result responding to uncertainty and making companies more similar. Organizations use the practices of more successful and legitimate companies so they can increase their legitimacy. Based on our findings there's a lot of uncertainty when it comes to IT and its development. Even though our case companies have solid control systems, the uncertainty comes mostly from external fraudsters. With the evolution of IT fraudsters will always find new ways to attack companies which make our representatives systems vulnerable and uncertain. Our findings demonstrate that in order to increase their legitimacy Company A and Company X model themselves on other organizations when it comes to fraud prevention. For example, both companies looked at how the Statoil and Telenor hacking was done so they could in return prevent the same thing happening to them. They also highlighted that they look everywhere for inspiration, whether it is online or abroad. The use of internal control systems such as ISO standards by Company X can be considered as an imitation because those standards are not required to

follow. Based on that some questions can come up as to why Company X chose those standards instead of systems such as COSO, COBIT or ERM. It can be because of the standards reputation (mimetic) or because those standards are a better fit for the services they offer.

DiMaggio and Powell (1983) stated that industry associations disseminate organizational practices and help companies imitate each other. Our findings show that three of the case companies (Company A, Company X and Company B) all participate in industry associations which are FinansCERT and HelseCERT. In those, companies in the same industry come together and share information about how to prevent, detect and combat fraudulent activities in their respective organization. Moreover, for the past years Company X has been implementing cloud-based equipment and services, which is online shared services that can be used by organizations who have access to. Company X are also member of a Norwegian information security forum where they can participate in discussion regarding information security.

5.3.3 Company responses to normative pressures

Boon et al (2009) posit that normative pressure are the different norms and values that professionals develop through formal education and professional networks, which increase the similarity of the skills and knowledge of the total workforce in an organizational environment. DiMaggio and Powell (1983, p153) stated that education and training institutions are considered to be important centers for the development of organizational norms. The findings demonstrate that our case companies security systems are mainly based on education and the training of employees. For example, Company A, Company X and Company Y denote that educating and training employees is the best systems there is because without it their control systems cannot work properly. When it comes to education and training institutions, our findings show that Norway don't have good enough institutions that deals with IT development and cybercrime. However, one of our respondents pointed out University of Gjøvik as one of the better institutions.

Moreover, those affected by cybercrime such as clients and customers also play a part in how organizations make their decisions. Social normative pressure which refers to pressure coming from society as a whole or public opinion play a role in how our case companies work. For example, our findings show that reputational risk is a big factor for our

representatives, everything they do is based on how external stakeholders view their organizations. That is why they have systems in place such as in house training of employees that will lead to professionalization to avoid any bad publicity towards their respective companies.

According to Pettigrew (1979) corporate culture refers to the shared beliefs, values, ethics and atmosphere of a company. Pettigrew added that corporate culture belongs to socialisation which is a process in which decision making follows the norms and values of the company. The findings demonstrate that our case companies have a good and well managed corporate governance. Meaning that our case companies embrace a strong corporate culture which is reflected in their management styles, communication methods and a way of reporting and working hierarchies.

5.3.4 Strength of institutional forces

Type	Main sources and mechanisms	Strength
Coercive	• The Finance Department • The Finance Supervision • Normen • ISO Standards • Computer Supervision	Strong Strong Strong Moderate Strong
Mimetic	• Industry vulnerability and uncertainty • Industry association • Imitation of others	Strong Strong Moderate
Normative	• National education and training systems • In house education and training systems • Public opinion • Corporate culture	Weak Strong Strong Strong

Table 8: strengths of institutional forces

The table above shows the different sources and mechanisms of institutional forces. The strength of these forces varies between strong, moderate and weak. The coercive pressures are derived from organizations that our representatives are dependent upon, and by expectations

from society as well. Most of the pressures comes from legal authorities and are forcing companies by contract law. Since these pressures are mandatory to comply with, there are consequences (e.g. fines) of not following them. On the basis of this, they are all categorized as strong. The one coercive pressure that is standing out as moderate is the ISO standards, which are voluntary to follow, and are therefore not categorized as strong. However, it cannot be categorized as weak because expectations from society are causing a pressure to develop and have safe information security systems. Developing safe security systems can be done by guidelines from other standards than ISO, but our respondents in the health sector is using ISO standards. Therefore, when decided to use ISO it becomes a coercive pressure to make sure that those clear and strict requirements are followed.

When it comes to mimetic pressure, our findings show that there are three main sources and mechanisms; which are industry vulnerability and uncertainty, industry association and imitation of others. Industry vulnerability and uncertainty is strong because many organizations including our case companies don't really know what to expect regarding IT development and cybercrime, they don't know when or how a fraudster is going to strike which put them in a position of being vulnerable and uncertain. They'll always be on their toes and wonder what is going to happen next. The strength of industry association is strong because our findings demonstrate that for our informants it is best to work together than apart to vanquish the threats they are all under. Consequently, they spend lots of resources and time on common systems such as FinansCERT and HelseCERT to share information about different ways they can prevent any fraudulent activities. Imitation of others is rated moderate because even though our representatives look elsewhere for inspiration, they look for ways to avoid cybercrime, by doing so they sometimes model themselves into companies that have been affected by it to prevent any activities of fraud happening to them.

Regarding normative pressure, our findings highlighted four main sources and mechanisms. National education and training systems is weak because of the lack of IT institutions in Norway. In house education and training systems is strong due to the fact that our case companies rely mostly on the employees concerning their control systems. They spend lots of resources and time on it. Public opinion is strong because our findings show that reputational risks are our representatives biggest risk. At last, corporate culture is rated strong because our informants underlined time after time how important it is to work towards having the right culture in place and avoiding a culture of fear.

5.3.5 The Norm and Action system

Included in the institutional theory, which was presented in the theory part, we have the action and the norm system. In order to explain how our case company's internal control systems are designed we could look at the norm and action system. These two systems are a good tool to break up and isolate the many elements of forming an internal control system. Bergevärn et al (1995) states that the norm system are dealing with how things are supposed to be, while the action system represent how things really are, this means how accounting is in practice and how it is used respectively. This theory is trying to explain whether a company is learning from experiences by the norm or the action system.

The norm system are concerning the environment around a company, which means rules and requirements that have to be complied with in order to receive support from the environment.
The environment around a company is in this case institutional forces like Normen, the Finance Supervision, the Ministry of Finance and the Computer Supervision. These institutional forces are all having their own contribution to designing the internal control system of a company, and was presented in the empirical part. Learning from experiences by legal authorities like those mentioned, is similar to coercive isomorphism since those experiences normally end up in regulations that are mandatory to comply with.
The action system on the other hand is dealing with the internal environment in an organization, like culture and traditions. Learning from the action system is internally motivated learning, and the ability to see what is necessary beyond what is required by law. From our findings we know that our case companies emphasize the importance of working with organizational culture and attitudes of employees towards the new picture of threat regarding cybercrime.

When comparing those two systems and connecting them to our findings it is important to distinguish between our case companies, whom is concerned with information security and who is not. Based on our findings we can see that for the companies who are concerned with information security it is most important to learn from the action system. While for more regular businesses learning from the norm system is the biggest contributor to design the internal control system. The reason for that is mainly because the experiences from the norm system are outdated compared to the experiences from the action system of a company concerned with information security. As one of our respondent stated "*we are in the frontline*

of the war", and being a soldier in the war is giving the most updated experiences. They are the ones that are most exposed, and thereby needs to have the best defense in place. Therefore, it is more important for them to learn from the action system. Learning from the norm system is still important, since doing not so might be to break the law, which have unwanted consequences.

Moreover, our findings show that companies that doesn't have sensitive information to protect is less concerned about the cyber threat and to have a good defense in place. This makes the norm system more important for them and to take into consideration only what the different ministries are forcing them to. The potential damages of an attack is less than for the companies who are exposed to a leak of sensitive information. This makes the protection of themselves towards fraudsters less prioritized, and therefore also the internal learning and learning from the action system less prioritized. On the basis of this it is reasonable to state that the coercive learning is most important for these kind of companies, while mimetic learning is more important for the companies concerned with information security.

5.4 Summary

In this chapter we have analyzed the data we had collected through our interviews. Our findings have been used to answer our three investigative questions through discussion and analysis, based on our opinion and knowledge. Theory about fraud, internal control and institutional theory, which is presented in chapter two, has been compared with the actual reality and practical processes that our respondents employ. We have elaborated on where the reality is similar to theory, but also discussed the areas where our findings diverge from it.

6 CONCLUSION

As discussed in the abstract, the purpose of this thesis is to investigate how Norwegian companies respond to the growing threat of cybercrime. In this final chapter we will present the main findings of our research by linking it to (Røvik, 2011) virus theory. Our problem statement was as follow:

"How have internal control systems developed to respond to growth in IT, and a need to prevent and detect fraud?"

While investigating this subject we have seen that many links can be drawn between the subjects cybercrime and virus. In his research, Røvik (2011) states that a virus spreads by infecting the body, evading its immune system response and being able to replicate. The situation for fraud is much the same way, as they have to beat the internal control system and intrude an organization in order to be successful.

During our research we have seen that IT based fraud instances have changed over time. Improvement of the immune systems of companies have almost led to extinction of some fraud types like investment fraud and telemarketing fraud. Moreover, new and innovative fraud types like phishing and CEO fraud have taken their place. Phishing is a scam that is targeting a huge number of victims, and is similar to the traditional flu virus. Most firms are able to block it, but it can do great harm if it attack a weak immune system. CEO fraud on the other hand is more like cancer in its description. A dangerous and sophisticated attack with a designated target that require careful planning.

Applying the right vaccines is necessary to update and monitor the immune system in order to stay protected against cybercrime. The most common immune system today is the COSO framework, but other systems such as COBIT and ISO standards are also widely used. Furthermore, vaccines can be divided into internal and external vaccines, in which internal vaccines is how managers are vaccinating their own company. Our respondents emphasized that due to the development of IT and cybercrime, the internal control practices today are mostly focused on the attitudes of employees and corporate culture. While working with the security measures of the immune system was considered more important in the past, today it is more important that the employees are provided with sufficient knowledge about how to use the immune system and how the different kinds of viruses work.

On the other hand, external vaccination of companies is the institutional forces that are having an impact on the design of internal control practices of companies. Institutions like the Ministry of Finance and the Finance Supervision is making sure that companies operating in the finance sector vaccinated are immune to viruses. Regarding the health sector, Normen and the Computer Supervision is playing an important role of protecting and vaccinating companies. Further, our respondents affected by the authorities mentioned above, emphasized that they do more than the institutional forces require of them, based on internal motivation to keep themselves immune.

Based on what we found on our empirical findings and discussed in our analysis, we can conclude with the following points:

1. Fraud types that require direct contact with the victims is going down: telemarketing fraud, investment fraud.
2. Fraud types that does not involve direct contact (except email) is going up: hacking, phishing, CEO fraud.
3. Internal control systems have developed to become more IT based.
4. Internal control systems is based on technical systems on one side, and corporate culture and training employees on the other, in which the last mentioned is most important.
5. Common control systems are better than individual control systems, it is best to work together than apart.
6. Companies storing sensitive information is more strict regulated by authorities.
7. Doing more than required by laws and regulations is necessary to stay satisfactory protected against cybercrime.

6.1 Limitations of the study

One of the main limitations of this research is the sensitive nature of our problem statement. Many organizations shy away when they hear internal control and IT fraud. When we first started to collect data, we wanted to see a contrast between big firms and small firms regarding internal control and frauds attempt. However, many firms especially small ones were not receptive to the idea of speaking about their security systems or whether those systems were good enough to sustain any types of fraudulent activities. Hence the reason our

research study focuses only four big firms which also the reason for the size of the sample interviews. Since our theme is about internal control and IT fraud, the only employees in each organization we interviewed that could really answer our questions were those in positions of IT governance. The contents of our findings can also be seen as a limitation, since we don't know whether or not our informants disclosed all the information truthfully.

Another limitation is the timeframe we had available to carry out our research, our topic is wide and quite relevant in today's society, however we were constrained to move on to meet a submission deadline even when we think that there is more we can do. Moreover, our research include only qualitative research methods, and we focus only on our different cases (viewpoints of each cases) which make us not being able to generalize our results beyond our case companies.

6.2 Suggestion for further research

Since our study was conducted with only four cases, we would suggest in the future to perform a wide scale research which include a big sample. By using quantitative research method, future researchers can work with a large sample of firms that will give them a chance to experiment their ideas on big amounts of organizations and see how their ideas/findings can be generalized. Another thing that would be beneficial for further studies would be to compare big firms with small/medium firms, and Norwegian companies with international companies as well. Furthermore, future research studies can also only focus on secondary data to collect their information as this can help to bring out a clear picture of the findings and remove the bias of the respondent responses when using primary data.

6.3 Implications for practitioners

We hope that this investigation can help others by enlightening the subject of cybercrime in today's society. First of all, we hope that our research can help companies to become more aware about the different kinds of fraud and how the critical the situation is. Three of our respondents are companies that are concerned with protecting sensitive information, which mean they take this subject very seriously. These three companies, Company A, Company X and Company B has proven to be very good examples of how to respond to this new picture of threat through cybercrime. We know that most companies in Norway do not have information security as their main concern, but rather developing of products and making profit in a market that are becoming more and more competitive on a general basis. Even

though the margins in the market are smaller, and the need to focus on profit have never been more important, it is still critical to pay attention to the emerging threat from cybercrime. Thereby we hope that many companies can read our work and learn from the companies we have cooperated with. During our research we have seen many examples of politicians, smaller and medium firms getting hit by hacking and phishing attempts from abroad. If the virus is strong enough and the immunity system weak enough, the virus is able to kill the body.

In this paper we have presented different kinds of fraud and several measures as a defense to those. Our intention is that practitioners can learn from this, what types of fraud that are dominating and dangerous today, and how they are performed. By looking at the frauds that are popular and outdated today it is easier to aim focus at the necessary areas and minimize the wastage of resources. People who don't speak Norwegian can also read it, because we chose to write our paper in English. Moreover, we hope that our research can be relevant and interesting for organizations that are not operating in Norway as well.

6.4 Contribution of the research

The research has shown us that with IT growth, internal control system has developed to become a more IT based system, which are based on technical systems, corporate culture and employees training/education. We were surprised to find that work towards organization culture and attitudes of employees actually are more important than the technical security barriers themselves. IT growth has also brought a change in fraud instances and a development in institutional pressures. Over the years we have seen how fraud instances have changed, in which we compared with Newman and Clarke (2003) major IT fraud areas. Some of the types of fraud that were dominating then (telemarketing and investment fraud) are not the same types that are dominating today (phishing and CEO fraud). Moreover, growth in IT has brought endless of opportunities for fraudsters. Additionally, since organizations are battling the same war, it is best for companies in the same industry to work together than apart because by helping each other, one could have many advantages on fraudsters.

REFERENCES

- Aisha Abdallah, Mohd Aizaini Maroof, Anazida Zainal (2016) "Fraud detection system: A Survey"

- Arena, Arnaboldi, Azzone (2010): "The organizational dynamics of Enterprise Risk Management", Accounting, Organizations and Society 35, 659–675.

- Association of Certified Fraud Examiner 2014 (ACFE), "Report to the nations on occupational fraud and abuse".

- Association of Certified Fraud Examiner 2016 (ACFE), "Report to the nations on occupational fraud and abuse".

- Belfo and Trigo (2013). "Accounting Information Systems: Tradition and Future Directions", Procedia Technology 9, 536 – 546 .

- Bharathy & McShane (2014) "Applying a Systems Model to Enterprise Risk Management", Engineering Management Journal, 26:4, 38-46.

- Bergevärn, Mellemvik, Olson,1995 "Institutionalization of municipal accounting: a comparative study between Sweden and Norway". Scandinavian Journal of Management,11 (11), 25-41

- Bogdan, R., & Biklen, S. K. (2007). Qualitative research for education: An introduction to theory and methods. Boston, MA. Pearson Allyn & Bacon.

- Boon, C, Paauwe, J, Boselie, P & Den Hartog, DN 2009, "Institutional Pressures and HRM: Developing Institutional Fit", Personnel Review, 38(5). 492-508.

- Brewerton, P, Millward, L. (2001) Organizational Research Methods: A Guide for Students and Researchers. London, GBR: Sage Publications Ltd

- Chartered Global Management Accountant (CGMA) 2011, "CGMA report: Fraud risk

management - A guide to good practice".

- Clarke, R. V. (1999): "Hot Products". Understanding, Anticipating and Reducing the Demand for Stolen Goods", Police Research Series Paper 98 London: Home Office
- COSO 2004. "Enterprise Risk Management – Integrated Framework". Executive Summary.

- Christoffersen, Tufte, Johannessen (2010) Introduksjon til samfunnsvitenskapelig metode. Akademia

- Dalen, M. (2004). Intervju som forskningsmetode – en kvalitativ tilnærming. Oslo: Universitetsforlaget

- Dalland (2007) Metode og oppgaveskriving for studenter. 4th edition, Gyldendal akademisk

- DiMaggio, P.J. & Powell, W.W. (1983). "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields". American Sociological Review, 48(2): 147-160.

- DiMaggio, P.J. & Powell, W.W. (1991). "The New Institutionalism in Organizational Analysis", Chicago: University of Chicago Press.

- Donald & Pamela 2014, Business research methods, 12th edition, McGraw-Hill Irwin, United States.

- Easterby-Smith, Thorpe, R., Jackson, P.R. (2004) Management research. SAGE Publications Ltd.

- Economist, "Ransomware attacks were on the rise, even before the latest episode" (2017)

- Evans, P. & Wurster, T.S. (1999)," Getting real about virtual commerce", Harvard Business Review, November-December 1999, 84-94.

- Gripsrud, Olsson og Ragnhild Silkoset. 2010. Metode og Dataanalyse. Kristiansand, Høyskoleforlaget AS.

- Hayne & Free (2014) "Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management" Accounting, Organizations and Society 39, 309–330.

- Heroux and Fortin, (2014), "Exploring IT Dependence and IT Governance" Information Systems Management, 31(2), 143-166

- Hoffman, A. J. (1999). "Institutional Evolution Change: Environmentalism and the U.S.Chemical Industry". Academy of Management Journal. 42(4). 351-371.

- IIA (2009). "Internal Audit Capability Model (IA-CM)", Altamonte Springs: The Institute of Internal Auditors, Research Foundation.

- IIA, (2012). "International standards for the professional practice of internal auditing". Altamonte Springs: The Institute of Internal Auditors, Research Foundation.

- ITIF (2013), "just the facts: the economic benefits of information and communications technology" Atkinson and Stewart.

- Jans, Lybaert,Vanhoof (2009) "A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR² Framework" The International Journal of Digital Accounting Research, 9, 1-29

- Johannessen, A., Christoffersen, L. & Tufte, P. A. (2011). Forskningsmetode for økonomisk-administrative fag. Oslo, Abstrakt forlag.

- Kareem, Owomoyela, Oyebamiji. (2014), "Electronic Commerce and Business Performance: An Empirical Investigation of Business Organizations in Nigeria" International Journal of Academic Research in Business and Social Sciences, 4(8), 215-223

- Lin, Guan, Fang (2010), "Critical Factors Affecting the Evaluation of Information Control Systems with the COBIT Framework", Emerging Markets Finance and Trade, 46(1), 42-55

- Lokanan (2015) "Challenges to the fraud triangle: Questions on its usefulness" Accounting Forum

- Lorences and Avila (2013), " The evaluation and improvement of IT Governance", Journal of Information Systems and Technology Management , 10(2), 219-234

- Mark Saunders & Philip Lewis 2009, Research methods for business students, 5th edition, Pearson Education, UK.

- Mehmetoglu, M. (2004). Kvalitativ metode for merkantile fag. Bergen: Fagbokforl.

- Meyer, JW & Rowan, B 1977, "Institutionalized Organizations: Formal Structure as Myth and Ceremony", American Journal of Sociology, 83(2). 340-363.

- Mignerat, M & Rivard, S 2009, "Positioning the institutional perspective in information systems research", Journal of Information Technology, 24(4). 369–91.

- Namrata Sandhu (2016). "Behavioral Red Flags of Fraud-A Qualitative Assessment"

- Newman, Graeme R. and Clarke, R.V.G (2003): "Superhighway Robbery; Preventing E-Commerce Crime" Willan Publishing

- Pettigrew, A, M (1979) on studying organizational cultures. Administrative science quarterly 24(4): 570-580

- Rezaee, (2004), " Corporate Governance role in financial reporting" Research in Accounting Regulation, 17, 107–149

- Rubino and Vitola (2014), "Corporate governance and the information system: how a framework for IT governance supports ERM", 14(3), 320-338

- Samuel and Wakogi (2014), " Assessing the role of internal control system components in Kenyan public universities: a case study of Jomo Kenyatta University of agriculture and technology" International Journal of Accounting and Financial Management Research, 4(2), 17-28

- Saunders, Lewis and Thornhill (2009) research method for business students 5th edition. Pearson education.

- Scott, W.R. (1995, 2001). "Institutions and Organizations". Thousand Oaks, CA: Sage Publications

- Scott, W.R (2008). "Approaching adulthood: the maturing of institutional theory", Springer science. 427 - 442.

- Sieber, Ulrich (2006): "The International Handbook on Computer Crime: Computer Related Economic Crime and the Infringements of Privacy", Wiley 276 Pages

- Silviu, (2014). "Analysis of internal audit practices on FTSE 100", Procedia Economics and Finance 15, 1265 – 1272 .

- Shi, Shambare, Jian 2008 "The adoption of internet banking: An institutional theory perspective" Journal of Financial Services Marketing, 12, 272 – 286

- Teo, HH, Wei, KK & Benbasat, I 2003, "Predicting intention to adopt interorganizational linkages: an institutional perspective", MIS Quarterly, 27 (1). 19–49

- Teo, TSH & Pok, SH 2003, "Adoption of WAP-enabled mobile phones among internet users", Omega, 31 (6). 483–98.
- Tuttle, Vandervelde (2007), " An empirical examination of COBIT as an internal control framework for information technology" International Journal of Accounting Information Systems 8 240–263
- Yin, R. K. (2009). Case study research: Design and methods, 4th. Thousand Oaks.

Appendix

Appendix 1: Interview guides

- **Interview guide 1 to auditor**

1. Hva går deres jobb ut på?

Er du ofte borti svindel gjennom jobben deres?

Hvilken type svindel er mest vanlig?

Hvilke eksempler av datakriminalitet har dere erfaring fra?

Hvilken type svindel er den mest kritiske/ skadelige (økonomisk vs omdømme?) ? Både innenfor datakriminalitet, men også datakriminalitet vs. andre kategorier

Hvilke eksempler av datakriminalitet mener dere er viktigst for norske bedrifter å beskytte seg mot?

2. Har du noe erfaring med svindel som kommer fra innsiden av bedrifter?

Hvilken type svindel?

Relatert til datakriminalitet?

Er man mer utsatt for dette i dag, pga utviklingen innen IT?

3. Hvilke næringer mener du er mest utsatt for datakriminalitet, eller er mest sårbare for datakriminalitet?

Stor/ liten?

Privat/ offentlig?

4. Hvilke næringer mener du er mest moden/ umoden for dette nye trusselbildet vi er blitt vitne til?

5. Hva mener du er det beste virkemiddelet for å beskytte seg mot datakriminalitet?

Hvorfor?

6. Kan du si noe om utviklingen av datakriminalitet?

7. Hvordan opplever du at bruken av internkontroll rettet mot cybercrime har utviklet seg de siste årene?

Nye typer nødvendige kontroller?

Er noen kontroller blitt ubrukelige?

8. Hva mener du er grunnen til at norske bedrifter oppdaterer og vedlikeholder deres internkontroll på dette området?

Intern?

Extern?

9. Hvordan tror du utviklingen fremover kommer til å bli?

Nye typer svindel? - Hvordan forberede seg best mulig på dette

Påstander

- En gjennomsnittlig norsk bedrift er umoden for det nye trusselbildet vi ser fra datakriminalitet
- Det er ekstra viktig for Bank, Politi og helsesektoren å ha et godt og fungerende cyberforsvar på grunn av sensitive personopplysninger
- Små eller middels store bedrifter er like utsatt, om ikke mer utsatt, for datakriminalitet sammenlignet med store bedrifter
- Norske bedrifter kommer til å måtte bruke mer ressurser på cyberforsvar eller internkontroll rettet mot datakriminalitet i fremtiden

Interview guide 2 to firms

FRAUD (svindel/ misligheter)

1.0 Har dere opplevd noen forsøk på svindel mot dere?

Kontrollspørsmål

1.1 Hvordan var det gjennomført?

1.2 Hvordan ble trusselen unngått/ tilintetgjort?

1.3 Hvilken kategori har de(n) vært relatert til?

1.4 Hvordan ble situasjonen behandlet?

1.5 Har noen av forsøkene faktisk blitt gjennomført til slutt? -omfang? skade (omdømme, finansielt)?

1.6 Hvis fraud: Føler dere at situasjonen er bedre ivaretatt i dag? (Lært av det som skjedde)

1.7 Har dere erfaringer med forsøk på svindel fra innsiden (egne ansatte)? - sensitivt

1.8 Utfordringer i forhold til at utvikling av ny teknologi åpner for nye typer svindel?

INTERNKONTROLL

2.0 Hvordan arbeider dere med internkontroll (styresystemer)? (COSO, COBIT, ERM)

Kontrollspørsmål

2.1 Hvilken modenhet opplever dere at dere har i forhold til datakriminalitet? Nåtid + fremtid

2.2 Har dere dratt fordel av de siste års utvikling innenfor IT, som for eksempel digitaliseringer av oppgaver eller automatiseringer av prosesser?

2.3 Føler dere dere truet av datakriminalitet, eller at dere er sårbare for datakriminalitet? (bank avhengig av teknologi kan føre til økt trussel?)

2.4 Hva mener du er det beste virkemiddelet for å forhindre svindel i virksomheten?

2.5 Hvordan er de ansatte påvirket av deres internkontroll?

2.6 Blir endringer i deres internkontroll møtt med positivitet eller negativitet?

2.7 Etter din mening, har veksten innen IT påvirket jobben din på en positiv eller negativ måte? Hvordan?

DRIVERE FOR INTERNKONTROLL

3.0 Hva er drivkraften eller motivasjonen for dere til å jobbe med, oppdatere og vedlikeholde deres internkontrollsystem?

Kontrollspørsmål

3.1 Har det blitt utviklet noen nye reguleringer, lover eller andre krav for internkontroll de siste årene?

3.2 Er dette en konsekvens av utvikling innen IT?

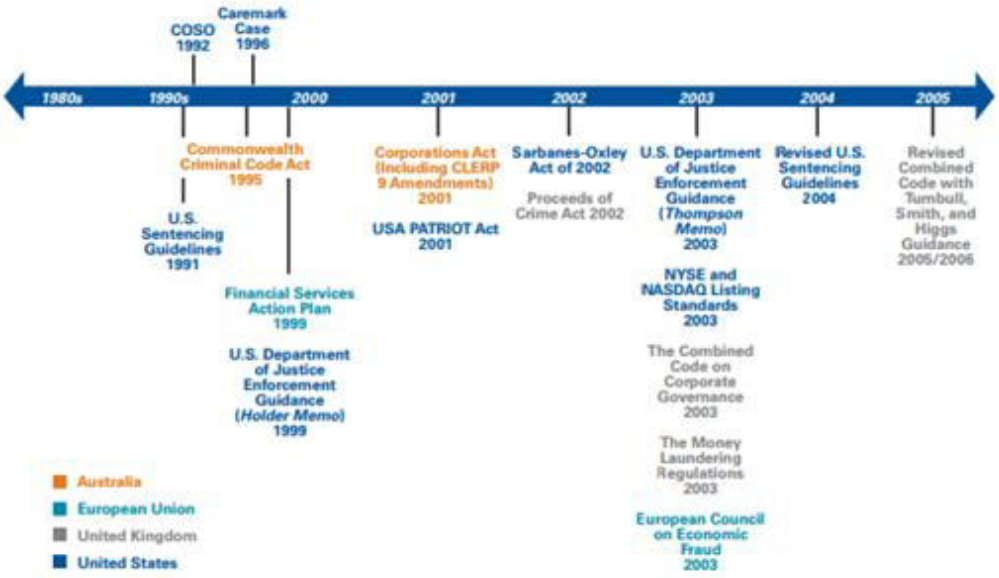
3.3 Er deres internkontroll påvirket av utenlandske lover og regler, eller banker?

3.4 Ble dere påvirket av Sarbanes Oxley law (SOX) da den ble innført i USA?

Andre spørsmål

- What are the 3 most effective internal controls your company have? and why?
- With internal control in place do you feel that the resources of the company are being used properly, so that there is a minimum wastage of resources?
- Do you feel that there are control systems in your company that are missing?
- What kind of procedures would you say your internal control system includes?
- In what ways do you think the growth of IT has affected the staffing needs of audit in your company/department?
- What is your assessment of the current and future directions of IT and internal control in your department?

Appendix 2: Timeline of important global regulations and events



Appendix 3: The Wannacry attack

The "WannaCry" attack spread to 150 countries

Appendix 4: Receipt from Norsk senter for forskningsdata (NSD)

Anatoli Bourmistrov
Økonomisk analyse og regnskap Nord Universitet
Postboks 1490
8026 BODØ

Vår dato: 07.04.2017 Vår ref: 53866 / 3 / BGH Deres dato: Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 27.03.2017. Meldingen gjelder prosjektet:

53866	*Impact on Norwegian firm's internal control system from a continuously increasing threat from cybercrime*
Behandlingsansvarlig	*Nord universitet, ved institusjonens øverste leder*
Daglig ansvarlig	*Anatoli Bourmistrov*
Student	*Runar Horn*

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, ombudets kommentarer samt personopplysningsloven og helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvernombud/meld_prosjekt/meld_endringer.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, http://pvo.nsd.no/prosjekt.

Personvernombudet vil ved prosjektets avslutning, 22.05.2017, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Kjersti Haugstvedt

Belinda Gloppen Helle

Kontaktperson: Belinda Gloppen Helle tlf: 55 58 28 74

Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning.

NSD – Norsk senter for forskningsdata AS Harald Hårfagres gate 29 Tel: +47-55 58 21 17 nsd@nsd.no Org.nr. 985 321 884
NSD – Norwegian Centre for Research Data NO-5007 Bergen, NORWAY Faks: +47-55 58 96 50 www.nsd.no

Personvernombudet for forskning

Prosjektvurdering - Kommentar

Prosjektnr: 53866

Utvalget informeres skriftlig og muntlig om prosjektet og samtykker til deltakelse. Informasjonsskriv og samtykkeerklæring er noe mangelfullt utformet. Vi ber derfor om at følgende endres/tilføyes:
- At deltagelse er frivillig og at en kan trekke seg når som helst uten begrunnelse
- At datamaterialet oppbevares konfidensielt og hvem som vil ha tilgang
- Hvorvidt enkeltpersoner kan kjennes igjen i publikasjonen
- Dato for forventet prosjektslutt (22.05.2017) og at innen denne datoen skal datamaterialet anonymiseres
- Kontaktinformasjon til veileder og studentene.

Personvernombudet legger til grunn at forsker etterfølger Nord universitet sine interne rutiner for datasikkerhet. Dersom personopplysninger skal sendes elektronisk eller lagres på privat pc, bør opplysningene krypteres tilstrekkelig.

Det oppgis at personopplysninger skal publiseres. Personvernombudet legger til grunn at det foreligger eksplisitt samtykke fra den enkelte til dette. Vi anbefaler at deltakerne gis anledning til å lese igjennom egne opplysninger og godkjenne disse før publisering.

Forventet prosjektslutt er 22.05.2017. Ifølge prosjektmeldingen skal innsamlede opplysninger da anonymiseres. Anonymisering innebærer å bearbeide datamaterialet slik at ingen enkeltpersoner kan gjenkjennes. Det gjøres ved å:
- slette direkte personopplysninger (som navn/koblingsnøkkel)
- slette/omskrive indirekte personopplysninger (identifiserende sammenstilling av bakgrunnsopplysninger som f.eks. bosted/arbeidssted, alder og kjønn)
- slette digitale lydopptak