NTNU
Norwegian University of
Science and Technology

Master's thesis

2019

Anar Meirkhanova

Master's thesis

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology and Electrical
Engineering
Department of Information Security and Communication
Technology

Anar Meirkhanova

Information security expertise and oversight among Norwegian boards of directors

Interpretive study

June 2019

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

Information security expertise and oversight among Norwegian boards of directors

Interpretive study

Anar Meirkhanova

01-06-2019

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Information Security and Communication Technology
Norwegian University of Science and Technology,

Supervisor: Assoc. Prof. Laura Georg Schaffner

Preface

This is a master thesis in Information Security at NTNU carried out during the spring semester of 2019. The idea for the thesis was provided by Laura Georg Schaffner, who is my supervisor. Upon hearing the approximate title, I got immediately interested and engaged. Though, one of the biggest challenges with this subject is the unavailability of the board members and the secretive nature of the information they possess. This challenge did not set me back but pushed forward to delivering results.

Preliminary research project planning was carried out during the fall semester of 2018.

This paper is written for those who are interested in the subject of information security management. Understanding of risk management and specifics of the information security risks are desired, but not necessary. The reader can have an information security management background, or be a member of the board of directors or anyone from information security research environment, i.e., professors and students.

01-06-2019

Oslo, Norway

Acknowledgment

I want to thank the following persons for their great help during this master thesis.

First of all, I am very grateful to Laura Georg Schaffner, who has supervised the project since September 2018 and provided helpful and valueble commentary and feedback. Those motivated me and encouraged to overcome the challenges.

Thank you, Sokratis Katsikas, for the tremendous help in the initial phase of this project, insights on the topic and connections to the respondents.

Many thanks to Margrete Rundtom for being helpful and connecting with several of the respondents.

Thank you, Ekaterina Shirokova, for introducing me to one of the respondents.

I am also grateful to all respondents who so generously gave their time and answered my many questions. And precisely one person, whom I cannot name, who connected me further to another respondent.

Thank you, Thomas Kildal, for supporting me during the whole master programme and making it possible for me to finish it on time.

A.M.

Abstract

Corporate governance is under pressure after world-wide large-scale scandals, which were caused by inadequate internal control and supervision. Reforms, such as the Sarbanes-Oxley Act, brought changes to the internal control processes and the frameworks that organizations had in place. As a supreme governing body, the board of directors is responsible for internal control and corporate governance. And since the scandals, there is a lot of focus on the boards and how they do their work. Typically, organizations have separate sub-committees within the boards: audit committee, compensation committee, and lastly risk management committee. The boards with risk management committees show due diligence and have stronger risk management expertise, and thus, could show sound and transparent corporate governance to the shareholders.

In this project, six board members were interviewed, and financial reports of 16 Norwegian organizations were analyzed. The main focus of the survey was on the perceived expertise in information security, cyber security related challenges, and board sub-committees association. Hilb's New governance model is used as a theoretical framework to structure the results and understand how Norwegian organizations compare to that framework.

In the era of information technology, organizations have to decide how to gain competitive advantage by employing new technology, but at the same time, they should not forget the importance of assessing the risks they are exposing themselves while proceeding with digitalization

The IT expertise within the board is vital for the correct strategical decisions on new technology, and information security expertise is necessary for the governance of IT risks matching the risk appetite of the shareholders and stakeholders.

In Norway, most larger organizations have audit and compensation committees. Additionally, forward-looking firms have included risk management committees as a separate committee, or combined it with the audit committee. Just two organization had board structure close to the New governance model. These organizations also disclosed extensive information on information security incidents and risks. Other reviewed organizations had no risk committees and had no connection to information security strategy. The strategy and security programmes existed within organizations but disconnected from the enterprise strategy.

It is beneficial for those organizations to move in the same direction as the two leaders. Particularly important is getting information security expertise into the board of directors. The next step after that is the disclosure of information security report as part of the annual report. Disclosure should include the information security framework and top-level performance indicators. Simply stating that cyber security is a critical risk is not sufficient.

An information security model is developed based on the findings from the interviews, reports, and literature. This model is useful to the boards of directors – it shows how information security

governance process flows from the board to the organization and back to the board with reporting and relevant metrics.

The primary limitation of this project is the number of respondents. Future research should expand the number of respondents and perform sampling in a balanced way representing all sectors and directors with various backgrounds. This data can be used to improve the model and to draw further conclusions.

Contents

List of Figures

List of Tables

1 Introduction

Nowadays, Information security touches all layers of society: businesses, governments and people individually, and society as a whole. Most of the companies are taking seriously the risk associated with information technologies. Digitalization and new technologies broaden risk exposure even more. Previously, information security was considered only a technical problem. However, the world is leaning towards an agreement that it is a managerial issue as well. Many small and medium-sized enterprises (SME) do not survive information security incidents and go bankrupt. That can be prevented if SMEs establish security strategy and security programme with comprehensive incident handling, risk management, and information security controls.

The leadership of the companies is changing toward inclusion of information security into the enterprise strategy, and not just as an operational task. The oversight of information security related risks is getting included together with other high risks, such as financial risks.

1.1 Topic covered by the project

Executive management and board of directors are the first to get blamed if information security incident takes place. Inappropriate information security governance can lead to enormous financial losses. Companies are trying to understand how to handle such risks and what is needed to be done. Some firms are so much further that they are promoting information security oversight among the board of directors (Telenor annual report for 2018 [10]). Information security risks should be handled at the same level as essential financial risks.

Board of directors' essential role is in overseeing risks. They are the central authority that has to supervise the accomplishment of the goals set by shareholders and sometimes, stakeholders. Typically, annual or interim reports are showing the current risk picture. If information security risks are not mentioned that would signal not proper governance or disclosure issues. Currently, boards are getting more and more aware of information security risks as IT systems take over all business operations. Understanding risks is not enough. Boards must govern the security programme and request follow-up and maintenance. This will convince shareholders of sound governance and due diligence culture.

There are existing frameworks for information security governance, and they are of great help to board members. It is imperative to get an understanding of the situation with the Norwegian boards' of directors take on information security. Additionally, the realization of the importance of board member expertise in cyber security is a task for all organizations in Norway. How it was handled up until now is revealed through interviews and reports.

1.2 Keywords

Corporate Governance, Board of directors, Norway, Information Security Governance, Information Security Expertise.

1.3 Problem description

Members of the board are exceptionally busy people who are working with confidential information about organizational performance. It is not easy to get to meet them, and it is hard to get information pertinent to the study. Another side of the boards is that it is not always clear how they operate, what background they have, how it is used and how it affects the development of the organization. With regard to Information Security Governance it is even more unclear. The topic is not often found in the literature, especially regarding Norwegian companies.

To learn more about Information Security Governance, it is necessary to survey various directors on how they deal with and supervise the Information Security risks. How Information security expertise among boards of directors affects the risks taken and what is the overall Information Security programme state within the organization.

1.4 Justification, motivation and benefits

Focus on corporate governance has come to light after Sarbanes–Oxley Act (2002) [11]. And Information Security Governance is a new field and is not excessively researched. To get a better understanding of how Information Security is governed it is necessary to have a dialog with various boards. Focus on Norwegian companies is self-evident, and nonetheless important.

Analysis and data acquired from this project produce insights and a certain explanation of the information security governance state in Norway. That in itself is beneficial to boards to help compare against such research findings and improve Information Security Governance.

Similar surveys held after this research project is finished can use acquired analysis for comparison or expansion.

1.5 Research questions

1. How do Norwegian non-executive boards perform Information Security Governance in comparison with Hilb's New Corporate Governance model [1].
    1. How is information security aligned with corporate governance and IT governance focus?
    2. How is oversight of Information Security risks affected by the board's structure?
    3. To what degree Information Security expertise is available among board members?
    4. How is responsibility for information security risks distributed within the board?

1.6 Planned contributions

This master project contributes with analysis of the qualitative data provided by a survey completed by Norwegian organizations' board members and financial reports of 16 organizations. Also, it offers a qualitative analysis of the current situation of the Norwegian board of directors involvement in Information Security subject. That includes the understanding of the differences between the New Corporate Governance model [1] and the current state of Information security governance in the Norwegian organizations. At the end of the research project, a combined information security governance model is suggested together with other insights on Information Security topic.

This research project is a step towards clarity of the Information Security Governance status in Norwegian organizations.

1.7 Limitations

As with many master thesis projects completed in one semester, there is a lack of time with regard to interviews. Board members usually are very busy and sometimes almost impossible to get a hold of for a short conversion, much less for one hour interview. I managed to get to interview six directors and one security expert who works closely with executive management and boards daily.

The analysis of the financial reports provides with a good premise. However, it shouldn't be forgotten that some information never gets to the report but discussed nonetheless.

1.8 Structure of the thesis

First, related literature is covered in chapter 2, starting with Martin Hilb's "New Governance Model", then covering the look at existing information security frameworks and, at last, the research related to the expertise of the directors in Information technology.

In chapter 3, I explain what methodology is used during this research. After that, I present the core of my project - the results, in chapter 4, and my model and insights from the findings in chapter 5.

The thesis is wrapped up with the conclusion (chapter 6) and further directions (chapter 7).

2 Background

2.1 Corporate Governance

Corporate governance is a set of rules, policies and processes used to direct and control the organization, as explained in Investopedia (2019) [12]. Every country has its technicalities surrounding corporate governance, but normally, two approaches are distinguished: shareholder-centric and stakeholder-centric, Hilb (2008) [1]. Board of directors is one of the elements of corporate governance and serves as the governing organ that sets current and the future strategy of the firm.

Corporate governance has been evolving in the past years due to many corporate crises [1]. It was affected by the Sarbanes-Oxley Act (SOX) reform in 2002 [11] with Section 404 that outlines a top-down risk assessment. The 2008-2009 financial crisis led to overwhelming losses and long-lasting severe consequences. That put further pressure on boards of directors and executive management as the main reason for the crisis were poor internal control processes and lack of proper supervision.

SOX reform led to the development of various frameworks and models. One of them was established by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. Their framework was additionally updated in 2013. The definition of internal control is as follows according to COSO [13]:

> It is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: Effectiveness and efficiency of operations, Reliability of financial reporting, Compliance with applicable laws and regulations

COSO framework defines these as main components: Control Environment, Risk Assessment, Control Activities, Information and communication, and Monitoring. Additionally, COSO broadens the framework and the components with 17 principles.

2.2 New Governance Model by Martin Hilb

Martin Hilb, in his book "New corporate governance" [1] is promoting a new holistic model for corporate governance. This model is trying to integrate and balance shareholders' wishes and requests and desires coming from stakeholders. Stakeholders are customers, employees, general society, anyone who has interests and involvement in the organization. The model has four parts:

Keep it:

- Situational
- Strategic
- Integrated
- Controlled

2.2.1 Keep it situational

Organizations are inherently dissimilar; they operate in different sectors, countries; they are different in size; they are state-owned or family-owned. All these differences have to be taken into account when forming boards and planning a future strategy. There is no rigid model which fits every firm. Every organization has to adapt to the surroundings of its own. And that is what the "situational" element is about.

Boards of directors have to adapt to external and internal business context. The external would be the culture of the country they are active in, the laws and regulations stipulated for the sector and in general.

The internal context among others suggests the ownership type: family-owned, cooperative, non-profit or governmental; the board configuration: the executive board model, non-executive board model; organizational complexity; the degree of internationalization [1].

2.2.2 Keep it strategic

The following four components are prerequisites for a good corporate strategy [1]:

1. A strategically targeted composition of the board team,
2. A constructive and open-minded board culture
3. An effective board structure, and
4. Shareholder and stakeholder oriented board measures of success

A well-diversified board is an aim for the first point, and each board member should have expertise in diverse fields. The members should be open-minded, aiming to learn and to get a holistic view of the business and company.

An effective board structure implies a board that is neither too big nor too small. For large organizations, seven members is the maximum number. For smaller organizations, the number should be even smaller.

For large firms it is suggested to have two sub-committees:

- an integrated audit and risk management committee (ARMC)
- an integrated board management committee

As it is evident from the name of ARMC, it is responsible for audit and risk management. The integrated board management committee deals with board remuneration, nomination, feedback and development. Both committees and the board as a whole have to establish and follow a vision for the organization that considers both stakeholders and shareholders [1].

2.2.3 Keep it integrated

The "integrated" part aims to help building the board as a team. The team that is carefully selected, gets timely feedback, compensated accordingly and developed while governing the organization [1]. Carefully composed and the efficiently functioning board will fulfil the vision and bring the company to success.

2.2.4 Keep it controlled

Boards should demonstrate a balanced directing and controlling team, that adds value to shareholders, employees and society without exclusions. Directors are fulfilling the monitoring function of the organization. Figure 1 shows the functions the board has to perform.

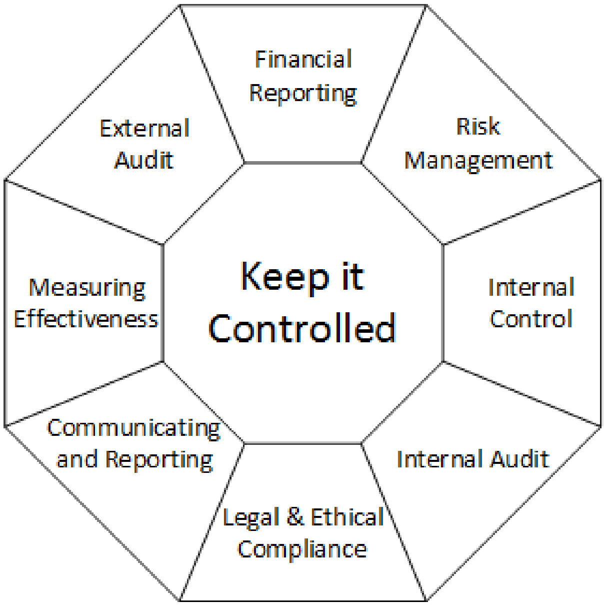

Figure 1: Keep it controlled functions as described in New Governance Model [1]

ARMC is the committee that is responsible for many of those functions. Its role is to oversee internal control systems including internal audit, annual and interim reports, be critical to external audits. Another quite substantial role of ARMC is to guarantee a complete and exhaustive risk management system that is in place in the organization.

The challenges for ARMC include both overreaction and underreaction to events and information. That leads to either excessive control or sloppiness. The underreaction can lead to negligence, especially when risk management appears only at the operational level and disjointed from other functions like IT and legal [1], while overreaction can choke the innovation and lead to missed opportunities.

COSO and Hilb's frameworks are essential in helping to make boards of directors and executive management more reliable and their work more transparent to the shareholders, stakeholders and everyone involved.

2.3 Socio-Technical Systems

Ongoing digitalization and transformation push organizations into the IT world. Even simple operations in the smallest companies are now dependent on information technology. IT presents new opportunities and risks. If organizations are preoccupied with the opportunities without addressing inherent information security risks, the outcome will be disastrous, both financially and for the reputation. And recent information security incidents are making executive management and boards of directors realize that information security risk oversight and governance are fundamental.

To understand the information security risks, it is necessary to look at them as a socio-technical system (STS). Bostron and Heinen (1997) [14] explain that the socio-technical system implies "a work system made up of two *jointly* independent, but correlative *interacting* systems - the social and the technical". The technical system represents all technical tasks and processes, and social system - skills and values of the people and relationships among them. Both Kowalski (1996) [15] and Bostron, Heinen [14] highlight that the outcome of such STS is the output of both systems interacting with each other, thus it is essential to address both sides equally.

STS approach has existed for a while and yet, not very wide-spread in real life projects and systems [14, 15]. Identifying technical and social systems as one whole system reveals far more flaws and gaps than when examining them separately. This holistic approach helps with analyzing risks associated with inherently technical systems.

Information security is intrinsically technical, and social side of it is often forgotten while organizations are trying to solve issues or incidents. Human side often plays a crucial role in said issues and incidents [15]. Socio-technical system approach can help to achieve "optimization of the psychological and social aspects of the individual or group requirements" [14]. Board of directors expertise is one of the elements of the social system that has to be optimized for the whole system to perform more efficiently.

Information security is one of the many subjects that is supposed to be handled by the board of directors. New governance model by Martin Hilb [1] looks, among other sides, at the social aspect of the board of directors and executive management. Their knowledge, expertise and motivations are all playing a role in how the organization is governed. In this way, New governance framework has the basis for efficient oversight of the information security risks.

2.4 Corporate Governance and Information Security

Let's look at how information security was addressed in some corporate governance models and frameworks. As it is, both COSO and the New governance model do not address information security risk specifically. However, they emphasized comprehensive risk management systems that imply cyber security.

For example, COSO published "COSO in the cyber age" in 2015 [16]. As mentioned in section 2.1, COSO has 17 principles. "COSO in cyber age" has mapped cyber security toward all principles and accentuated those principles that are relevant to it [16]. COSO emphasizes that cyber risk is unavoidable and must be handled. Board of directors and their involvement is another focal point COSO mentions for sound internal control and governance. "COSO in cyber age" aids the board with a framework for better communication of their business objectives and risk appetite [16].

In 2010, U.S. Securities and Exchange Commission (SEC) had also released guidelines for cyber security risk inclusion [17].

When it comes to Information Security, it is not apparent that executive management and board of directors are to be involved in the governance process. However, all of the guidelines I have looked at are suggesting exactly that.

For the financial institutions, there is the Bank for International Settlements (BIS) that sets the regulation into practice with guidelines and other useful material. BIS has played a crucial role after several crises in improving collaboration between banking and financial institutions with the focus on financial stability. BIS is one of the oldest financial institutions. Right now it is owned by 60 member central banks from around the world. One of the BIS organizations, called The Basel Committee on Banking Supervision (BCBS), has prepared and published a document on Cyber resilience practices in December 2018 as part of Basel III.

This report was based on the surveys conducted in April 2017 among financial institutions that follow BCBS requirements. It focuses on four main parts: (1) cyber-governance; (2) approaches to risk management, testing and incident response and recovery; (3) communication and sharing of information; (4) interconnections with third parties. For this master project, the most relevant parts are cyber-governance and risk management.

Cyber security strategy is expected but not required. BCBS has concluded that cyber security strategy is enforced in the surveyed institutions by the combination of these approaches:

1. Financial institutions are following the requirements generated by the authority (government)
2. The financial institutions develop and implement their cyber security strategy, which is then reviewed by the authority as part of the assessment
3. Financial institutions are inspected to determine if IT strategies exist and cyber security is included in it

This report's findings are representative, in my opinion, of the larger Norwegian banking institutions. Even though this report is aimed at financial and banking institutions, it is insightful and useful for other industries [18].

2.5 Information Security Governance

Whitman (2013) [19] is clear that "Integration of Governance, Risk management, and Compliance is important at the board or executive level". If a security programme is developed from the IT department, the probability of it to be successful and efficient is less than if it is integrated with the board's views.

The articles on information security governance (ISG) always include the board of directors involvement. However, ISG literature, with its frameworks and related information, is in some degree, detached from the corporate governance subject as a whole. There are, undoubtedly, main elements that go through both corporate governance and ISG, such as board of directors, executive management, risk management and strategy. Though, ISG still feels disconnected from the holistic corporate governance. Another downside of these ISG frameworks, I will describe in the following paragraphs, is that they do not talk about social sides that were pointed out in section 2.3: skills, expertise, motivations. And still, the following frameworks and models are noteworthy for this research project.

ISG framework designed by IT governance Institute (ITGI) is defined in the guidance (2006) [2] that was developed specifically for boards of directors and executive management. The guideline goes through various aspects of information security governance, including what it is and why it is vital to the leadership of the organization. It also helps with useful sets of questions that boards can ask to understand their organization's situation regarding ISG. Additionally, ITGI describes the difference between the executive management role and the role of the board. Here is how Information security governance is defined by ITGI [2]:

> Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security programme.

ITGI stresses that it is time to count information just as another asset or a resource. Subsequently, protection of the information is the initial step of the comprehensive ISG. Each organization needs to establish and maintain its own ISG framework, because that is a prerequisite for a sound and cost-effective security program. In Fig. 2, ITGI shows a conceptual framework where the cyclic nature of ISG is illustrated.

The most important part of this framework is the feedback loop to the management and board of directors. This feedback should include a security report with a set of high-level measures and metrics that give a complete picture of the current security posture. This loop should also imply the reports prepared as a response to the inquiries from the board or executive management.

The five essential outcomes of the ISG are Strategic alignment, Risk management, Resource management, Performance measurement and Value Delivery [2].

Center for Audit Quality (CAQ) has prepared an equivalent to ITGI's guidance – a Cyber security information risk management oversight: a tool for board members (2018) [20]. It is shorter, compared to ITGI's, and concentrates on the questions that the board of directors, executive management need to ask to deal with Information security in their organization. This guideline touches on the subject of Certified Public Accountant (CPA) firms being valuable in connection with Information security risks. Examples of such a company are Deloitte, KPMG and EY.

The questions from the two guidance documents can be used as a basis for a survey of the executive management and board of directors. At the same time, there are questions and directions for boards to inquire for comprehension and identification of information security responsible departments and personnel.

ISACA, in its study from 2018 has uncovered a crucial detail [21]: the board has a higher trust level than in previous years, but there is a mismatch in organizational alignment. In other words, employees have a hard time identifying the correct person or department to report their findings. The feedback loop with metrics and reports is a critical element in the whole Information security governance process. Without this, there is no way the security programme will work as it should; it will never get developed and maintained through time.

The information security expertise is necessary at the board level. As to where it should reside,

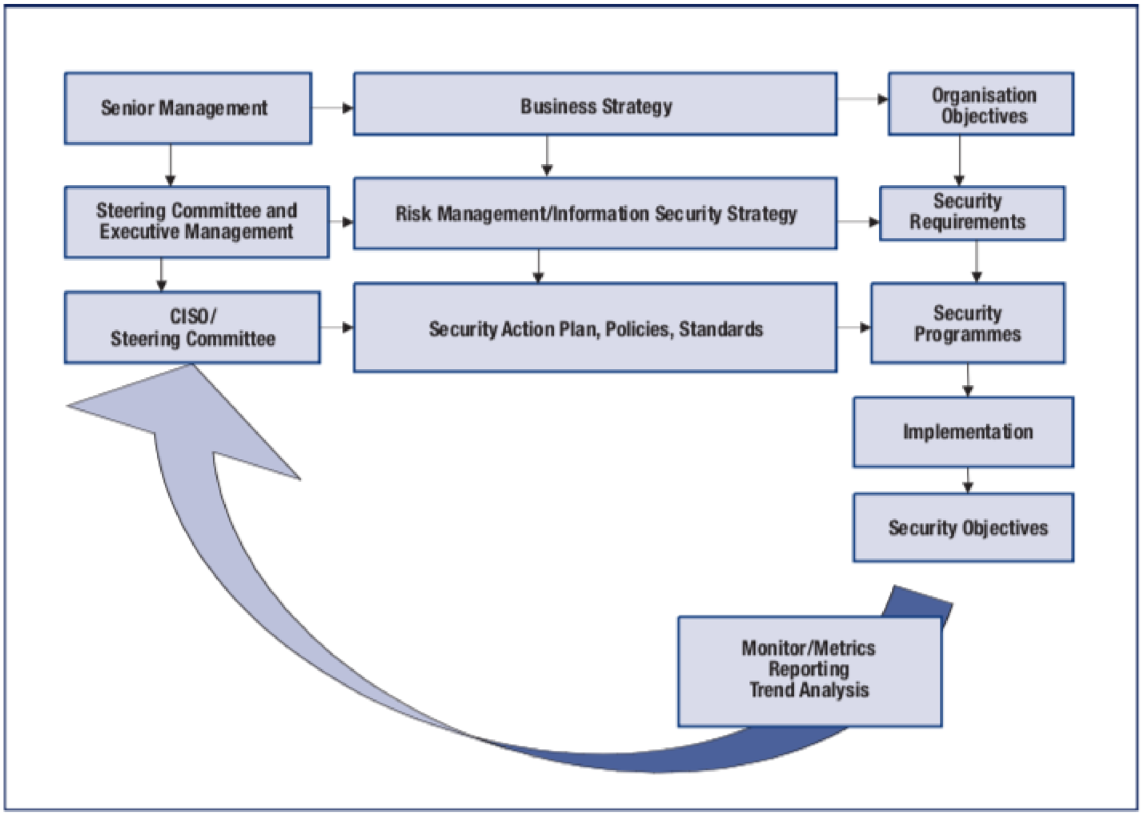
Senior Management
Business Strategy
Organisation Objectives
Steering Committee and Executive Management
Risk Management/Information Security Strategy
Security Requirements
CISO/ Steering Committee
Security Action Plan, Policies, Standards
Security Programmes
Implementation
Security Objectives
Monitor/Metrics Reporting Trend Analysis

Figure 2: ITGI Conceptual Information Security Governance [2]

the answer is not that simple. According to Trautman and Altenbaumer-Price (2010) [17] and Deloitte report (2013) [22], larger organizations often have risk committees or a combined audit/risk committee. And the risk committee is the first contender. However, most risk committees do not have expertise in information security or IT in general, and often enough audit committee has that. Even audit committees do not withstand the requirement of the information security governance. Usually, audit committees cover information security risks in connection with the financial system and not overall security programme [23]. However, IT audit reports are, nevertheless, helpful and might uncover some issues, but boards should keep in mind that those reports are not a complete representation of security posture. There are still organizations that have no risk committees within the board [22] and rely solely on audit committees. Therefore they are neglecting a substantial area of risks, including information security risks.

To add to the importance of the risk committees, the research of Malaysian firms done in 2010 by Yatim [24] demonstrated that those “firms with greater board expertise and board diligence are also likely to establish a risk management committee". The conclusion was that "stronger boards demonstrate their commitment to and awareness of improved internal control environment" [24]. This paper examines risk handling and risk committees in general and does not touch on cyber security. However, the results are valuable for evidence of risk expertise value for the governance quality.

Another research paper that was published in 2011 has insightful results - a survey among Saudi Arabian organizations by Abu-Musa [25]. The outcome was such that the companies recognize and understand the value of ISG, but at the same time, a good part of those firms do not even have Information Security strategy. Additionally, around half of the companies did not have staff that is assigned for the creation, development and maintenance of the information security programme. Most of the respondents had an opinion that risk assessment was not enough to satisfy the requirement of laws and regulations. Many firms also revealed lack of recovery programs, crisis management and planning in case of cyber attacks. In some organizations, information security reviews were performed but not reported up to the board and usually stopped with the CEO. This paper's findings are relevant to this thesis, in that, it shows that some boards of directors stop at the recognition of the importance of ISG and, therefore, do not address the information security risks in a sound and appropriate manner. In this article, the author had also introduced his own ISG framework, which is based on several frameworks described by ITGI and other research papers.

There is not much research done among board members in Norway and their take on Information security.

2.6 IT governance and expertise within the board of directors

In the articles with the IT governance as a research subject, authors look at the IT oversight, which sometimes includes IT risks as well. They also discuss IT expertise within the boards.

In [26], Nolan and McFarlan (2005) rightfully state that the board should not question if they have to be governing IT, but should question how they should supervise IT decisions. The authors developed four modes of strategic dependence on IT: defensive IT with high and low strategic impact and offensive IT with high and low strategic impact. The example of a high strategic with offensive IT is a financial institution. After the mode is defined, the organization has to discuss the IT expertise within the board. The authors suggest that offensive IT companies should have IT governance committees within the boards, while the ones with defensive IT have just IT expertise within the audit committee.

> The IT expert's job is to challenge entrenched in-house thinking. He or she must be a skilled communicator who does not hide behind technology jargon or talk down to board members. [26]

IT security is mentioned as part of the overall IT system and that boards should have an understanding of those.

Huff et al. (2006) [27] used in their research the four modes described by Nolan and McFarlan. This article goes over IT expertise among boards in Canada by surveying 17 Canadian organizations. The authors tried to see how much attention is given by the board of directors to the IT and how much expertise there is within boards. In this article, they have also presented the results of the Chief Information Officers (CIO) surveys of the corresponding companies to compare their opinion to the directors'. Information security risks were one of the topics. The results were quite insightful [27]:

1. "Full boards spend almost no time addressing IT issues directly."
2. "Boards generally only receive post-hoc updates on major IT issues."
3. "The limited discussions of IT issues generally occur only in board committees."
4. "Audit committee IT discussions are reactive."
5. "Boards view IT issues as too “technical”."
6. "Boards are concerned most about IT risk."

Even though almost all were concerned about IT risks, only three boards had such discussion, and the other 14 were never addressing this subject. Of those who discussed IT risks, they were handled by audit committees, though authors highlighted that audit committees are quite busy with other tasks, so information security was given just fleeting attention only when exceptionally necessary.

CIO's responses were taken into account when authors generated a list of suggestions [27]:

1. "Include IT on the Board Agenda."
2. "Invite the CIO to Board Meetings."
3. "Elicit Brief CIO Presentations."
4. "Recruit IT Experience onto the board."
5. "Get the Board Talking About IT."
6. "Realize That Boards Now Operate in an IT Era."

In this research, the authors focused on IT in general. At the same time, boards were concerned about information security, though this concern did not lead to any feasible information security oversight strategy. In the previous sections, it was discussed which committee should have the expertise in information security. This section covers how IT expertise, including information security, is vital to be present in the board as a background.

Rhee et al. (2012) [28] argued that information security management executives are prone to optimistic bias when assessing information security risks. The optimistic bias implies the underestimation of the probability of a risk due to lack of information or willingness to undervalue the risk [28]. The results had shown information security executives had an optimistically biased view over information security risks of their own organization and the ability to control the cyber threats. To eliminate such biases, authors suggested a carefully constructed training. The idea is to show that cyber incidents are not less likely to happen to them than to other organizations. "Individual organizations need to develop a long-term plan and practice procedures to security management instead of relying on ad-hoc approach to the implementation of security measures" [28].

2.7 Legislative regulations and directives valid in Norway: from corporate governance to information security

Norwegian organizations and their board members need to be aware of the legislation which applies to the industry they belong to. All organizations listed on the Norwegian stock exchange market should follow the Norwegian code of practice for corporate governance [29]. This code of practice, updated in 2018, is divided into 15 sections (see Appendix B). All of the sections need to be addressed by the board of directors in the corporate governance report with a clear statement of compliance or explanation of the deviation [29].

The objective of this code is to make these organizations [29]:

> practice corporate governance that regulates the division of roles between shareholders, the board of directors and executive management more comprehensively than is required by legislation.

The Information Security Risks are not mentioned explicitly but implied as part of risk management and internal control section [29]:

> the board of directors must ensure that the company has sound internal control and systems for risk management that are appropriate in relation to the extent and nature of the company's activities.

Senior management is responsible for providing the board of directors with the correct and comprehensive information on risks and internal control of said risks. If any framework is used for internal control, it should be disclosed and reported by the board of directors in the annual report [29].

Now, let's look at the European legislation related to Information Security. Norway is one of the countries in the European Free Trade Association (EFTA) and subsequently has to adopt the regulations and directives put in place by the European Union (EU). Historically, only confidentiality had been addressed by EU legislative regulations. One of such legislation addressed handling and sharing of confidential information between member states, and the other is General Data Protection Regulation (GDPR) addressing user data usage, storage and handling.

From a Confidentiality, Integrity and Availability (CIA) triad standpoint, there was no regulation which covered all of them until The Directive on security of network and information systems (NIS directive) was introduced in 2013. NIS directive's objective is:

> to achieve a high common level of security of network and information systems in the Union

This directive ensures that Member states are prepared for cyber attacks through the appointment of the computer security incident response team (CSIRT) authority and adoption of a national strategy on the security of network information and systems. NIS directive sets up a cooperation group which will support the CSIRT network and sharing of information on incidents and threat landscape. Another crucial part of this directive is to ensure a "culture of security" across various industry sectors. Particular focus is on "operators of essential services" [30], in other words, organizations whose services are of critical significance to the society and nation as a whole. The nation itself defines these critical operators. Every member state has to transition it to the national law [30].

Newly updated Norwegian security act (Sikkerhetsloven) [31] is somewhat connected to the NIS directive. National Security Authority (NSM) was defined as the national CSIRT point of contact and facilitator for sharing information on the threat landscape and the incidents [31] for the whole country. National security act covers more than NIS directive, in that, overall security is covered by it and not just information security. NSM and Agency for Public Management and eGovernment (Difi) have released guiding material on how to adapt to the updated security act [32, 33].

Various industry sectors have their laws and regulations in Norway. These were established while specific industries were adopting different information and communication technologies (ICT). Typically, these laws and regulations cover all ICT related requirements where information security is merely a part of it.

The Regulations on the use of information and communication technology (ICT regulation) [34] is aimed at the financial and banking institutions and is in place since 2003. Paragraph §5 is the main section with the requirements for information security. Here, the organization is required to establish procedures which would protect equipment, systems and information of value to the organization's activities against damage, misuse, unauthorized access or changes, and vandalism. These procedures should include guidelines for assignment, update, deletion and control of authorized access to ICT systems. Security requirements, as much as practically possible, should be measurable [35].

The financial industry was one of the first to have regulation on information security and risk assessment. The internal control and governance model in financial organizations can be used as an example of how to manage and govern information security risks. ICT regulation states that the board of directors is responsible for proper securing of the organization, as well as establishing security strategy and policy, reporting should be in place for governance and control [34]. The Financial Supervisory Authority (Finanstilsynet) has provided a guideline with the mapping of ISO 27000-series standards for ease of use and better comprehension [35].

The health sector has NORMEN [36] - Norwegian Code of conduct for information security in the health and care sector. It describes

> the organizational and technical measures that are considered appropriate in order to achieve a satisfactory level of information security and privacy and data protection regarding such processing of personal health data and personal data.

Although Normen came to existence in 2006, fast-paced digitalization and lack of proper controls lead to rather significant information security incidents. It shows that legislation cannot solve the problems of information security by itself.

The health sector is still laying behind, but the update of Normen in 2018 is one of the steps on the way to proper governance of Information security [36]. All of the legislative regulation mentioned above emphasize the role of the executive leadership and the board of directors [32, 35, 36]. Importance of information security risks governance is at the same level as financial risks governance.

3 Methodology

The research method of this project is based on applied research and qualitative techniques. The main goal is to explore non-executive boards of Norwegian organizations for expertise in information security. The principal method of data gathering was semi-structured interviews and financial reports investigation. The New Governance Model of Hilb (2008) [1] stands as a theoretical framework for structuring collected data and helps with analysis of the data.

The connections to respondents were established through personal contacts or contacts at NTNU. Boards of directors are quite busy, so I agreed to every contact I could get hold of. The initial set of the organizations whose financial reports were investigated were chosen because the respondents represented them. Later, the collection of organizations was expanded to include 16 essential companies. The selection was affected by the presence of information security information in the financial reports.

The interview was based on the questionnaire prepared by Laura Georg Schaffner [37]. The same questions are available under Appendix A, section A.1. As interviews were held in a semi-structured nature, additional questions were asked which are also available under Appendix A and section A.2.

During Research Project planning stage of this thesis, both qualitative and quantitative research methods were considered. Later during the initial data gathering stage, it was clear that there will not be enough respondents and thus not enough quantitative data. Therefore, I focused on qualitative methods.

3.1 Qualitative research

Qualitative research originated from social sciences, where researchers aimed to explain cultural and social phenomena, as described by Myers et al. in 1997 [38]. The history of qualitative research in some fields has had its share of bad reputation by being dismissed as not a proper approach for research, Leedy (2013) [39]. Nevertheless, it has overcome the issues and persists nowadays, expanding to other scientific areas, such as information systems.

The difference between qualitative and quantitative research is that qualitative expects more preparation and the path is never straight forward. At the same time, it is possible to start data analysis as soon as the first data is available.

The goal of qualitative research is one of the following: revealing the nature of the phenomenon; obtaining new information related to the phenomenon; validating a specific hypothesis; evaluating the effectiveness of the researched techniques [39].

3.1.1 Qualitative techniques for data gathering

When it comes to data gathering, there are multiple ways of obtaining it:

- Survey
- Interviews
- Observations
- Documents research

The interviews are going to be held in a semi-structured manner, meaning that they are based on a questionnaire, but with the allowance to answer some question as an open-ended question. Additionally, supplemental questions will be asked to expand on received answers, if necessary. The interview questions and additional ones are listed in Appendix A.

The observations include side comments during interviews and observation of the respondents during the interview process.

Documents applicable for this research project are publicly available reports and materials from organizations where respondents are or were employed as non-executive board members. Additional companies were selected for expansion of data sources. Relevant information is extracted and analyzed and rated for importance to the research project.

3.1.2 Qualitative data analysis

Face-to-face interviews, together with observation and documents, are the basis for the qualitative analysis.

Neuman (2013) [40] explains that to perform a qualitative analysis means

> to systematically organize, integrate, and examine; as we do this, we search for patterns and relationships among the specific details. Analysis allows us to improve understanding, expand theory, and advance knowledge

As mentioned before, qualitative analysis can start as soon as data is obtained; however, the analysis process is not as systematic as with quantitative analysis. The qualitative approach allows conceptualizing and building new theories, and it is often enough based on approximate and diffuse data.

Most qualitative analysis involves coding, analytic memo writing and outcroppings. Qualitative coding differs from quantitative, in that, it is not in machine-readable form. Data is arranged into categories and concepts. It is suggested to carry out the process of coding three times [40]. First coding is called "open coding" where data is sifted through to find initial categories and themes. These initial themes and categories can be changed and adjusted in future analysis. The level of detail in coding depends on the researcher and the research questions.

The second pass through data is called "axial coding" [40]. The focus of this coding process is preliminary codes and categories to determine more about each of them [39]. The goal of this process lays in "organizing ideas and themes and identifying the axis of key concepts in analysis" [40]. This coding helps to understand and expand on the connection between categories: causes and consequences, interactions; if they form clusters; or if there is a need for subcategories.

The third and the last pass through original data is called "selective coding". Main themes should be identified, core concepts established before selective coding can be started [40]. During the process of selective coding, the researcher goes through the data and selects the examples that demonstrate the core concepts and can explain the studied phenomenon [40, 39].

During the coding processes notes are made for various purposes: research strategy, analysis method, associated code, related literature and comments. The analytic memo is writing a memo about raw data while analyzing it. Another important aspect of qualitative analysis is outcroppings, which identifies the event with profound structural interconnection [40].

As suggested in [40], there are seven types of qualitative analysis: ideal type, successive approximation, illustrative method, domain analysis, analytic comparison, narrative analysis, and negative case method. I will expand on three of those. Successive approximation is an approach where the researcher goes through analysis stages and then iterates through them several times. After each iteration, the researcher comes to a better understanding and more concrete findings. Finally, these iterations lead to detailed answers to the research questions [40].

The illustrative method applies theoretical concepts to empirical evidence by setting said evidence in boxes. The final result of this method would be that evidence is proving the theory, rejecting it or adds to it [40].

The analytic comparison uses "the method of agreement and the method of difference to discover causal factors that affect the outcome among set of cases" [40]

3.1.3 Data triangulation

In social studies, triangulation means observing the phenomenon from multiple angles [40]. With triangulation, the researcher learns more than if the study was performed only from one perspective. There are four types of triangulation in research:

- triangulation of measures -
  implies the phenomenon is measured multiple times from different angles.
- triangulation of observers -
  multiple observers with different tacit knowledge bring separate perspectives.
- triangulation of theory -
  basis theoretical focus will bring out various findings into focus for comparison to other theoretical findings.
- triangulation of method -
  the combination of qualitative method results can be expanded by the causality explanations brought by quantitative methodology.

In this project, I use the triangulation of measures, where I look at the data received from the interviews and the data from the reports and try to analyze and make conclusions from both angles.

4 Results from Interviews and Financial Reports

In this chapter, results will be presented. The first section is covering information obtained from both interviews and reports. All sections, until the last one, cover data gathered mostly from interviews [3, 4, 5, 6, 7, 8, 9] and some from the reports. The last section contains results from financial reports for the 2016-2018 period with the focus on DNB, Telenor, and Statkraft.

Interviews were held in a semi-structured way and followed questionnaire, and additional questions as in the Appendix A. Questions included topics on several subjects within Information Security. Namely, Information Security metrics available for the boards, Information Security Expertise, and Information Security Risk Oversight within the board. Additional questions were asked as the interviews progressed to expand or clarify obtained information. Duration of the interviews varied from 1 to 3 hours.

Financial reports were analyzed for board of directors background and training, corporate governance frameworks and any information related to the Information Security. Organizations whose reports are used are not only the ones that are represented by respondents but also a set of large companies with mature internal control and governance.

4.1 Board of directors background throughout various industries

To get an insight into how boards are composed in terms of expertise in Norway, I have looked at 16 major companies. These organizations are essential to Norwegian society, and most of them are part of critical infrastructure. Another aspect that played a role in the selection of the industries was the dependence on IT. Therefore I chose following sectors: Financial and Banking, Energy, Telecommunications. What I was looking for was to see how many of the members have IT experience or education. Section 2.6 shows that IT background is crucial [27, 26]. That is especially fundamental as all organizations in Norway go through digital transformation and automation.

Members with IT expertise are counted among non-employee elected independent members. There are, of course, employee-elected members with IT expertise but this is primarily determined by the industry the organization is operating in. For example, Yara employee-elected members of the board had a background in chemistry. This is expected, as Yara is a large manufacturer of various chemicals.

Here are the essential Norwegian financial institutions that were chosen for this research: Norges Bank, KLP, DNB, Sparebank 1 and Nordea. From the energy sector: Statnett, Statkraft, Eidsiva. Manufacturing or production sector: Orkla, Hydro, Yara, Norges Gruppen. Services, telecommunication and other industries are represented by Telenor, Aker Solutions, ABB, EAB, Høyskolen Innlandet.

Table 1 shows all those organizations, where the total number of board members is in the first column, then follows the number of members with IT education or IT expertise, and the last column contains the number of members and the field of their expertise.

Name of the organization	Total	Employee-elects	IT expertise	Other Expertise / Background
Norges Bank [41]	10	2	-	1 Legal; 7 Finance, Economics, Business Administration
Nordea [42]	13	3	3	2 Legal; 5 Finance, Economics, Business Administration
KLP [43]	9	3	2	5 Medical, Legal, Business administration and Economics
DNB [44]	7	2	2	3 Finance, Economics, Business Administration
Orkla [45]	11	4	-	7 Business administration
Hydro [46]	9	3	-	2 Engineering; 4 Finance, Economics, Business Administration
Norges Gruppen [47]	12	4	-	8 Variety (not mentioned)
Telenor [10]	10	3	2	2 Engineering; 3 Finance, Economics, Business Administration
Yara [48]	8	3	-	3 Engineering, 2 Finance, Economics, Business Administration
Eidsiva [49]	8	2	-	6 Engineering, Legal, Political and Social sciences
Statnett [50]	9	3	1	1 Legal; 4 Economics, Business Administration
Statkraft [51]	9	3	-	6 Finance, Economics, Business Administration
Aker Solutions [52]	8	3	-	1 Legal; 2 Engineering; 2 Economics, Business Administration
ABB	8	2	-	6 Variety (not mentioned)
EAB	5	1	-	4 Finance, Legal, Economics
Høyskolen Innlandet	14	10	-	Variety (Special case as this is an educational institution)

Table 1: Number of directors in various boards and presence of IT expertise

They all have similarities and differences. All have employee representatives as it is stipulated by law. The total number of members is fluctuating; the average in this set is nine. Production industry has the highest number of board members, while energy has the lowest. The only organization with seven members is DNB.

IT expertise is prevalent in financial institutions. Telenor and Statnett are the only ones with it from their sector in this list of firms. It is possible to assume that there is a tendency in hiring people with IT experience, specifically IT management, as board members. This result compares to what Nolan and McFarlan have suggested in [26] (see section 2.6). With automation, digitalization and adoption of the new technologies, such as machine learning (ML) and artificial intelligence (AI), the IT expertise is necessary for sound and educated decision making.

So far, DNB is the best in terms of IT-related background, but, of course, having that background does not mean that they are competent in the information security field as well. Although it is an immense step forward. DNB is going through reorganization and re-inventing themselves by aiming on being a technology firm first rather than a banking institution. They have put a tremendous amount of effort to increase expertise within the company, specifically to get personnel up to speed with the latest innovation in the IT field.

4.2 Information security expertise

Information security expertise among the board of directors is necessary for better governance. Understanding the exposure to new types of risks while transitioning to a more digital, connected, everyday activities, is crucial for tackling future threats.

Understanding and including the social side of the system, such as skills and background, helps to make the system work as a whole. Social aspects are as important as technical ones for the whole socio-technical system (STS) to work correctly (see section 2.3). When a new technical system works as it should, the lack of knowledge and resistance to change can cripple the efficiency of the complete STS. That is the reason for assessing the expertise of the board of the directors.

Interviewees were asked two questions connected to their own perception on their expertise level:

1. With regard to digitalization (i.e. exponential companies, API design, Privacy-by-design (GDPR), smart technologies, process automation), I consider myself...
2. With regard to cyber security (i.e. Maximum Possible Loss, Data Leakage Prevention, Deep Packet Inspection), I consider myself...

For the first question, respondents expressed that they carry an informed or higher level of expertise in digitalization (Table 2). For the second question, the respondents perceived themselves as informed or well informed on the subject of cyber security (Table 3)

Expert	4
Well informed	1
Informed	1

Table 2: Digitalization expertise

Well informed	4
Informed	2

Table 3: Cyber security expertise

Table 4: Own perceived expertise

Additionally, five answered that they wish to receive better training on cyber security. Only one replied better training is not necessary, as it was not a priority at the moment. The same person has identified as well informed in cyber security.

As it was described in [28], leadership optimism of information security posture and how much control they have makes the organization more vulnerable to cyber threats. The expertise and unbiased view are essential for board members to perform sound information security governance.

Three of six questioned had expertise within management in IT or disruptive technology or had a career within the IT field. All three respondents are currently part of audit and risk committees in the financial organizations.

Among the other three interviewees, one was part of the nomination committee, and the last two were part of small boards which did not have any committees and took discussions and decisions as a full board.

It is essential to mention that it is not expected that board members are experts in information security. However, to be able to ask correct questions and properly govern Information security, it is vital to have some expertise in identifying and managing information security risks. In other words, understanding such risks and consequences is crucial and essential for board members and the whole organization.

The directors themselves might not possess the skills, but almost all the respondents were convinced of the access to the correct Information Security personnel and materials both inside and outside the organization. Reliance just on experts is not a panacea. Experts would not be able to consider all distinctive details of the information security strategy that supports enterprise strategy. This knowledge and direction should come from the board of directors. That is why I emphasize on the expertise among board members and they can not relax just because experts are available.

Knowledge of the best practices or documents prepared by such organization as COSO and ITGI were not known among the respondents. That is, of course, in some way due to those being American based organizations and not heavily circulated in Norway.

Three respondents answered that other board members consider them specialists in information technology and strategy. One respondent was identified by their colleagues as strategy and governance specialist, another one as technology and business specialist, and the last one as IT specialist. (see Table 5)

Strategy and Information Technology	3
Strategy and Governance	1
Technology and business specialist	1
Information Technology	1

Table 5: Expetise perceived by other members

4.3 Information security roles within organization

Question 21 (Appendix A) is directed at the role within the organization that should have expertise in cyber security.

The answers varied greatly. Most respondents were vague and gave rough answers. One had no particular opinion at the time and needed time to consider the subject. Although, two of the respondents answered with standard roles of Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

Other interviewees, when talking about CIOs, were either in support of CIOs taking on information security role additionally to existing one or strictly against and mainly in favour of a separation of security role and IT department. This separate role could be a compliance officer or a security officer. The respondents stressed that the name is not crucial, as long as the duties are defined clearly and accurately.

Another problematic aspect that was discussed is the separation of security among IT department and business units. Two respondents had expressed immediate necessity in having these two separate groups in alignment with the overall security posture and strategy. They had experience with many examples where decisions were made without proper security in mind by some business units which lead to delays and incidents that could have been avoided. As a suggestion to this situation, the interviewee indicated the requirement of a technical security lead in every business unit, who are collaborating among themselves and with the IT department. There might be a need for an overall head of technical leaders. This role can fall either on compliance officer, CISO or any other appointed in coordination with enterprise structure.

One of the participants concluded that CIO would primarily cover defensive or preventive security. The aim of this is that there will be enough resources only for intrusion detection and configuration of the controls for the prevention of incidents, such as security awareness and training, access management and control.

CISO would introduce proactive security in addition to the defensive role. That includes but not limited to, vulnerability detection software and threat intelligence suites.

4.3.1 Crisis Management

When asked about disaster handling, respondents generally understand it as a natural disaster that destroys physical premises, infrastructure or personnel. None of the respondents has answered that they do crisis handling for the IT-related incidents at the board level. However, they let me know that crisis handling departments are available, but boards of directors are not involved directly and not aware of the information security drills.

While analyzing DNB's financial report for 2018, DNB has had cyber security drills and crisis management plans established and tested during the last year. Same is valid for Telenor, as it has information security drills since 2016 [53]. Other financial institutions have not identified such information.

Statkraft is another organization that had information security incident response mentioned in their report from 2018 [51]. The Emergency response management was introduced in 2017, and it held extensive training in 2018 for various crises scenarios, including cyber-attack simulation.

The rest of the organization didn't have information on crisis management with regard to information security.

4.4 Information Security Metrics

Out of the six interviewed respondents, only one has confirmed that the board was presented with a security report with high-level Key Performance Indicators (KPI).

One of the interviewees was the information security professional from a major security firm in Norway. This firm works closely with senior leadership and boards of various organizations and provides a wide variety of services. One of those services is virtual CISO, where the security firm takes the role of CISO and performs necessary managerial work. Virtual CISOs are answering and reporting to CEOs.

This security professional suggested that the board of directors would/should be interested in the following metrics. These metrics are part of question 25 (Appendix A).

- Level of maturity of Security Organization
- Successful intrusion attempts
- Quality of equipment used (state-of-the-art, degree of patching, etc.)
- Level of maturity of operational processes
- Number of business critical incidents
- *Number of compliance breaches
- *Number of high probability incidents

From security professional's words, those marked with stars (*) are dependent on the type of report board members receive. In that, these metrics are not always necessary, as they are not top-level metrics and would not be of interest to the board in some situations. Though, if a specific internal audit was requested, then these will appear in the report aiding a more detailed look. For example, as a report of an audit of a specific system.

There was a lot of fluctuations in the board members' responses. Some preferred to have almost all from the list, and the others were more modest in choice. Though, one of the respondents has answered similar to the security professional.

Table 6 shows the metrics used in the questionnaire and the choices of the respondents. The last column represents the Security professional's opinion on relevant metrics. This professional is working with Senior leadership on a day-to-day basis.

Metric	**1st**	**2nd**	**3rd**	**4th**	**5th**	**6th**	**S.P.**
Degree of application of Security Policy			X		X	X	
Level of maturity of Security Organization	X			X	X	X	X
Attacks originating from or using employees or other stakeholders as attack vectors		X			X	X	
Quantified losses related to assets (information, infrastructure etc.)			X	X	X	X	
Successful intrusion attempts	X	X	X	X	X	X	X
Disclosure of non-public information (breach of encryption)		X	X		X	X	
Attacks addressing the physical premises		X					
Quality of equipment used (state-of-the-art, degree of patching, etc.)					X		X
Level of maturity of operational processes	X	X			X		X
Number of attacks addressing information in transit (communication lines, networks, etc.)		X				X	
Degree of resiliency of Supply Chain (supplier agreements, security risks encountered in IT acquisition)				X	X		
Number of business critical incidents		X	X	X	X	X	X
Number of compliance breaches	X				X	X	*
Number of high probability incidents					X	X	*
Security Awareness							X
Information security personnel availability and competence							X

Table 6: Information Security Metrics as identified by respondents [3, 4, 5, 6, 7, 8, 9]

The last two metrics were suggested by the security professional but were not in the questionnaire. During the conversation and answering not directly to this question, one of the respondents mentioned that it is useful to know the competence and availability of the staff working with Information Security.

So, if we look at the responses of the board members and compare to the security professional, there is a mismatch and seems that board members are interested in much more metrics than security professional would suggest to them. One explanation can be that board members are unsure what to expect since they never received security reports. And as they lack control over what is happening, they would prefer to see as much as possible.

Information Security Metrics are essential. Before measurements are in place, there is no real understanding of the situation. Strategic goals come with the KPIs, and strategic security objectives should also come with major KPIs. These KPIs should be built on a hierarchy of lower-level, more detailed metrics.

4.5 Information Security challenges for board of directors

In this section, I am going through the answers from the questions regarding challenges in cyber security for members of non-executive boards.

4.5.1 Identifying biggest challenges

The questionnaire included a question (#26 - Appendix A) where respondents were asked to set a priority to the most significant challenges. There was a possibility to add extra challenges, but none of the respondents chose to do so.

- Knowing the legal responsibilities of the company
- Understanding the technical complexity in cyber security of the company
- Receiving the relevant information on security environment (reporting)
- Knowing the risk appetite of company stakeholders

If the answer got first priority, it got 5 points, second priority - 3 points, third - 1 point, no priority - 0 points. Answers varied extensively for this question (see Table 7).

	1st 5p	**2nd** 3p	**3rd** 1p	**None** 0p	**Total score**
Knowing the legal responsibilities of the company	2	2	1	1	**17**
Understanding the technical complexity in cyber security of the company	2		4		**14**
Receiving the relevant information on security environment (reporting)	2	4			**22**
Knowing the risk appetite of company stakeholders	2		1	3	**11**

Table 7: Ranking of the challenges by priority. Numbers show how many respondents set certain priority to a selected challenge

Let's look at what was the prevailing first priority. Each of the answers was chosen by two respondents. The reason for that was that two respondents identified two answers as first priority.

As for the second priority, respondents agreed more, and four chose "receiving relevant information" as their answer. Similarly, respondents agreed on the third priority to be "understanding the technical complexity", four persons have chosen it.

Three respondents have given no priority to the "knowing the risk appetite of company stakeholders". Same persons have given the first two priorities to "knowing legal responsibilities" and "understanding technical complexity".

Looking at the total score, the most important one comes out to be "receiving relevant information", the second "knowing legal responsibilities" and the third - "understanding technical complexity". It is curious that risk appetite was not considered as a challenge for the participating directors. I would have assumed it should have been in the first place by total score. This result can get focus in further research.

Two interviewees had similar answers, in that, they gave first priority to "knowing risk appetite" and second to "receiving the relevant information".

Another two had completely identical answers:

- 1st - "receiving the relevant information",
- 2nd - "knowing legal responsibilities",
- 3rd - "understanding technical complexity",
- none - "knowing risk appetite".

One respondent has given the most dissimilar response, "understanding the technical complexity" was given first priority, "receiving the relevant information" - second, and third - "knowing the risk appetite".

During interviews, other challenges were pointed out as important but were not given any priority. One of the respondents explained that when it comes to information security, it is not a mature field from the perspective of the board member. While it is addressed internally in the company during day-to-day operation, the board of directors is not aware of all aspects which are handled — for example, the state of the human resources availability and their level of expertise.

4.5.2 Externalization of cyber security

This section is expanding on question #27 (Appendix A) connected to experience with challenges in cyber security. All, except one, have given answers to this question, the last one has abstained due to lack of experience with the subject of information security governance as a board member.

Externalization of cyber security is the one which was chosen by all five. Outsourcing of security to security firms like Mnemonic was given as an example. The challenge is with the ability to outsource but at the same time have control. In reality, security can never be outsourced fully, as there should always be a contact point in the organization responsible for the overview, oversight and direction. Another unfortunate side of outsourcing security is emerging for companies with smaller budgets. Better security firms are unattainable due to cost. Therefore they will decide for cheaper alternatives, such as the decision to buy security software instead of security as a service. Intrusion detection can never be an answer to all security risks.

Additionally, companies are creating partnerships with service providers from the same sector that have more experience than others in secure operations. Thus, organizations have trust in those specific companies to govern security adequately. That can lead to many firms in one sector being brought down simultaneously during one attack on a service provider.

Also, the challenges are quite apparent in the companies which are part of a larger concern. These corporations have global IT departments where information security group is just part of it. The challenge here is that smaller daughter-firms are set into hard limits and sometimes unable to perform their standard operational tasks efficiently. Exceptionally inconvenient is the time it might take for global IT department to resolves issues (some geographical locations are not as prioritized as others). Boards of directors of such daughter organizations are not able to overthrow the routine set by the concern, especially when it comes to IT operations. These boards are, in a way, "puppet" boards with no real power to decide.

At the same time, smaller daughter companies establish separate IT infrastructure. Those are normally maintained by daughter-firm security personnel belonging to a specific business unit. In such cases, project or business unit related information security is not adequately aligned with overall security strategy and poses additional risks. Although, other examples exist that represent the opposite, where project security personnel are far better experts than the IT department's information security group personnel.

4.5.3 Conflict of interest

Conflict of interest between stakeholders and executive management was identified as a challenge by two out of five respondents. They have experienced it or understand how that can be a challenge for the organization they are governing.

Among issues the following ones were given as examples:

- operational issues were decisions are made regarding the equipment, software and services. The conflict might arise between security strategy and vendor selection when business units are disconnected from the overall security strategy. Hardware, software and services that are cheaper and have insufficient security focus might prevail and get purchased by the organization in contrast to the security strategy direction.
- Similarly, outsourcing might be desirable by executive management, but in conflict with the view of the stakeholders. Here, we can have examples from a health sector organization where people would like to have their personal data stored in the country and not in the cloud solutions outside of the country. Furthermore, outsourcing of the development presents identical conflict where management has their own incentives while stakeholders have others.

4.5.4 Information asymmetries

Two types of information asymmetries are present for organizations and board members, also identified in the IMF backed article by Kopp (2017) [54]:

1. the information to make the best decisions to manage cyber risk
2. the information disclosed to the shareholders and stakeholders of the company to preserve the reputation

The first type of asymmetry comes from the reports on the past security incidents in the sector or the world. It is not always possible to get information on the most recent situation, and the information might be incomplete or non-existent as some incidents are not disclosed. Most of the time, zero-day attacks are impossible to predict, and therefore, they are not included in the risk management system.

All of the board members have agreed that information security is a complicated field to operate.

Three of five board members have identified information asymmetries as a challenging area in information security. All three are board members in IT-intensive organizations.

None of the respondents gave specific examples to this challenge but agreed on importance of understanding such a challenge. Disclosure of the information on recent security incidents and overall security posture should be treated the same way as disclosure of sustainability of the organization. Shareholders will appreciate the information for more informed decision making. And stakeholders will understand that the subject of information security is governed by the board of directors and executive management.

4.6 Information Security focus within Board of Directors

From the interviews, it was clear that information security is an emerging subject and was not discussed as a standard and common topic. Out of 6, only two have answered that it was a fixed topic but only sometimes in recent years. Another respondent said that this subject was introduced just during the fall of 2018. Board of directors was given a task to familiarize itself with ISO 27002 standard for adoption during the coming years.

After a look at the financial reports, it is apparent that some organizations are setting focus on Information security by disclosing facts on incidents, security strategy and future goals. Others are entirely omitting it. The third group consists of the organizations which mention it briefly.

Those which included only brief information are Hydro, Yara, Orkla, Norges Gruppen, Statnett and Aker Solutions. These all shared more or less similar information: cyber risks recognized as ones of the most important, that they have specific controls in place, but no mention of the information security strategy. From such explanations, it seems that information security is handled but only from a technical perspective, i.e., security controls.

Hydro has included cyber risk into the list of major risks [46]. The description referred to several initiatives that are in place to avoid information security incidents. They have also had a focus on security awareness training in 2018. In the risk review, they pointed out that security controls which are in place might prove to be inadequate. And that is exactly what happened when Hydro was infected with ransomware and lost quite a large sum trying to return to normal operations. The report did not contain any information on security strategy or board involvement.

Eidsiva was the one which surprised by not including any information on cyber security [49]. While Statnett and Stakraft were much better and their reports contained moderate amounts of information regarding information security. From Statnett's report [50], it is apparent that there are security controls and systems in place. They are using a 4 area approach: "anticipate, identify, prevent, react" [50]. This type of information points into a direction of the possibility of a security strategy. Though it is not mentioned explicitly and it is not clear if the security programme is connected to the enterprise strategy and boards of directors.

From the financial institutions, KLP and Norges Bank had the least information in their reports, while Nordea had somewhat more and DNB with the most. Nordea had a strategy and defined information security as one of the strategic focus areas for 2019 [42].

4.6.1 Spotlight on Statkraft

Statkraft included information security into the chapter "Social disclosures" together with health and safety, labor practices and human rights [51]. They have also disclosed KPIs regarding incidents and their severity. The information was useful, though they have not included an explanation about some of the serious incidents: if they were resolved, how fast and the extent of the damage.

> Information security is of the highest priority and Statkraft follows international good practice for information security management. The aim is to build and continually improve a strong information security culture that ensures the confidentiality, integrity and availability of Statkraft's information. [51]

All of those statements give hope and assure that the information security governance is in place. Security strategy is not explicitly mentioned, though previous points suggest that it exists. It is unclear how much board of directors is involved, and if the security strategy is aligned with the enterprise strategy.

4.6.2 Spotlight on DNB

One of the organizations with the most information on Information Security was DNB. Annual financial reports and "Risk and capital management" reports for 2016-2018 years show the development and changes in risk management reporting [44, 55, 56, 57]. In 2016 report [57], information security is mentioned but not as extensively as in 2017 report [55]. In 2017 report cyber security occupies its own chapter. That could be due to change of Basel III requirements [18].

In the 2016 report, information security is mentioned only briefly and mostly focused on operational stability. That is also visible from the high-level metrics: (1) Operational losses and significant operational events; (2) Number of critical IT events; (3) Data quality in the registrations of customer information [57]. These metrics are not very representative of all security risks. In the same year, DNB has established a three-year plan to reinforce the information security and defense against threats [55] (this was mentioned in the 2017 report and not in the one from 2016).

Fortunately, 2017 report comes with extensive cyber risk information [55]. Here, even definitions and taxonomy of the relevant risks was explained. While in 2016 report it seemed that information security was treated as a technical problem, in 2017, it was expanded to managerial dimension: "the group management team and the Board of Directors completed training in information security" [55] during 2017.

DNB's security department is called Group Security and is supervised by a CISO who is reporting to group executive vice president for People & Operations [55]. In the latest report, it appears that DNB has heightened the information security control and management [44, 56]. The information is clear and stresses crucial areas. The board had a whole month of April dedicated for the work on the action plan and threat evaluation [44]. Following improvements were established during the last financial year by DNB:

> multiple levels of robust security measures, continuously enhancing and upgrading IT solutions, strengthening security competence among employees and further developing national and international cooperation

Additionally, DNB has carried out crisis management drills with the newly established crisis management group for information security incidents [44]. As indicated in the report [44], DNB has divided operational security from overall security work and created separate units in 2017. That has set focus on strengthening the information security posture, expertise of the employees. In 2019, they will push the plan further in integrating IT governance into risk management. That will accelerate the inclusion of IT risks into overall risks, and thus improve not only the governance of the Information security but DNB's posture against cyber threats [44].

Establishing of the compliance unit in 2017 and group privacy officer in 2018 is another aspect related to the information security and legislation. Appointment of the privacy officer was most certainly triggered by GDPR, which took effect in May 2018 in the EU.

Identifying the need to incorporate IT risk into overall risks shows that DNB is on the right track with regard to Information Security Governance and correct signals are sent from the executive management and the board of directors to the shareholders and stakeholders.

In the latest financial report, DNB points out the importance of viewing risks and opportunities from a long-term perspective. DNB owners indicated that these risks and opportunities are to be reflected in corporate governance.

DNB has security frameworks in place and also has been implementing a system for Governance, Risk and Compliance (GRC) in 2018. "This tool is meant to support the implementation of operational risk management, compliance and internal control over financial reporting" [44]. Part of this system is the framework for risk appetite, which "represents the operationalization of the policy and guidelines for risk management". This type of implementations is a strong sign of proper risk culture. It is clear that Information security risks are getting included in the same system and providing adequate management and oversight.

The same GRC system is used to follow up financial, operational and strategic performance indicators. That covers both financial performance and also non-financial values monitoring.

4.6.3 Spotlight on Telenor

Another organization with a substantial amount of information in the financial reports is Telenor. It is the leading telecommunication operator providing a wide range of services including mobile, TV and broadband services. They are operating in many countries, having strong positions in Scandinavia and Asia with almost 20 000 employees.

In 2015-2016, Telenor started transformation processes in the whole organization, including restructuring the board of directors [53]. Digitization and digitalization are the drivers of this process. Since 2015, Telenor has been conducting training to adjust and prepare personnel for existing and forthcoming new technological challenges [53].

Recently, they have implemented a new digital channel called MyTelenor, which is gaining popularity and has already grown to 11 million users. Various services are developed with the national specifics of the country they are operating in [10].

As the shift from simply telecommunication provider to a digital services provider continues, Telenor looks at new technological opportunities and innovation, such as machine learning (ML), artificial intelligence (AI), self-healing and cognitive automation of workflows [10].

> Telenor has embarked on a vital transformation agenda to adapt accordingly. Failure to respond to these dynamics and to drive a change agenda to meet the developing demands in the marketplace, may impact Telenor Group's position in the value chain, service offerings and customer relationships.

The same technological opportunities are helping "both at operational and business process layer, uplifting security capabilities, processes, competences, governance and vendors management" [10].

Cyber security is recognized as a key risk at Telenor. It is seen as a high priority risk since security strategy was established in 2015 [53]. Telenor has set a target for 2020: "to have security at the core of everything the company does, in order to protect people in their digital life" [53]. Various Security policies and manuals were updated during 2016. At the same time, all business units got their own Business Security Officers to reinforce the local security organizations.

Telenor has a unique set of committees compared to other firms listed on the stock exchange. The board has four committees: the Risk and Audit Committee, the People and Governance Committee, the Sustainability and Compliance Committee and the Innovation and Technology Committee.

Decisions are made by the full board, but reports and in-depth information are gathered and prepared by each of the committees. Very rarely, committees are deciding on their own but with specifically given permission of the whole board.

The Risk and Audit committee is a standard committee that supports the board within risk management, internal control and audit. People and Governance Committee supports such areas as "governance, remuneration, leadership and culture development" [10]. Sustainability and Compliance Committee covers responsibilities concerning climate and environment, human rights, labour standards and anti-corruption.

And lastly, the Innovation and Technology Committee is responsible for digital transformation in rhythm with the state of the art of the technology, and most importantly, "monitoring the formulation and execution of Telenor's security strategy, security governance, and operational status with an emphasis on cyber security as a top enterprise risk" [10, 58]. This committee is the newest one and was established in June 2016. The focus since the inception was on technologies that can affect their business model and uncover new opportunities. The security is a huge part of this committee's focus since 2016 and into the future [53].

To avoid and limit the number of security incidents, Telenor has established "a global function and implemented advanced global monitoring, surveillance and incident handling" [10]. They have developed a long-term security strategy that covers the whole group. The focus is on establishing global security operating model and constant improvement of crucial security competencies in all organizations that are part of Telenor Group.

> To Telenor, security is our license to operate.
>
> Telenor Group

There are two operational groups available: Telenor Norway Security Operations Centre (TSOC) and the Telenor Computer Emergency Response Team (TCERT). TSOC is dealing with thousands of incidents [59] on behalf of Telenor and its customers. These are the types of events which will cause harm and damage if not stopped on time. Telenor calls TSOC as the first line of defense [59].

TCERT's primary purpose is to investigate and deal with advanced threats such as digital espionage and sabotage.

Both groups required considerable investments to raise personnel's competence to get the advantage of new technologies and tools available in the information security field.

Telenor has completed a survey among executive management of Norwegian companies [59], and found out the most significant challenges for the businesses in Norway are:

- Information security competence, as it is hard to understand the field
- No overview over security posture and what part of the business is vulnerable
- no knowledge on who can help and who to contact in case of an incident

The first is the most prevailing, and it shows that Norwegian firms are not comfortable with the level of expertise among employees. That, however, doesn't reflect on the board of directors stance. Though, it is important to remember that many executive directors are also employed as members of the board in other organizations. And the perceptions and experiences as an executive affect the work as a board member.

4.7 Summary

There are several areas of Information Security that were covered by the questionnaire and reports:

- Expertise
- Metrics
- Challenges

Additionally to that, three organizations' financial reports were analyzed and presented in the last section, as they contained more information on cyber security than others.

Main findings

- Organizations with higher IT intensity tend to hire IT experts to the boards.
- The board members understand the gravity of information security threats and risks.
- Own perceived expertise is quite high for digitalization. And a little lower for cyber security but in the upper level. That could be due to most of them having technical backgrounds.
- Respondents wish to have more cyber security related training. From the interviews, none had received such training. From the reports, DNB and Telenor have indicated specific training for the board of directors in information security. These two firms, most likely, do not represent the common practice, and most of the directors in Norwegian organizations have not received cyber security training.
- Information security experts are available to the boards, both internal and external resources.
- Information security roles within the organization gave the most inconclusive results. Respondents had different opinions. Some were fine with CIOs taking information security role, others were quite against and suggested a separate role, which can be CISO as well.

- Information security crisis management is not a common topic for boards. Only three organizations had mentioned security drills in their reports.
- Most of the respondents were part of audit and risk committees, specifically those with the IT background.
- The directors were concerned that they did not receive security reports. The interest in such reports is particularly high. They wish to see the overall status of the security environment in the organizations, and additional details on risks and specific metrics.
- Metrics are not mature yet; boards are not informed, generally. Financial reports present a better, more controlled picture of ISG. There was a disagreement between interviewees which metrics are right to have in the security reports. That can be due to a lack of experience with such reports.
- The challenges understood or experienced by board members
  - The externalization of information security was a known challenge for all respondents who answered.
  - Information asymmetries were identified as a challenge by three of five
  - Challenge with conflict of interest is identified just by two of five.
- "Knowing the risk appetite of company stakeholders" is selected as a first priority only by two respondents
  "Receiving the relevant information on security environment" is the first most important by the score among respondents and chosen by the most as a second priority challenge.
  "Understanding the technical complexity in cyber security of the company" was given the third priority by most of the respondents.
- Telenor, DNB, and Statkraft are examples that are disclosing cyber security related information. The reports are bringing transparency and increasing the trust of shareholders. These three companies are setting a premise for other organizations to follow.
  The security strategy is apparent from the reports, and that boards are involved and supervise relevant risks.

The above results are serving as the input for chapter 5 "Discussion: Qualitative analysis".

5 Discussion: Qualitative analysis

Interviews and financial reports provided me with information to draw several conclusions. Though it is not a high number of interviewees, some results are quite similar, and some are a reasonable basis for suggestions.

Using New governance model [1] and qualitative analysis techniques, such as coding I will create a sub-model and suggest what improvements should be made to better Information Security Governance (ISG) based on the results from interviews and financial reports.

Analysis of the board of directors and their expertise is a study of the social aspect of a complete socio-technical system, that is, information security in the organization. This whole system comprises of the two substantial parts – social and technical – where the social part is regularly forgotten. Though it often plays a leading role.

5.1 Applying New Corporate Governance Model

In this section, I am following through main elements of the New corporate governance model and explaining insights from the interviews and reports which are already as in the model or the ones needing adjustments according to the model. In section 2.1, elements of the framework were revealed to be as follows [1]:

Keep it

- Situational
- Strategic
- Integrated and
- Controlled

The next subsections are following the same order as elements of the framework. "Keep it controlled" section puts focus on a framework for the governance of information security by the board of directors.

There are companies in Norway which have already implemented some of the elements of the New governance model. Though it is clear that there are areas that can be improved in large companies. As for smaller firms, there are even more significant benefits for them.

5.1.1 Keep it Situational

As covered in section 2.1, New governance model emphasizes on the dismissal of a "one-size-fits-all" approach. Considering the organizations I have looked at, all are highly focused on the country they are in, type of sector and business they are operating. All in all, I would assume Norwegian organizations are well calibrated to the "situation" surrounding their businesses. In other words, they are adequately prepared regarding the normative context, corporate governance development level, and size and complexity.

Lately, media publishing reports on various security incidents and attacks directed towards Norwegian organization has become a regular occurrence. Large corporations, governmental organizations, and critical infrastructure operators are among those, and therefore, media gives much attention to such incidents. These incidents had different severity levels, but all belonged to the higher levels. Thereby, the Norwegian government is aware of the immense importance of information security governance and is continuously working on updating and introducing new legislation. Current information security legislation and regulations in Norway were described in section 2.7. Though the pace is fast and legislation is lagging behind.

All of the organizations, mentioned in this research project, have had information stipulated by the legislation available in their financial reports. Though each industry has its own regulations as well. Moreover, in terms of regulation and disclosure of exposure to risks, several industries are better regulated than others, e.g., financial and banking sector have stricter risk regulation and have to produce an additional annual report.

Many production companies disclose sustainability key indicators. That is an ongoing tendency, and even financial institutions are releasing analogous information. They have started ranking financial products on how sustainable they are, i.e., to what extent businesses behind the financial product are sustainable [44].

That gives an idea that comparable disclosure can be done about information security. High-level security performance indicators should be included in the financial reports. At the same time, the following information should also be reported: what has been done and what will be done to improve those indicators.

Another interesting aspect that came up through all interviews is the Norwegian "optimism" toward each other. The first example of it – trust between board members. In smaller firms board members tend to trust the one with some IT background with questions regarding information security. This one member plays the role of a "mini-CISO" and suggests decisions on subjects without enough expertise. The rest of the board supports the decisions typically unanimously. That might hold up in some situations, but in most cases, it is a sub-optimal solution and should be avoided.

This "optimism" comes through in other examples, such as full trust to the vendors and suppliers who live by the "same trust" rules. These boards are expecting sound and proper level of security and management from all vendors without additional controls in place. Pure trust and optimism are not going well with such field as information security.

5.1.2 Keep it Strategic

Keep it Strategic element of the New governance model implies a "strategically targeted composition of the board, open-minded culture, effective board structure, and shareholder and stakeholder oriented measures" [1].

From the interviews, the respondents appear open-minded and focused on doing an excellent job as a board member and holding responsible to not only the shareholders' requirements but also stakeholders'. Though, it is not easy to generalize just from these respondents toward all of the boards in Norway.

Boards are comprised of people who are aware of the business, and suitable to understand the market and necessary steps for the organization to succeed.

The New governance model suggests a maximum of seven members [1]. Most of the organizations I looked at are large firms and have more than a maximum of seven members and more than two committees. Notably, the medium and small companies I reviewed had fewer directors, which is correct and in line with the size of the organization.

In Norway, all organizations with more than 50 employees should have employee representatives on the board. For larger organizations, the number should be two or more. All of the organizations I have examined had the correct number of employee representatives: two, three, or in some cases, even four (Tab. 1). Per the New governance model, two employee representatives out of seven are the optimal composition.

The New governance model also suggests only having two committees for large organizations: integrated audit and risk management committee (ARMC) and integrated board management committee.

Norges bank		Audit com.	Compensation com.	Ownership com.
Nordea	Risk com.	Audit com.	Remuneration com.	Operation & Compliance com.
KLP	Risk Management com.			
DNB	Risk com.	Audit com.	Compensation com.	
Orkla		Audit com.	Compensation com.	
Hydro		Audit com.	Compensation com.	
Norges Gruppen		Audit com.	Compensation com.	
Telenor	Risk and Audit com.	Sustainability and Compliance com.	People and Governance com.	Innovation and Technology com.
Yara		Audit com.		HR com.
Eidsiva		Audit com.	Compensation com.	HR and ethics com.
Statnett		Audit com.	Compensation com.	Project com.
Statkraft		Audit com.	Compensation com.	
Aker Solution		Audit com.		

Table 8: Committees of the Norwegian boards of directors

With the connection to information security, first and foremost, I was interested in how boards were handling general risk oversight. Did they form separate committees for that? What types of risks are governed by those committees?

As seen in Table 8, the majority of the boards in Norway have Audit and Compensation committees. For most of these organizations, the audit committee helps with oversight of internal control and financial reporting. They do not handle different types of risks and risk appetites of the shareholders and stakeholders. In other words, even if this audit committee governs risks, they are not overseeing all types that the company is exposed to.

New governance model has recognized the need to combine audit and risk in one committee for complete picture over the scope of the risks and better alignment of risk appetite with controls.

From Table 8, Telenor is an outlier with four committees and ten board members. Each independent member is a member of at least two committees. This composition and structure feel cumbersome, and committees are overlapping in their tasks and focus areas.

Regarding information security, we can look at the Risk and Audit committee and the Innovation and Technology committee. Telenor has put the Innovation and Technology committee to the task of handling cyber security. At the same time, Risk and Audit committee is involved when preparing a complete overview of the risks. So, these two committees are overlapping on information security risks. Therefore, Innovation and technology committee feels redundant as a board committee. However, as a council to the board, it would be perfect.

In DNB, some of the directors sit in both audit and risk committees. Therefore, there is a premise for combining those as in Hilb's model. In KLP, there is only one sub-committee, and it is a risk committee. At least two members of that committee have an IT background.

Members of the audit and risk committees are the ones expected to have higher expertise in risk management. Here, I would add another requirement to have a better understanding of information security risks than other board members. Again, there is no requirement to be an expert in Information security. Board members should realize that for them *expertise* means expertise in governing cyber security and not in-depth technical knowledge.

Aligning the Information Security strategy with the overall strategy is the main subject necessary to understand the overall posture and threat landscape. From the financial report with superficial information on information security, it was hard to understand if security strategy and overall strategy align. In my opinion, this shows that they are not fully aligned, though recognized and existent.

As stated in [26] the best for most organizations is to have one IT expert on the boards. And I would add to that, one information security expert is also necessary. Authors have also suggested a separate IT committee within the board. In my opinion, the best would be that the full board allocates time to consider technological development of the organization and if there are opportunities for competitive advantage. And information security expert member is there to help direct the rest of the board towards balanced decision and strategy.

5.1.3 Keep it Integrated

Keep it Integrated element of the New Governance Model implies four critical processes: targeted selection of board members, targeted feedback on performance, targeted compensation, and targeted development [1].

If the Information Security thread goes through all those processes, then the board is on the correct way of sound and strong information security governance.

Selection of board members should have a focus on changing perspectives of the organization and new risks it is exposing itself. E-banking does not have the same risks as conventional banking. Physically enclosed production facilities have risks that are adding up to the new ones if the facility goes online as a smart production site. Board members that do not accept and understand changing risk landscape should be exchanged. Otherwise, the organization will not reach its goals.

Digitalization and transformation towards complete automation and robotics set the strategic goal to another level, and thus, board selection has to follow.

At the same time, the board of directors should be developed and get courses and necessary updates on possible opportunities and risks. And for information security risks, the threat landscape and technology are exceptionally fast-changing areas that need to be followed up closely and precisely.

The correct expertise is vital in connection to information security. It is not enough to simply understand the gravity of the situation. It is crucial to be able to ask correct questions and react if the risk is too high and see where the opportunity lies before it is too late.

New members that are missing specific training should get one as fast as possible. Development of the board members should be monitored and adjusted by the integrated board management committee.

5.1.4 Keep it Controlled

Keep it Controlled element of the New Governance Model focuses on the functions as in Figure 1. The board should take on a "control-preneurship" role and not just a corporate administrator's role [1]. That means that the board should balance between direction and control, entrepreneurial actions and simple administration, short-term results, and long-term sustainability [1].

Among those I interviewed, I can conclude that two presented themselves in position for "direct and control" role. Others were more prone to a corporate administration role. That in itself does not mean that these four respondents are bad board members; they have other strengths, roles, and focus.

Information Security Governance Framework

Information security is the one risk that is valid for all organizations in Norway. Everyone is using emails, PCs, and are online almost all the time. The organizations are recognizing the importance of information security governance. Though, from interviews and financial reports, information security governance focus among board members is not developed to a mature state yet. That said, all of them recognize the threats and working in the correct direction.

In larger organizations, there are already specific systems in place that support board members. These systems usually are corporate administration tools for better internal control and governance.

Three of the six respondents are employed to the board in financial organizations. Moreover, financial organizations are coming very well off from the reports. Comparing their answers and financial report information, I can say that I got a more positive impression from the report than from the respondents themselves. That points me in the direction that if the information about information security presented in the report is superficial and only mentions that its gravity is understood then the board is not giving enough focus to cyber security governance.

The financial reports of DNB and Telenor had extensive information on cyber security compared to other reports [10, 44]. It concerns that before the board of directors are proficient in the information security governance, substantial incidents might take place and do extensive damage.

I have developed a framework for information security governance (Fig. 3) based on New governance model (Fig. 1) and ITGI's information security governance framework (Fig. 2) and several insights from financial reports. The framework shows the board of directors how different elements fall into place in the ISG.

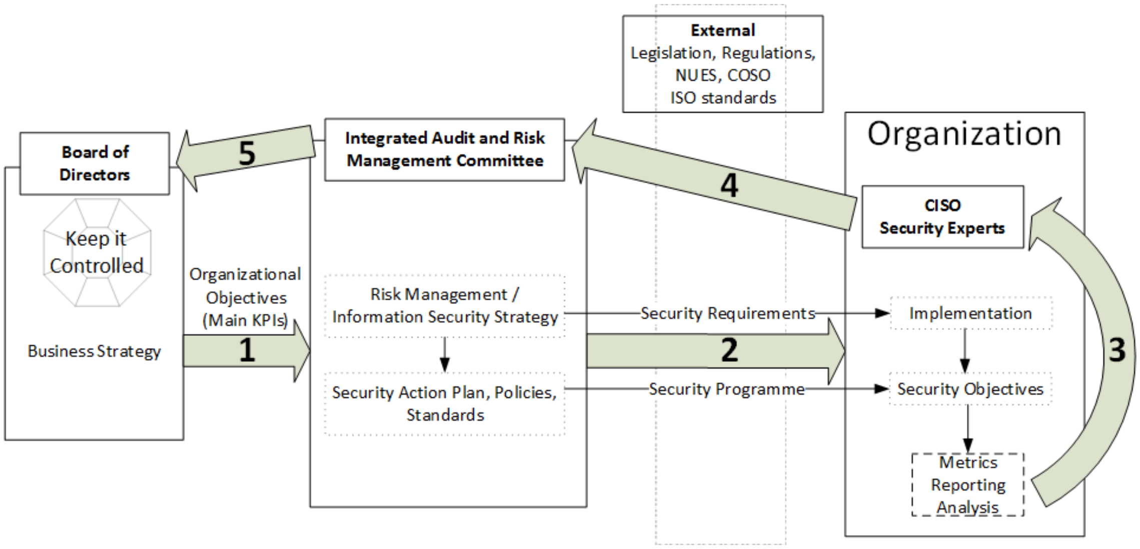

Figure 3: Information Security Framework based on New governance model [1] and ITGI framework [2]

The process has five overarching steps:

1. Board of directors works and prepares strategy together with executive management and presents the organizational objectives.
2. These objectives serve as an input to the Integrated Audit and Risk Management Committee (ARMC) that works closely with the CISO and security department and draws up an information security strategy. ARMC should always feel comfortable in developing information security strategy by involving CISO or other security experts from within the organization or outside of it. That can also be a special assembled security council closely working with ARMC and the whole board.

   The strategy, usually, produces elements of the security program, such as action plan, policies, standards. The outcome is affected by the relevant external frameworks, such as regulations and international standards. Security requirements and programme are always made in compliance with the current legislation and regulations.

The departments, business units within the organization receive all the necessary enterprise documents for adaptation into next level system-specific policies, guidelines and manuals. All of the prepared policies must be implemented and maintained. The implementation of the security programme and requirements achieves security objectives.

3. When a strategy is developed, a particular hierarchy of metrics is established at the same time. The board usually is interested in the top-level KPIs, while operational departments deliver the lower-level KPIs that serve as building blocks to the high-level KPIs.
   When the security objectives are met or at a specific time in the year, all of the KPIs are gathered and included in a security report. This report demonstrates a comprehensive overview of the security posture of the organization. The report is then forwarded to the CISO or the security lead.
4. CISO or the security lead is preparing a concise security report appropriate for the board of directors. ARMC should have a meeting where CISO will present this report and will be open for inquiries from the committee.
5. At last, either ARMC presents the report to the full board and if necessary raises concerns or actions requiring a full board decision. The full board can be attending the CISO presentations as well.
   Security report should be served as a starting point for what should be disclosed in the annual report. The discussion should be held by the full board.

With this 5-step process board of directors is "keeping control" over the information security programme.

The information on external legislation, regulation, and standards should be reflected in the financial reporting as well.

This process of information security governance is cyclical and regularly repeats in order to better the governance and maturity of the information security programme.

When it comes to the council to the ARMC, it would be valuable to require certified personnel. Certifications as the following should be considered:

- Certified Information Security Manager (CISM),
- Certified in the Governance of Enterprise IT (CGEIT),
- Certified in Risk and Information Systems Control (CRISC),
- Certified Information Systems Auditor (CISA)

Information Security Metrics

Information Security Metrics and measures are a crucial element of the Information Security Governance. It is not possible to control anything when there are no measures and feedback on the performance of the implemented controls.

All of the respondents agree that they are interested in seeing reports with security metrics. I have learned that only one of the six has seen security report as a board member. Moreover, it was presented only once so far.

Another vital bit of information, that the interviewees shared, is that the importance lays not only with such report but also what is presented and how. The report should contain only essential metrics connected to the strategical objectives to present the security posture of the organizations how it supports the strategy. If the report is requested in connection to a specific inquiry, then metrics should be in line with that.

The metrics should be presented in a transparent manner, where metrics are ranked as more important than others. For example, if one metric out of ten shows negative or worrying signs, then it should be clear if other metrics have the same importance and weight as the negative one. With such a report, directors might think that nine out of ten positive results is a good outcome, when in reality, that one negative metric has more weight than all the others combined.

Absence of security reports presented to the board can indicate a lack of information security strategy approved by the board. Typically, if the board is involved in the development of a strategy, they work out efficiency and performance metrics that they would monitor. The most probable explanation to the absence of reports is that the information security strategy exists but is not aligned with the enterprise strategy and only maintained by a security department without oversight from the board.

Security metrics right now are not mature, and not always represent what is really happening. The reason for this is that many measures are representing past events, for example, the number of attacks in the past month. Those metrics are still necessary, but they are not forward-looking enough and it is hard to measure future risk from them directly.

Name	**Description**
Budget	The budget for operational IT and, particularly, outsourcing, investment and adoption of the new technology should be aligned with how much is allocated for the management of the risks related to those activities
IT priorities	Strategical focal points for IT strategy, and consequently, Information Security strategy are to be defined. Both of those have to be reviewed and updated regularly.
IT Assets	IT assets are documented and monitored. That includes data valuable to the stakeholders. IT asset interconnection is another aspect for the management to review
Relations with vendors and partners	The plan for outsourcing, purchase of new equipment, software, and services should be clear and aligned with the strategy. Information security requirements should be defined and monitored. Additionally, cooperation with partners regarding information security threat landscape should be defined and followed.
Information Security staff and competence level	Information security personnel structure should be defined and approved. Competence level among these employees should be monitored. Risk assessment over employee workload is also advisable.

Table 9: Higher level Information Security metrics' areas

The need for forward looking security metrics in all sectors is fundamental. In Table 9, a list of measurement areas and descriptions is suggested; these were based on the suggestions from various reports and the report by BCBS on cyber resilience in financial sector [18]. These areas are valid to any organization. Lower level performance indicators would come under them and would depend on the various risks exposure, industry, and strategical goals.

5.2 Summary

Martin Hilb's New governance model assists with structuring and aligning the information security governance approach into a holistic and integrated corporate governance. The results and findings from the six board members' responses and financial reports provided me with information on the situation surrounding information security subject and boards of directors.

The Norwegian organizations are following legislation set in Norway, and in the countries, they operate in. They are compliant and trying to be sustainable. All of them are describing the changing era - the technological era. The introduction and implementation of online, smart, automated, and digitized processes is mentioned in all financial reports. It is promising that the largest companies in Norway are putting a focus on new technologies, sustainability, and social responsibility. At the same time, they are a little behind in disclosure of information security frameworks, risks, and other details in their financial reporting.

For the board of directors, it is not easy to start with proper ISG without any experience with it from before. It is apparent that boards of directors need at least one information security expert. Additionally, all board members should go through training in cyber security governance and information security risk management.

The model I have presented is based on ITGI's framework and the new governance model. The model gives an overview of the involvement of the board members and the integrated audit and risk management committee. The governance of information security is achieved in a more holistic and better way with the help of this model.

The list of metrics was suggested in the previous section. Even if every organization is exposed to their specific risks, the top-level or strategic metrics are more or less the same for every company.

6 Conclusion

In this research project, I tried to answer the overarching question on how Norwegian non-executive boards perform Information Security Governance in comparison with the New Corporate Governance model [1]. For that, I held interviews with six directors and one security expert. Additionally, I have investigated financial reports of 16 Norwegian companies.

To answer the overarching question, I needed to divide it to another four questions:

1. ***How is information security aligned with corporate governance and IT governance focus?***
   Let us look at the reports' analysis and what interviewees had said. All interviewees except one said that they had not received security reports. It means that they are not participating in security strategy development and security programme oversight. Thus, ISG is not alighned with the corporate governance.
   Three organizations stood out from the financial reports' analysis: DNB, Telenor, and Statkraft. They all had extensive information on information security and that the board is involved in the ISG. Additionally, Statkraft and DNB had disclosed the number of incidents. From that information, it is apparent that a security programme is in place with reporting and feedback to the board of directors. DNB and Telenor also specifically mention that they are working on strategic information security risks inclusion into enterprise risk management.
   From the remaining reports and some interviewees, it is apparent that the board involvement in ISG in Norwegian organizations is not at the desired level.
2. ***How is oversight of Information Security risks affected by the board's structure?***
   Those of the respondents who were not part of risk or audit committees were less aware of information security terms and challenges. They have had less to say concerning information security role within the organization.
   The boards with the risk committee show stronger due diligence compared to those boards without the risk committee. Same applies to information security due diligence. Existence of risk committees indicated the hiring of directors with relevant risk management background. All IT-intensive organizations chose to have risk committees. These companies also show better reporting and disclosure.
   This indicated that oversight of information security risks is affected by the board structure.
3. ***To what degree Information Security expertise is available among board members?***
   From the interviews, the self-perceived expertise of information security was not too bad. Three interviewees had an IT background and could be sitting with information security expertise, which is not utilized by the organization. The contradiction to the perceived high-level expertise is that board members did not receive security reports and make decisions on it. Most probably, they are disconnected from the security strategy, which is handled by the se-

curity department. Also, one respondent mentioned that they were asked to familiarize with ISO 27002. That is curious, in that, reading ISO 27002 can be tedious for board members without IT background.

IT expertise improves the firms' success rate. If the future of the company is dependent on technological development, it is vital to have members with IT expertise. These people are better suited for discovery and the follow-up of a correct course with new technologies as primary drivers. The same is valid for Information security – those boards with expertise and focus on information security will gain and achieve better results.

From the financial reports, it is apparent that boards of Telenor and DNB have information security expertise within the board because the security strategy is visible and more aligned with enterprise strategy.

4. ***How is the responsibility for information security risks distributed within the board?***

   The responsibility as in legal accountability lays with the full boards in Norway. The follow-up and control responsibility for the security risks is with the risk committee for DNB and the Innovation and Technology committee for Telenor.

   DNB has separate audit and risk committees; that means, the risks are covered either by both or some risks fall through because of the separation.

   The ideal structure for information security governance is to include an integrated audit and risk management committee.

   Both DNB and Telenor has started with this information security focus during 2016 and 2015 correspondingly. So, before those years, there was not much focus within the board. And 2015-2016 is quite late.

   DNB and Telenor are large companies that are the leaders in terms of reporting and disclosure. Statkraft is also worth mentioning. They used a layout in the annual report, which was easy to read and contained information on several metrics.

   These organizations are examples of the minimum reporting of information security, and other companies need to look up and implement similar reporting routine. Moreover, they should do it very soon, primarily because of the increasing frequency of security incidents.

   The directors are quite positive on the access to correct security resources, both internally and externally. The reason for this is that these directors represented mostly larger corporations. I would expect a different outcome for directors from smaller organizations.

This thesis covered the topic which has not gotten enough attention in the organizaitons and in the research environment in Norway. An information security governance model was developed as a result of the analysis of the interviews outcome, reports and available literature. The board of directors is the supreme governing organ but is often forgotten when security programs are implemented within the organizations. To close that gap, the board should use the presented model to understand better what is expected from them and how the ISG process is built. The directors should prioritize information security training in the near future. The analysis identifies inferences which can be used for an open discussion in the boards and organizations in general. The developed model should also be tested and expanded in future research. This research also shows that there is not enough support from the government, i.e., laws and regulations are behind the developments in the threat landscape and organizational control. The government should aim to create supporting legislation that helps to shape boards for the task of governing not only financial risks but other risks, including information security risks. The board development and training should be one of the topics discussed by the lawmakers and internally in the organizations. The requirement for a security disclosure as part of the annual report is an appropriate first step. Financial institutions are already creating similar documentation in risk reports. Thus, the premise is already there for the authorities to initiate the process.

The key findings were that even at the financial institutions, there is a lack of focus on information security on the board's agenda. That should change not only for the benefit for organizations but also for the sake of society. The adversaries are becoming more and more experienced and started to organize themselves. If the security strategy is not in place, then the outcome is going to be as devastating as the worst case scenario. Overall, it is well overdue for the boards and organization to pick the subject of the information security governance.

7 Further challenges and directions

This project was an exploratory study that was performed on a limited number of respondents. Here is the list of the possible further directions of the research:

- The first step is to gather more data, specifically survey an appropriate number of board members to have a good set of data on which quantitative analysis can be done.
  The more respondents, the better, but at the same time, there should be a focus on finding a diverse set of representatives: various sector, size of the firm, ownership type, various backgrounds of the members.
- Quantitative data can help with analyzing multivariate relationships. Probably, helping with investigating causality between variables. That will help with inspecting how the director's expertise affects the governance level.
- Variation in the data set will provide a basis for analysis on how each of the sectors is doing in terms of information security governance. Also, how smaller organizations are compared to larger ones with regard to cyber threats.
- Qualitative analysis can be expanded to shed light on what is disclosed in the financial reports and how it is compared to the responses in the interviews.
- A case study, done on one organization can help with understanding how the board is governing in reality and how far the theory is from practice. Here, every member of the board should be interviewed, and then annual reports and other materials should be compared to the interview results.
- If enough data is gathered there might be a premise for expansion and comparison to other European countries.
- The challenge of this type of research is that the environment is changing; the directors will get more training and will look at the questions in a changing way. That might also be positive for the research to follow-up the development of the expertise and success of the organization.

All of the above will generate results that would be invaluable for boards of directors and should be made available to them. Presenting the results would be even more beneficial.

Bibliography

[1] Hilb, M. 2008. *New corporate governance*. Springer.

[2] Institute, I. G. 2006. *Information Security Governance: Guidance for Boards of Directors and Executive Management*. ISACA.

[3] Respondent 1. 2019. Interview 1 on 30.01.2019.

[4] Respondent 2. 2019. Interview 2 on 31.01.2019.

[5] Respondent 3. 2019. Interview 3 on 11.02.2019.

[6] Respondent 4. 2019. Interview 4 on 15.02.2019.

[7] Respondent 5. 2019. Interview 5 on 28.02.2019.

[8] Respondent 6. 2019. Interview 6 on 08.03.2019.

[9] Respondent 7. 2019. Interview 7 on 25.03.2019.

[10] Telenor Group. 2019. Telenor Group Annual report 2018. https://www.telenor.com/investors/reports/annual-reports/. Accessed: 2019-04-01.

[11] Act, Sarbanes-Oxley. 2002. Sarbanes-Oxley Act. *Washington DC*.

[12] Investopedia. 2019. Corporate Governance. https://www.investopedia.com/terms/c/corporategovernance.asp. Accessed: 2019-04-01.

[13] The Committee of Sponsoring Organizations of the Treadway Commission. 2013. Internal control — integrated framework. https://www.coso.org/Pages/ic.aspx. Accessed: 2018-12-01.

[14] Bostron, R. & Heinen, J. S. 1997. Mis problems and failures: a socio-technical perspective. *MIS Quarterly*, 3(3), 1–4.

[15] Kowalski, S. 1996. IT insecurity: A multi-disciplinary inquiry.

[16] The Committee of Sponsoring Organizations of the Treadway Commission, Deloitte LLP. 2015. COSO in the cyber age. https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf. Accessed: 2018-12-01.

[17] Trautman, L. J. & Altenbaumer-Price, K. 2010. The board's responsibility for information technology governance. *J. Marshall J. Computer & Info. L.*, 28, 313.

[18] Basel Committee on Banking Supervision. 2018. Cyber-resilience: Range of practices. https://www.bis.org/bcbs/publ/d454.pdf. Accessed: 2019-03-20.

[19] Whitman, M. E. & Mattord, H. J. 2013. *Management of information security*. Nelson Education.

[20] Center for Audit Quality. 2018. Cybersecurity risk management oversight: a tool for board members. https://www.thecaq.org/file/4881/download?token=7OWoaQ8X. Accessed: 2018-10-24.

[21] ISACA. 2018. State of cybersecurity 2018. http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2018-part-1_res_eng_0418.PDF. Accessed: 2018-10-24.

[22] Deloitte. 2013. Audit committee brief: Cybersecurity and the audit committee. http://deloitte.wsj.com/cfo/files/2013/08/ACBrief_August2013.pdf. Accessed: 2018-10-24.

[23] Center for Audit Quality. 2014. Caq member alert: Cybersecurity and the external audit. https://www.thecaq.org/file/269/download?token=8yX_7eKg. Accessed: 2018-10-24.

[24] Yatim, P. 2010. Board structures and the establishment of a risk management committee by malaysian listed firms. *Journal of Management & Governance*, 14(1), 17–36.

[25] Abu-Musa, A. 2010. Information security governance in saudi organizations: an empirical study. *Information Management & Computer Security*, 18(4), 226–276.

[26] Nolan, R. & McFarlan, F. W. 2005. Information technology and the board of directors. *Harvard business review*, 83(10), 96.

[27] Huff, S. L., Maher, P. M., & Munro, M. C. 2006. Information technology and the board of directors: Is there an it attention deficit? *MIS Quarterly Executive*, 5(2).

[28] Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. 2012. Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221–232.

[29] Norwegian Corporate Governance Board. 2018. The norwegian code of practice for corporate governance. http://wpstatic.idium.no/nues.no/2018/10/NUES_eng_web_okt2018_2.pdf. Accessed: 2018-10-24.

[30] European Parliament. 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. Accessed: 2019-03-20.

[31] Department of Defence. 2019. Lov om nasjonal sikkerhet | Norwegian Security Act. https://lovdata.no/dokument/NL/lov/2018-06-01-24. Accessed: 2019-03-20.

[32] Nationalt Security Authority (NSM). 2019. Veiledninger tilhørende ny sikkerhetslov i 2019. https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/. Accessed: 2019-03-20.

[33] Agency for Public Management and eGovernment (Difi). 2019. Internkontroll i praksis – informasjonssikkerhet For toppleder. https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/for_toppledere_-_internkontroll_informasjonssikkerhet.pdf. Accessed: 2019-03-20.

[34] The Financial Supervisory Authority. 2003. Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) | ICT Regulation. https://lovdata.no/dokument/SF/forskrift/2003-05-21-630. Accessed: 2019-03-20.

[35] The Financial Supervisory Authority of Norway. 2013. Veiledning til IKT-forskriftens §5 "Sikkerhet". https://www.finanstilsynet.no/contentassets/c1970a306e2a4400858ae7ca192bf498/veiledning-ikt-forskrift-5-sikkerhet.pdf. Accessed: 2019-03-20.

[36] The Norwegian Directorate of eHealth. 2018. Code of conduct for information security and data protection in the healthcare and care services sector. https://ehelse.no/Documents/Normen/Engelsk/Code%20of%20coduct%205.3.pdf. Accessed: 2019-03-20.

[37] Georg Schaffner, L. 2018. Cybersecurity on non-executive boards. https://emstrasbourg.eu.qualtrics.com/jfe/form/SV_3vNrA2HcrJ9sB13.

[38] Myers, M. D. et al. 1997. Qualitative research in information systems. *Management Information Systems Quarterly*, 21(2), 241–242.

[39] Leedy, P. D. & Ormrod, J. E. 2013. *Practical Research: Planning and Design*. Upper Saddle River, New Jersey: Pearson, Merril Prentice Hall, 10th edition.

[40] Neuman, W. L. 2013. *Social research methods: Qualitative and quantitative approaches*. Pearson education.

[41] Norges Bank. 2019. Norges Bank Årsraport og Regnskap. https://static.norges-bank.no/contentassets/0524ac869e7344a2b899c100eee1b22e/nb_aarsrapport_2018.pdf?v=02/26/2019130902&ft=.pdf. Accessed: 2019-04-01.

[42] Nordea Group. 2019. Nordea Annual Report 2018. https://www.nordea.com/Images/33-304448/Annual%20Report%20Nordea%20Bank%20Abp%202018.pdf. Accessed: 2019-04-01.

[43] KLP. 2019. KLP Årsrapport 2018. https://www.klp.no/polopoly_fs/1.42287.1555072925!/menu/standard/file/KLP%20årsrapport%202018.pdf. Accessed: 2019-04-01.

[44] DNB Group. 2019. DNB Group Annual report 2018. https://www.ir.dnb.no/press-and-reports/financial-reports?page=/en/reports/dnb%27s-annual-report-for-2018-is-published-today-1666295. Accessed: 2019-03-09.

[45] Orkla. 2019. Orkla Annual Report 2018. http://hugin.info/111/R/2238608/886256.pdf. Accessed: 2019-04-01.

[46] Hydro. 2019. Hydro Annual Report 2018. https://www.hydro.com/Document/Index?name=2018%20Annual%20report.pdf&id=8525. Accessed: 2019-04-01.

[47] Norgesgruppen. 2019. Norgesgruppen Årsrapport 2018. https://www.norgesgruppen.no/globalassets/finansiell-informasjon/arsregnskap-2018.pdf. Accessed: 2019-04-01.

[48] Yara. 2019. Yara Annual Report 2018. https://www.yara.com/siteassets/investors/057-reports-and-presentations/annual-reports/2018/yara-annual-report-2018-web.pdf. Accessed: 2019-04-01.

[49] Eidsiva Konsern. 2019. Eidsiva Årsrapport 2018. https://www.eidsiva.no/globalassets/dokumenter/finansiell-informasjon/arsrapporter/arsrapport-eidsiva-energi-2018_endelig.pdf. Accessed: 2019-04-01.

[50] Statnett. 2019. Statnett Annual Report 2018. https://www.statnett.no/globalassets/om-statnett/investor-relations/annual-reports/statnett-annual--report-2018.pdf. Accessed: 2019-04-01.

[51] Statkraft AS. 2019. Statkraft Annual Report 2018. https://www.statkraft.com/globalassets/1-statkraft-public/05-investor-relations/4-reports-and-presentations/2018/annual-report-2018/2018-annual-report-statkraft-as.pdf. Accessed: 2019-04-01.

[52] Aker Solutions. 2019. Aker Solutions Annual Report 2018. https://akersolutions.com/globalassets/huginreport/2018/annual-report-2018.pdf. Accessed: 2019-04-01.

[53] Telenor Group. 2017. Telenor Group Annual report 2016. https://www.telenor.com/investors/reports/annual-reports/. Accessed: 2019-04-01.

[54] Kopp, E., Kaffenberger, L., & Jenkinson, N. 2017. *Cyber Risk, Market Failures, and Financial Stability*. International Monetary Fund.

[55] DNB Group. 2018. DNB Group Risk and capital management 2017. Disclosure according to Pillar 3. https://vp267.alertir.com/afw/files/press/dnb_asa/201803072699-2.pdf. Accessed: 2019-03-09.

[56] DNB Group. 2019. DNB Group Risk and capital management 2018. Disclosure according to Pillar 3. https://vp267.alertir.com/afw/files/press/dnb_asa/201903066039-1.pdf. Accessed: 2019-03-09.

[57] DNB Group. 2017. DNB Group Risk and capital management 2016. Disclosure according to Pillar 3. https://vp267.alertir.com/afw/files/press/dnb_asa/201703089555-2.pdf. Accessed: 2019-03-09.

[58] Telenor Group. 2018. Telenor Group Annual report 2017. https://www.telenor.com/investors/reports/annual-reports/. Accessed: 2019-04-01.

[59] Telenor Group. 2018. Digital Sikkerhet 2018. https://www.telenor.no/binaries/FINAL%20Digital%20sikkerhet%202018_tcm94-351447.PDF. Accessed: 2019-04-01.

A Appendix A: Survey questions

A.1 Questionnaire

1. Are you member of a non-executive board?

   □ Yes
   □ No (please continue to answer questions, under the assumption you were)
   □ I was in the past
   □ I will be soon

2. I have held a position as non-executive board member in...

   □ 1 company
   □ 2-5 companies
   □ 6-10 companies
   □ >10 companies
   □ None so far.

3. The sector of the company/ies I intend to or have worked for as non-executive board member are in...

   □ Financial Services Industry / Insurance
   □ Manufacturing
   □ Pharmaceutical
   □ Telecommunications
   □ Non-Governmental Organization / Non-for-Profit Organization
   □ Consulting
   □ Other ________________

4. I have worked as non-executive board member in IT related industries, which include industries such as...

   □ 1 (please describe the industry) ________________
   □ 2 (please describe the industry) ________________
   □ 3 (please describe the industry) ________________
   □ None so far ________________

5. I have worked previously as...

   □ Executive Board Member
   □ Manager
   □ Chief Information Officer

- □ Chief Information Security Officer
- □ Non-IT related positions
- □ Other ________________

6. The company/companies I worked for was a /were mostly...
   Definition according to "What is an SME? - Small and medium sized enterprises (SME) - Enterprise and Industry". ec.europa.eu. Archived from the original on February 8, 2015. Retrieved 2015-06-12.
   - □ Large Corporation(s)
   - □ Medium sized organization(s): <250 staff headcount; <€50m turnover; <€43 balance sheet total.
   - □ Small sized organization(s): <50 staff headcount; <€10m turnover; <€10 balance sheet total.
7. My company/ies is/are based in, please provide the country name (i.e. USA, Canada, Switzerland, South Africa, etc...)
   - □ Company 1 ________________________________
   - □ Company 2 ________________________________
   - □ Other ________________________________
8. The markets my company/ies majorly operate(s) in are in...
   - □ the United States of America/ Canada
   - □ EU countries
   - □ EFTA countries (Switzerland, Norway, etc.)
   - □ Africa
   - □ Australia / New Zealand
   - □ Middle East
   - □ Asia
   - □ South America
   - □ Other ________________________________
9. With regard to digitalization (i.e., exponential companies, API design, Privacy-by-design (GDPR), smart technologies, process automation), I consider myself...
   - □ an expert (all above I can explain in detail)
   - □ well informed (all above I have a reasonable understanding)
   - □ informed (most of the above I have a good understanding)
   - □ fast learner (I have read/heard all of the above)
   - □ novice (most of the above I now little about)
   - □ Remark ________________________________
10. I am familiar with the concept of Distributed Ledger Technology/Blockchain.
    - □ Yes, we have discussed it on board level

- □ Yes, out of personal interest
- □ No, not in particular

11. How was DLT discussed?

    - □ As a calculated business case
    - □ As a strategic business area
    - □ As an innovation, but without follow-up ______________________

12. With regard to cyber security (i.e., Maximum Possible Loss, Data Leakage Prevention, Deep Packet Inspection), I consider myself...

    - □ an expert
    - □ well informed
    - □ informed
    - □ fast learner
    - □ novice
    - □ Remark ______________________

13. My educational background is in...

    - □ Business Administration
    - □ Engineering
    - □ Arts
    - □ Computer Science
    - □ Natural Sciences
    - □ Languages
    - □ Law
    - □ Other ____________

14. I received non-executive training/education on...

    - □ Legal Advice
    - □ Business Administration (Finance, Governance, Organizational Design, etc.)
    - □ Business Administration (Major Information Systems)
    - □ Digitilization
    - □ Cyber Security
    - □ Other ____________
    - □ I did not receive specific training/education for my board role

15. This education has been taken/ updated...

    - □ In the last year
    - □ In the last two years
    - □ In the last 5 years
    - □ In the last 10 years

□ Longer

16. I wish to receive better training on Cybersecurity.

    □ Yes. Why:____
    □ Not necessary. Why:____

17. In the boards of directors I participated, I was a member of...

    □ the Audit Committee
    □ the Risk Committee
    □ the Strategy Committee
    □ the Nomination Committee
    □ Other _______________

18. Was Cybersecurity a fixed topic in any of the board meetings?

    □ Yes, at every meeting
    □ Yes, sometimes
    □ Yes, once
    □ Never

19. Non-executive board meetings were held...

    □ Once per year
    □ Half-yearly
    □ Quarterly
    □ More often. Please specify ___________________________
    □ On demand
    □ I would suggest ___________________________
    □ Calls for meetings were made almost in real-time if necessary

20. Expertise in Cybersecurity in the non-executive board existed...

    □ through an expert that was a member of the board"
    □ through one or more external expert(s) that served as advisor in case of specific situations. Such as... ___________________________
    □ among most/all member of the board
    □ potentially but was not explicitly defined

21. Expertise should exist with.. Please name two roles in the organization.

    □ ___________________________
    □ ___________________________

22. The tasks for cybersecurity in the board were...

    □ shared among all board members
    □ with the Audit Committee

- □ with the Risk Committee
- □ with another committee. Which ________________________
- □ Shared among two committees. Which ________________________
- □ Not explicitly attributed

23. I can quantify the monetary value of information for the organization(s) I have worked for.
    - □ Yes
    - □ Likely
    - □ Hardly
    - □ No
24. When I was confronted in my non-executive board role with decisions on Cybersecurity,...
    - □ I had all the information I needed and was confident in being able to take the best decision.
    - □ I was taking a supportive role.
    - □ I felt not sufficiently informed and educated on the topic.
    - □ I was never confronted with a decision on Cybersecurity.
25. I wish to see metrics covering the following areas in a security report (if considered as non relevant, please ignore):
    - □ Degree of application of Security Policy
    - □ Level of maturity of Security Organization
    - □ Attacks originating from or using employees or other stakeholders as attack vectors
    - □ Quantified losses related to assets (information, infrastructure etc.)
    - □ Successful intrusion attempts
    - □ Disclosure of non-public information (breach of encryption)
    - □ Attacks addressing the physical premises
    - □ Quality of equipment used (state-of-the-art, degree of patching, etc.)
    - □ Level of maturity of operational processes
    - □ Number of attacks addressing information in transit (communication lines, networks, etc.)
    - □ Degree of resiliency of Supply Chain (supplier agreements, security risks encountered in IT acquisition)
    - □ Number of business critical incidents
    - □ Number of compliance breaches
    - □ Number of high probability incidents
26. The biggest challenges for non-executive boards in cyber security are...

	First priority	Second Priority	Third priority	No priority
Knowing the legal responsibilities of the company	□	□	□	□

Understanding the technical complexity in cybersecurity of the company	□	□	□	□
Receiving the relevant information on security environment (reporting)	□	□	□	□
Knowing the risk appetite of company stakeholders	□	□	□	□
Other ____________________	□	□	□	□

27. I have experienced and/or understand the challenges in cyber security for non-executive boards when it comes to...

    □ Conflicts of interest between stakeholders and executive management i.e. the definition of risk appetite and investment strategy. An example has been ____________________

    □ Externalization of cyber security i.e., the concept to rather leave securing the market place to others, such as providers, customers, public services. An example has been ____________________

    □ Asymmetric information i.e. creating a balanced level of transparency that informs organization's stakeholders appropriately without disclosing sensitive information. An example has been ____________________

28. Other non-executive board members would consider myself as a specialist in...

    □ Strategy
    □ Governance
    □ Legal Affairs
    □ Information Technology
    □ Finance
    □ Other ____________________

29. I am...

    □ Female
    □ Male

30. My age is...

    □ <30
    □ 30-40

□ 40-50
□ 50-60
□ 60-70
□ >70

A.2 Additional Questions

a) Are you aware of the organizations such as COSO or ITGI and their guidance material?
b) What is your take on organizational structure for more efficient information security programme (CISO, various roles and departments)?
c) Does your board do the crisis scenario as a table-top exercise?
d) Which committee in your opinion be responsible for informations security governance?
e) Have you ever been shown and/or reviewed the security report with top-level KPIs?

B Appendix B: Norwegian Code of Practice

Sections of the Norwegian Code of Practice [29]:

1. Implementation and reporting on corporate governance
2. Business
3. Equity and dividends
4. Equal treatment of shareholders and transactions with close associates
5. Shares and negotiability
6. General meetings
7. Nomination committee
8. Board of directors: composition and independence
9. The work of the board of directors
10. Risk management and internal control
11. Remuneration of the board of directors
12. Remuneration of executive personnel
13. Information and communications
14. Take-overs
15. Auditor