Jiri Vidgren

TOP MANAGEMENT COLLABORATION WITH CYBERSECURITY GOVERNANCE

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2020

ABSTRACT

Vidgren, Jiri
Top Management Collaboration with Cybersecurity Governance
Jyväskylä: University of Jyväskylä, 2020, 109 pp.
Cybersecurity, Master's Thesis
Supervisor: Niemimaa, Marko

Cybersecurity is a holistic field, which demands cooperation from all levels in the companies. Notably, the collaboration between the top management and cybersecurity governance is in a critical position. This collaboration must work in both directions, and the companies need to embed the cybersecurity in strategic actions and decisions that top management drives. In return, the collaboration essentially delivers control and visibility to the actions' results as a response from the company. The literature about the topic grounded the two-part literature review in the study comprehensively. However, there is an empirical research gap concerning real implementations of cybersecurity governance. The study aimed to fill this gap by examining how the collaboration between the top management and the cybersecurity governance works in a company. The study also aimed to determine which aspects drive cybersecurity governance in the company and how the different levels of the organization produce the company's cybersecurity. These practical manifestations of cybersecurity governance include implementation, measurement, assessing, and reporting to the top management. The overarching methodology of the study was a qualitative research design, and the empirical research was conducted as a multiple-case study. Empirical data was gathered via thematic interviews from five (5) cybersecurity professionals and analyzed utilizing theory-guided thematic content analysis. As the main result of the research, the study suggests that the collaboration between top management and cybersecurity governance appears to be driven by a holistic and continual cybersecurity maturity development. The study also revealed insights indicating that companies should consider utilizing their chosen best practice framework to the full extent to support the company's cybersecurity governance pursuits, like addressing the aspect of the continual improvement more deliberately.

Keywords: Top management, collaboration, cybersecurity, information security governance, direct-control model

TIIVISTELMÄ

Vidgren, Jiri
Ylimmän johdon ja kyberturvallisuuden hallinnon yhteistyö
Jyväskylä: Jyväskylän yliopisto, 2020, 109 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Niemimaa, Marko

Kyberturvallisuus on kokonaisvaltainen ilmiö, joka vaatii yhteistyötä yritysten kaikilla tasolla. Erityisesti kriittistä on yritysten ylimmän johdon ja kyberturvallisuuden hallinnon (engl. cybersecurity governance / information security governance) välinen yhteistyö. Tämän yhteistyön on toimittava molempiin suuntiin ja kyberturvallisuus tulee sisällyttää kaikkiin strategisiin toimiin, joita ylin johto ajaa. Vastineeksi yhteistyö tarjoaa näkyvyyden toimien seurauksiin. Aiheesta saatavilla oleva kirjallisuus taustoitti tutkielman kaksiosaista kirjallisuuskatsausta kattavasti. Kyberturvallisuuden hallinnon käytännön toteutuksiin liittyy kuitenkin empiirisen tutkimuksen vaje. Tutkielman tavoitteena oli täyttää tätä vajetta selvittämällä, kuinka ylimmän johdon ja kyberturvallisuuden hallinnon välinen yhteistyö toimii yrityksessä. Lisäksi tutkimuksen tavoitteena oli selvittää, mitkä asiat ohjaavat kyberturvallisuuden hallintoa yrityksissä ja kuinka organisaation eri tasot tuottavat yrityksen kyberturvallisuutta. Nämä kyberturvallisuuden käytännön ilmentymät sisältävät implementoinnin, mittaamisen, arvioinnin ja raportoinnin ylimmälle johdolle. Tutkimuksen metodologinen lähestyminen oli laadullinen, ja sen empiirinen tutkimus suoritettiin monitapaustutkimuksena. Empiirinen aineisto kerättiin haastattelemalla viittä (5) kyberturvallisuusalan ammattilaista teemahaastattelun mukaisesti. Haastatteluaineisto analysoitiin käyttäen teoriaohjattua temaattista sisällönanalyysia. Tutkimuksen päätulos viittaa siihen, että ylimmän johdon ja kyberturvallisuuden välisen yhteistyön ajurina näyttäisi olevan kokonaisvaltainen ja jatkuva kyberturvallisuuden kypsyystason kehittäminen. Tutkimuksen näkemyksiin perustuu myös suositus, että yritysten tulisi harkita parhaisiin käytäntöihin perustuvan viitekehyksen hyödyntämistä täysmääräisesti, kuten esimerkiksi pyrkimällä tietoisemmin informaatioturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen yrityksen turvallisuushallinnon tavoitteiden tukemiseksi.

Avainsanat: Ylin johto, yhteistyö, kyberturvallisuus, informaatioturvallisuus, hallinto, ohjauskontrollimalli.

FIGURES

TABLES

TABLE OF CONTENTS

1 Introduction

Information security and cybersecurity are often seen as just a technical matter from the corporate strategic level, which implementation then remains as the responsibility of the enterprise IT management (von Solms, 2001; Siponen & Oinas-Kukkonen, 2007; Siponen et al., 2014; Rothrock et al., 2018). Enterprise IT management has traditionally been responsible for information security practices that focus on securing enterprise information capital, and preferably from a purely technical point of view. These measures are inadequate to meet the challenges of securing and protecting modern, ubiquitous information systems and environments. Technology is becoming embedded in everything, which extends the security-related challenges and responsibilities even further, up to the top management level. (Islam & Strafford, 2017; Alreemy et al., 2016; Dufva, 2019.)

The challenge for the top management is making the paradigm shift from just outsourcing things to taking the holistic approach and respecting the cybersecurity in the strategy, mission, and vision of the company. Addressing this all is not just a simple pivot maneuver in the strategy work, but a fundamental, deliberate change to embed and connect the cybersecurity into the decision-making processes, messaging, and leadership in general. There are many motivations and reasons why companies initialize and execute this change, for example, legislation, industry regulations, stakeholder requirements, company reputation, and digitalization.

According to Kayworth and Whitten (2012), an effective information security strategy must incorporate technical competence, aligned with the corporate strategy. This alignment needs to be established both organizationally as well as socially to the company culture. Therefore, information security strategy and cybersecurity strategy have to address three primary objectives: Balancing information security and business needs, ensuring compliance, and maintaining cultural fit (Kayworth & Whitten, 2012).

Information security management systems (ISMS) are in the heart of employing the strategic-level decisions in information security and cybersecurity through the tactical level and finally to the operational level of the company (von

Solms & von Solms, 2004). These ISMS's of different companies have been, and still often are fundamentally grounded on the industry best practices regarding information security management (Nicho, 2018). ISO/IEC 27001 is one of the most common and widely implemented standards (Humphreys, 2016).

However, implementing and operating information security and cybersecurity according to industry best practices and certifying the company's ISMS against a well-known standard is not trivial. Information security and cybersecurity governance must be directed and controlled with a suitable methodology (von Solms and von Solms, 2009). To govern the implementations of decisions from top management's strategy work, companies need to have frameworks, guidelines, and models in place. (Gashgari et al., 2017; Alqurashi et al., 2017; Nicho 2018; von Solms & von Solms, 2006.)

Top management and cybersecurity managers must have a holistic and collaborative approach for directing the actual implementation of cybersecurity measures. Regarding corporate governance overall, the same principles apply to control the assessments, measurements, and feedback from the measures — the indicators of the operations, which fuels the continual improvement of the company. Hence, cybersecurity is no exception here.

1.1 Research Motivation

According to Lehto and Kähkönen (2015), multidisciplinary research is typical in the cybersecurity field, as cyber environments link to companies on many organizational and technical levels, representing strategic assets to the companies. However, the current field of research is missing the holistic view about the cybersecurity in the corporate strategy, the top management collaboration to governing and implementing the according to measures and utilizing the results for strategy work.

The subject of the study is significant from a practical view; since digitalization has taken over every industry, technology embeds in everything (Dufva, 2019), and the companies must think about cybersecurity from an entirely new standpoint. Cybersecurity needs to be addressed comprehensively and holistically. Taking responsibility, showing the commitment and embedding the cybersecurity to everything ignites from the top management, connects through governance to develop throughout the company and its organizations, and finally yields to all stakeholders of the company.

The scientific contribution of the study is to explore and observe the phenomena related to the strategic leadership of cybersecurity and the aligned governance aspects. Albeit cybersecurity is a 'hot topic' right now and leadership has been researched already for centuries, this area has been neglected by scholars and researchers so far, especially from the combined point of view of top management and cybersecurity governance. Also, since the topic area is quite large, the study is priming many new themes for further research, which adds

value to the qualitative research in the future regarding the leadership and cybersecurity's strategic position in companies.

1.2 Research Aim and Scope

The research aim of the study is to find out how the company's top management collaborates with the cybersecurity governance of the company. To explore and explain this collaboration, the study approach this from several aspects, including; interest, commitment, prioritizing, dialogue, support, messaging, presence, influence, and activities in general that the top management performs with the entire company and vice versa. The top management's general route to drive these activities is utilizing the collaboration with the department of cybersecurity management of the company. This collaboration is, in essence, what the research aim of the study is striving to explore and explain. Therefore, the research aim forms the main research question of the study:

- **How does the top management collaborate with the company's cybersecurity governance?**

To support in finding the answer to the research question, I formed three sub-questions to examine the relevant aspects regarding cybersecurity governance from the company's department of cybersecurity management's point of view. Therefore, I created the first sub-question as:

- What aspects drive the cybersecurity governance and management in the company?

Secondly, cybersecurity governance includes directing measures, which delivers the top management influence further in the organization through the tactical level to the operational level. The second sub-question forms the support in finding the answer to the main research question:

- How are the cybersecurity measures **directed** in the company?

Finally, the cybersecurity governance includes controlling measures, which focus on assessing the effectiveness of the directions as well as reporting the outcomes of the directing measures back to the top management via the department of cybersecurity management. Therefore, the third sub-question forms the support in finding the answer to the main research question from this point of view:

- How are the cybersecurity measures **controlled** in the company?

As a fundamental theoretical underpinning for the study, the sub-questions follow the model based on the direct-control cycle (von Solms & von Solms, 2009). This model is introduced in the chapter 3.2.2.

I conduct the research aligned to interpretive research philosophy. A qualitative research design underpins the multiple-case study. The empirical material is gathered via thematic, semi-structured interviews and analyzed utilizing theory-guided thematic analysis. Research setting and content analysis is introduced in chapter 4.

The focus and topic areas of the study are corporate strategy, collaboration with the cybersecurity governance, directing/controlling cybersecurity, and finally reporting back to the top management. Figure 1 illustrates these relations and the information cycle.

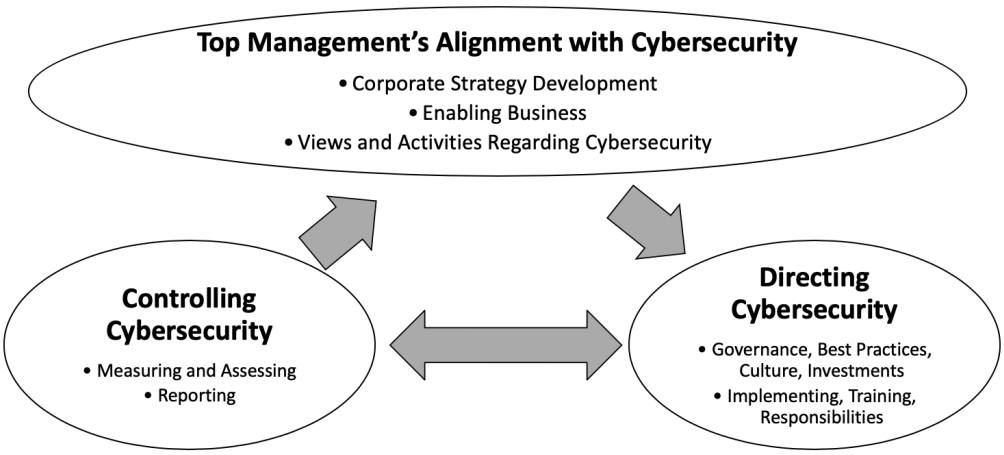

FIGURE 1 Relations of the study focus areas

The study's scope is limited to information security and cybersecurity in corporate strategy development and the connection between top management and information security management. Technologies related to cybersecurity are out of scope.

1.3 Literature Review

Literature reviews are conducted for the essential definitions in chapter 2 and building the theoretical base in chapter 3. Throughout these chapters, scientific research materials, such as peer-reviewed articles, literature, research reports, international standards, and publications from research institutes, are examined. The source material's evaluation and qualification are utilizing Publication Forum's (2020) quality assessment for the scientific publishing channels. Emphasis is on levels 1 to 3.

Material for the literature review is found from JYKDOK service by the University of Jyväskylä Library, Scopus by Elsevier, and Scholar by Google. The study underpins the source material qualification to the level rating of the publication channels, and additionally to the source references in Google Scholar service.

1.4 Outline of the Thesis

The study contains six chapters in addition to the introduction. Chapter two is based on a literature review and contains essential definitions of elemental terms and concepts applied in the study. The second chapter aims to define and explain cybersecurity from the business, risk, and strategy viewpoints.

The third chapter forms the actual theoretical reference framework using the literature review methodology. The chapter begins from the top management focus areas and continues with information security governance, including security measure implementations. Then, cybersecurity effectiveness measurement and assessment, as well as reporting to the top management, are reviewed. Also, the implications for the strategy are reviewed based on the literature. Finally, the third chapter ends with the motivation for the empirical research based on the shortcomings and areas to be focused more on.

The fourth chapter describes the research setting thoroughly, including methodologies and processes applied in the study. The fifth chapter focuses on the empirical findings analyzed from the interview data. The sixth chapter is where the comparison and evaluation of the empirical findings in dialogue with the literature review are conducted. The sixth chapter also contains implications and recommendations based on the discussion, significance, usability, and assessment of the research quality. Finally, a discussion of the study's limitations and concerns is taking place with some further research recommendations. The seventh chapter is for conclusions, learnings, and outcomes as the summary. The summary of the study provides a clear picture of the findings achieved and their significance. To conclude, a summary of the research methods, findings, and limitations of the study is presented.

2 Strategy and Cybersecurity

Strategy and cybersecurity are essential components of modern businesses that prosper through organized leadership and secures their valuable assets in a governed manner. However, these concepts are not uniform and straightforward to explain. There are also sub-concepts and related concepts that need explanation. Therefore, this chapter defines the strategy, extends into corporate strategy, and goes through the different views on strategy development. On the cybersecurity side, this chapter defines key sub-concepts, reviews cybersecurity from the business point of view, and closes logically via risk and threat management and concluding the chapter finally to cybersecurity strategy concepts. This chapter's overall purpose is to give a contextual foundation to the study's theoretical background, which is formed by a literature review in chapter 3.

2.1 Strategy

There is no simple, undisputed description of what strategy is. According to Mintzberg (1987), the field of strategic management cannot even rely on a single definition of strategy. Recognizing the multiple explicit definitions of strategy will help scholars and researchers maneuver through this challenging field.

Mintzberg (1987) explains strategy with the summary of '5 P's': *Plan, Ploy, Pattern, Position,* and *Perspective*. Johnson et al. (2008) explain strategy through the concept of *strategy lenses* in the modern school view for strategy research. These approaches have similarities and are complementing each other in explaining what strategy essentially represents.

Johnson et al. (2008) justify these Mintzberg's definitions with *strategy as ideas*. This perspective of strategy highlights the importance of variety and diversity in and around companies that potentially helps generate new ideas. Critical implications behind this strategy lens are to nurture experimentation, questioning and challenging, interaction and co-operation, and recognizing patterns in the strategy work. Johnson et al. (2008) observations and thoughts align seamlessly with Mintzbergs (1987) views on strategy as *Plan, Ploy, Pattern,* and *Position*.

Finally, according to Mintzberg (1987), a strategy is overall, a concept. One crucial implication regarding this is that all strategies are abstractions that exist only in the minds of interested parties and stakeholders. A strategy is not an artifact but an invention, conceived of as intentions to regulate behavior before it takes place or inferred as patterns to describe behavior that has already occurred. The fundamental importance of defining strategy as a concept is that the perspective is shared, and when discussing strategy in this context, a realm of

collective mind is entered. According to Mintzberg (1987), this reveals significant issues in the study of strategy formation. (Mintzberg, 1987.)

Defining the strategy undisputedly is impossible, but narrowing the theme with keywords like plan, ploy, pattern, position, perspective, concept, idea, design, experience, and discourse, is giving an overview. Johnson et al., (2008, p. 22) condenses the definition of the strategy for corporations and businesses as:

> The direction and scope of an organization over the long term, which achieves advantage in a changing environment through its configuration of resources and competences with the aim of fulfilling stakeholder expectations.

2.1.1 Corporate Strategy

Andrews (1997) detaches corporate strategy apart from business strategy and presents clear definitions for both. The corporate strategy usually applies to the whole enterprise. In contrast, business strategy is less comprehensive and defines the choice of product or service and market of individual strategic business units in the company. A business strategy determines how a company will compete and position itself among the competition, while corporate strategy defines the businesses in which a company will compete. (Andrews, 1997.)

Johnson et al. (2008) declare corporate strategy as a top-level strategy concerning the company's overall scope and how value will be added to its different business units. An example of these kinds of services and resources would be the cybersecurity management, which is governed from the corporate level to support all strategic business units. Many corporate support functions, like human resources, marketing, and communications, would fall into this category of activities also.

Strategy, in general, is not solely a top management matter. Middle and lower-level managers are obliged to work within their company's strategy and meet the strategy's objectives while observing the constraints. Managers at every level must communicate strategy to their teams and will achieve higher performance from them; the more convincing they are in interpreting the strategy. Every employee of the company should execute the same strategy for higher performance; therefore, the strategy matters to everyone in the company. (Johnson et al., 2008.)

A large amount of resources is utilized, developing a strategy and planning its implementation, but all these resources are sacrificed for nothing if the strategy is not in the *heads, hearts*, and *hands* of the people who need to execute the strategy in practice (Jones, 2008). Heads are the metaphor for that the strategic implementation starts from people understanding the strategy and adopting the general idea and logic behind that. Hearts symbolize the need for emotional commitment and engagement of the people towards strategy, which makes the big difference about how people feel about working for the company and how the company's community and society affect them. This collective feeling is where the passion and commitment supporting the strategy are generated by

communicating the strategy message. Finally, hands are denoting the execution of the actions in the operational level of strategy. (Jones, 2008.)

2.2 Strategy Development

Johnson et al. (2008) explain strategy development in two distinguished views, which are not mutually exclusive. The first view is associated with the idea of the *intended strategy*, which emphasizes that strategies are a result of careful deliberation with top management. The second view is *emergent strategy*, which raises from the idea that strategies are not developed under the strict process, but instead in the company as a result of the discussion, experience, and ideas; in emergence.

Both explanations add up finally into the *realized strategy*, but not to the full extent. Mintzberg (1987) separates the elements from the intended strategy to subsets, which are contributing the realized strategy (*deliberate strategy*) from the subsets which patterns are developed in the absence of intentions and therefore got never realized (*unrealized strategy*). Figure 2 combines and illustrates these views by Johnson et al. (2008) and Mintzberg (1987).

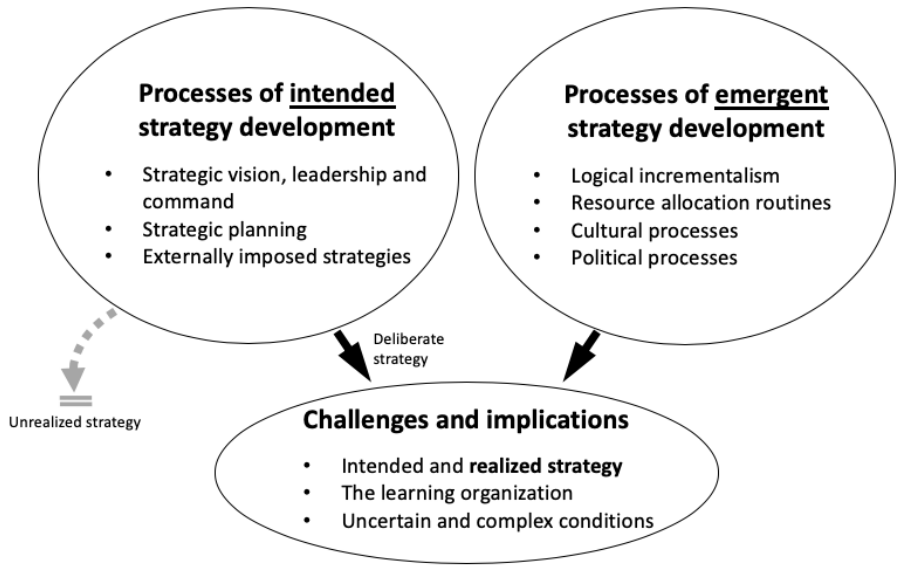

FIGURE 2 Strategy development process (Adapted from Johnson et al., 2008, p. 400 & Mintzberg, 1987, p. 14)

2.2.1 Intended Strategy Development

Intended strategy development is often a result of planning systems, which are carried out objectively and dispassionately. These strategic planning systems may take the form of systematized, step-by-step, chronological processes (Johnson et al., 2008). Quinn and Voyer (2003) present critique against these

methods and argue that this 'systems-planning approach' focuses on quantitative factors, and underemphasizes qualitative, organizational, and power factors. This kind of approach should be utilized as just one building block in the continuous stream of events, which eventually creates an organizational strategy for the company (Quinn & Voyer, 2003).

2.2.2 Emergent Strategy Development

Strategy development is not always an intentional process, which follows guidelines and frameworks to produce the actual development. Quinn and Voyer (2003) support this by pointing out that strategic change processes are typically fragmented, evolutionary, and intuitive. According to Quinn and Voyer (2003), real strategy evolves as internal decisions and external events flow together to create new, widely share consensus for action. Johnson et al. (2008) agree by explaining the emergent strategy coming about through everyday routines, activities, and processes in companies and creates utterly new thinking through cultural processes and logical incrementalism.

Effective strategies tend to emerge incrementally and opportunistically when subsystems of organizational activity (e.g., acquisitions, divestitures, or significant reorganizations) are blended into a coherent pattern (Quinn & Voyer, 2003). This logical incrementalism is the deliberate development of strategy by experimentation and partial commitments (Johnson et al., 2008). Quinn and Voyer (2003) argue that logical incrementalism makes it easier to avoid the adverse effects of large-scale organizational moves (e.g., strategy implementation) in organizational politics and the companies' social structure. Incrementally proceeding companies can assess the new roles, capabilities, and individual reactions of those involved in restructuring. Logical incrementalism gives executives the chance to move and decide more opportunistically. Besides, the final commitments can be made as late as possible. (Quinn & Voyer, 2003.)

A cultural explanation of strategy development occurs as the outcome of the taken-for-granted assumptions and behaviors in companies. In other words, culture is about that which is taken for granted, but it contributes to how groups of people respond and behave with issues they face. This behavior, albeit, has essential influences on the development and change of organizational strategy of the company. (Johnson et al., 2008.)

2.3 Cybersecurity

Creating, maintaining, and developing cybersecurity is a continuous process that requires constant trial and error to evolve and refine the needs and challenges of each company. A business company should never stop developing its cybersecurity strategy, tools, tactics, and technologies. The moment the IT team

stops evolving and developing its tools tactics and technology is the moment it will fail. (Kim, 2017.)

However, cyber is not synonymous with technology, and therefore cybersecurity is not only about IT team evolvement and development. According to the World Economic Forum (2020), operational technologies are at increased risk because cyberattacks could cause more traditional, kinetic impacts as technology are being extended into the physical world. Dufva (2019) agrees in the Sitra's megatrends 2020 report, that technology is becoming embedded in everything, and that will affect to cyberspace as well with its full extent.

Indeed, cybersecurity must be built and maintained from a completely different perspective than, for example, physical security (von Solms & van Niekerk, 2013). Choo (2011) considers it vital that our societies, businesses, governments, and research institutions innovate faster than criminals and other harmful actors.

This subsection explains the fundamental manifestations of cybersecurity from a corporate perspective. Also, this subsection will discover how cybersecurity strategies are applied and implemented in companies.

2.3.1 Cybersecurity in Business Companies and Organizations

Businesses are responsible for their overall security, including all (physical-, information-, ICT- and cyber-) aspects. The company should identify the assets, processes, and information to be protected. The ability to anticipate, detect, prevent, and limit the risk to business operations is essential, regardless of the manifestations of the anomalies. (Merete Hagen et al., 2008.)

Additionally, Huang et al. (2010) argue that not only are technical means to protect the information and prepare for threats, but the actions of every individual employee, manager, or staff member are human and play an essential role in maintaining cybersecurity.

Kim (2017) suggests that even though the technical implementation of information security is commonly falling under the IT department's responsibilities instead of end-users, it is crucial that employees are aware of the security threats and trained following the company's security strategy. Besides, von Solms and von Solms (2004) state that employees cannot be held accountable for maintaining information security unless they have first been trained in understanding what information security risks are and what should be done to address them.

2.3.2 Risk and Threat Management

Hiller and Russel (2013) admit that the company can face risks and threats that are affecting the state of cybersecurity from a variety of sources, for example, from competitors who may be motivated to sabotage their target company processes or steal business secrets. The threat can also come from inside of the company and not necessarily by intentionally malicious actors, but for example,

because the staff relies too much on intuition when making decisions about related to cybersecurity (Julisch, 2013).

Vulnerabilities can result from the negligence of the employees and the technical vulnerability of the infrastructure (Hiller & Russell, 2013). To increase and maintain the resilience of its cyber operating environment, a company must have a clear, tested plan for various scenarios (Rothrock et al., 2018). Also, mitigations, or company-specific security measures that can be implemented internally to reduce the risk of cyber-attacks, should be considered. These may include, for example, technical solutions, practices and procedures, and possible agreements with suppliers and customers that contain specific information security specifications. (Hiller & Russell, 2013.)

According to Rothrock et al. (2018) and von Solms and von Solms (2009), corporate management is responsible for evaluating and prioritizing risks in the company's cyber environment. Von Solms and von Solms (2004, p. 373) have discovered two of the most typical questions for the Chief Information Security Officer or Chief Executive Officer. These are: "against which risks must the information resources be protected?" and "what set of countermeasures will provide the best protection against these risks?". These questions are relevant and must be answered. Otherwise, the company will waste resources on ineffective countermeasures (von Solms & von Solms, 2004). Hiller and Russell (2013) note the consequences that information leaks or other cybersecurity breaches can negatively impact in a variety of ways, such as customer privacy, the leakage of business secrets, and loss of competitiveness and jobs.

Despite the industry, maturity, or even organization size, for governing the cybersecurity, a sound plan is needed. A cybersecurity strategy is often paramount for successful tactical as well as operational control of cybersecurity in the company.

2.3.3 Cybersecurity Strategy

According to von Solms & von Solms (2004), all international standards and best practices for information security and cybersecurity management stress that an appropriate information security policy is at the core and the foundation of any successful information security management system (ISMS). This short 3 to 4-page policy, signed by the CEO for executive management's commitment, is the starting point and theoretical framework on which all other information security sub-policies, procedures, and eventually the information security strategy must be based. (von Solms & von Solms, 2004.)

However, having some security policies signed off by top management and then concentrating on implementation are not adequate measures for cybersecurity management. Von Solms and von Solms (2004) adds that the information security strategy should be based on a well-known, industry-standard framework (e.g., ISO/IEC 27001) and preferably in a governed manner. Since strategy, in general, is touching every function and employee of the company, the same interrelation applies to cybersecurity strategy in an even

more obvious way. As cybersecurity is truly a multi-dimensional discipline, these identifications of cybersecurity relations by von Solms and von Solms (2009) underlines the critical position and role of cybersecurity in every aspect of the corporate business:

- The (Corporate) Governance Dimension
- The Organizational Dimension
- The Management Dimension
- The Policy Dimension
- The Best Practice Dimension
- The Ethical Dimension
- The Certification Dimension
- The Legal Dimension
- The Insurance Dimension
- The Personnel/Human Dimension
- The Awareness Dimension
- The Technical Dimension
- The Measurement/Metrics (Compliance Monitoring/Real-Time IT Audit) Dimension
- The IT Forensics Dimension

This catalog above is not an exhaustive collection of all information security-related dimensions regarding business organization but more of a list of acknowledged and identifiable ones. Some of these dimensions are working together, while some are more independent and even overlapping. Albeit, the essential interdependency between these is that all these dimensions must work together and be taken into account when developing a comprehensive cybersecurity strategy. It is also worth noting that most of these dimensions are non-technical by nature, which emphasizes the essence of cybersecurity over traditional information security. (von Solms & von Solms, 2009.)

Whitman and Mattord (2014) suggest that for the effective cybersecurity strategy, the company must first establish a governance structure for cybersecurity. Using existing generic IT governance structure is a common mistake here, and it is generally not recommended. The role of Chief Information Officer (CIO) is to look after the IT governance structure and be responsible for the information processing efficiency. Reciprocally, the inherent nature of information security, protecting that information, tends to impede that efficiency. Therefore, it is generally advised to separate these governance structures. Also, Chief Information Security Officer (CISO) operates not just with the IT department, but with every business unit and part of the company. (Whitman & Mattord, 2014.)

Regarding the future of separate cybersecurity strategies, Limnéll (2020) argues that those are going to be aligned and fixed to generic security strategies because it is not adequate to have parallel universes in the converged world, where technology is embedded to everything (Dufva, 2019).

The concepts described and explained during this chapter are enabling us to shape a view to a theoretical framework regarding strategic leadership from a cybersecurity governance point of view. However, since these topics are not easily digested, an additional chapter is required to establish a sound theoretical base and reference framework as the foundation for the empirical research in the study.

3 Corporate Cybersecurity Framework

Cybersecurity must support the company's corporate strategy. Documented cybersecurity guidance, such as cybersecurity strategy or cybersecurity policy, must protect the company's strategic objectives. Cybersecurity should also be understood as a value-add to the company rather than hindering progress, which requires a positive cybersecurity culture with appropriate investments to the management of cybersecurity (Traficom, 2020; NCSC-UK, 2019.)

In addition to the company's corporate strategy supported by cybersecurity strategy, multiple researchers and scholars are arguing, that corporations and companies need an Information Security Governance (ISG) framework. This ISG framework should be applied to governing their information security throughout the company organizations (Alqurashi et al., 2013; Chalaris et al., 2005; Garigue & Stefaniu 2003; Gashgari et al., 2017; Whitman & Mattord, 2014).

Finally, the cybersecurity strategy program needs to be adequately implemented, meaningfully measured, and understandably reported to help the top management operate and eventually, the company's corporate strategy to evolve for its success (von Solms & von Solms, 2009).

In this chapter, the cybersecurity is contemplated from the corporate dimension, top-down. The building of theoretical background continues as the relevant literature, and assistive publications are being reviewed. Firstly, the company's top management role is reviewed, and the concept of Information Security Governance (ISG) is introduced. Secondly, the cybersecurity implementation is reviewed from the measures and activities point of view. Then, the effectiveness of the cybersecurity measures is assessed and evaluated. Finally, the loop is closing back to the top management, and the improvements are assessed from the performance point of view.

The purpose of this chapter is to continue the literature review and form a theoretical base based on corporate cybersecurity strategy work, governance, management, implementation, measurement, reporting back to top management, and applying the performance assessment. This theoretical base is then utilized as the theoretical framework in the empirical part of the thesis.

3.1 Top Management's Leadership, Responsibility, and Commitment

Regarding general guidelines in achieving sustained success in the company, the International Organization for Standardization (ISO/IEC, 2018a, p. 75) states three principles:

> Top management, through its leadership, should:

1. promote the adoption of the mission, vision, values and culture in a way that is concise and easy to understand, to achieve unity of purpose;

2. create an internal environment in which people are engaged and committed to the achievement of the organization's objectives;

3. encourage and support managers at appropriate levels to promote and maintain the unity of purpose and direction as established by the top management.

These principles are rather generic by nature, but if we look at these from the cybersecurity governance perspective, the relevancy is apparent. Von Solms (2001) emphasizes in his article that there is no other option for the top management than to commit and take the cybersecurity's responsibility. For justification, von Solms (2001) is appealing to the law that requires corporate management to be responsible for good governance in their company, thus implicitly referring to the fact that good governance also includes the consideration of cybersecurity.

The Finnish law (Section 8 of the Finnish Companies Act 2006/624) states that "the management of the company must act in the best interests of the company." Also, regarding corporate management's commitment to cybersecurity is GDPR[1], which is directing by imposing sanctions such as "administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher" (European Commission, 2016, Art. 83(6)).

The top management should note that most of the regulations (e.g., GDPR mentioned above) transfers the responsibility for security breaches to the company itself instead of individuals that may have caused the breach to happen. Therefore, the top management, as a governing body, is eventually responsible for any deviations in the cybersecurity of the company. (Traficom, 2020.)

The essential understanding of strategic cybersecurity planning on top management level is the role of technology. It is evident in the modern business company's top management level, how technologies are assisting, enabling, and even the reason for existence for many advanced business functions in the age of digitalization. From this viewpoint, it should also be understood that these technologies and their concrete, physical world relations need to be resilient and secured accordingly (Islam & Stafford, 2017). Traficom (2020) emphasizes that jeopardizing business factors with inadequate cybersecurity could damage the reputation or cause financial losses like personal information held by the company, the company's intellectual properties, public websites or information channels, and industrial control systems. Discussing withstanding the losses related to technology and the survival of corresponding business operations are direct measures to seek commitment from top management regarding cybersecurity (Islam & Stafford, 2017).

[1] General Data Protection Regulation of European Union (2016/679) (European Commission, 2016).

Top management must also be able to prioritize their assets and align security accordingly. As with business risks, it is impossible to remove or mitigate all cybersecurity risks. Therefore, the top management's risk assessment must be broad and comprehensive. Active, ongoing, and bi-directional communication between all relevant stakeholders must be present. The top management has information related to the business; for example, information related to partnerships may be beneficial for technical security specialists seeking mutual cybersecurity measures. In return, technical specialists have information on the prerequisites for achieving the key objectives, like which systems or information are partner dependent. (Traficom 2020.)

Research results by Kwon, Ulmer, and Wang (2013) show that senior CIO's position in top management and commitment to strategic planning regarding cybersecurity negatively affects the likelihood of cybersecurity breaches. The study also revealed that the risk of cybersecurity breaches was higher for IT managers that were paid performance-based than monthly-paid IT managers, under whose management the risk of cybersecurity breaches was decreasing (Kwon et al., 2013). Researchers argue that this could be because cybersecurity management tasks are often insecure, whereby monthly salaries play a critical role in motivating the IT managers in the long run than the performance-based salaries. (Kwon et al., 2013.)

A sound approach for a company's top management to take control and leadership in the organization is to implement a governance framework. These frameworks exist in many levels of the organization and are not mutually exclusive. For example, top-level corporate governance (CG), information technology governance (ITG) for IT-related management, and information security governance (ISG) play well together.

3.2 Information Security Governance (ISG)

According to many scholars and researchers, information has become the lifeblood of modern companies and core to most business processes. Therefore, information security must be aligned and unified into corporate governance and regarded as a governance challenge that addresses risk management, accountability, strategic alignment, resource management, performance measurement, value delivery and reporting. (Gashgari et al., 2017; Alqurashi et al., 2017; Nicho 2018; von Solms & von Solms 2006.)

Nicho (2018) points out that the increased potential of cyber-attacks combined with a lack of an optimal mix of technical and non-technical information technology controls has led to increased adoption of ISG frameworks and controls. Gaining control of security processes is the priority when the companies are considering establishing an ISG, but the second priority of having the cybersecurity alignment with business strategies is as essential (Nicho, 2018).

The relative main concepts behind ISG are Information Technology Governance (ITG) and corporate governance (CG). On behalf of IT Governance

Institute, Guldentops et al. (2003, p. 6) explains corporate governance as to "set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are utilized responsibly." This description is widely adopted and expressed to explain the essence of corporate governance in scientific articles and literature.

ITG plays a vital role in uniting IT and corporate governance. Guldentops et al. (2003) explain that the responsibility of ITG, like other governance subjects, belongs to the board and top management. ITG is an integral part of corporate governance consisting of the leadership, company structures, and processes, ensuring that the company's IT sustains and extends its strategies and objectives (Guldentops et al., 2003). ISG is strongly related to ITG, aligned with information security as a fundamental foundation. The different dimensions mentioned before describes the information security as a multi-dimensional discipline, which applies to ISG as well (von Solms & von Solms, 2009).

Information security has also moved away from its embodiment as a technical matter, and cybersecurity is one example extending this range of facets regarding the scope of information security in general. Figure 3 illustrates the relations and positions regarding different dimensions of different scopes.

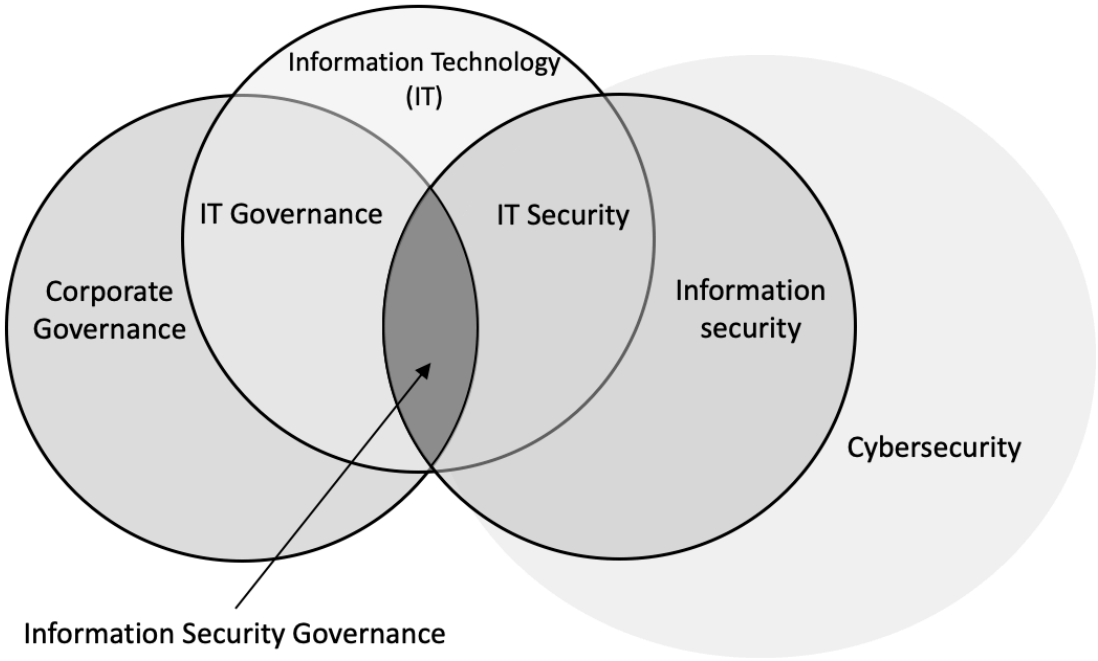

FIGURE 3 Information security governance positioned with cybersecurity (Adapted from von Solms & von Solms, 2009 p. 26)

Johnston and Hale (2009) demonstrated via empirical results that the companies addressing their information security from reactive, technological standpoints

without any ISG model are having ineffective information security levels in general and therefore are more prone to cybersecurity breaches. The other test group of companies with proactive, top-down ISG models was the opposite, delivering well organized and governed information security for the whole company (Johnston & Hale, 2009). However, ISG frameworks are often mixed with ISMS Standards. Therefore, the distinction and relation between these are necessary to explain briefly as well.

3.2.1 ISMS Standards Related to ISG Frameworks

According to von Solms & von Solms (2004), the actual content of ISG is the company's Information Security Management System (ISMS), which should be based on, and preferably certified against, the international best practices in information security. It is widely acknowledged, that typical implementation of ISMS is following the Deming's Plan-Do-Check-Act (PDCA) cycle due to the alignment with the ISMS standards (Sheikhpour & Modiri, 2012; Nicho 2018; Humphreys, 2016; von Solms & von Solms, 2009; Whitman & Mattord, 2018; Mataracioglu & Ozkan, 2011).

Regarding the PDCA-cycle, the *plan* stands for establishing ISMS policies, objectives, processes, and procedures relevant to information security. The planning phase also includes the alignment with the company's overall objectives. The *do* refers to the actual implementation and operation of what has been planned in the previous phase. *Check* stands for monitoring, assessing, measuring, reviewing, and auditing the performance and compliance of the ISMS. Check is also the phase where the results from previous phases are being compounded. Results are then turned to reports and delivered to the management for review. Finally, the *act* refers to taking corrective and preventive actions based on the PDCA-cycle so far. The important role of the act phase is to ensure that the continual improvement of the ISMS takes place in a controlled manner. This PDCA-cycle is illustrated in figure 4. (ISO/IEC, 2015; ISO/IEC, 2017; ISO/IEC, 2018b; Ristov et al., 2012; Pelnekar, C., 2011.)

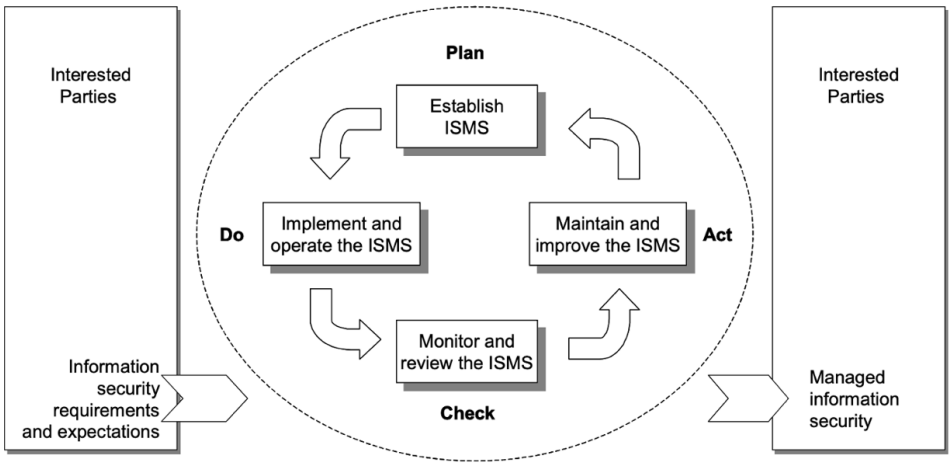

FIGURE 4 PDCA model applied to ISMS processes (ISO/IEC, 2005 p. vi)

3.2.2 Governance Model Based on Direct-Control Cycle

An example of governance execution methodology is a model discovered by von Solms and von Solms (2009), which is based on a direct-control cycle. This model is at the heart of the corporate governance (CG) and revisited during this subchapter regarding Information Security Governance (ISG). The '*direct*' stands for executing strategies and orders to establish responsibilities. '*control*' stands for guiding the outcomes, ensuring implementations, enforcing compliance, and getting feedback from directing. (von Solms & von Solms, 2009.)

According to Posthumus and von Solms (2004) and Higgs et al. (2016), there should be a separation of governance and management in the ISG. The governance side of ISG involves the top management for commitment, the company's strategic direction (Posthumus & von Solms 2004), and board-level technology committee, which signals the company's ability to detect and respond security breaches (Higgs et al., 2016). The management side is more concerned with implementing and managing the information security strategy (Posthumus & von Solms, 2004) and reporting back to the top management (Higgs et al., 2016). This separation is also the fundamental idea of von Solms and von Solms (2009) direct-control theme illustrated in figure 5.

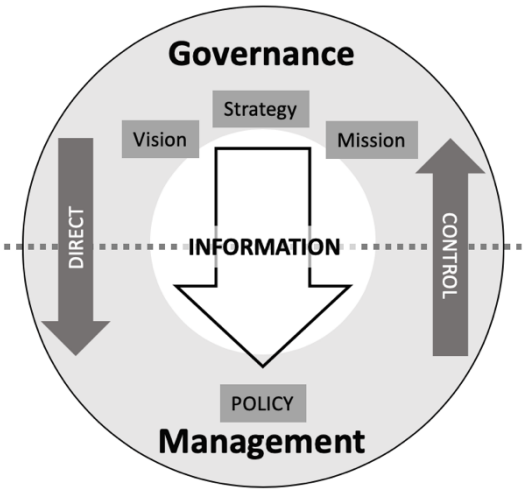

FIGURE 5 The governance and management sides of information security (Posthumus & von Solms, 2004, p. 645)

According to Chalaris et al. (2008), parties involved in CG include the regulatory body, which consists of the Chief Executive Officer (CEO), the board of directors, management and shareholders, but also all other stakeholders inside and outside of the company. These parties include suppliers, partners, employees, creditors, customers, and the community at large (Chalaris et al., 2008). To follow this direct-control cycle further, von Solms and von Solms (2009) divides and assigns the employees of the company to three levels: 1) the board of directors and executive management, 2) senior and middle management, and 3) lower

management, and administration. These levels are sometimes characterized as the strategic level, the tactical level, and the operational level (von Solms & von Solms, 2009). Based on this direct-control cycle, von Solms and von Solms (2009) introduced a model built on two dimensions; Front (Core Part) and Depth (Expanded Part). These dimensions are illustrated in figure 6.

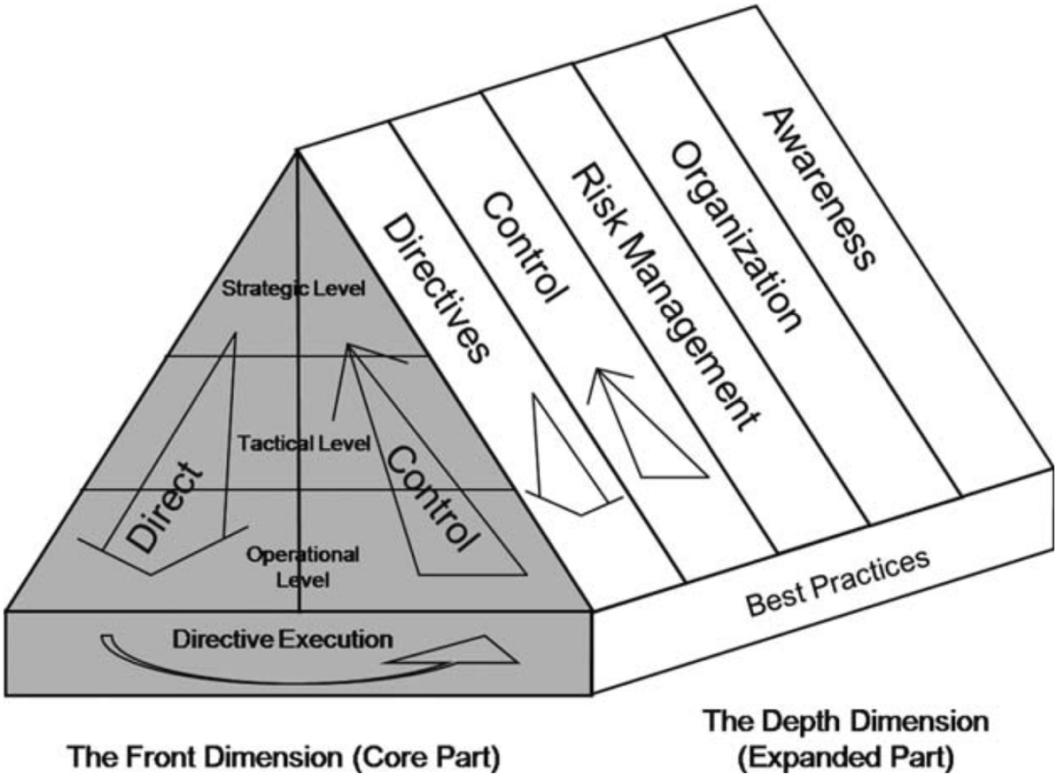

FIGURE 6 The detailed direct-control model for Information Security Governance (von Solms & von Solms, 2009, p. 31)

At the front dimension, the direct arrow 'grows' in size going from top to bottom, which indicates the expansion of the initial directives and cumulation of the content moving down to the tactical level and subsequentially to the operational level. The control arrow is functioning inversely, 'decreasing' in size, which indicates the size of the information and the feedback that flows back to the tactical and, eventually, to a strategic level as reports. Also, the width of the shape of the pyramid presents the amount of information at each level. The amount of information on the strategic level is less than on the operational level, but the information on the strategic level is more significant and refined. (von Solms & von Solms, 2009.)

Alqurashi et al. (2017) explain the directing motion on a strategic level as defining the importance of protecting information assets. Continuing on the tactical level, the alignment to the strategic level is concretizing in formulating appropriate information security policies, standards, and procedures, which also aligns with the 'plan' phase in the PDCA-cycle (see figure 4).

Finally, the administrative guidelines and procedures are implemented and realized on the operational level (Alqurashi et al., 2017). The inputs and outputs of each level are explained in table 1.

TABLE 1 Inputs and outputs of the direct principle (von Solms & von Solms, 2009, p. 34-35)

Level	**Inputs**	**Outputs**
Strategic	External factors • Legal and regulatory prescriptions • External risks	• Set of directives reflecting the expectations of the top management.
Tactical	Directives from the strategic level expanded.	• Documented policies, company standards, and procedures. • Proper alignment of all the above with the input directives.
Operational	The set of policies, standards, and procedures expanded.	• Administrative guidelines and procedures • Necessary technical measures for implementation and management • Directive execution (see figure 6)

While the direct motion of the model resembles the 'do' phase in the PDCA-cycle (see figure 4), the control principle is aligned with the 'check' element. Regarding the control principle of the model, von Solms & von Solms (2008) emphasizes the importance of 'measurability,' which sets the principle that all statements in the directives, documents, and policies to be monitored needs to be measurable. Alqurashi et al. (2017) observe that the operational level utilizes electronic sources for the measurement data, such as log files. The operational level is responsible for collecting data via interviews, questionnaires, and inspections if there is no electronic source for such data. These measurements are then reported to the tactical level, which is responsible for employing the aggregated or abstracted reporting data to determine the compliance against policies, standards, and procedures defined. (Alqurashi et al., 2017.)

Finally, the strategic level gets the reports prepared and targeted for the top management in terms of content, language, and presentation type (Whitman & Mattord, 2014; Garigue & Stefaniu 2006; Peltier 2006). According to von Solms & von Solms (2008), these reports should contain compliance and conformance status as well as reflect the relevant risk situations concerning cybersecurity. This final phase of the direct-control cycle is aligned with the 'act' phase of PDCA-cycle, which is reviewed in detail later.

The depth dimension in figure 6 (an expanded part) provides the base for the other dimensions in the form of best practices (von Solms & von Solms, 2009), which could be based on ISO/IEC 27002, for example. The content of this dimension varies from 'in-house' frameworks to strictly defined, multi-layered governance frameworks and especially in the mix of these approaches.

3.3 Cybersecurity Measures and Activities

To simplify and clarify things for the study's scope, the cybersecurity measures, methods, techniques, and procedures are separated into two main categories. These categories are technical-administrative security measures and security awareness generating activities.

3.3.1 Technical-Administrative Information Security Measures

As discussed already, information security has traditionally been founded, developed, governed, and managed in a coordinated manner. These traditions are often presented in the form of standards, best practices, and guidelines. Regarding actual information security measures, the first line and the foundation of the measures is the information security policy (von Solms & von Solms, 2009). Linked directly to the overall security guidelines and eventually to the corporate strategy, the information security policy is its place as a category of company's information security measures (Merete Hagen, et al., 2008).

When following the logical development of information security activities in the technical-administrative path, the next measures are procedures and controls directly derived from the previously mentioned information security policy. Instructions, security plans, and non-disclosure agreements, as well as controls and disciplinary enactments, are solid examples describing these methodologies. (Merete Hagen, et al., 2008.)

Administrative tools and methods are representing one category of technical-administrative cybersecurity measures. These measures are including asset classification and management, risk analysis, responding to audits, and ensuring compliance. (Merete Hagen, et al., 2008.)

Finally, many of the technologies related to cybersecurity implementations (e.g., firewalls, intrusion detection/prevention systems, honeypots, and virus scanners) are examples of technical-administrative information security measures. However, since technologies are not in the scope of this thesis, those are not handled here either.

3.3.2 Cybersecurity Awareness Generating Activities

According to Wolf et al. (2011), information security awareness is the foundation for cybersecurity programs; by making users aware of security issues, users have a better understanding to protect themselves, which cumulates protecting the company (Wolf et al., 2011). Peltier (2006) agrees by arguing that an adequate cybersecurity program cannot be implemented without implementing an employee security awareness and training program. Scholl et al. (2017) suggests qualities like behavioral awareness and self-responsibility for all employees to be educated, trained, and measured. According to Albrechtsen and Hovden (2010), the active participation of staff in information security training and knowledge

building resulted in positive changes in information security awareness and information security behavior throughout the organizations in the company.

Peltier (2006) argues that an information security awareness program is driven by fundamental confidentiality, integrity, and availability triad. Understanding the business objectives and customer needs are the first steps to build up such a program. In other words, the information security awareness and cybersecurity program need to make sense to the management, and it needs to be aligned with the business. (Peltier, 2006.)

An adequate cybersecurity program must be developed and tailored to fit (Peltier, 2006). This development does not have to start from the ground. For example, Wilson and Hash (2003), on behalf of National Institute of Standards and Technology (NIST), have released comprehensive guidance named: 'Building an Information Technology Security Awareness and Training Program.' This guidance (Wilson & Hash, 2003) identifies the four critical steps in the life cycle of an information security awareness and training program:

- Awareness and Training Program Design
- Awareness and Training Material Development
- Program Implementation
- Post-Implementation

In terms of cybersecurity education, it must be understood that different types of people are differently receptive to education, using different methods and practices. Security awareness and training programs are the vehicles for disseminating information that every person in the company, including top management, need to make the right decisions in their daily jobs. Staff security behavior training should also be tailored to different types of training for conscientious, risk-averse, and rational decision-making users. (Peltier, 2006; Gratian et al., 2018; Albrechtsen & Hovden, 2010; Wilson & Hash, 2003.)

The awareness-training-education continuum starts with security awareness, builds up to training and finally, evolves into education. This continuum is illustrated in figure 7.

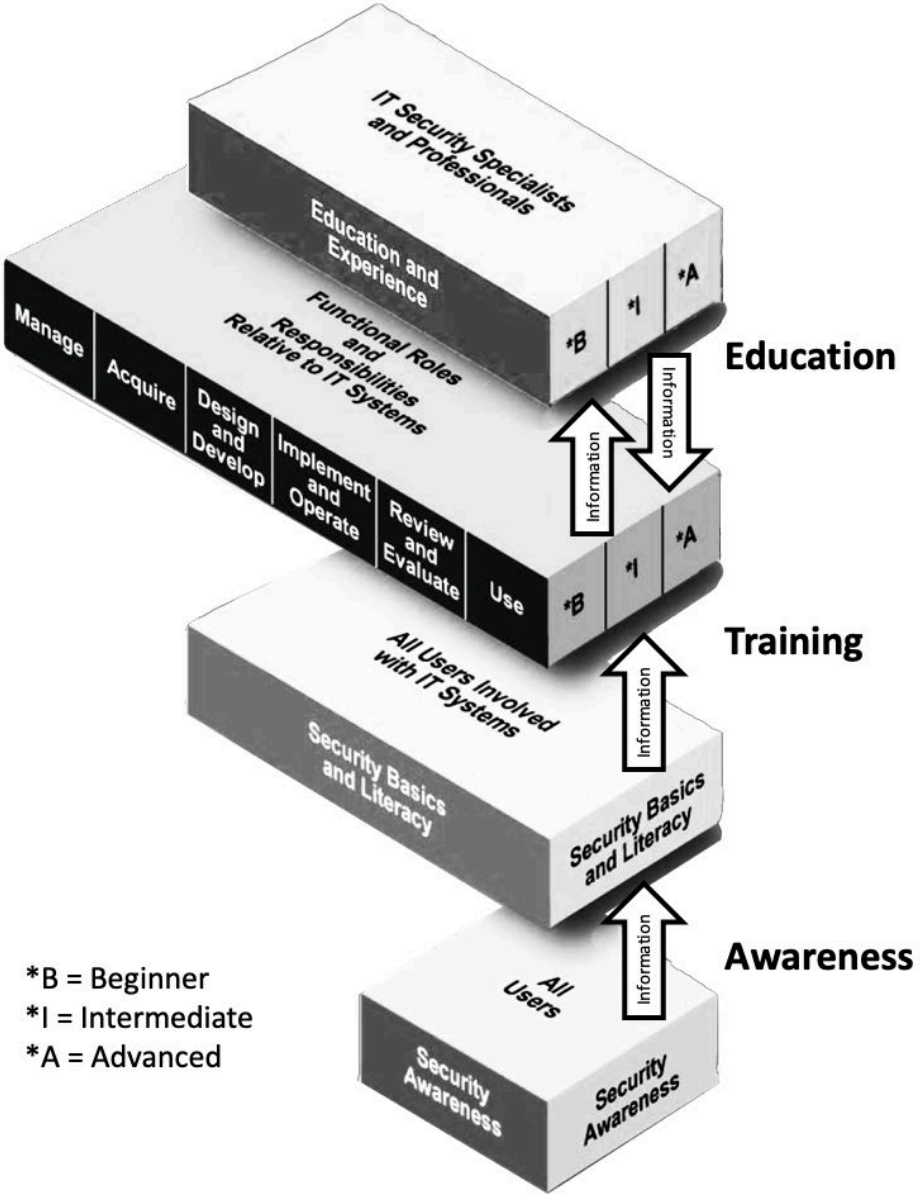

FIGURE 7 The IT Security Learning Continuum (Wilson & Hash, 2003, p. 8)

Wilson & Hash (2003) separates security awareness from training by arguing that security awareness is just getting the focus on security and allowing individuals to recognize information security concerns. According to Whitman & Mattord (2018), a security awareness program is one of the least frequently implemented but beneficial programs in a company. Whitman & Mattord (2018) support these views by agreeing that the security awareness program's primary purpose is to keep information security at the forefront of every employee's mind. Security awareness programs can be built on many dimensions, but the most typical examples are newsletters, security posters, videos, bulletin boards, flyers, and trinkets. The second role of the security awareness program is to provide a foundation for the security training level (Whitman & Mattord, 2018; Wilson & Hash, 2003).

The security training level of the continuum is targeted to the practitioners of functional specialties other than information security, like management, systems design and development, and auditing (Wilson et al., 2009). On this level, the attendees are getting detailed hands-on security training to perform their roles and duties in a more secure manner (Whitman & Mattord, 2018). An example of security training is a course for system administrators, which should address three different levels of controls: management, operational, and technical. Management controls include; policy, IT security program management, risk management, and life-cycle security. Operational controls include personnel and user issues, contingency planning, incident handling, security awareness and training, computer support and operations, and physical and environmental security issues. Technical controls include; identification and authentication, logical access controls, audit trails, and cryptography. (Wilson & Hash, 2003; Nieles et al., 2017.)

The education level of the continuum is the integration of all the security skills and competencies of the various functional specialties into a common body of knowledge, which adds a multidisciplinary study of concepts, issues, and principles. (Wilson et al., 2009). While the security training level above could comprise courses including multiple classes and even leading to certifications, the education level is aiming higher and more comprehensive approach. An example of education level accomplishment is a degree program at a college or university. (Wilson & Hash, 2003.) Comparing different levels of security awareness generation with different characteristics, according to Whitman & Mattord (2018), is composed of table 2.

TABLE 2 Comparative framework of security education, training, and awareness (Whitman & Mattord, 2018, p. 212)

	Security Awareness	**Security Training**	**Security Education**
Attribute	What	How	Why
Level	Information	Knowledge	Insight
Objective	Exposure	Skill	Understanding
Teaching method	Media: • Videos • Newsletters	Practical instruction: • Lectures • Case study workshops • Posters	Theoretical instruction: • Discussion seminar • Background reading • Hands-on practice
Test Measure	• True or false • Multiple choice (identify learning)	Problem-solving (Apply learning)	Essay (interpret learning)
Impact timeframe	Short term	Intermediate	Long term

3.4 Cybersecurity Program's Effectiveness

Cybersecurity measures implementations are demanding the scarce resources of the company: time, money, and the willingness of the employees (Scholl et al., 2017). For these technical-administrative measures and security awareness generating programs and activities, the top management wants to see the return on investment (ROI) in one way or another. However, drawing a straight cause-effect line between the investments and the actual level of cybersecurity is impossible (Khansa & Liginlal, 2009; Boone, 2017; Whitman & Mattord, 2014). Berghel (2005) further argues that the risks that information security investments are mitigating should not always be measured in ROI. If legislative mandates and related risks (e.g., securing privacy in the health care industry) are not addressed and accounted correctly, those could even potentially lead to incarceration (Berghel, 2005).

Khansa and Liginlal (2009) have shown direct, tangible benefits in their research from investing in enterprise information security. Overall, the essential profit has been the generally improved security and the ability to withstand attacks (i.e., resilience) against the company, which eventually contributes to reducing the impact of attacks, which is resulting in less financial loss and negative publicity (Khansa & Liginlal, 2009).

According to Boone (2017), adequately implemented and maintained cybersecurity is not only a defense strategy but also a significant enabler for the enterprise's performance. In companies where top management prioritizes cybersecurity is not just minimizing the risk, but also promoting and enabling the company to reach their business goals (Boone, 2017). Khansa and Liginlal (2009) discovered that the benefits above positively influence the valuation of the company in the stock market. There are many ways to assess the effectiveness of organizational information security measures. Merete Hagen et al. (2008) are approaching the effectiveness of organizational security measures from four interrelated perspectives, described in table 3.

TABLE 3 Perspectives on the effectiveness of organizational information security measures (Merete Hagen et al., 2008, p. 379)

Perspective	**Goal**	**The expectation of effectiveness of a measure**
Risk management	To reduce unwanted incidents	The ability to reduce risk to an acceptable level.
Economic	To give a positive return of investment (ROI)	The ability to give a positive ROI.
Legal	To avoid violations of legal requirements	The ability to assist the company organization in meeting the legal requirements.
Cultural	To create a good security culture	The ability to influence individual and organizational security awareness and behavior in a positive direction.

The first three perspectives on the list are related to technical-administrative information security measures, while the fourth perspective is an archetype of security awareness generating activity. The table 3 is not a comprehensive list of different perspectives regarding organizational information security measures, but enough for an example of different expectations and especially the difficulty of adequately estimating security awareness generating activities.

Dhillon and Backhouse (2001) have discovered in their studies regarding the corporate information security management attitudes some remarkable difference between weighting of formal security measures (e.g., technical-administrative measures) and security awareness generating activities. These findings are supported by Merete Hagen et al. (2008), whose main argument is that the least implemented measures have been estimated to be the most effective ones to promote the level of information security in the company. Reciprocally, the technical-administrative measures have been implemented the most but are estimated to be less effective than the security awareness generating activities (Merete Hagen, et al., 2008).

Merete Hagen et al. (2008) presents this inverse relationship between the security measure implementation and evaluation of the security measure effectiveness in figure 8 in the form of stairs. The most implemented measures are the first three stairs of the left, in that order. These three steps are constructed from formal, technical-administrative measures. As the logical development regarding the information security in the company moves towards the security awareness generation measures, the assessed level of information security performance increases. (Merete Hagen, et al., 2008.)

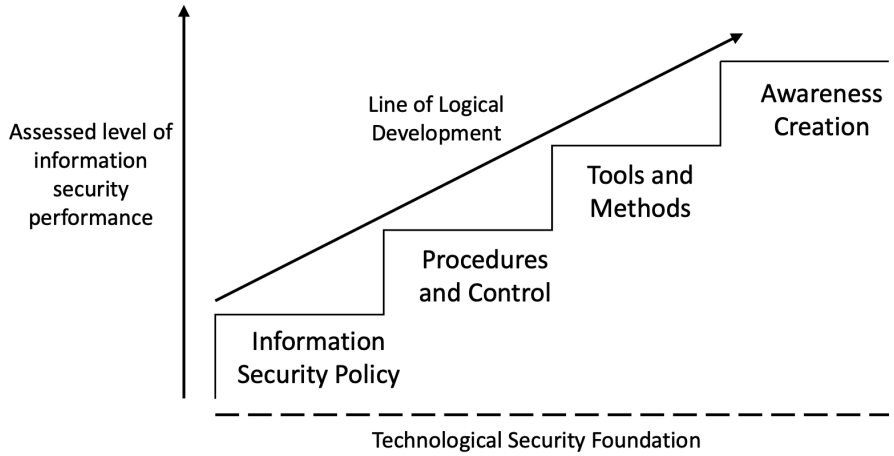

FIGURE 8 Organizational information security staircase and assessed performance (Adapted from Merete Hagen et al., 2008, p. 391

Merete Hagen et al. (2008) explains the staircase in figure 8 from the resource usage point of view as well; the measures are going more expensive and resource-intensive when moving up the stairs towards upright. So even the security awareness creation is assessed as an effective way to increase the security

in the company, the security awareness generating activities should be planned adequately to have a favorable outcome and return on investment (Scholl et al., 2017).

Finally, Merete Hagen et al. (2008) argues that the technological security foundation needs to be in place (bottom of figure 8) since there is no need to have administrative measures without technological security solutions. Merete Hagen et al. (2008) justify this by stating that technological solutions prevent, detect, and react to unwanted incidents, where technology has some role. However, from the traditional information security view, this is contradictory, since there could be information security assets, which are not dealing with technology in any way (von Solms & van Niekerk, 2013).

3.5 Reporting Back to Top Management

Regarding the direct-control model by von Solms & von Solms (2008), the accuracy, timeliness, and effectiveness of top management's decision-making depend on the feedback that the company can produce and provide. This feedback is the 'control' in the direct-control model. According to Whitman and Mattord (2014), there are two fundamental premises in order to meet the effective communications between information security and executive management.

Firstly, the efforts must occur as an ongoing collaboration between the people working in the 'field' and the top management (Whitman & Mattord, 2014), which reflects the operational, tactical, and strategic levels in the model by von Solms and von Solms (2008). The company cannot afford to risk a 'filtering effect,' which means that bad news is filtered out from the communication. The measured, aggregated, and informed facts need to be reported with transparency for the top executives to understand the state of their organizations fully. (Whitman & Mattord, 2014.) Garigue and Stefaniu (2006) point out also that the top management is not that interested in reading a report where everything is fine since that is a state as expected.

Secondly, the expressed language and wording must match the language of the audience (Whitman & Mattord, 2014). Just like the direct instructions to the users are written in the language of the users, the information security reports and presentations must be delivered to top management in a language that they communicate. Tying the message to risk, policy, procedures, standards, and tangible actions like business continuity planning are crucial to keeping the message relevant and meaningful for the top management. (Whitman & Mattord, 2014; Garigue & Stefaniu 2006; Peltier 2006.)

3.5.1 Achieving ISMS Continual Improvement

Continual improvement is a top management commitment that must be driven by the objectives set by the top management (Humphreys, 2016). In ISO/IEC

27001:2017 standard, continual improvement is compulsory, and the standard (10.2) states clearly: "The organization shall continually improve the suitability, adequacy, and effectiveness of the information security management system." (ISO/IEC, 2017, p. 14). Still, continual improvement is not merely an ISO/IEC 27001 'feature,' but a critical element of the organization's ISMS, regardless of applied standard or framework (Ristov et al., 2012).

Continual improvement could be targeted to many different sections, like processes, policies and procedures, security awareness, and training. However, the priority is that improvement is appropriately planned and implemented accordingly. Usually, the need for improvement rises from the nonconformity, which means nonfulfillment of a requirement against a standard, framework, or custom good practice guideline in the company's ISMS. (Humphreys, 2016.)

Nicho (2018) emphasizes the importance of the feedback loop in the ISG process to ensure timely corrective actions, which eventually contributes to continual improvement. This feedback loop involves communicating deviations and corrections eventually throughout the company and its organizations. Therefore, an employee security awareness training program must be implemented to address the ongoing information delivery to all stakeholders. Thus, the employee security awareness program is indirectly contributing to continual improvement (Peltier, 2006.)

As acknowledged before, the typical implementation of ISMS is following the Deming's Plan-Do-Check-Act (PDCA) cycle (Nicho 2018; Sheikhpour & Modiri, 2012). The last phase, act, play a critical role in the continual improvement of the company's ISMS. The corrective and preventive actions based on the reports, audit results, and management reviews are aligned with the act phase (Mataracioglu & Ozkan, 2011), but the top management view for cybersecurity performance needs to be addressed separately.

3.5.2 Top Management view on Cybersecurity Performance

Top management is viewing and assessing the performance of information security and cybersecurity, mainly based on the reports and information delivered from the tactical level (Nicho, 2018; Humphreys, 2016). The ISMS performance is measured and reviewed on the tactical level in the check phase of the PDCA-cycle. For ISMS general performance review, Humphreys (2016) is suggesting three viewpoints to assess the performance:

- Effectiveness: Is ISMS producing a desired or intended result successfully?
- Adequacy: Does the ISMS deliver acceptable quality and amount of cybersecurity?
- Suitability: Is the ISMS right and appropriate for the company's needs, purpose, and business?

The challenge in the cybersecurity performance assessment for the whole company, including top management, is that the ISMS is continuously changing.

And not only the ISMS is changing via the company's change management process intentionally, but the operating environment is changing as well. The new legislation, regulations, and the changes in the market need to be addressed, and usually, these are implicating the ISMS as well. (Humphreys, 2016.)

According to ISO/IEC's 27001:2017 standard, point 10.1d-e states, "the organization shall review the effectiveness review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary" (ISO /IEC 27001, p. 14).

ISMS itself, indeed, is supposed to change regularly, for continual improvement. However, are the changes evaluated adequately as improvements, or are the changes just tracked as implemented? Every change in the ISMS is not necessarily an improvement. For this, the changes need to be tracked over time and evaluate accordingly, if the changes made were improvements, and therefore taking the performance in the right direction, and eventually advancing the ISMS. (Humphreys, 2016.)

3.6 The Empirical Research Gap

There is quite negligible visibility in the research literature to the top management work regarding cybersecurity governance since it has been a traditionally challenging area to access information and conduct research. Things related to governance are typically in the background and behind the scenes. Governance frameworks, methods, and models are presented thoroughly in the literature, but the real implementations and realizations of such tools are absent from the research literature.

Research literature contains studies and information regarding both technical-administrative security measures as well the security awareness generating ones. However, the benefits and consequences of mutual existence and utilization of these measures seem to be absent from the scientific literature. The top management needs to have a clear vision of the effectiveness and performance of the directives that they have decided on as a company's strategy. Top management needs to know if the changes eventually turned to performance improvements and worked in benefit for the company. Cybersecurity-related strategic decisions are not an exception to this rule. The research literature does not have visibility into this phenomenon, and neither does address this collaboration between the top management and cybersecurity governance. There is also an empirical research gap concerning real implementations of cybersecurity governance.

The study addresses the perspectives mentioned above and conducts a qualitative study on these. Empirical research aims to fill this gap by examining the collaboration between the top management and cybersecurity governance. It is exciting to see the empirical perspective and get more focused and timely answers to the research question and the sub-questions.

4 Research Setting and Content Analysis

Conducting research is developing knowledge in a particular field. Development of knowledge has a *system of beliefs and assumptions* as a foundation, which is called the research philosophy (Saunders et al., 2019). Albeit, the researcher, is not making just assumptions and trusting beliefs, but a well-justified and evaluated decisions in every phase, based on the philosophical underpinnings of information security research, which leads the research process throughout the journey. (Eskola & Suoranta, 1998.)

The purpose of this chapter is to reveal, explain, and justify the assumptions and especially decisions that I have made during the research process. These decisions need to be aligned with each other and to be mutually supportive of fitting the research aim of the study.

4.1 Interpretive Research Philosophy

It is worth mentioning that a vast majority of qualitative research in the information security research area is using the interpretive philosophy approach and especially in research based on case studies and interviews, like in this research (Cascaca & Florentino, 2014). Since the research aim is focusing on the experiences from top management strategy work, cybersecurity direct-control measures, and reporting back to top management, interpretivism was justified as an appropriate philosophical approach to conduct this research (Dhillon & Backhouse, 2001; Saunders et al., 2019).

4.2 Qualitative Research Design Methodology

For the research aim in the study, I adopted a qualitative research design as an overarching research methodology. The qualitative research design involves a wide variety of traditions, approaches, data collection, and analysis methods to study meanings that manifests in most diverse ways. Therefore, it is not reserved for any particular discipline; neither is it just one way of researching. (Eskola & Suoranta, 1998; Hirsjärvi et al., 2009.)

4.3 Case Study Research Strategy

I chose to implement a case study approach for the research strategy in the study. The case study is an in-depth inquiry into a topic or phenomenon within its real-life setting, with the capacity to generate insights leading to detailed empirical

descriptions and development of the theory, without limiting the methodological choices, disciplines or analysis methods (Eisenhardt, 1989; Eisenhardt & Graebner, 2007; Yin, 2018).

Case study research aims to obtain detailed and intensive information from a small number of related cases (Hirsjärvi et al., 2009). Yin (2018) adds that thorough consideration and examination of cases is essential since the goal of the case study is not to seek causality or typical features. From these groundings, the case study research strategy is justified and aligns naturally with the research aim and the research question.

4.3.1 Multiple-Case Study Design

In this research, a single case was referring to a company whose collaboration between the top management and cybersecurity governance was in the focus of the thematic interviews. Multiple companies were attending the study as cases, which adjusted the design of the research strategy in the study to be conducted as a multiple-case study. The actual cases are introduced later in this chapter.

4.3.2 Case Study Participants

The participant recruiting for this initiated through a professional network, which consisted of people working in different cybersecurity organizations. The nature of this business network is strictly professional, so the bias from selecting friends or relatives as participants was ruled out (Saunders et al., 2019; Sarajärvi & Tuomi, 2018).

Also, I based the criteria for the companies to participate in the study on three factors regarding the companies and the participants. Firstly, the company must have a full-time responsible person for cybersecurity management (and governance). Secondly, this person should have been in collaboration between top management. Thirdly, this person and the company accepts voluntarily to be a participant for this case study research. These selection criteria were formed by estimating industry professionals' characteristics, which could have information that might help answer the research question. These selection criteria were also reviewed and evaluated with the help of the aforementioned professional network.

I selected five (5) participants from five (5) companies to participate in the study in two weeks. None of the companies nor participants canceled or denied participation in any way during or after the study. Instead, all of the participants were motivated by the research aim. All participants expressed their personal and professional interest in the study.

According to DiCicco-Bloom and Crabtree (2006), the sample of participants should be reasonably homogenous. Therefore, from the resemblance perspective, the selected participants were representing somewhat the same role in their companies. Also, the participants had direct responsibility regarding cybersecurity. They had the mandate for cybersecurity from the company's top

management. Furthermore, the participants were involved in implementing the cybersecurity in their company.

From a divergent perspective, the companies that selected participants represented were all from different industries; IT services and consulting, software development, financial services, business intelligence, and media. Table 4 contains the necessary information about the cases. Case company names were pseudonymized to protect the privacy of the participants and comply with the agreement about the privacy and data protection with the case companies. However, some background information about the companies is in table 4. The aim is to offer some kind of personality for each of the cases.

TABLE 4 The companies and participants in the case study research

Case Company Name	**Participant Role**	**Company Industry**	**Size in no. of Employees**	**Company Age in Years**
IT Company	CSO	IT Services and consulting	1000+	Over 20
Software Company	CISO	Software development	100-1000	Under 20
Financial Company	Director of Cybersecurity	Financial Services	1000+	Under 20
BI Company	CISO	Business Intelligence	1000+	Under 20
Media Company	CISO	Media	1000+	Over 20

Right after the participants accepted the invitation, their participation was to the study was personally confirmed. The first information delivered was about the schedule of the study in the form of a research plan, including the data collection plan. Also, I delivered the preliminary interview questions to the participants at this point so that they could prepare for the actual interview. The participants were allowed to comment on the research plan and its contents, data collection plan, and the preliminary interview questions, but none of the participants saw this necessary. The interview questions were then reviewed, evaluated, and qualified with the aforementioned professional network's help.

After the initial participant informing, the study continued with research plan development for a month. In January 2020, I presented the research plan in the Pro Graduate seminar. The feedback from the peers and supervisor regarding the thesis adjusted the research plan accordingly. Subsequently, I delivered the finalized research plan to the case study participants. At this point, I suggested a pre-scheduled event for the interview with all participants. After minor adjustments to the schedule, we were able to schedule all interviews to be held during February-March 2020. Only one interview was postponed by a week by personal reasons of the participant. The final set of interview questions and some generic guidance about the interview process were delivered a day or two before each interview for each participant. All interviews were conducted on time and

held at the premises of the participants. A lunch was offered to participants after the meetings as compensation from the participation in the research.

4.3.3 Assessing the Quality of the Research Design

Case study research has been criticized for the lack of scientific rigor, reliability, and generalizability (Yin, 2018; Noor, 2008). These are, however, addressed by executing multiple case studies instead of single ones (Noor, 2008) and explaining the research setting thoroughly (Darke et al., 1998). According to Yin (2018), the most significant criticism against case studies is about the flexibility of case studies, which is initially a strength. The flexibility could indeed be a problem if the case study is not designed, framed, scoped, and conducted correctly. (Yin, 2018.) The quality of the research is assessed thoroughly in chapter 6.6.

Since time was a constraint on this research, the time horizon was limited. Therefore, the research was conducted in a cross-sectional fashion, meaning that, for example, I conducted the data collection only once per case. According to Saunders et al. (2019), case studies based on interviews can be conducted over a short time. The downside of the cross-sectional time horizon is that there is no opportunity to examine the development of the phenomena over time.

4.4 Data Collection Process

I conducted the data collection process for the empirical part of this research as thematic interviews. Intention to record the interviews were presented to the participants already in the data collection plan, and none of the participants took their opportunity to comment or modify the plan. Therefore, the participants agreed at the consent to the recording of the interview. As Eskola and Suoranta (1998) suggest, the agreement about the interview recording should be obtained before the actual interview.

To justify thematic, (aka. semi-structured) interview as a data collection method, Sarajärvi, and Tuomi (2018) argues the flexibility as an essential advantage. The interviewer has the opportunity to repeat the question, correct misunderstandings, clarify the wording of the expressions, and have a discussion with the participant (Sarajärvi & Tuomi, 2018). Hirsjärvi and Hurme (2015) add that the interviewer has an opportunity to process the answers briefly and is, therefore, able to immediately evaluate each response's adequacy. Since the interview themes are based on the research aim and theoretical framework of the study, the interviewer was able to start the analysis already preliminarily during the interview. Hirsjärvi and Hurme (2015), supports this approach by stating that the analysis of the data begins on the data collection phase already.

The weakness of the interview compared to the survey is time and money. Interviewing is an expensive and time-consuming method of data collection.

Interviews are also criticized for the interviewee's inconvenience, the fatigue, and lack of motivation from the interviewer's side. The difficulty of the interview environment can also lead to the failure of the interview. (Hirsjärvi & Hurme, 2015; Sarajärvi & Tuomi, 2018.) Hirsjärvi and Hurme (2015) argue that one of the disadvantages of the interview is also that anonymity cannot be guaranteed to the interviewees. The risks are addressed in chapter 4.4.2.

4.4.1 Data gathering: Thematic Interviews

I conducted interviews in the native language of the participants (Finnish). I made this decision so the participants could focus on the actual interview instead of the language. I transcribed and translated the recordings to the English language right after the interview so that the interview was still in the researcher's working memory. The transcript was not produced as literal word-by-word repetition since the goal was not to examine the language, wording, or expressions. Though, I formed the transcript without losing nor adding any information or meanings to the content.

After the transcription, as Hirsjärvi and Hurme (2015) suggest, I offered for the participants an opportunity to review, comment, and correct their interview, which I transcribed to as the first person. Some of the participants took this opportunity. Finally, I collected an acceptance for the final interview data from all participants after transcription.

Questions (see appendix 1) were mostly formulated as open-ended questions to guide the interviewee to answer openly within the research aim and interview theme boundaries. These themes were then derived from the focus areas and from the theoretical framework of the study. I categorized the questions forming three themes:

- Cybersecurity aligned to the strategy work of the company.
- Cybersecurity implementation and governance.
- Assessing and reporting the effectiveness of cybersecurity.

The questions were ordered by priority under each theme to support the unlikely event that I would need to reduce the interview material by leaving answers to low priority questions out from the data. This need for reduction never realized, and every participant has answered every question. We reserved 1,5 hours for the interviews, but all of them concluded in under an hour. Therefore, the data collection for the analysis was complete. However, the interview data needed to be protected adequately between the interview and analysis.

4.4.2 Interview Anonymity and Data Protection

According to Saunders et al. (2019), as part of the ethical considerations of the research, the continuing anonymity of the participants must be in place. As a part of the study, I conducted a risk assessment. The interview data, especially when

linked to the companies, is highly confidential. Therefore, I identified the risk that the names of the participants or the companies might get disclosed. I controlled and mitigated the risks by three main measures, which were all implemented to the full extent:

1) Not mentioning any names of people or companies or any indirect descriptive terms, which could relate to participating people or companies in any phase before, during, or after the study.
2) Pseudonymization of the interview data during the transcript process.
3) Destroying the recordings immediately after the transcribing.

I recorded the interviews on a voice recorder (Sony ICD-BX140), which cannot transfer the recordings to any other device or network services. Thus, the recordings were not susceptible to intrusion through the network or devices. The recording device was kept near the data collector for the duration of the collection and transcribing to ensure physical security. All of these risk mitigation measures were successful. I was able to keep the anonymity of the participants and the companies throughout the research, as planned.

4.5 Theory-Guided Thematic Content Analysis

Hirsjärvi and Hurme (2015) state that the processing of qualitative data involves many steps. At its core is both *analysis* and *synthesis*. Where the analysis specifies and classifies the data, synthesis aims to create an overall picture and present the phenomenon in a new perspective (Hirsjärvi & Hurme, 2015), which is summarized in figure 9.

The analysis part (upper section in figure 9) of the content analysis is applied during this chapter. The synthesis-part (lower section in figure 9), however, is examined during chapters 5 and 6.

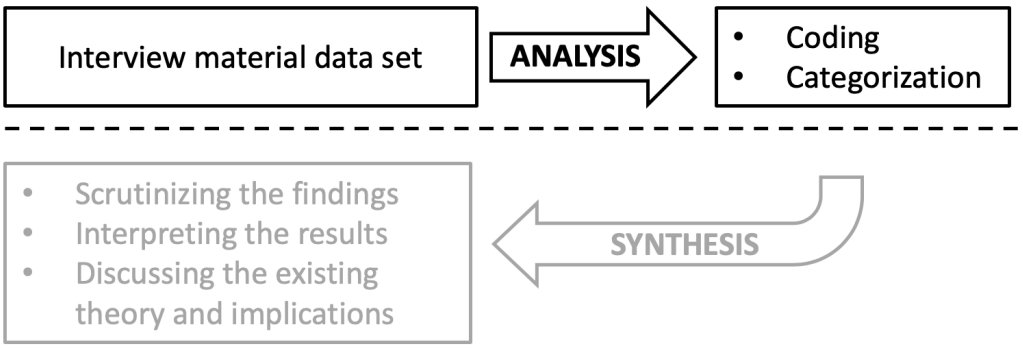

FIGURE 9 Content analysis emphasized (Adapted from Hirsjärvi & Hurme, 2015, p. 144)

The primary method of analysis that can be employed in all traditions of qualitative research is *content analysis*. Content analysis can be considered not only as a single method itself but also as a loose theoretical framework that comprises multiple different sets of analyzes. Since I grounded this research into the interpretive paradigm, I was able to rule out the epistemological positioning and data-driven approach (Eskola & Suoranta, 1998) to the analysis. The problems of data-driven analysis can be solved by *theory-guided content analysis*, which has theoretical connections so that the theory can serve as an aid, but the analysis is not directly based on theory (Sarajärvi & Tuomi, 2018). The theory-guided content analysis approach aligns naturally with the research aim and the previous decisions applied in the research setting.

Thematic, theory-guided content analysis has been chosen as an analytical method for this research already in the research planning phase, as Hirsjärvi and Hurme (2015) suggests. Therefore, this chosen method of analysis was the guideline for this research from planning the interviews through unwinding the raw interview data and underpinning the actual thematic content analysis.

To be exact, I started the actual analysis of the interview material already in the interview phase. According to Hirsjärvi and Hurme (2015), the researcher must strive to reach the interview response's essential content. The information from raw recordings to the transcribed material has already passed the thinking process of the researcher. Therefore, the researcher has already made decisions and assumptions about the material, i.e., analyzed the material (Hirsjärvi & Hurme, 2015).

Content analysis, in general, has been criticized for the incompleteness, which could occur when content analysis is applied just to organize the collected data for concluding (Sarajärvi & Tuomi, 2018). Following the findings by Eskola and Suoranta (1998), I separated the analysis phase (chapter 4.5) from the interpretation (chapter 5) phase, yet tightly interconnected.

In the analysis phase, I separated the material relevant to the research aim from the raw, transcribed interview material via thematic analysis, using coding and categorization techniques. Eskola and Suoranta (1998) argue that in practice, it is challenging to construct intact interpretations from the interviews before even a rough grouping of the interview material, despite the technologies utilized or not.

All in all, utilizing the theory-guided content analysis approach is justified in this research, but with two remarks. 1) Decisions made during the analysis are subjective, and I scoped the themes tolerably from the research aim already. 2) The new insights and interpretations emerged from the empirical research data during the coding and categorization phase and when the findings were discussed with the literature, rather than via thematization.

According to Sarajärvi and Tuomi (2018), the logic of reasoning in the theory-guided analysis is often abductive. The thinking processes during the content analysis were varying between the theoretical orientation and ready-made modeling. Consequently, the abductive reasoning was underpinning the content analysis as well as the approach behind inference in this research.

4.5.1 Preparing for the Analysis

The preparation for analysis was begun by reading the transcribed interview material couple of times with an active or even interactive approach, as suggested by Eskola and Suoranta (1998), and supported by Hirsjärvi and Hurme (2015). Hirsjärvi and Hurme (2015) argue that the quality of the analysis depends on how familiar the researcher is with the material. At this phase, especially things and themes like circumstances, definitions, processes, activities, events, strategies, and structures were targets of interests.

4.5.2 Describing the Material

According to Hirsjärvi and Hurme (2015), the first step of the actual analysis is describing the material, and by describing, they denote the practice of mapping the characteristics or traits of people, events, or objects. At this phase, I imported the transcribed interview material to the computer-assisted qualitative data analysis software (CAQDAS) ATLAS.ti. Each interview was imported into the analytics software project as its entity, a document. Saldaña (2015) suggests using CAQDAS as part of the qualitative research, as it helps to handle the material, build structural networks between the coded content, and to visualize the findings.

Eskola and Suoranta (1998) argue that if the research remains at the level of just a description of the data, the output could be as well called just a statement using qualitative methods. Therefore, for maintaining the quality in this research, the content analysis of the transcribed interview material was continued in ATLAS.ti software towards coding and categorizing.

4.5.3 Coding and Categorizing in Theory-Guided Analysis

As the approach for analysis theory-guided, it was natural to assign the three themes of the thematic interview to act as a red thread of the coding and categorizing in this research as well. These themes guiding the analysis were derived directly from the research setting. Those aligned naturally to the theoretical framework of the study and driving the analysis with those were justified. Before going into coding or further in the analysis, the base unit of the analysis '*code*' needs to be defined. Saldaña (2015, p. 4.) describes code as:

> In qualitative data analysis, a code is a researcher-generated construct that symbolizes and thus attributes interpreted meaning to each datum for the following purposes of pattern detection, categorization, theory building, and other analytic processes.

Saldaña is providing a comprehensive list of over 40 different analytic approaches to coding with their strengths and weaknesses. From that list, 'themeing the data' was the analytic approach applied as a coding method for this research. This selection was justified by the suitability of the approach in

interpretive research philosophy. I conducted this phase of the analysis by systematically going through the material and assigning codes to the transcribed interview material following the ATLAS.ti best practices (Contreras, 2020).

The coding process was quite straightforward, since the themes derived from the research setting were delimiting the scope clearly, and the interview material was prepared accordingly, as described previously. However, there is one layer of information between the transcribed interview material and the codes. This layer is *a quotation* is, which is required as a base structure. The *quotes* are excerpts from the interview material, where the codes are *linked*.

4.5.4 Coding Process

I conducted the quotation and coding of the interviews by going through the transcribed interview material of all five cases in an iterative fashion. The quotations were extracted as pieces of information (Saldaña, 2015) from each interview. The codes were recognized as in the scope of each quotation at this phase.

In the first round of coding, on average, I made 50 quotations per each interview. It is worth noticing that quotations after the first iteration were quite broad and over mainly overviewing at this phase, consisting of full sentences and even full answer blocks containing multiple sentences. I was able to identify a total of 153 individual codes linked to these quotations from the transcribed interview material after the first round. Then the recognized codes were categorized into four categories aligned to the research aim accordingly. These initial categories are presented in table 5.

TABLE 5 The categories after the first round of analysis

Category name	**No. of codes**
Top Management's Alignment with Cybersecurity	54
Cybersecurity Governance and Management	39
Cybersecurity Directing	38
Cybersecurity Controlling	22

Since the quotation, coding, and linking was an iterative process in nature, I conducted the second round of coding after forming the first categories. The second iteration of the transcribed interview material was conducted even more deliberately and meticulously than in the first round. The second iteration started with going through every individual interview, just like in the first round of quotation and coding.

In this second round of quotation, coding itself, categories, and the quotations altered remarkably. I extracted the quotations from full sentences to smaller units, grounding only the linked codes. This refinement increased the value of the analysis remarkably via more granular oversight. New quotations were made, new codes were introduced, and new categories were formed. Also,

subcategories were born in this phase. Subsequently, I assigned some of the new codes to different categories and refined the analysis.

Finally, after the second iteration, I conducted a third iteration. However, this was merely an oversight of the transcribed interview materials with the new codes discovered in the second iteration, which induced few minor alterations to the coding and concluded the quotation and coding process of the transcribed interview data. The list of final categories and subcategories after the second and third rounds is in table 6.

TABLE 6 The categories after the second and third round of analysis

Category name	**No. of codes**
1. Top Management's Alignment with Cybersecurity	10
1.1 Strategy Work	22
1.2 View on Cybersecurity	12
1.3 Top Management Activity	25
2. Cybersecurity Governance and Management	8
2.1 Culture	11
2.2 Best Practices	14
2.3 Governance, Organization, and Cybersecurity strategy	18
3. Cybersecurity Directing	17
3.1 Training	14
3.2 Measures	9
4. Cybersecurity Controlling	10
4.1 Measuring	16
4.2 Reporting	11
Total	**197**

As an additional insight into the analysis, between the first and second round, the average quotations per each interview raised remarkably from 50 to 105. The original transcribed interview material as data was abstracted even more and 'made visible' via the coding and categorizing. Table 7 sheds some light on the number of quotations and codes in each analyzed case.

TABLE 7 Total quotations and codes of each case

Case Company Name	**Total Quotations**	**Total Codes Grounded to Quotations**
IT Company	149	244
Software Company	48	94
Financial Company	109	228
BI Company	124	339
Media Company	93	272
Total	**523**	**1177**

Appendix 2 contains all codes grouped by code group and the groundedness[2] of each code. The codes' groundedness reveals the most frequently linked codes and prioritizes the synthesis accordingly.

4.5.5 Codes-to-Theory model

The coding and categorizing process followed the basic *codes-to-theory* model by Saldaña (2015), as illustrated in figure 10. Process in the codes-to-theory model moved (left to right) from individual codes to optional subcategories, categories, followed by identifying themes and concepts. These themes and concepts would eventually develop into assertions and even theories. At the same time, the material was adapting more abstract forms.

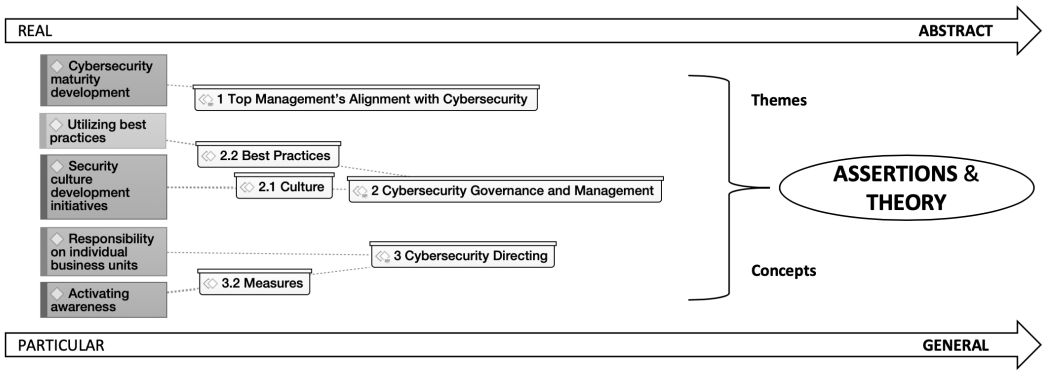

FIGURE 10 A streamlined codes-to-theory model for qualitative inquiry (Adapted from Saldaña, 2015, p. 13)

Since the research aim underpinned the categorization, it produced somewhat predictable findings concerning themes and concepts. It is necessary to clarify that, according to Saldaña (2015), the themes and concepts in figure 10 are typical outcomes of the coding and categorization and, therefore, not necessarily directly related to the research aim. However, as discussed before, in this research, the themes align with the research aim by theory-guided approach.

4.5.6 Summary of the Content Analysis

The empirical data analysis consisted of theory-guided analysis, which was conducted by coding and categorizing. Despite the absence of 'naturally emerging themes' (Saldaña, 2015), the data has revealed many new insights during the analysis so far. These insights – i.e., themes and concepts (see figure 10) – were then examined more closely from the case study dimension via the synthesis in the next chapter as empirical findings.

[2] Groundedness is a numeric indicator of how often the corresponding code is linked to a quotation.

5 Empirical Findings and Insights

After the content analysis for the empirical research data, the research process turns from analysis to synthesis. The analysis refined the *research data* to *empirical research material* via coding and categorization. The categorization acts as a 'gateway' into the research data. Hence, the function of categories is to bridge the insights to the research data and vice versa. Illustration of the current phase of the research process is in figure 11.

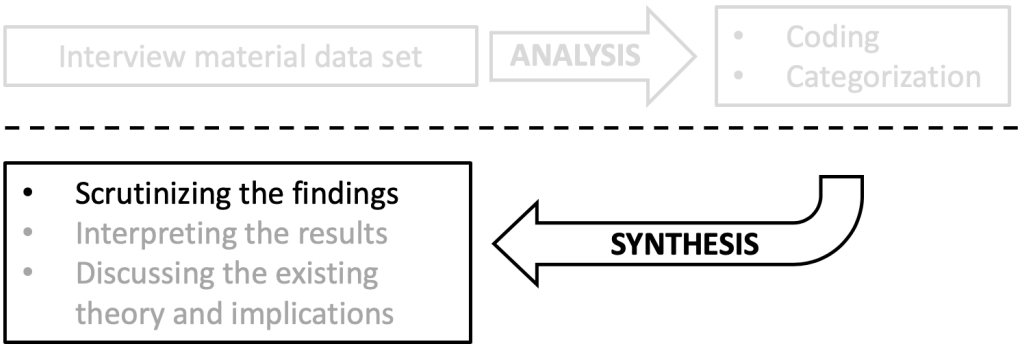

FIGURE 11 Scrutinizing the findings as to the first phase of synthesis (Adapted from Hirsjärvi & Hurme, 2015, p. 144)

The purpose of this chapter is to reveal the empirical findings of the research. The majority of the discoveries in this chapter are emerged from the empirical research material directly, using the voice of the participants. Some insights are, however, more indirect and ensued from the perceptions of the researcher. These insights are based on a throughout examination, combination, and linking excerpts from the empirical material rather than detailed interpretation, which belongs to the next chapter.

This chapter concerning the empirical findings divides into four subchapters (5.1, 5.2, 5.3, and 5.4). These four main categories emerged during the analysis (see table 6). Through each of these subchapters, the examination concerns the most remarkable insights related to each main category and the research questions. The focus was prioritized particularly by relevancy for the research aim, but also by the groundedness of the findings. This approach respects the most relevant, most collective, and most exciting insights in the spotlight.

The primary sources for findings in each category were the answers to the interview questions under the theme aligned to the category. Table 8 explains this alignment. Albeit, some of the findings were supported by the interview answers under other themes as well.

TABLE 8 Primary interview sources for the result categories

Finding category	**Primary interview theme source for the insights**
5.1 Top Management's Alignment with Cybersecurity	Theme 1: Cybersecurity aligned to the strategy work
5.2 Cybersecurity Governance and Management	Theme 2: Cybersecurity implementation and governance
5.3 Cybersecurity Directing	Theme 2: Cybersecurity implementation and governance
5.4 Cybersecurity Controlling	Theme 3: Assessing and reporting the effectiveness of cybersecurity

As a guide to the text in this chapter, the format of findings is '**bold text in single parenthesis (groundedness)**,' when the finding is mentioned for the first time**.** When referring to the finding again in the text, it is typed without bolding**.** The quotations from the interviews behind the findings are animating, characterizing, and supporting the discoveries.

5.1 Top Management and Cybersecurity

This category emerged during the analysis from the discoveries concerning top management while focusing primarily on the strategic level of the participating companies. Considering the relevancy for the research aim, the insights from this subchapter align with the main research question*; 'how does the top management collaborate with the company's cybersecurity governance?*' from the 'top-down' point of view. Also, the 'bottom-up' perspective is scrutinized for this phenomenon, in chapter 5.4.

The focus findings in this category are Cybersecurity maturity development, enabling business, views on cybersecurity in general, activities regarding cybersecurity, and corporate strategy development. Through these findings, the insights are revealing the collaboration measures, events, and priorities of the top management. Moreover, these perceptions are demonstrating the differences in the manifestations of such collaboration in the participant companies.

5.1.1 Cybersecurity Maturity Development

A key insight from this category is the prevalence of the major finding '**Cybersecurity maturity development (32)**'. All of the participants acknowledged cybersecurity maturity development as a remarkable principal theme regarding alignment and connection between the top management and the department of cybersecurity management of the company. Besides, the participants mentioned cybersecurity maturity development, even if the question was concerning the tactical or operational level of the organization. The expressions of cybersecurity maturity development manifested somewhat

differently in different companies. Still, the common factor between the participant's views was understanding the cybersecurity maturity development as a continual, interactive, and collaborative process with the top management.

For example, the participant of BI Company referred to the cybersecurity maturity development from cybersecurity strategy development and capability maturity model perspective, while emphasizing the connection to the company's top management:

> Strategic thinking in our company is related to the cybersecurity strategy from the long-term development point of view. Focus areas are reflecting on the cybersecurity strategy, which is under substantial development. (BI Company)

> To develop our operations, we have a capability maturity model (CMM), which guides our development in general. (BI Company)

> We have a real dialogue going on with the top management, and we are developing our information security and cybersecurity together. (BI Company)

The Financial Company's participant echoed the perspective of cybersecurity strategy as well, while also explicitly mentioning the top management's support:

> We have developed our company situational awareness about our cybersecurity maturity level on a wide front. Last year, our own dedicated cybersecurity strategy was born with support from top management. (Financial Company)

The participant of Media Company revealed their viewpoint on cybersecurity maturity development as from 'ground-up.' The accent was on utilizing the expertise of external partners for understanding the baseline and 'ground-level' of the current cybersecurity maturity level:

> We have also found the external partners and specialists very effective in helping us to understand our baseline and the ground to start the actual information security maturity development. (Media Company)

Also, the Media Company's participant underlined the importance of the foundational approach in cybersecurity maturity development as well as measuring the progress. Aligning to the Media Company's strategy, the BI Company's participant highlighted the value of (external) audits as the driver for cybersecurity maturity development:

> External audits are also one very effective and sovereign perspective to our information security and cybersecurity effectiveness and performance levels. (BI Company)

> When the basics are in place, the dashboard begins to provide more useful and richer measurement results. (Media Company)

Likewise, in the IT Company, (internal) audits were powering the cybersecurity maturity development. Their participant tied the cybersecurity maturity development to the co-operation inside the (quite a large) company:

> Views to improve the level and performance of the information security in our company arises from the internal audits as well from discussions and information sharing among security professionals. (IT Company)

The participants linked the cybersecurity maturity development to pursuits for industry best practices. Going forward with the opinions of the participants, these were often related to ISMS development, as the activities were often associated with the initiatives and projects for attaining official certifications for the ISMS's (e.g., ISO/IEC 27001):

> We have set the continual improvement goals based on the ISO/IEC 27001 requirements. (BI Company)

The perceptions from the material identify the continual improvement process in ISO/IEC 27001 (ISO/IEC, 2017) as a tailwind for cybersecurity maturity development in all companies, except in Financial Company. The participant of the Financial Company explained their dissenting approach. Their line was the major contributor to the finding '**Industry regulations (6)**.' Also, the divergence of responsibilities compared to other companies in this research affects their line regarding (for example) ISO/IEC 27001 certification:

> Because the regulations are directing our company already in quite a strong manner and we are mainly producing the cybersecurity work for our company itself, we haven't seen it necessarily useful for us to certify against yet another standard. For example, we don't have immediate plans to certify our ISMS against ISO/IEC 27001. (Financial Company)

In conclusion, all participants alluded (sometimes indirectly, but still) frequently to the cybersecurity maturity development throughout their responses. Those answers related to virtually all activity in the company connecting with cybersecurity. The cybersecurity maturity development emerged as an overarching and holistic theme regarding the alignment and connection between top management and cybersecurity management of the company.

5.1.2 Cybersecurity as a Business Enabler

The second striking insight from this main category is based on the finding '**Cybersecurity as a business enabler (17)**'. Again, participants were unanimous about the subject and expressed the significance of cybersecurity to the company's actual business. The participant of Software Company stated that there is not just one way of business enablement by cybersecurity. Moreover, the security and privacy requirements were not only from the business' demand but also emerging from the customer requirements:

> We see information security and cybersecurity in our company as a business enabler in many ways. Our commitment to our customers is demanding effective information security, cybersecurity, and privacy measures in place. (Software Company)

However, the analysis of the empirical data did not focus on the obvious point, that 'should the cybersecurity enable the business or not?' – but more to the insights behind. This approach also revealed the thought of 'connection' between the compulsories and the business enablement in the participant's views:

> The customer requirements are quite well in our top management's knowledge. Therefore, this support function turns into a strategic business enabler. (BI Company)

> Cybersecurity is definitely both; support function as well as a strategic partner. Due to the new cybersecurity strategy, the strategic partnership has become visible and as an opportunity to the top management. (Financial Company)

> At the early steps of organized information security management and governance, the business unit leaders did think these initiatives more as a compulsory and cumbersome measure. But with the corporate top management support, the mindset was aligned after a while in the whole company towards the strategic partnership. (Media Company)

The IT Company's participant countered the previous comments and estimated that the business enabler role of cybersecurity could be more of a future direction in their company:

> In principle, the security organization is seen from the top management as more of a regulatory compliance department. Lately, there have also been some initiatives regarding business enablement. (IT Company)

Albeit, the same participant, admitted that in a large company with different, distinct (security) organizations is dangerous to make generalizations about the business enablement factor:

> Our company is also providing information security services, which has created visibility and attention to information security in our company as a whole. On the other hand, this is its own business unit and not necessarily seen as a business enabler for other lines of business. (IT Company)

The perspective of this insight could also be explicitly tuned to reflect the business **enablement**. Denoting that this finding – 'Cybersecurity as a Business Enabler (17) –' represents the abilities of cybersecurity measures to enable the business **at all**. I.e., without cybersecurity, the business is not permitted to operate, whether the operation would be secure or not. From this standpoint, the participant of BI Company stated:

> The strategic goals of the company are revealing new business opportunities and models, which need to be secured from the ground up. (BI Company)

> We see the cybersecurity as an enabling function in general, but our business models are actually positioning us as a critical part of our customers' production chain as well. (BI Company)

Promotion for justifying investments was one of the standpoints regarding the criticality of the issue. The participant of Software Company revealed:

> Investments in security and privacy are somewhat easy to motivate since the subject is critical for the business. (Software Company)

The participant of the IT Company took this even further and justified the cybersecurity as a business differentiator for their company:

> We wouldn't be able to do basically any IT-production if we haven't got these measures audited and certified. (IT Company)

> We can reply to tenders and offer services to the areas which are extremely sensitive to information security and cybersecurity. We also have some examples where our information security has been a specific selling point and a requirement. (IT Company)

The Financial Company's participant explained their tactic to business enablement in a proactive sense. Early engagement in the development cycle demonstrates their foundational business enablement approach:

> Important targets in the cybersecurity work are the big focus areas of the company, like cloud services, for example. (Financial Company)

> We have frequent round-table discussion forum with the specialists, where we develop new business models. We are constantly reviewing these models and indicating information security and cybersecurity-related issues in the development phase already. (Financial Company)

The perceptions from the material show in general, that the alignment with the cybersecurity and business is adjacent. However, understanding or examining the **actual business** any further was not in the scope of this research. All in all, the discoveries show that role of cybersecurity in the participant companies covers both sides: The compulsory security measures as well as the enablement of the business.

5.1.3 Top Management Activity

A third outstanding insight from this category is a group of related findings. These findings were categorized in the analysis subcategory of '1.3 Top Management Activity' and are listed in table 9. This subcategory focused on the scrutinization of these findings.

TABLE 9 Findings in subcategory '1.3 Top Management Activity' comprised

Name of the finding (code)	**Groundedness**
Top management activity	16
Top management commitment exists	16
Top management interest	16
Top management dialogue	14
Top management channel	13
Top management visible in security	12

As stated at the beginning of this subchapter, the discoveries regarding top management's activity are particularly remarkable from the main research question point of view. The findings regarding this insight are all grounded to the top management's interactions with relevant stakeholders.

The participants of Software Company and IT Company expressed their somewhat aligned, general views about the top management activities. They referred to the inadequate level of commitment and visible actions from the top management:

> Our top management is committed to cybersecurity and values it as an important factor in our company, business, and customer operations. However, there hasn't been any practical initiatives or operations from that level, except hiring a CISO. (Software Company)

> I wouldn't say that cybersecurity is visible in the deeds and speeches of top management. (IT Company)

According to the IT Company's participant, the challenges related to engaging with top management could be intricated in nature and manifested, even as missing members in relevant bodies. The participant elaborated a bit around the issue:

> From my point of view, the top management's attitude is inadequate. When discussing with an individual top management member, the attitude is that cybersecurity is important and information breaches are unwanted. But the message targeted to the whole company from the top management, for example from CEO, doesn't emphasize cybersecurity. (IT Company)

> We are still missing the proper linking to the top management. We would need one more representative to the top management level. (IT Company)

Also, it was discovered from the material that the absence or presence of top management regarding cybersecurity depends on the people and context, as the participant of IT Company explains shortly:

> The clear directing path from top management to the actual operations is missing. Although we have the pieces in place. (IT Company)

> The CEO of the company has indicated in his message that it is not necessarily adequate to just comply with the compulsory security trainings offered by the company but also be active, aware and follow the security as an individual how the state of security is developing in general. This is a strong message from the CEO. (IT Company)

In the light of these two examples and corresponding quotations above, the material shows that the commitment from the top management is not always straightforward, tangible, nor visible regarding cybersecurity. However, the discoveries also opened different experiences concerning top management engagements. The Financial Company's participant demonstrated several clear examples of the top management activities and concrete actions:

> Company's top management commitment can be seen on many levels. (Financial Company)

> Directing from top management includes a lot of cybersecurity-related topics. (Financial Company)

> Top management is committed to the practical level with initiatives and interests. This is strongly visible in our internal and external communications. For example, when a big influencer in our industry, the European Central Bank (ECB), raised cybersecurity risks as a remarkable threat in the financial industry, our top management responded to this. (Financial Company)

These actions also themed the quotation from the participant of BI Company. In their company, the top management support seems to be clear, holistic, and straightforward. According to the participant of BI Company, their top management actions are interactive and bi-directional with their department of cybersecurity management, which has manifested in the form of a workshop:

> Certifications and attestations were goals for the last year. Our company's CEO has pointed out many times in his messaging, how important achievements these have been. Rather new CISO position is also a concrete action from top management, which supports the commitment towards cybersecurity in our company. This has also been the target for the investors. (BI Company)

> For example, we have presented cybersecurity workshops to the top management, and it has generated good feedback. Top management values and emphasizes the importance of information security in our company, and they are also messaging it out. (BI Company)

The Media Company's participant described the top management commitment and engagement from the organizational structure point of view, and justified the company's actions with positive experiences:

> We have our own security governance board in every business unit. From each business unit, also the CEO and CTO are present in the security governance board. Also, on the corporate level, there is the information security and privacy board, which

> consists of the corporate CFO, compliance director, head of IT-group, CISO, EDPS, and the responsible person of internal auditing. (Media Company)
>
> Our company's corporate CEO from the top management level, understands and promotes the information security message in the whole company. The corporate CEO has created controls for each and every business unit, which the corresponding CEO must comply with. (Media Company)
>
> This also sets the quarterly security governance board meetings as compulsory for the business unit CEO's. This commitment from the concern level corporate CEO is very welcomed in the security organization. The corporate CEO has also visited many of the security organization's events as a speaker, to emphasize the importance of information security and privacy to our customers. (Media Company)

As stated in the discernments regarding the finding 'cybersecurity maturity development (32)' (see chapter 5.1.1), the company's initiatives pursuing certification for their ISMS were promoting the top management activities, commitment, and interest in cybersecurity of the company. Notably, the participants of Media Company and BI Company brought this explicitly up in their answers. The perceptions from the material reveal the same energizing motion promoted by GDPR, which most of the participants mentioned as a catalyst for the top management interest.

The discoveries indicate that there are as many approaches as there are companies. The level, intensity, and visibility of top management commitment vary from company to another. Since causalities regarding the phenomena here were out of scope for this research, those are not examined further.

5.1.4 Strategic Development and Cybersecurity

In addition to the key insights and related findings earlier in this category, there are other rather noteworthy discoveries from the material worth of a brief walkthrough. The participants expressed their thoughts regarding the company's corporate strategy, mission, and vision from a variety of perspectives.

Linked to the finding '**Traditional strategy development (6)**,' the participant of IT Company explained their strategy work as 'traditional,' denoting that their top management more or less dictates the corporate-level strategies, which then falls forward as given. The department of cybersecurity management then aligns correspondingly with the corporate strategy, mission, and vision. Their unified values and mutual acceptance of major lines are fundamental in the big picture. The IT Company's participant continued by describing that the connection with the top management is working at a reasonable level in their company but had no indication if the experience is mutual or not.

The participants of Software Company, Financial Company, and BI Company gave strong support to the IT Company's approach in the sense of complete alignment between their corresponding corporate strategies, missions, and visions in general. The findings '**Cybersecurity as a strategic priority (10)**,'

and '**Cybersecurity aligns with corporate strategy (9)**' were often perceived together with these companies. The participant of Software Company underlined these findings and the relevance of these to their company:

> Our business is living or dying through the information security abilities, which are concretized to our customers in their daily operations with us. We would say that information security is a strategic level priority to us. (Software Company)

The participant of BI Company took another angle to the alignment of cybersecurity and the corporate strategy of the company. They saw the cybersecurity automation initiatives supporting their growth going forward:

> A few years ago, we didn't have that many employees, so the growth is our main strategic driver. (BI Company)

> The level of automation regarding the information security and cybersecurity will grow going forward, because we need to support and align with the company growth without compromising security. (BI Company)

The interrelated findings '**Bi-directional development with top management (11)**,' and the '**Emergent strategy development (6)**' were linked especially in two companies: Software Company and BI Company. The insights regarding these findings reveal that these companies were influencing the strategy development work emergently:

> Regarding cybersecurity, our company strategy work is utilizing the emergent ideas and initiatives from the actual cybersecurity operations. (Software Company)

> Strategy work is interactive, bi-directional development, which is led by the top management directing and showing the way. (BI Company)

The perceptions also revealed related cybersecurity challenges regarding top management. The minor finding '**Cybersecurity challenges in top management (5),** demonstrates challenges like leadership issues and the absence of clear direction and challenges in determining the focus areas. The participant of the BI Company believed that one challenge for the strategic leadership of cybersecurity is the difficulty in determining the short- and long-term focus areas of the company. On the other hand, the participant of Media Company estimates, that the challenges are related to information security awareness on top management level and argues the '*safety*-oriented' approach as a reason behind:

> I'd say that the challenges are more in the information security awareness level of the top management, especially in organizations where safety has been the major line for security in general. (Media Company)

In summary, the findings from this main category reveal insights concerning the top management's connection, interaction, and collaboration with the participating companies' departments of cybersecurity management. However,

the perceptions from the material show that from a holistic perspective, the relevant stakeholders for cybersecurity are the whole company and its organizations. The next subchapter moves forward from the strategic level towards the tactical level and focuses on the companies governing and managing the cybersecurity.

5.2 Cybersecurity Governance and Management

The findings and insights of this category are correlating mainly with the tactical level in the participating companies. The focus findings behind the insights include the utilization of industry best practices, cybersecurity culture development, and considerations regarding investments, like hiring (and keeping) the talent. Also, cybersecurity governance and management – as the title states – is an overarching theme knitting this category together.

From the research aim perspective, the findings on this category are revealing insights and answers according to the first research sub-question; '*what aspects drive the cybersecurity governance and management in the company?*'. The observations and perceptions are exposing views to the building blocks of the cybersecurity governance and management in the responding companies.

As Sarajärvi and Tuomi (2018) instructed, it is essential regarding the aim of the research that the participants are experienced professionals in their field of work. Hence, the subchapters under this category are focusing on the day-to-day governance and management work of cybersecurity directors and officers in the department of cybersecurity management of the corresponding responding companies.

5.2.1 Utilizing Best Practices

The most dominating insight from this category correlates with the major finding '**Utilizing best practices (31)**'. Industry best practices were found to guide, enable, and assist in the cybersecurity's tactical approach in all of the participants' represented companies. Best practices were often linked and mentioned together with already mentioned ISO/IEC 27001 industry standard as an empowerment for the 'cybersecurity maturity development (32)'. Also, the finding '**ISO/IEC 27001 (17)**' is mentioned distinctly under this category, which emphasizes the role of ISO/IEC 27001 as a 'de-facto-standard' regarding industry best practices in the field of information security.

However, the participants mentioned some other industry best practices, and some of them were at least partly utilized, for instance, the finding '**Multiple best practices (11)**' suggests. Concerning information security, these were the

minor findings of '**ISO/IEC 27002 (5)**,' the '**ISF Standard of Good Practice[3] (5[4])**,' and the '**ISAE 3000 Family[5] (3)**'.

The finding '**industry regulations (6)**' was the dissenting factor for Financial Company's approach for utilizing best practices. Albeit, their tactic was still to apply industry best practices where industry regulations are absent:

> Since our company is working in the financial industry, it is obvious that we are heavily regulated. We are a member of ISF, which enables our company to practice the ISF's SoGP. (Financial Company)

> ISF SoGP is directing our operations in units and areas where there are no other regulations in place. (Financial Company)

The approach with ISF's SoGP was not unanimous. While the Financial Company informed its ongoing ISF membership and utilization with SoGP, the Media Company had different views. The Media Company found the SoGP quite laborious and replaced the framework with the ISO/IEC 27000 family approach with the top management's support:

> We have also been a member of the International Security Forum (ISF), which Standard of Best Practices has been our tool to measure and report the information security maturity level to top management. However, this has been found to be quite laborious. (Media Company)

> When we presented to top management the initiative to replace the ISF SoGP framework with ISO/IEC approach, the message received very positive feedback. (Media Company)

The 'ISAE 3000 Family (3)' finding applies mainly to the IT Company and the BI Company. For both companies, the needs for ISAE 3000 and other official standards emerged from their customer requirements:

> Customer-specific audits, PCI-DSS certified environments, and ISAE 3000/3402 audits are the baseline for our added value to customers regarding information security. (IT Company)

However, the BI Company participant explained their approach to ISAE 3000 also from the international perspective and highlighted the vast extent of the attestation process in comparison to ISO/IEC 27001. BI Company also referred to the minor finding '**NIST Cybersecurity Framework (1)**' as the only company. According to the discoveries from the material, the general approach of the BI Company to best practices was selective:

---

[3] The SoGP stands for 'Standard of Good Practice for Information Security,' which is published by Information Security Forum (ISF) (Information Security Forum, 2020).

[4] The groundedness of ISF Standard of Good Practice active (2) and inactive (2) is combined here.

[5] The ISAE stands for 'International Standard for Assurance Engagements,' which is issued by International Federations of Accountants (IFAC) (2020).

> We are also operating overseas, where ISAE 3000 attestation is more applicable. This is attested by the external audit committee, and this is much larger and specific measure than ISO/IEC 27001. (BI Company)

> We are using best practices from ISO/IEC. Also, NIST CSF has been on the table regarding some good practices. Overall, we are not reinventing the wheel here but selectively using industry best practices. (BI Company)

Concerning IT-governance, the finding '**ITIL[6] (6)**' was brought up by almost every company in the study. The perceptions show that ITIL is utilized widely in these companies as an IT-governance framework, IT-production baseline framework, SLA[7] measurement tool and security incident management tool for internal IT. However, the Media Company's participant stated that they are not utilizing ITIL at all:

> To my surprise and bewilderment, I've noticed that the IT production does not comply really with any (IT) governance framework. I personally found this problem when talking to them because there is no common language about the services, products, assets, processes, configurations, etc. (Media Company)

Concerning common language between different departments, business units, and organizations in the company, the material shows that ITIL was frequently mentioned together with the '**common language (9)**', which is examined later in-depth during chapter 5.4.

The companies widely recognized the best practices and applied for different use cases, for example, systematic ISMS directing and development. According to the material, it is clear that ISO/IEC 27000 families were the most commonly utilized approach for the best practices and all, but two companies have certified their systems against the ISO/IEC standards. The Financial Company was mentioned in this light before, but then another without ISO/IEC 27001 certification was the Media Company. However, they have active plans and ongoing pursuits to achieve the certification as well. They were underpinning this with customer requirements:

> We think that the certification is necessary immediately when customers require it. In any case, it is good to have the information security management system managed in a standard and directed way, even if there is no actual certification of ISO27001 in target. (Media Company)

As mentioned above by the participant of the Media Company, their approach towards ISMS standardization has been systematic, directed, and justified from the beginning. The insights show that the industry best practices were seen in the companies more as a foundational starting point than as a final target.

[6] ITIL stands for 'Information Technology Infrastructure Library,' which is a set of detailed practices for IT service management that focuses on aligning IT services with the needs of the business (Axelos, 2020a).

[7] SLA stands for Service Level Agreement (Axelos, 2020b).

Discoveries also revealed that companies were using parts of many different best practices selectively to suit their needs accordingly.

5.2.2 Security Culture Development

Another significant insight under this category associate with the major finding of '**Security culture development (21)**'. The Software Company's participant was the only participant overlooking this aspect. In contrast, all other participants referred to the development initiatives and actions regarding the company's security culture. The finding '**Co-operative culture (12)**' is juxtaposed with the previous finding 'Security culture development (21)'. All participants emphasized co-operation, and the common viewpoint was the central position of cybersecurity in the companies. All participants admitted that it is critical for all business units and organizations in the company to co-operate with the cybersecurity 'department' of the company.

The Financial Company's participant holistically expressed that the foundation for the development of security culture emerges from the standard base values throughout the company and its organizations. The perceptions from the Financial Company's views revealed that they were focusing on the security culture development with intentional actions and projects instead of waiting for the security culture to 'emerge.' The financial Company implemented the security culture development activities vigorously throughout the company:

> We started a large initiative last year regarding the cultural change of cybersecurity in our company. We are going through a holistic program that aims for the cybersecurity awareness and culture development. The goal is to have every employee to think and respect cybersecurity in their everyday work. (Financial Company)

As an example, the Financial Company has a specific security approach to software development. This 'shift left' (Firesmith, 2015) model of thinking was a consequence of the cultural development on a broader scale inside the company:

> In everything that we do, we have a "shift-left" model of thinking. It's embedded in risk management culture as well. (Financial Company)

The participants experienced the development of the security culture as an ongoing, long-term project in the responding companies. The development was in different phases in different companies, however. Some of the companies were just starting with development. The others were already in the stage of nurturing and shaping the processes:

> It will take some time for top management to understand how information security and cybersecurity contribute to creating and maintaining an entire security culture of the company. (Media Company)

> This is also aligned with the compulsory security training, which is tracked on a yearly level. We are also aiming to update this yearly so that even the multi-year employees would have something new to learn. (IT Company)

However, the material shows that the means for the companies' security culture development in different phases were somewhat similar, at least in some respects. The participants of Media Company and IT Company reported that their security organization was more interested in engaging with the audience in their events and context in general. The traditional option would have been trying to tempt the audience to attend in the actual security presentations arranged by the department of cybersecurity management of the organization:

> The corporate security management is also keener to deliver the information security message and awareness generation activities in the business unit's own forums (IT Company)

> We have trained DevOps teams to adapt security to their operations and to consider different threat scenarios from their viewpoint. (Media Company)

The adjacent finding aligning 'security culture development (21)' was the '**Security culture development as a challenge (7)**'. The IT Company participant brought the challenges in culture development up, and mentioned the concern about the top management commitment:

> Security culture development is a large challenge, and the top management commitment is related also. (IT Company)

Also, the participant of the BI Company raised a fundamental concern about security culture development in general. Firstly, in the light of the external workforce. Secondly, from the viewpoint of balancing between their security culture development and supporting the company growth with its requirements, and finally, by understanding their top management's bias to business:

> When it comes to buying expertise from outside, it is challenging to maintain your own security culture and policy. Does culture even exist? (BI Company)

> Building a partner network and, at the same time, building your own know-how are imperative steps to meet the future challenges. (BI Company)

> The challenge is to get the information security and cybersecurity to be interesting because the top management priorities are on the business side. (BI Company)

The insights about security culture development demonstrated that almost every company has initiatives and pursuits regarding this. It is clear from the perceptions that security culture development is not always straightforward and trouble-free for the companies.

However, according to the material, a continuous, active approach seems to be the driving force behind the companies that work with the security culture

development initiatives and projects. As the minor finding '**Security culture development as priority (5)**' states, it is evident that the companies see the security culture development essential and worth prioritizing.

5.2.3 Cybersecurity Investments and Hiring Security Professionals

As a third focused finding from the category of cybersecurity governance and management, I noticed the '**Cybersecurity investments (12)**'. Due to the research scope, the related insights focused mainly on investing in hiring talent. All of the companies had experiences of investments regarding cybersecurity. Based on the material's perceptions, the common factor was that the investments regarding cybersecurity are generally easy to motivate.

The participant of BI Company elaborated widely about their investments in cybersecurity. They were tying the investments to providing support in terms of security to the company's significant growth. Another factor was the need for automation that the growth brings to the security systems and processes. The participant of BI Company also emphasized that they should evaluate *any* new investments from the security point of view – not just from cybersecurity and technology perspectives:

> The level of automation regarding the information security and cybersecurity will grow going forward, because we need to support and align with the company growth without compromising security. This denotes new technologies, systems, and partners that should be selected from the security point of view. (BI Company)

From the human resourcing point of view, the BI Company and Software Company had made a significant cybersecurity investment lately by investing in an officer-level position for cybersecurity:

> Rather new CISO position is also a concrete action from top management, which supports the commitment towards cybersecurity in our company. This has also been the target for the investors. (BI Company)

As a countering insight, the material shows that hiring security personnel is not always an easy task. The finding '**Hiring security professionals is a challenge (10)**' emerged from the difficulties in finding and keeping talent. The participants from BI Company and Financial Company described the problem as:

> Finding software security experts is difficult. When we want to develop things agile and fast, it is challenging to ensure that security remains with the development and gets embedded into the final product. (BI Company)

> Skill shortage is a rather chronic situation that has been widely discussed for the last 4-5 years. The basic IT or security skills are not enough. You also need to have business skills and knowledge of modern technologies such as artificial intelligence and machine learning, for example. This pretty much cuts off the talent. (Financial Company)

> Requirements are ever-growing. Generalist-type profiles, like professional board members as well as deep experts, are needed. (Financial Company)

The Financial Company's participant brought up the issue that mere security skills are inadequate for operating in a modern cybersecurity environment while working with a variety of separate business units. The participant of Financial Company also raised apprehension about hiring a workforce for cybersecurity shortly, and estimated, that the attractiveness of cybersecurity is going to be any higher in the foreseeable future than right now.

The participant of Media Company was echoing the message by Financial Company and added their view about keeping the talented 'own people' in the company. They justified this by the expertise and knowledge about the company's systems by the long-term employees, rather than always instructing the systems to external resources:

> It would be great if companies would have the possibility to have incident response capabilities in in-house functions – nevertheless, it is still hard to find and keep the talent. Outsourced SOC functions are often too generic, while the own people are the best experts on their own environment and threat landscape. (Media Company)

A striking insight was also the approach of the IT Company. Their participant explained that hiring and employing the information security professionals is under control, and they can utilize their information security business area as well if needed. However, the challenges are related more to the efficient utilization of such resources:

> We think that there are enough information security professionals and we even have our own business area and consults to utilize if needed. The question and the challenges are more around that we are efficient enough to use the information security professionals in the business units. (IT Company).

In conclusion, based on the material, the insights show that security investments are not as challenging or difficult to motivate. There are, however, some challenges related to hiring adequate talent and mainly to keep the talented workforce in the company.

5.2.4 Information Security and Other Governance Frameworks

The findings **'information security governance development (5)'** and **'information security governance development (5)'** emerged from the material as a clear insight for this category. The information security governance (ISG) approach split the participating companies into two groups and left one company in between. The participants of IT Company, Software Company, and BI Company reported that they ground their ISG approach on ISO/IEC 27000 family practices. In contrast, Financial Company's participant stated that their approach to ISG follows the ISF SoGP framework. However, the response from

the participant of Media Company put them right between those mentioned above:

> We used to have an ISF SoGP framework with governance structures from COBIT. Now we are implementing ISMS and looking for ISO/IEC 27001 certification. (Media Company)

In addition, the Media Company's participant described the approach to their ISG development, which challenges the corresponding C-suite members from business units to participate as well. According to the participant, their approach has generated positive feedback from top management as well:

> From each business unit, also the CEO and CTO are present in the security governance board. We have good experiences with this approach. (Media Company)

> It is important to be honest, and realistic in these information security development initiatives, so be able to see the true maturity level. (Media Company)

> Top management understood and saw the ISO27001 Framework and ISO27002 best practices as a globally well-known approach and based on that as a suitable framework to us and also as an evolvement in the information security governance development. (Media Company)

About other governance frameworks – like corporate governance (GC) and information technology governance (ITG) – the implementations and utilization were actualized differently in the participating companies. Regarding the GC approach in IT Company, they are utilizing a GRC-framework. Financial Company's participant argued that they have 'strong corporate governance' in place but did not mention any well-known governance frameworks. According to the BI Company's participant, their approach to CG was under construction, but the risk management frameworks and strategy were already in an advanced state. The Media Company and Software Company did not mention anything tangible for their CG approach. The finding '**Information technology governance (3)**' aligned perfectly with perceptions that were observing 'ITIL (6)', which walkthrough is already conducted during chapter 5.2.1.

Now that the governing level of cybersecurity is scrutinized, it is natural to pivot into the implementation and actualizing the strategies. The next subchapter aligns with a more operational approach.

5.3 Cybersecurity Directing

In this category, the focus is moving from the tactical level to the operational level and dismounts eventually into individual business units. The insights in this category are emerged from the findings regarding responsibilities for

cybersecurity, balancing between technical-administrative and security awareness generating measures, and cybersecurity training.

From the research aim's point of view, we are now looking for answers to the second research sub-question, which seeks to *'how the cybersecurity measures are **directed** in the company?'* This subchapter examines based on the material, how the different participating companies are experiencing the cybersecurity directing, and what are the most dominant findings in this category. Therefore, the approach in this subchapter is more from the actual tangible measures and business unit's point of view.

5.3.1 Responsibility for Cybersecurity

The outstanding insight from the category of cybersecurity directing is the responsibility for cybersecurity and how it seemed to distribute to many different levels and actors in the participating companies. The total groundedness for the findings behind the insight is 60. It explains the emergence of responsibility for cybersecurity as a holistic theme from the material. These different variants regarding responsibility for cybersecurity are listed with their corresponding groundedness value in table 10 and examined throughout this subchapter.

TABLE 10 Findings of responsibility for cybersecurity

Name of the finding (code)	**Groundedness**
Responsibility for cybersecurity is on the individual business units	25
Responsibility for cybersecurity is on the security organization	18
Responsibility for cybersecurity is on the individual employees	8
Responsibility for cybersecurity is on the security specialists	6
Responsibility for cybersecurity is on the top management	3

The major finding '**Responsibility for cybersecurity is on the individual business units (25)**' is the most prominent of the perceptions in this category. The material shows that all participating companies except one were part of this finding, and the IT Company, Media Company, and BI Company being the most significant contributors.

The participant of IT Company referred to their 'top-down' approach, where individual business units are leading the information security with broad responsibilities. Also, the participant detailed about the international operations with bi-directional information sharing:

> Operations are directed top-down from the company security towards the business units, where the security officers of the business units are directing and leading the information security with a wide responsibility. (IT Company)

> Since we are operating in multiple countries, we have country aligned security managers. Information is shared bi-directionally on monthly cadence between business security officers and the corporate security. (IT Company)

The finding '**Responsibility for cybersecurity is on the security specialists (6)**' highly related to the IT Company as well. According to the perceptions, the security officers of the business units mentioned above are the responsible specialists in their company. Also, the IT Company's participant stated that their security specialists are assessing the cybersecurity measures and proposing implementations from the strategic goals point of view.

The participant of Media Company described that their method for responsibility distribution requires a foundational preparation in the business unit for the beginning. Before this, they could not expect the business unit to correspond with the responsibilities. The top management role was aligned accordingly and mentioned particularly:

> The initial situation with regard to information security maturity and the self-assessments of different business units is that we have had first the need to create controls and a framework. (Media Company)

> The corporate CEO has created controls for each and every business unit, which the corresponding CEO must comply with. (Media Company)

The BI Company's approach was somewhat on the same foundation. They are necessitating the individual business units responsible for the cybersecurity scoped to the controls and structures level. As a part of describing their organization, the participant of BI Company explained their approach to top management responsibilities, which relates to the minor finding '**Responsibility for cybersecurity is on the top management (3)**':

> At the top management level, CTO is responsible for the cybersecurity in our company. CISO is reporting to CTO. There are also information security and cybersecurity-related responsibilities on every member of the top management. (BI Company).

Based on the material, all participating companies admitted that the security organization[8] is seen widely as responsible for the company's cybersecurity. The finding behind the insights is '**Responsibility for cybersecurity is on the security organization (18)**'. However, the views on the responsibilities differ among the participating companies. The Financial Company's approach to security organization's responsibilities was the holistic view, separated into two cybersecurity organizations:

> We have two official cybersecurity organizations. The first one is the cybersecurity unit, whose responsibility is the company-wide cybersecurity governance with people, processes, and technology focus. The second one is the IT-production information security unit; whose practical responsibility is the IT-infrastructure and the security infrastructure. (Financial Company)

[8] Security organization is commonly referred to as the cybersecurity management department in the study as well.

The holistic approach was also the justification behind the Software Company's responsibilities on the security organization. From their top management point of view, the responsibility for cybersecurity rested on dedicated resources, which was the recently hired CISO. The BI Company's participant gave an example of this responsibility as a part of the reporting chain, where the messages regarding information security from the individual business units are composed and refined:

> The security management team is responsible for the security reporting chain. Supporting the business unit on information security occurs via controls and responsibilities (BI Company)

Collective insight for IT Company and Financial Company about the security organization's responsibilities was the planning and arrangements around training. The participants of the companies explained the responsibilities regarding training. Also, mentioning the importance of the tools for secure operations:

> The top-level information security awareness training is the corporate security's responsibility. (IT Company)

> We should be able to offer secure and simple tools for the employees to execute the cybersecurity. (Financial Company)

The material reveals that in addition to the individual business units, the top management, and the security organization, liabilities also distributes between professionals and individual employees in general.

The finding '**Responsibility for cybersecurity is on the individual employees (8)**' disclose that the companies were also demanding responsibilities from individuals. According to the material's perceptions, this responsibility was mostly concerning individuals to comply with security policies and rules. The IT Company's participant explained their approach to individual employee responsibility and the manager's responsibility. Also, according to the participant, the IT Company's CEO has indicated that individual employees should take more responsibility for their security awareness themselves:

> The responsibility of the information security of the team is on their manager. Individual employee conforms the information security with their prowess in the subject, and the manager is responsible that the prowess of individual exists. (IT Company)

> Also, the CEO of the company has indicated in his message that it is not necessarily adequate to just comply with the compulsory security trainings offered by the company but also be active, aware and follow the security as an individual how the state of security is developing in general. This is a strong message from the CEO. (IT Company)

The participant of Software Company described their strategy concerning the individual employee responsibility. They explained that due to the rather small size of the company, it is possible to train every individual contributor to being more aware and responsible for their actions and operations.

To conclude on the topic with general insight, the participating companies' cybersecurity responsibilities are variegated and multidimensional. The security training and awareness twinkled already during scrutinization of these findings, but the next subchapter is focusing on these dominant themes thoroughly.

5.3.2 Activating Security Awareness via Cybersecurity Training

Under this category, the runner-up in groundedness is the major finding '**Activating cybersecurity awareness (22)**'. All participants shared this approach and emphasized it as vital cybersecurity directing measure. IT Company's participant described their approach to cybersecurity awareness creation as a multi-level, multi-channel, and continuously active program. Their cybersecurity awareness creation starts from the first new-hire training of an employee. Financial Company, as well as BI Company, echoed the approach regarding the new-hire training. Also, the Financial Company has the previously mentioned (see subchapter 5.2.2) holistic program aiming for cybersecurity awareness and culture development. The material shows that the major finding 'security culture development (21)' is closely aligned with the cybersecurity awareness activation events and measures.

In general, according to the material's perceptions, the value of cybersecurity awareness creation and activation were emphasized. Also, almost every participant mentioned the holistic approach. For example, the participant of Media Company expressed their approach to the cybersecurity awareness activation with the customization perspective:

> Awareness-raising training has been executed at the level of the entire organization, but above all, training has been conceived of different types according to different target groups. These have been customized differently. (Media Company)

While the major finding 'Activating cybersecurity awareness (22)' is more of an overarching concept and generic finding, the cybersecurity awareness training, in contrast, is a more detailed insight from this category. The training was often connected and mentioned together with security awareness creation.

The tailoring (customization) which Media Company's participant reported above is manifested unquestionably in two accordingly aligned findings that emerged from the material: '**Cybersecurity training tailored by role (16)**' and '**Cybersecurity training tailored by level (11)**.'

All participating companies were tailoring their training based on role and level. By 'level,' some companies noted the level in the organization hierarchy, where in contrast, the Software Company's and BI Company's participants indicated the level of cybersecurity skills/knowledge of the employee. For the BI

Company, however, the level was dependent on whether the targeted audience is owning security controls or not:

> Basic awareness generation training is executed for every employee upon start. Owners of the controls are having tailored, ongoing information security training. (BI Company)

According to the material, the insights show that tailored training was not a routine task for the participant's companies. Instead, it was a real opportunity to generate specific cybersecurity knowledge where needed and when needed. The participant of Media Company explained their approach of specially tailored escape room themed experience, which outcomes were reflecting as cybersecurity awareness creation:

> We have also tried different methods in information security awareness, such as gamification. We have had very good experiences from the escape room training, which was tailored for the audience. We have seen that when people are trying to solve escape room security challenges, the method enhances user engagement and their awareness -they start to observe more information security-related things. (Media Company)

The participant of BI Company also reported that in addition to the tailored training for the specific IT-specialists, they are encouraging their employees to go even further; on the educational level with cybersecurity training. According to their participant, this was also their desired future direction:

> Supporting the business unit on information security occurs via controls and responsibilities. Certified trainings have also been arranged and offered. IT-Infrastructure and services are receiving compulsory, tailored training for their information security skills. (BI Company)

> We are encouraging our employees also to educational training regarding information security and cybersecurity. For example, some study and thesis supervising has been done, and this is desirable going forward as well. (BI Company)

All in all, the insights reveal that the training is at the core of cybersecurity directing in all companies. A closely related theme is how the companies have addressed technical-administrative information security measures in contrast to security awareness generating activities. This is examined in the next subchapter.

5.3.3 Technical-Administrative Measures vs. Security Awareness Generating Activities

The third striking finding regarding cybersecurity directing from the material is the '**Technical-administrative approach as a baseline (12)**'. The self-explanatory nature of this finding is that all of the participating companies shared the 'baseline-approach' regarding the utilization of technical-administrative measures. Based on the material's perceptions, the participating companies

understood the 'baseline' as cybersecurity policies, rules, and controls, which the company's cybersecurity strategy often dictates and drives.

Among the others, the participant of IT Company emphasized the importance of these formal, technical-administrative security measures. The IT Company sees these measures as foundational for the security work. Also, the participant praised the approach from its effectiveness:

> Formal technical-administrative policies and procedures are very important, especially for the information security specialists in the business units, because they are relying on these. Specialists can use these measures as a baseline from the top management and also the level of the agreements, which are part of the customer promise. This is working effectively. (IT Company)

The importance of the technical-administrative measures was also underlined by the Media Company's participant, who described asset management as an outstanding example of these measures:

> It is really important that technical-administrative measures are in place. Asset management, in particular, is an important issue in implementing information security. If you do not know where your assets are – how can you protect them? (Media Company)

The participant of the IT Company also admitted that in some business units, the cybersecurity is inadequately based solely on the technical-administrative measures. However, based on the perceptions, this approach is seen more like a compulsory underpinning and mandatory compliance requirement for the participating companies. In contrast, according to the participant of BI Company, the actual cybersecurity was created and developed via security awareness generation activities:

> Because of the control frameworks, we must have the structures and documents for every technical-administrative control, but the actual information security and cybersecurity are created with awareness-raising measures. Controls and structures are under every business unit's own responsibility, but the awareness-raising measures are the spirit of the information security and cybersecurity. (BI Company)

The discoveries from the material show that all participating companies exercised security awareness generating activities. The walkthrough of the actual training related insights and efforts is in the previous subchapter.

The Financial Company's participant described their approach to security awareness generating based on real use cases. They were guiding their cultural development while utilizing security awareness generation to reveal pain-points from the technical-administrative measures. They also admitted that there are some challenges in their approach:

> Existing use case models are assisting people to understand what we are pursuing with the cybersecurity in our company. These models are guiding our cybersecurity cultural development campaign and helping to reveal the pain-points from these

> technical-administrative measures. We need technical-administrative models, but sometimes these can also cause dead-ends with the current legislation. (Financial Company)

In general, the perceptions show that the security awareness generating activities are under constant development and utilization in all participating companies. These activities are tailored and customized even for the phenomena. The participant of the BI Company gave an example of their approach to this:

> We are also reacting to the phenomena and events when those are occurring. For example, when the CEO-fraud started to emerge, we conducted immediate, tailored security trainings targeted to whose it may concern. These kinds of activities are also raising some new initiatives in the form of more frequent trainings and information packages to larger audiences in our company. (BI Company)

The next subchapter focuses on cybersecurity controlling. Then, according to the direct-control cycle (von Solms and von Solms, 2009), make a U-turn at the operational level and focus the reporting back to the top management at the strategic level via the company's department of cybersecurity management at the tactical level.

5.4 Cybersecurity Controlling

The focus is moving once more, from the operational to the tactical level, and eventually back to the strategic level. The insights regarding the cybersecurity controlling divided mainly into two subsections; measuring and reporting. This category joins together themes of measuring and assessing the effectiveness of the cybersecurity measures with delivering the results eventually to the top management of the company.

According to the research aim, this subchapter seeks the answer for the third research sub-question; *'how the cybersecurity measures are **controlled** in the company?'*. This category also examines the collaboration between the top management and the department of cybersecurity management of the participating companies. This phenomenon was already scrutinized in the subchapter 5.1 before. However, the perspective in this subchapter is from bottom-up, considering the collaboration initiated from the cybersecurity governance side towards the top management. Hence, the insights here are helping to answer the main research question as well; *'how does the top management collaborate with the company's cybersecurity governance?'*.

5.4.1 Measuring Perspectives for Cybersecurity

The insights revealed that the participating companies were taking multiple perspectives for measuring the 'general level of cybersecurity.' Although the

names of these findings contain the word 'measuring,' some of these are rather assessments and evaluations than precise measurements. Table 11 lists a subset[9] of these perspectives with their corresponding groundedness value.

TABLE 11 Findings of some measuring perspectives

Name of the finding (code)	**Groundedness**
Measuring perspective: Compliance	13
Measuring perspective: Risk	10
Measuring perspective: Implementation	8
Measuring perspective: Performance	6
Measuring perspective: Maturity	5

Based on the findings '**Measuring perspective: Compliance (13)**' and '**Measuring perspective: Risk (10)**,' all of the participating companies were taken the risk, compliance, or both as an approach towards measurements concerning cybersecurity. Based on the answer from the participant of Media Company, the compliance as a measurement can also contain other measurable structures, referring to the finding '**Measuring perspective: Implementation (8)**':

> We measure the cybersecurity level via compliance, which is also a reflection of what we have implemented and promoted as information security measures. (Media Company)

According to the material, the discoveries about measurements raised frequently the risk as a measurement perspective. The participant of Financial Company described their approach to measuring risk as a one clear perspective:

> We have an operative risk management model in use. Internal audits related to the finance industry, like ISAE-responses, are executed by the official inspectors. Risks are one clear perspective here. (Financial Company)

BI Company's participant seconded the approach by Financial Company and added their views about constant development to the picture. Also, they brought up the effectiveness perspective:

> Our company's risk-assessment methodology is developed and reviewed constantly. We are also assessing how the risks are monitored, managed and reported. Also, we are interested in how our tools work within our processes so that we can assist the management's effectiveness with true impact. (BI Company)

Other remarkable percepted perspectives to measurements were performance and maturity. The actions regarding finding '**Measuring perspective: Performance (6)**' manifested interestingly in several participating companies. The discoveries from material show that benchmark information against

[9] Groundedness >= 5 was required on this list. The full list of the findings is available in appendix 2.

competitors, as well as the internal benchmark, was compelling for the top management. The Financial Company saw this also as a way to assess cultural development:

> Information security benchmark information regarding our competition is also interesting information to our top management. (IT Company)

> Business wants to have benchmark information regarding information security level of our company. These are also directly reflecting our information security and cybersecurity performance. (BI Company)

> Cybersecurity effectiveness levels are also examined from team to team perspective, which generates internal, healthy sparring between the teams. This is also one way to assess the cultural development. (Financial Company)

The insights show that measuring the cybersecurity maturity levels is done mainly via quantitative methods. The participants in different companies reported systematic and frequent maturity level measurements and assessments, which were based on questionnaires, gamification, and general capability maturity model (CMM). However, even if the methods were simple, the magnitude can be remarkable as the participant of Financial Company explained about maturity measurements, while referred to the performance as well:

> We have quantitative measurements on many levels; for example, we can measure how many cyberattacks we are able to stop and how our employees are performing from the information security point of view using gamification methods. We are also following cybersecurity maturity with different frameworks, and we can see from certain security mechanism utilization reports that the actual level of cybersecurity performance has been enhanced. (Financial Company)

According to observations, there were challenges related to the measurements, which emerged as the finding '**Measurements as a challenge (6)**'. IT Company's participant connected these challenges to the measuring culture, echoed by the participant of Financial Company:

> We measure from the risk point of view as well as from the commercial (business) point of view. Measuring or assessing culture would be interesting, but that is considered a bit challenging at the moment. (IT Company)

> Measuring or assessing cybersecurity effectiveness is challenging. For example, one of the goals in our cybersecurity training program is to develop and change the culture. Measuring this cultural change is reliably is hard. (Financial Company)

Material's perceptions show that the effectiveness was a challenging concept for the participants to actualize in their operative model. Despite the challenges, the participating companies were looking forward to overcoming the issue and developing a means to measure the effectiveness as well.

These development initiatives emerged as the finding '**Developing strategic effectiveness measurement (5)**'. According to the participants, the

responding companies had interests and actual efforts for measuring the strategic effectiveness of cybersecurity activities. The participant of Software Company expressed this simply, while the BI Company's and the Media Company's participants described concrete plans about the issue:

> This is not yet ensured, but as a very interesting topic, this is something that we are looking into currently as a development initiative. (Software Company)

> Assessing the effectiveness of information security and cybersecurity measures in a reliable manner is hard and challenging. We are aiming to predict and foresee the effects of different changes in the information security behavior when we implement new controls. We see it very important that the top management is supporting these initiatives. (BI Company)

> Nothing remarkable yet, but we see a clear path here to the customer trust. Customer trust is clearly stated in the corporate strategy as a strategic initiative and goal. These issues are the ones that still need to be developed. (Media Company)

The perceptions show that the measures and assessments are the lifeblood of the reports from the operational level to the tactical level. However, this content and vital information are also contributing to the aggregate reports for the top management. According to the material's observations, these final reports upwards from the tactical level were in a more refined and thought form. The next subchapter examines the views about this aspect in detail.

5.4.2 Reporting the 'State of Cybersecurity'

The insights about reporting are collective in the sense that all findings support each other, and none of them are mutually exclusive. According to the perceptions from the material, the participating companies were all actively developing reporting. The development was recognized from many levels and in co-operation with other stakeholders in the participating companies. The '**Report development (11)**' emerged as a significant finding in this category. The participant of IT Company explained this common approach of development among the participating companies, while BI Company's participant seconded this and added their experimental workshop approach:

> We have developed the information security report from the ground-up on the terms of the top management on a monthly basis. Feedback and direction were helping us to make the report better for top management. (IT Company)

> Reporting must be developed together with the top management. Reporting can also be in the form of a workshop or other enablement session, for it also engages and challenges the top management. (BI Company)

Also, the insights reveal that while it is essential to tell the bad news, the cybersecurity reports should not intimidate or frighten the audience. According to the participants, the report language and vocabulary should respect the

terminology and language of the top management. The Software Company's participant crystallized this in their description of the top management report:

> The most important feature in reports and discussions with the top management is the language and vocabulary used. The information needs to be understandable and easily utilized by the top management. Things in the report must be based on their point of view to support decision-making processes and strategy work. (Software Company)

Another striking finding in this category is '**Report usefulness (8)**,' which manifests in the participating companies as thoughtful, planned, and goal-oriented when preparing and delivering the reports to the top management. According to the participant of Financial Company, the usefulness of the report emerged from the preparation work:

> An important feature of the reporting is that it must be able to condense the complex message in the language that the top management understands. Also, it is important to tell the things without filtering or trying to "protect" the top management from the bad news. This is a cultural factor that we have the relationship between the top management in the state that we are able to present the things as they are. (Financial Company)

The most comprehensive approach to cybersecurity reporting according to the material was the IT Company's view. They described their reporting to the top management as positive, customer-focused, and delivered in regular cadence:

> We include our goals achieved, ongoing security awareness-campaigns statuses, reports from governance bodies, and overall timely information about information security and cybersecurity. The main goals of the report are that it is useful, easy to digest, and inspiring for the top management to catch and look for more if needed. (IT Company)

According to the insights from the material, the Financial Company aimed to create a dialogue with the top management. They were also expressing that the conversation is not always a natural task to participate since their top management is aware of cybersecurity and the related messaging:

> Reporting to top management is creating dialogue, questions, and hard questions. Top management understands very well the information security and cybersecurity-related messaging, and they are indicating their commitment to challenging and asking even detailed questions. (Financial Company)

In conclusion, the material shows that reporting is understood not only as a communication channel, but also as an essential way for the department of cybersecurity management to initiate and activate collaboration with the top management. All participating companies expressed that they are actively reporting to the company's top management and getting feedback from the reports as well. The reporting is critically dependent on the company's internal message delivery ability, which is inspected during the next subchapter.

5.4.3 Alignment of Internal Message Delivery

The most striking finding in this category is the '**Alignment of internal message delivery (16)**'. The perspective of the finding is expressly from the cybersecurity point of view. Participating companies contributed actively to this finding by highlighting the role of message delivery. It is good to note here that these concerns also separate communication from the top management reporting. The material shows that the participating companies focused on developing their cybersecurity-related messaging holistically and bi-directionally throughout the company, between individual employees, business units, and cybersecurity department.

The participants of BI Company and Financial Company described their approach to internal messaging by dedicated forums, who meet regularly. The participant of Financial Company accentuated the role of cybersecurity in the new business initiatives from the ground up and mentioned the 'side-channel' for top management as well:

> The Information security roundtable is our information-sharing forum, which meets on a monthly basis. All business units have their own representatives attending the forum with the topical information regarding their area of business, for example, IT, HR, and service production. This model has proven to be useful as these security awareness-sessions are focused on the most important functions in our compliance framework. (BI Company)

> We want to work together with the new business initiatives and enable the information security and cybersecurity functions and measures during the development. We have frequent round-table discussion forum with the specialists, where we develop new business models. We are constantly reviewing these models and indicating information security and cybersecurity-related issues in the development phase already. Top management is also aware of these discussions and developments through the active reporting channel. (Financial Company)

However, even if BI Company admitted the importance of the internal message delivery, they were still debating internally, if the message should eventually be delivered the business unit leaders or the department of cybersecurity management collectively:

> We still think if the security organization should collect and compile the information security information and reports from different business units and report then to top management, or if the business units themselves should report the information security-related topics and issues in their own communication and reports towards to top management. (BI Company)

These insights show that the department's cybersecurity management role in internal messaging is not always fully established. However, IT Company made an exception to this rule and took an active role in the cybersecurity messaging and discussions in their company.:

> On the corporate level, we are including security in our messaging in our internal information channels like the intranet. Also, our internal discussion forum has a security section, which our corporate security professionals are actively maintaining and collaborating on. Our mission is to keep information security discussion as part of everyday communication. (IT Company)

The participant of Media Company described the benefits of an active internal messaging channel from the other way around too. In the Media Company, the bi-directional channel enabled an easy way for the individual employees to report the anomalies and deviations detected from their day-to-day activities.

To conclude with the observations from the internal message delivery, the findings support clearly that internal messaging is playing an essential role in building security awareness. Moreover, the perceptions add that internal messaging is utilized bi-directionally as well.

5.4.4 Continual Improvement of ISMS

The discernments regarding continual improvement were mainly related to the finding 'cybersecurity maturity development (32),' which was scrutinized already in the chapter 5.1.1. Albeit, the continual improvement is aligned to this category as well. According to the perceptions regarding cybersecurity controls, one of the interesting findings is the '**continual improvement of ISMS (5)**'.

The interest to this finding raises mainly from the fact that these codes are grounded on the quotations from two companies only. The participants of BI Company and Media Company explained their approaches:

> We are directing our ISMS by ISO/IEC 27001 and the corresponding PDCA-cycle. We have set the continual improvement goals based on the ISO/IEC 27001 requirements. External audits are also one very effective and sovereign perspective to our information security and cybersecurity effectiveness and performance levels. (BI Company)

> The continual improvement process of ISO/IEC 27001 is in development. We have also thought and discussed what the appropriate KPIs would be to measure the long-term effects of decisions. When the basics are in place, the dashboard begins to provide more useful and richer measurement results. (Media Company)

The BI Company seemed to be more in the continual improvement phase, while the Media Company's approach was still in development. Other respondents did not mention the continual improvement of their ISMS at all.

Now that the material is considered thoroughly, these findings and insights revealed through the chapter are taken forward and discussed with the theoretical framework and base theories. The next chapter focuses on interpretations, implications, limitations, and recommendations of the research.

6 Discussing the Findings

The research aim of the study was to find out how the company's top management connects and collaborates with the cybersecurity governance of the company. The findings from the material were scrutinized in the previous chapter. The purpose of this chapter is to continue the synthesis, aiming to discuss the concrete results of the study. Chapters 2 and 3 of the study conducted a literature review, which constructed the theoretical framework for the research. This framework is referred to as literature during this chapter. Therefore, the research results consist of an interpretation of the empirical findings and dialogue with the literature.

Finally, I raise some implications and propose recommendations based on the discussed results. The significance, usability, reliability, validity, and limitations of the research is evaluated critically. Figure 12 illustrates the current phase as the last phase of the research process.

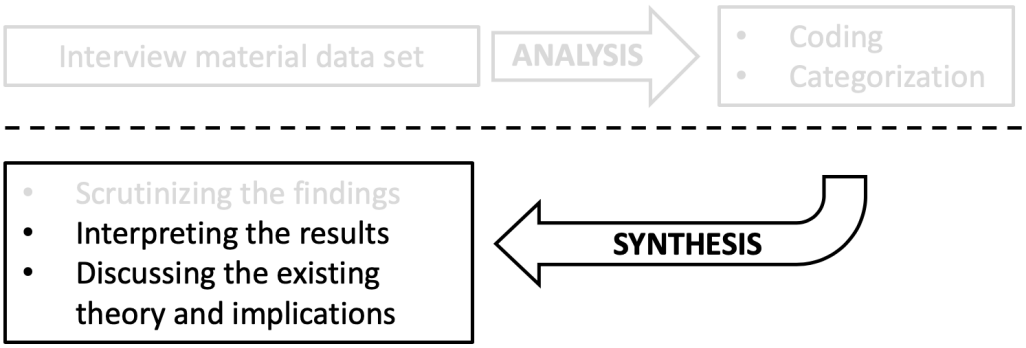

FIGURE 12 The last phase of the research process (Adapted from Hirsjärvi & Hurme, 2015, p. 144)

The main research question was: **How does the top management interact with the company's cybersecurity governance?** The rest of the chapter discusses the results concerning the main research question and the sub-questions.

6.1 Top Management Collaboration

Based on the insights that emerged from the material and in respect of the research aim, the most significant finding of the research was the **cybersecurity maturity development as an overarching, holistic driver for describing the collaboration between the top management and the cybersecurity governance**. The insights seem to indicate also that cybersecurity maturity development is a continuous and collaborative process between the top management and the department of cybersecurity management of the company. The literature

supports this identified approach from the company's corporate strategy development perspective. As a holistic approach, the cybersecurity maturity development relates to all P's (Mintzberg, 1987; see also chapter 2.1) from the corporate strategy perspective. Based on the material, the role of cybersecurity was emphasized in the strategic development from the standpoints of corporate strategy and strategic partnership. Hence, these insights show clear mutual support between the theory and the findings of the research.

6.1.1 Strategy and Guidelines

The findings regarding unified values and major strategic lines suggest support to the literature and the emergent strategy development approach. As Johnson et al. (2008) argue, a strategy is not solely a top management matter, but also the managers at every level need to communicate the strategy forward to achieve higher performance from the team. Also, in the literature, Jones (2008) argues that the strategy needs to be in heads, hearts, and hands of the people executing the strategy. In this light, the findings suggest that cybersecurity governance and management also have implications for the corporate strategy.

The material shows these corporate-strategy related matters manifesting clearly through the bi-directional collaboration between top management and cybersecurity governance, which was identified primarily in the participating companies whose strategy development was emergent. The theories of strategy development by Johnson et al. (2008) and Mintzberg (1987) are therefore supported, according to the findings, from both sides; emergent and intended. As the findings reveal, the logical incrementalism, cultural, and political processes were visible and active in the organizations developing their strategy emergently.

In contrast, the IT Company's strategic vision, leadership, and command were based on a more intended choice of strategic development. The organizational maturity, size of the company and security organization, and well-established governing hierarchies seem to explain the approach of IT Company in this matter.

Regarding the general course of the top management towards cybersecurity, the companies were broadly in line, and therefore appear to be supported by the general guidelines of the International Organization of Standardization (ISO/IEC, 2018a). These guidelines by ISO/IEC (2018a) are demanding three critical points from the companies' top management:

1. Promoting the mission, vision, values, and culture of the company;
2. Creating the environment in which people are engaged and committed;
3. Encouraging and supporting managers of the company.

According to the theoretical framework, von Solms (2001) emphasizes the commitment and responsibility of the top management. It is clear from the material that the top management of the participating companies is building their

collaboration with the cybersecurity governance on these qualities. Therefore, the results of the research indicate strong support for the theory demanding leadership, responsibility, and commitment from the top management (von Solms, 2001).

6.1.2 Top Management Activity

Other remarkable manifestations of this collaboration were the findings related to the business enablement factors of cybersecurity and top management activities in general. As Islam and Stafford (2017), and Traficom (2020) emphasizes, the top management should understand the criticality of the assets in the company's cyber operating environment and take an active role in providing adequate resources for cybersecurity governance for the protection of these assets. The insights from the material appear to support these theoretical approaches, and in general, the findings show that the top management of responding companies is relating to this adequately.

According to the findings from the material, the top management activities concerning cybersecurity varied from interests, visibility, and influence on more tangible actions, e.g., hiring a CISO, originating cybersecurity initiatives, and conducting communication-related activities. In the literature, Traficom (2020) calls for the active, ongoing, and bi-directional communication between top management and all relevant stakeholders. The material supports widely that the top management has taken an active role in communication in the participating companies.

However, there were some contradicting findings as well regarding the top management activity. As an example, the Software Company was experiencing the absence of tangible initiatives. In this case, the possible explanation could be the somewhat early stages regarding cybersecurity maturity development. On the other hand, another possible explanation for the issue could be that the Software Company's top management is treating the cybersecurity as a technical matter and outsourcing the related actions to the CISO. Literature has identified the approach of outsourcing cybersecurity widely (von Solms, 2001; Siponen & Oinas-Kukkonen, 2007; Siponen et al., 2014; Rothrock et al., 2018).

Since the top management collaboration with cybersecurity governance is a bi-directional activity, the insights also show that the 'bottom-up' direction of the collaboration was functioning effectively in the participating companies. The material also confirms that the internal message delivery is operational, and the general collaboration and interaction with the top management is satisfactory.

Whitman and Mattord (2014) argue in the literature that the report content to the top management must occur as an ongoing collaboration without filtering, facts need to be aggregated, and language must match the audience. Also, the message needs to be relevant and meaningful (Whitman & Mattord, 2014). The findings indicate support for these suggestions. Moreover, the delivered reports are accepted, understood, and utilized by the top management.

6.1.3 Continual Improvement of ISMS

Von Solms & von Solms (2004) argue in the literature that the actual content of Information Security Governance (ISG) is the Information Security Management System (ISMS). Furthermore, many scholars agree that a typical implementation of ISMS is following the Deming's Plan-Do-Check-Act (PDCA) cycle for the continual improvement of the ISMS (Sheikhpour & Modiri, 2012; Nicho 2018; Humphreys, 2016; von Solms & von Solms, 2009; Whitman & Mattord, 2018; Mataracioglu & Ozkan, 2011).

The continual ISMS improvement in ISO/IEC 27001 is linked to the act-phase of the PDCA-cycle (ISO/IEC, 2005), and the need for improvement usually rises from nonconformity (Humphreys, 2016). However, there was no evidence in the material about references on how nonconformities are handled. Only one participant company mentioned the PDCA-cycle and connected it to their continual improvement goals. Another company participant responded that their approach for continual improvement is still under development.

This absence of the PDCA's act-phase was an unanticipated, yet significant finding. From the four respondent companies using ISO/IEC 27001, only one mentioned PDCA explicitly. I was predicting the participants to elaborate on the continual improvement of their ISMS when asked about the ISG (see question 11 in appendix 1). As a researcher, I did not intentionally ask any specifying questions concerning this question because I did not want to lead or inject the answers. I was expecting the participant to answer this question in regards to their ISG framework and its key elements (e.g., ISO/IEC 27001, or ISF SoGP and the corresponding continual improvement guidelines). It should also be noted that this specific question was 'closed-ended' and, therefore, not asking for an explicit explanation.

However, the finding's significance is based on the fact that I could not get any more than one participant's support from the material if the participant companies had been systematically and deliberately conducting their continual improvement as instructed by ISO/IEC 27001 standard. One of the respondent companies had an approach to ISG based on ISF's Standard of Good Practice. However, there is no evidence in the material about this company and the systematical approach to the ISMS's continual improvement.

Conversely, the findings show that the feedback loop between top management and cybersecurity governance is in its place in the participating companies. In the literature, Nicho (2018) emphasized the importance of the feedback loop in the ISG process to ensure timely corrective actions, which eventually contributes to continual improvement. The feedback loop could be applied to deliver and drive continual improvement.

The main research question is answered from various perspectives, while the cybersecurity maturity development is suggested being the overarching, holistic driver for this collaboration. Another significant finding concerning the main research question is the missing support for the continual improvement of the ISMS, which falls under the responsibility of cybersecurity governance.

The research results contribute a clearer understanding of the top management leadership, responsibility, commitment, and tangible actions concerning the company's cybersecurity governance.

6.2 Driving the Cybersecurity Governance

The first sub-question for the study was: *What aspects drive the cybersecurity governance and management in the company?* According to the material, the cybersecurity governance and management was driven by two remarkable aspects, which emerged clearly from the material as major findings. These qualities are the **industry's best practices** and **security culture development**.

The utilization of industry best practices manifested mainly in the form of ISO/IEC 27000 family-related pursuits, but there were some contrasting approaches as well. For example, the material identified a company changing from standard to another, and another company 'cherry-picking' the most relevant aspects of various best practices. According to von Solms & von Solms (2004), the actual content of ISG is the ISMS, and these ISMS's should be based on the international best practices. In that sense, the findings regarding cybersecurity governance are gaining support from the literature.

Another essential finding was security culture development. Many insights supported this finding, and it aligned mutually with various other findings as a holistic theme. The Software Company was the only participant company where the material could not reveal any signs of security culture development. This matter regarding Software Company was already discussed earlier in the chapter 6.1.2. An inference based on this finding can be made that even if the company has tangible information security attainments (e.g., ISO/IEC 27001 certified ISMS), the security culture might be absent. According to Traficom (2020) and NCSC-UK (2019), the value-add from security to the company requires a positive cybersecurity culture. The findings support this guidance since material shows that the vast majority of the companies invested deliberately in security culture development.

The results regarding this sub-question were somewhat what I expected. However, more of an unanticipated finding was that the cybersecurity strategy was not as visible in the material as the literature emphasized. According to the material, cybersecurity strategy was identified instead as what von Solms and von Solms (2004) described as an *information security policy*. The insights show that even if the companies did not emphasize an actual, tangible cybersecurity strategy, they might still have a healthy approach to cybersecurity governance. Based on the findings, it seems that cybersecurity governance is grounded on the ISMS, and it appears that it is driven by the ISMS rather than a cybersecurity strategy.

6.3 Directing and Controlling the Cybersecurity Governance

The second and third sub-questions for the study were: *How are the cybersecurity measures **directed** in the company?* Furthermore; *How are the cybersecurity measures **controlled** in the company?* The literature review introduced an information security governance (ISG) model (see chapter 3.2.2), which is based on the Direct-Control cycle (von Solms & von Solms, 2009). I was able to identify a variety of cybersecurity governance activities from the material, supporting the theories grounding the direct-control model.

6.3.1 Directing the Cybersecurity Measures

According to the *directing* phase of the cycle in the model, the most outstanding major finding was the **responsibility** considering cybersecurity in the participating companies. Responsibility for cybersecurity was assigned to different parties in the companies, but most often to the individual business units or the security organization. However, the findings reveal that the individual business unit responsibility was often indirectly connected eventually to the security organization. In the literature, von Solms and von Solms (2009) are also addressing the responsibility aspect regarding different flavors of governance, including information systems governance (ISG). In a limited company, the ultimate responsibility lies with the top management, which is the argument of von Solms and von Solms (2009). However, in the cybersecurity governance aspect, the additional responsible parties, according to von Solms and von Solms (2009), are; information security management, business units, risk management department, and users. Therefore, the findings are likely to support the direct-control model from this quite foundational perspective.

Another striking insight from the material was the training approach, and especially the security awareness generation perspective. The findings reveal that training was 'tailored to fit' in the participating companies, as many scholars suggested in the literature review (Peltier, 2006; Gratian et al., 2018; Albrechtsen & Hovden, 2010; Wilson & Hash, 2003). There was also evidence in the material that the training was aligned with the 'awareness-training-education' continuum (Wilson & Hash, 2003). For example, Media Company had their DevOps teams trained on a specific level and focus, and BI Company had even experiences from dissertation supervising.

According to findings from the material, the relation between technical-administrative measures and security awareness generation activities was seen instead as a continuum than competing sides in the participating companies. The insights from the material reveal that the role of technical-administrative seems to be more of a 'compulsory baseline' to the training approach, which is supported by findings, where the creativity and actual cybersecurity enablement is reported to happen on the security awareness generation side of the continuum. This approach was identified by Merete Hagen et al. (2008) in the

literature review. The theory by Merete Hagen et al. (2008) is supported by the findings concerning the relation between technical-administrative measures and security awareness generation.

In conclusion, the findings support that the directing of cybersecurity measures is divided into strategic, tactical, and operational levels, as von Solms & von Solms (2009) suggests in theory. However, the findings from the material do not fully support the inputs and outputs between the different levels, which are stated in theory by von Solms and von Solms (2009).

6.3.2 Controlling the Cybersecurity Measures

Based on the findings, the cybersecurity measures are *controlled* in the participating companies by **measuring and assessing** 'the state of cybersecurity' from different perspectives. The measurement perspectives concerning cybersecurity varied in the participating companies. The material shows that most of the participating companies were measuring their cybersecurity level via traditional measures like compliance and risk. As a development initiative, the participating companies also had the interest to measure culture, business value, and the effectiveness of cybersecurity measures. These different approaches were in line with descriptions and theories by Merete Hagen et al. (2008) and Boone (2017).

In addition to these classic measurement perspectives, some participating companies measured cybersecurity performance from the benchmark point of view. This performance perspective was an unexpected finding regarding controlling cybersecurity measures and the theory aligned. The approach in the literature to measuring performance was more from the PDCA-cycle, and specifically the *check* phase (Humphreys, 2016). In contrast, the findings from the material suggest utilizing the information security benchmark from the performance perspective. Interestingly, there is no evidence in the material of any of the organizations connecting the performance measurement to the PDCA-cycle.

The findings also show that the controlling phase of the cybersecurity measures according to the direct-control model consists of reporting, internal messaging, and continual improvement. However, these aspects are related more to the main research question and, therefore, have been discussed already in chapter 6.1.2 earlier.

According to von Solms & von Solms (2009), the control part of the direct-control model focuses on monitoring, controlling, information security compliance management, and reporting to executive management. The direct-control theory (von Solms & von Solms, 2009) supports the results, which suggest that controlling the cybersecurity measures appears to be primarily based on measuring, assessing, reporting, and utilizing the content in the continual improvement of the ISMS in the company.

6.4 Implications and Recommendations

The study revealed that companies are utilizing functions, practices, and tools, which are vital parts of a generic ISG framework. Similarities between the operational model of the participating companies and the direct-control model (von Solms & von Solms, 2009) were detected. However, the results of the study revealed, there might be some gaps in the implementations of the current ISG frameworks, standards, and guidelines. The implication is that this negligence could slow down cybersecurity maturity development, which was the significant finding of the study. Moreover, if the ISG framework is not utilized to its full extent, the full value from the outcomes of the utilization cannot be expected.

The study recommends that companies should utilize the cybersecurity maturity development as a holistic driver to support and improve collaboration between the top management and the cybersecurity governance. The implications of cybersecurity maturity development appear to be positive and may positively affect the (cyber)security culture development.

As a second recommendation, the study suggests that the continual improvement of the ISMS should be addressed deliberately. The continual improvement of ISMS is an essential opportunity to build also the collaboration with the top management. The top management will likely be more interested, committed, and proactive with the cybersecurity governance if the improvement, especially the effectiveness of the ISMS, can be proven. The meticulous approach might have a positive impact on justifying investments also. As the findings show, the feedback loop between top management and cybersecurity governance is active and operational. Therefore, the compulsory element of ISO/IEC 27001, '9.3 Management review' (ISO/IEC, 2018a) would benefit the continual improvement greatly from this ongoing collaboration.

Finally, the study recommends that there should be active pursuits in reviewing and assessing – or even measuring – the effectiveness of the corrective actions. The changes in the ISMS should not be applied to satisfy the audits but to genuinely and continually pursue the improvement of the company's cybersecurity holistically.

6.5 Significance and Usability

At the end of the literature review, I indicated the quite negligible visibility of the research literature to the top management's relationship with cybersecurity governance. Also, the empirical research gap was recognized. The study was able to enlighten the collaboration between top management and cybersecurity governance while contributed to filling the empirical research gap.

The results of this research are of interest and significance to members of top management and cybersecurity leaders. The study results are essential for the companies to evaluate and assess the collaboration in their companies. The

insights gained from the study also helps companies to evaluate and prioritize the most effective measures for the cybersecurity governance implementations. E.g., Utilizing the ISG framework to its full extent, tailoring the security awareness generation training appropriately, enabling the cultural development, and clarifying responsibilities throughout the organizations in the company.

From an academic point of view, the study lays the groundwork for future research into top management and cybersecurity governance research. This research's broad topic area led to a broad scope, which affects the generalizability of the results. However, from a further research point of view, the study is usable as a foundation or source of ideas for many researchers to come.

6.6 Assessing the Quality of the Research

In scientific research, the authenticity and accuracy of the information have a significant role. Eskola and Suoranta (1998) state that the starting point for qualitative research is the open subjectivity of the researcher and the recognition that the researcher is the central research tool of her or his research. In qualitative research, the main criterion of authenticity and accuracy is the researcher himself; therefore, the assessment of these properties applies to the entire research process (Eskola & Suoranta, 1998).

Traditionally, these properties have been measured by reliability and validity in the field of quantitative research. However, Denscombe (2014) argues that measuring reliability in qualitative design is being criticized by many scholars since a social setting is virtually impossible to replicate. Taking also the validity to account, discussion of assessing the quality of the qualitative research has moved towards the credibility, transferability, and dependability of the study. Table 12 explains the parallel alignment with these alternative criteria. (Denscombe, 2014; Saunders et al., 2019.)

TABLE 12 Alternative quality criteria (Saunders et al., 2019, p. 217)

Criterion	**Traditional parallel alignment**
Dependability	Reliability
Credibility	Internal validity
Transferability	External validity / generalizability

I identified the threats to dependability in this research before the actual research process started and minimized the participant error and bias by keeping the interview situation similar across the cases. This approach was successful since all interviews were conducted at a pre-arranged time, in the participant's premises, in closed conference rooms without any interference. All participants received the same interview questions beforehand and were able to prepare for the interview adequately. To avoid researcher bias and error, the researcher was

well prepared and conducted the interviews without any subjective steering or intervention. All possible misunderstandings were solved immediately during the interview without affecting the answer content. In terms of dependability, I utilized a non-probability sampling technique based on volunteering and self-selection to select the cases for the study (Saunders et al., 2019). According to Saunders et al. (2019) and Sarajärvi and Tuomi (2018), qualitative research is likely to utilize non-probability sampling.

The non-probability sampling has been criticized for the lack of generalizability (Yin, 2018; Noor, 2008). However, in this qualitative research, there were not even aiming to make any statistical generalizations. Instead, this qualitative research aimed to understand and describe particular collaboration in the companies. Therefore, the participants needed to be experienced professionals regarding the aim and subject of this research. The respondents' role was credible from the research questions' point of view since the respondents were operating with the top management of their companies on an almost daily basis concerning cybersecurity. According to Sarajärvi and Tuomi, (2018), the relatively small (5) number of participants is satisfactory from the credibility point of view as the study is a thesis after all.

Firstly, the credibility of the study is based on the instructed, evaluated, and justified research setting. Secondly, I have contributed the credibility by deliberately explained, executed, and documented theory-guided thematic content analysis. Finally, I have enhanced the credibility of the study by scrutinizing the findings of the study as openly as possible. The voice of the participants is loud and clear, which opens a clear vision to the researcher's view on analysis, synthesis, and interpretations in general.

The transferability is closely related to the generalizability, which is criticized already from the research design and sampling method/size viewpoints. These aspects are unchallenged. However, according to Denscombe (2014), the question with the transferability is different and asks: 'To what extent the findings in this research could be transferred to other instances?' In general, the answer regarding this research is: 'Where applicable.' For example, the findings with strong support from the theory, like measuring and reporting cybersecurity in the company, could be transferred to other instances. In this sense, the recommendations of this research were also practical.

6.7 Limitations and Concerns

The generalizability of the results is limited due to the methodological choices and a small sample of participants. The broad topic area of this research led to a broad scope even with pruning to only the essentialities. While providing a central view and position in the organization, the concern relates to the narrow scope considering the whole organization. However, this has been considered in the research design, and the more comprehensive view is a place for further research.

7 Conclusion

This study was aimed to discover how the company's top management collaborates with the cybersecurity governance. Based on the qualitatively conducted multiple-case study research, the study was concluding that the cybersecurity maturity development appears to be a holistic driver for describing the collaboration between the top management and the cybersecurity governance. The results also have indicated that a company's Information Security Management System (ISMS) might benefit from more deliberate and holistic utilization of the chosen Information Security Governance (ISG) approach, for example, in terms of improved effectiveness.

I had gathered the empirical material for the research from five (5) cybersecurity leaders from different companies and various industries via thematic interviews. The interviews were analyzed using theory-guided thematic analysis, which revealed interesting findings and insights from the real-life scenarios considering the research aim and theme. Some of the findings were expected and anticipated, while some findings were surprising. The voice of the participants had been emphasized intentionally during the walk-through of the findings. The participants' real voice had enlivened the insights and had revealed the thinking behind the research's interpretation process.

The research was able to contribute to filling the empirical research gap, which existed in the field of information security concerning the top management collaboration. In general, the results of this research provided new insights into the collaboration and relationship between the company's top management and cybersecurity governance. This collaboration manifested through cybersecurity maturity development, enabling business, bi-directional activities and dialogue, and strategic development with mutually aligned values. These results should be taken into account when considering how to establish and maintain the collaboration between top management and company in the realm of cybersecurity.

Based on the results of the research, the study suggested that practitioners should embrace the cybersecurity maturity development as a holistic driver for the collaboration between the top management and cybersecurity governance. Moreover, the study suggested that the companies should have active and continual pursuits considering the company's cybersecurity improvement. As an approach to this, the effectiveness of corrective actions should be assessed deliberately.

7.1 Further Research

The broad scope of the study raised limitations and concerns. In contrast, considering further research recommendations opens a lot of new possibilities.

In this research, I collected empirical data from an officer-level of cybersecurity departments. This level represents already 'top management' related to the security organization, and the views would have been much broader and varied in perspectives if the other people from the security organization would have been interviewed as well. Security specialists in the security organization, business units, and security champions at the operational level would have insights into the information unheard of within the management level. This type of research could be a single-case study instead, but thematic interviews with theory-driven content analysis would suit adequately to this approach as well.

The more thorough research of specific topics of the study might have opportunities as well. For example, focusing on the 'technical-administrative – security awareness generation' continuum would have significant implications for organizing the cybersecurity training in the companies. A cross-disciplinary study with cognitive sciences about the effectiveness of the cybersecurity training might be necessary from a scientific perspective.

The study touched a bit the developing strategic effectiveness measurement. Further research of this area is needed to get an ampler understanding of the phenomenon, particularly from the viewpoint of cybersecurity governance. It would make sense to research in focus on how the companies are ensuring the effectiveness of their strategic decisions concerning cybersecurity. These decisions could be corrective actions to nonconformities as well as investments or strategic pivots.

Finally, the ISG frameworks, standards, and governance models are developing and expanding steadily. Further research is needed continuously on multiple perspectives concerning this broad and significant theme of the information security and cybersecurity industry. The research should not focus solely on the whitepapers, checklists, and standards themselves, but more on the implementation and especially the utilization. 'Were the implemented corrective actions *effective* or not?'

REFERENCES

Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445. https://10.1016/j.cose.2009.12.005

Alqurashi, E., Wills, G. & Gilbert, L. (2013). A viable system model for information security governance: Establishing a baseline of the current information security operations system. In *IFIP International Information Security Conference*, 245-256.

Alreemy, Z., Chang, V., Walters, R. & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management*, *36*(6), 907-916. https://doi.org/10.1016/j.ijinfomgt.2016.05.017

Andrews, K. R. (1997). The Concept of Corporate Strategy. In N. J. Foss (Ed.), *Resources, Firms and Strategies: A reader in the resource-based perspective* (pp. 52-59). Oxford University Press.

Axelos. (2020a). *ITIL - IT service management.* https://www.axelos.com/best-practice-solutions/itil

Axelos. (2020b). *SLAs of the future: measuring outcomes, not IT availability: ITIL 4 - The Evolution of ITSM Part 5.* https://www.axelos.com/news/blogs/february-2019/slas-of-future-measuring-outcomes-not-it-availity

Berghel, H. (2005). The two sides of ROI: return on investment vs risk of incarceration. *Communications of the ACM*, *48*(4). 15-20. https://doi.org/10.1145/1053291.1053305

Boone, A. (2017). Cyber-security must be a C-suite priority. *Computer Fraud & Security*, *2017*(2), 13-15. https://doi.org/10.1016/S1361-3723(17)30015-5

Chalaris, I., Lemos, P. P. & Chalaris, M. (2005). IT Governance: The safe way to effective and efficient governance. *E-Journal of Science and Technology*, *1*(1), 59-63. https://doi.org/10.18780/e-jst.v1i1.516

Choo, K-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731. https://doi.org/10.1016/j.cose.2011.08.004

Contreras, R. B. (2020). Overview of ATLAS.ti 8 Mac [Video]. YouTube. https://www.youtube.com/watch?v=43U7503Rm20

Darke, P., Shanks, G. & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. *Information systems journal*, *8*(4), 273-289. https://doi.org/10.1046/j.1365-2575.1998.00040.x

Denscombe, M. (2014). *The good research guide: for small-scale social research projects*. (5th ed.). McGraw-Hill Education.

Dhillon, G. & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2). 127-153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

DiCicco-Bloom, B. & Crabtree, B. F. (2006). The qualitative research interview. *Medical education*, *40*(4), 314-321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Dufva, M. (2019, December 31). *Teknologia sulautuu kaikkeen*. Megatrendit 2020. Sitran selvityksiä, 162. Sitra. https://www.sitra.fi/julkaisut/megatrendit-2020/

Eisenhardt, K. M. & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*(1), 25-32. https://doi.org/10.5465/amj.2007.24160888

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550. https://doi.org/10.5465/amr.1989.4308385

Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino.

European Commission. (2016). General Data Protection Regulation (EU) 2016/679. European Parliament and Council of the European Union.

Finnish Companies Act 2006/624. (2006). Helsinki 21.7.2006.

Firesmith, D. (2015). *Four Types of Shift Left Testing*. Carnegie Mellon University. https://insights.sei.cmu.edu/sei_blog/2015/03/four-types-of-shift-left-testing.html

Garigue, R. & Stefaniu, M. (2003). Information security governance reporting. *Information Systems Security*, *12*(4). 36-40. https://doi.org/10.1201/1079/43855.31.6.20031201/78849.3

Gashgari, G., Walters, R. J. & Wills, G. (2017). A Proposed Best-practice Framework for Information Security Governance. *In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - Volume 1: IoTBDS*. 295-301. https://doi.org/10.5220/0006303102950301

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & security*, *73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Guldentops, E., Lainhart, J. W., Hardy, G., & Schuermans, E. (2003). Board briefing on IT governance. (2nd ed.) *IT Governance Institute*. *Information Systems Audit and Control Association*.

Higgs, J. L., Pinsker, R. E., Smith, T. J. & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, *30*(3), 79-98. https://doi.org/10.2308/isys-51402

Hiller, J. S. & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review*, *29*(3), 236-245. https://doi.org/10.1016/j.clsr.2013.03.003

Hirsjärvi, S. & Hurme, H. (2015). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Gaudeamus.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita*. (15th ed.). Tammi.

Huang, D. L., Rau, P. L. P. & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221-232. https://doi.org/10.1080/01449290701679361

Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard* (2nd ed.). Artech House.

Information Security Forum. (2020). *Information Security Forum*. https://securityforum.org

International Federation of Accountants (IFAC). (2020). *International Federation of Accountants*. https://ifac.org

International Organization for Standardization, ISO/IEC. (2005). ISO 27001:2005 *Information technology. Security techniques. Information security management systems. Requirements.* ISO, Geneva.

International Organization for Standardization, ISO/IEC. (2017). ISO 27001:2017 *Information technology. Security techniques. Information security management systems. Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015).* ISO, Geneva.

International Organization for Standardization, ISO/IEC. (2018a). ISO 9004:2018 *Quality Management. Quality of an organization. Guidance to achieve sustained success.* ISO, Geneva.

International Organization for Standardization, ISO/IEC. (2018b). ISO 27000:2018 *Information technology. Security techniques. Information security management systems. Overview and Vocabulary.* ISO, Geneva.

Islam, M. & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: The Security Savviness of Board of Directors. 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation.

Johnson, G., Scholes, K. & Whittington, R. (2008). *Exploring corporate strategy* (8th ed.). Prentice Hall Financial Times.

Johnston, A. C. & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126-129. https://doi.org/10.1145/1435417.1435446

Jones, P. (2008). *Communicating strategy*. Gower. https://doi.org/10.4324/9781315259840

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, *57*(10), 2206-2211. https://doi.org/10.1016/j.comnet.2012.11.023

Kayworth, T. & Whitten, D. (2012). Effective Information Security Requires a Balance of Social and Technology. *MIS Quarterly executive*, *9*(3). 163-175. https://ssrn.com/abstract=2058035

Khansa, L. & Liginlal, D. (2009). Quantifying the benefits of investing in information security. *Communications of the ACM*, *52*(11), 113-117. https://doi.org/10.1145/1592761.1592789

Kim, J. (2017). Cyber-security in government: reducing the risk. *Computer Fraud & Security*, *2017*(7), 8-11. https://doi.org/10.1016/S1361-3723(17)30059-3

Kwon, J., Ulmer, J. R. & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27*(1), 219-236. https://doi.org/10.2308/isys-50339

Lehto, M. & Kähkönen, A. (2015). Kyberturvallisuuden kansallinen osaaminen. *Informaatioteknologian tiedeunnan julkaisuja.* 20(2015). https://jyx.jyu.fi/handle/123456789/47116

Limnéll, J. (Speaker). (2020, January 13). *Teknologia, turvallisuus ja tuleva vuosikymmen* [Audio podcast]. https://areena.yle.fi/1-50398099

Mataracioglu, T. & Ozkan, S. (2011). Governing Information Security in Conjunction with COBIT and ISO 27001. *International Journal of Computer*

Science and Information Technology, *3*(3). 288-293. https://doi.org/10.5121/ijcsit.2011.3321

Merete Hagen, J., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377-397. https://doi.org/10.1108/09685220810908796

Mintzberg, H. (1987). The Strategy Concept I: Five Ps for Strategy. *California Management Review*, *30*(1), 11-24. https://doi.org/10.2307/41165263

National Cyber Security Centre UK (NCSC-UK) (2019, March 21). *Board Toolkit.* Government Communications Headquarters GCHQ. https://www.ncsc.gov.uk/collection/board-toolkit

Nicho, M. (2018). A process model for implementing information systems security governance. *Information and Computer Security*, *26*(1), 10-38. https://doi.org/10.1108/ICS-07-2016-0061

Nieles, M., Dempsey, K & Pillitteri, V., Y. (2017). An Introduction to Information Security. *NIST Special Publication*, *800*(12). US Department of Commerce. https://doi.org/10.6028/NIST.SP.800-12

Noor, K. B. M. (2008). Case study: A strategic research methodology. *American journal of applied sciences*, *5*(11), 1602-1604. https://doi.org/10.3844/ajassp.2008.1602.1604

Pelnekar, C. (2011). Planning for and Implementing ISO 27001. *ISACA Journal*, *4*(28). 1-8.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *EDPACS*, *33*(1), 1-18. https://doi.org/10.1201/1079.07366981/45423.33.1.20050701/89329.1

Posthumus, S. & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8). 638-646.

Publication Forum. (2020). Julkaisufoorumi. https://www.julkaisufoorumi.fi/en/

Quinn, J. B. & Voyer, J. (2003). Logical Incrementalism: Managing Strategy Formation. In H. Mintzberg (Ed.), *The Strategy Process: Concepts, Contexts, Cases* (4th ed., pp. 183-188). Prentice Hall Financial Times.

Ristov, S., Gusev, M. & Kostoska, M. (2012). Information Security Management System for Cloud Computing. *ICT Innovations 2011, Web Proceedings ISSN 1857-7288*, 49.

Rothrock, R. A., Kaplan, J. & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12-15.

Saldaña, J. (2015). *The coding manual for qualitative researchers*. (2nd ed.). Sage publications.

Sarajärvi, A. & Tuomi, J. (2018). *Laadullinen tutkimus ja sisällönanalyysi*. (3rd ed.). Tammi.

Saunders, M. N. K., Lewis, P. & Thornhill, A. (2019). *Research methods for business students.* (8th ed.). Pearson.

Scholl, M., Leiner, K. B. & Fuhrmann, F. (2017). Blind Spot: Do You Know the Effectiveness of Your Information Security Awareness-Raising Program? *Journal of Systemics, Cybernetics and Informatics*, *15*(4). 58-62.

Sheikhpour, R. & Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Applications*, *6*(2), 13-28.

Siponen, M. T. & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *38*(1), 60-80. https://doi.org/10.1145/1216218.1216224

Siponen, M., Mahmood, M. A. & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2). 217-224. https://doi.org/10.1016/j.im.2013.08.006

Traficom (2020, February 6). *Cyber security and the responsibilities of boards.* Finnish Transport and Communications Agency Traficom. National Cyber Security Centre Finland. https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas

von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376. https://doi.org/10.1016/j.cose.2004.05.002

von Solms, B. (2001). Corporate Governance and Information Security. *Computers & Security*, *20*(3), 215-218.

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*. 97-102. https://doi.org/10.1016/j.cose.2013.04.004

von Solms, S. H. & von Solms, R. (2009). *Information security governance*. Springer Science+Business Media. https://doi.org/10.1007/978-0-387-79984-1

Whitman, M. E. & Mattord, H. J. (2018). *Principles of information security*. (6th ed.) Cengage Learning.

Whitman, M., Mattord, H. (2014). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education*, *11*(1).

Wilson, M. & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50). US Department of Commerce. https://doi.org/10.6028/NIST.SP.800-50

Wilson, M., Stine, K & Bowen, P. (2009). Information Technology Security Training Requirements: A Role-and Performance-Based Model. *NIST Special Publication*, *800*(16). US Department of Commerce. https://doi.org/10.6028/NIST.SP.800-16

Wolf, M., Haworth, D. & Pietron, L. (2011). Measuring an information security awareness program. *The Review of Business Information Systems*, *15*(3). 9-21. https://doi.org/10.19030/rbis.v15i3.5398

World Economic Forum (2020, January 15). The Global Risks Report 2020. World Economic Forum. https://www.weforum.org/reports/the-global-ris ks-report-2020

Yin, R. K. (2018). *Case study research and applications: Design and methods.* (6th ed.) Sage publications.

APPENDIX 1 INTERVIEW QUESTIONS

Theme 1: Cybersecurity aligned to the strategy work of your company

1. **How the cybersecurity responsibilities are arranged on the top management level?**

2. **Have you used or planned to use any best practices-based information security or cybersecurity management/control standard or parts of the standard?**

3. **Have you certified or planned to certify your information security management system (ISMS) to any well-known standard?**

4. **How would you describe the attitude towards cybersecurity in your company's top management?**
    a. *In which kind of practical initiatives or concrete actions this have been epitomized?*

5. **Is your company's top management seeing cybersecurity more as a compulsory security measure or more as a business enabler?**
    a. *Supporting function or strategic partner?*

6. **Do you see that the cybersecurity is guiding your company's strategy work or vice versa?**

7. **How does your company's cybersecurity strategy take in account your company's corporate strategy, mission and vision?**
    a. *Are the company's strategic "big lines" taken into account?*
    b. *Is there a unified set of values (between strategies)?*

8. **What challenges you see in the future of strategic leadership of cybersecurity?**

Theme 2: Cybersecurity implementation and governance

9. **Is your company directed with support of any higher-level governance framework?**

10. **Are your company's IT-production/operations directed with support of any governance framework?**

11. **Is your company's information security directed with support of any governance framework or structure?**

12. **How the information security is directed in your company on the level of the whole organization?**

13. **How do you see the relationship between the formal, technical-administrative security measures and the awareness-raising measures in your company?**
    a. *Are both approaches considered necessary and useful?*
    b. *Do you see any confluence or continuum between these?*

14. **How is your company managing the staff training regarding cybersecurity?**
    a. *Is the training divided on different levels?*
    b. *Is the training tailored for the corresponding job descriptions and roles?*

Theme 3: Assessing and reporting the effectiveness of cybersecurity

15. **How is it ensured, that the strategic decisions were correct from the cybersecurity effectiveness point of view?**

16. **From which perspectives the cybersecurity effectiveness level is measured or assessed in your company?**

17. **Have you attempted to evaluate and utilize the added value from the cybersecurity measures in business, strategy work or decision making?**

18. **Which features of the (cybersecurity) report to the top management are particularly important in your company and why?**

19. **How the before mentioned reports are welcomed (in the top management)?**
    a. *Is this epitomizing the top management attitude / commitment regarding cybersecurity?*
    b. *Are the presentations or deliveries of these reports creating dialogue?*

APPENDIX 2 CODES AND CATEGORIES

Categories and Codes

1 Top Management's Alignment with Cybersecurity (10 codes)	Groundedness
Cybersecurity maturity development	32
Customer requirements	10
Customer demand for cybersecurity	10
Telling the truth	8
Customer trust as a priority	7
Customer satisfaction	3
Employee satisfaction as a key	1
Easy to motivate investments	1
Credible forum members	1
COBIT	1

1.1 Strategy Work (22 codes)	Groundedness
Developing security organization	15
Cybersecurity as a strategic priority	11
Bi-directional development with top management	11
Traditional strategy development	6
Strategic effectiveness not measured	6
Holistic view on cybersecurity	6
Emergent strategy development	6
Unified values	5
Managing company growth	5
Developing strategic effectiveness measurement	5
Commitment to the customers exist	5
No corporate governance framework used	4
Corporate governance framework in place	4
Strategic threat model	3
Risk framework in place	3
Communication as a priority	3
Top-down directing model in target	2
Supporting strategy work	2
Corporate governance integration	2
Three lines of defense	1
Supporting decision-making	1
Strategic vision missing	1

1.2 View on Cybersecurity (12 codes)	Groundedness
Cybersecurity as a business enabler	17
Cybersecurity aligns with corporate strategy	10
Cybersecurity in top management message delivery	9

Cybersecurity integrated in company	8
Cybersecurity is business critical	7
Cybersecurity challenges in top management	5
Cybersecurity in active dialogue	4
Cybersecurity as a support function	4
Cybersecurity as a business differentiator	4
Cybersecurity message delivery inadequate	2
Cybersecurity has attention	2
Cybersecurity as a competitive advantage	2

1.3 Top Management Activity (25 codes)	**Groundedness**
Top management interest	16
Top management commitment exists	16
Top management activity	16
Top management dialogue	14
Top management channel	13
Top management visible in security	12
Top management support	9
Top management commitment inadequate	7
Top management awareness and encouragement	7
Top management feedback	6
Top management challenging	6
Organizational changes	6
Top management link missing	5
Top management questioning	4
Responding to external phenomena	4
Tangible initiatives from top management	3
Responsibility for cybersecurity is on the top management	3
Operational changes	3
Top management information security directing	2
Top management acceptance for security management	2
Operative connection missing	2
Missing tangible initiatives from top management	2
Individual top management commitment	2
Top management cost awareness	1
Security management for top management	1

1 Top Management's Alignment with Cybersecurity Total 69 Codes	**417 Links to Quotations**

2 Cybersecurity Governance and Management (8 codes)	Groundedness
Cybersecurity Investments	12
Certified / Attested against standard(s)	12
Information security benchmarking	4
No common language with IT	3
Growth as a challenge	3
Physical security	1
Lack of rigorous support	1
Customers evaluating cybersecurity performance	1

2.1 Culture (11 codes)	Groundedness
Security culture development	21
Co-operative culture	12
Interest in measuring culture	10
Security culture development as challenge	7
Security culture development as priority	5
Positive internal feedback	5
Positive external feedback	5
Individual security culture development as challenge	3
Cybersecurity going out of style	3
Emphasizing human factor	2
Fighting against finger-pointing	1

2.2 Best Practices (14 codes)	Groundedness
Utilizing best practices	31
ISO/IEC 27001	17
Multiple best practices	11
Importance of external audits	7
ITIL	6
Industry regulations	6
ISO/IEC 27002	5
Importance of internal audits	5
ISF Standard of Good Practice inactive	3
ISAE 3000 family	3
PCI-DSS	2
ISF Standard of Good Practice active	2
Quality initiatives	1
NIST Cybersecurity Framework	1

2.3 Governance, Organization and Cybersecurity Strategy (18 codes)	
Hiring security professionals is a challenge	10
Large security organization	8
Multiple responsible roles for cybersecurity	7
Mature security organization	7

Cybersecurity strategy exists	6
Need for multi-talent workforce	5
Information security governance	5
Information security governance development	5
Full-time employee (FTE)	5
Young security organization	3
Information technology governance	3
Hiring security professionals	2
Cybersecurity strategy absence	2
Custom corporate governance	2
Corporate governance in place	2
Small security organization	1
No information security governance framework used	1
Dedicated resources	1
2 Cybersecurity Governance and Management Total 51 Codes	**286 Links to Quotations**

3 Cybersecurity Directing (17 codes)	Groundedness
Responsibility for cybersecurity is on the individual business units	25
Responsibility for cybersecurity is on the security organization	18
Using 3rd party	17
Internal information sharing	15
Integrating the security message with the company culture	14
Buying cybersecurity consultancy from outside	11
Systematic scheduling	8
Responsibility for cybersecurity is on the individual employees	8
Cybersecurity as a service	7
Systematic directing-model	6
Structured approach to information security directing	6
Early engagement by security	6
Responsibility for cybersecurity is on the security specialists	6
Technical assistance	5
Cybersecurity in software development	4
Organic directing	3
Automation in cybersecurity	2

3.1 Training (14 codes)	Groundedness
Cybersecurity training tailored by role	16
Cybersecurity training tailored by level	11
Cybersecurity champions enablement	11
Continual development of training	8
Systematic training schedule	7
Vendor-specific training	6
Additional training offered	6
New hire security training	5
Trust on proper training in organizations	4
Dedicated training for managers	4
Cybersecurity training tailored by phenomenon	3
Training based on awareness generation	3
Multi-channel awareness generation	3
Education as security training	1

3.2 Measures (9 codes)	
Activating cybersecurity awareness	22
Technical-administrative approach as a baseline	12
Awareness generation campaigns	8
Reasoning behind technical-administrative approach	7
Technical-administrative approach as justification	6
Setting the baseline with awareness generation	3
Awareness generation as authorizing technical-administrative approach	2
Awareness generation as justifying technical-administrative approach	1

Awareness generation as future direction	1
3 Cybersecurity Directing Total 40 Codes	**311 Links to Quotations**

4 Cybersecurity Controlling (10 codes)	Groundedness
Alignment of internal message delivery	16
Common language	9
Continual improvement of ISMS	5
Estimation and assessment difficulties	4
Training as a challenge	3
Cybersecurity as a compliance	3
Positive about the future	2
Awareness generation as a challenge	2
Other interested parties	1
Efficiency as a challenge	1

4.1 Measuring (16 codes)	Groundedness
Measuring perspective: Compliance	13
Measuring perspective: Risk	10
Measuring perspective: Implementation	8
Measuring perspective: Performance	6
Measurements as a challenge	6
Measuring perspective: Maturity	5
Measuring perspective: Incidents	4
Measuring perspective: Awareness	4
Measuring perspective: Quantitative	2
Measuring perspective: Legal	2
Measuring perspective: Information security projects	2
Measuring perspective: Breaches	2
Measuring perspective: Qualitative	1
Measuring perspective: Policies	1
Measuring perspective: Initiatives	1
Measuring perspective: Availability	1

4.2 Reporting (11 codes)	Groundedness
Report development	11
Report usefulness	8
Report language	7
Reports are easy to consume	5
Reporting is not filtered from bad news	4
Reporting benchmarks	4
Report vocabulary	4
Reporting positively	2
Reporting narratives	2
Reporting don’ts	1
Report delivery method	1

4 Cybersecurity Controlling Total 37 Codes	**163 Links to Quotations**

Grand Total 197 Codes	**Total 1177 Links to Quotations**