Student: Emilie Kronhjem

Student number: 101339

Thesis supervisor: Irfan Kanat

Hand-in date: 15-05-20

COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

An empirical study on the impact of the IT organization on cyber risk management

MSc in Business Administration and E-business

Master’s thesis

Spring 2020

129,865 characters

58 pages

Abstract

Cyber risks pose a growing threat to both private and public organizations as the world moves towards increased digitalization and interconnectedness. Recently, several high-profile cyber incidents have shown the enormous financial and reputational burdens that cyberattacks place on the victims. At the center of these risks are the information technology (IT) assets and capabilities that support and drive a growing array of business functions. This paper examines how the configuration of these assets and capabilities – as organized within the IT organization – impact the cyber risk management maturity of an organization. Based on a review of the existing literature, a conceptualization is developed to describe the IT organization through four related components: decision-making rights, resource allocation, interdepartmental communication, and the outsourcing strategy. This model is then tested empirically through primary data collection. Using a web-based questionnaire, data is collected about these four components as well as cyber risk management activities. This resulted in a survey of 53 respondents with insight into business strategy, IT, or cybersecurity from various organizations in Denmark. Using multiple linear regression analysis, this data was used to generate insights about the influence of the IT organization on the cybersecurity program maturity in the participating firms. The results show that decision rights structures, financial resource allocation, and IT outsourcing significantly impact the cyber risk management maturity level. For decision rights and resources, the IT and cybersecurity domains showed reversed centralization/decentralization patterns. These findings imply that the internal configuration of the IT organization is complex, and that IT and cybersecurity activities should be organized separately. IT outsourcing should be kept at a minimum in order to retain in-house IT competences that are important to cyber risk management. This study contributes to the academic and practical understanding of IT and cybersecurity in a management context. Previous research has primarily focused on either IT or cybersecurity activities, and by considering the two together, this study provides a novel perspective on the organizational factors that influence cybersecurity.

Table of contents

1. Introduction

The Scandinavian countries are some of the most digitalized in the world, and they consistently rank highly on digitalization parameters such as e-government adoption, ubiquity of digital services and users, and e-commerce popularity (OECD, 2017; UN, 2018). Scandinavian business leaders are more likely to consider cybersecurity a growth risk than their international counterparts (KPMG, 2019, p. 8), but despite this increased awareness, data breach response efforts in these countries are remarkably slow (IBM Security, 2019, p. 53). Bridging the gap between management concerns and cybersecurity execution calls for a greater convergence between these two organizational domains, a fact that is echoed among both practitioners and academics. For instance, according to one survey, 50 percent of responding business leaders indicated that they believed their company would recover from a security breach "within a few days" (Deloitte, 2019a, p. 18). Another report indicates that the average data breach actually has a lifecycle of 279 days, increasing to 314 days if the breach is carried out with malicious intents (IBM Security, 2019, p. 52). Similarly, only half of a survey's respondents report having tested their incident response plan within the last six months (Deloitte, 2019a, p. 16), despite the fact that extensive and continuous testing of the incident response plan is one of the most impactful means of reducing the cost of a data breach (IBM Security, 2019, pp. 38–41). As these findings indicate, there is room for improvement in the alignment of management and cybersecurity knowledge.

This thesis will explore cybersecurity from an organizational perspective. Specifically, I aim to explore the influence of the IT organization on a company's cybersecurity procedures and internal structures, i.e. its cyber risk management program (FFIEC, 2017b). Convergence between IT and the remaining organization yields a number of benefits, such as improved innovation, strategic alignment, and better IT outcomes (Johnson & Lederer, 2003; Weill & Ross, 2004; Winkler & Brown, 2014). However, the connection between a firm's IT organization and its cyber risk management processes remains largely unexamined in the academic literature. The existing literature does point to the existence of this relationship, for instance in its examination of the financial performance impact of resource allocation to cybersecurity (Chai et al., 2011) or in its discouragement of a siloed organizational approach to cyber risk management (Marotta & McShane, 2018). Furthermore, the cybersecurity strand of management research has established the criticality of a holistic perspective on cyber risk management processes where cybersecurity is integrated throughout the organization’s technical and social structures (Kosub, 2015; Parsons et al., 2015; Richter et al., 2015). In my thesis, I want to expand on these existing strands of research and consider them within an organization design perspective.

Finding the optimal organizational configurations for the IT function has been the subject of academic research for a long time, with the usual conclusion being “it depends” (Sambamurthy & Zmud, 1999; Venkatraman, 1997; Weill & Ross, 2004; Winkler & Brown, 2014). This thesis should be seen in this same light: while the research objective is to shed light on the ways that the design of the IT organization impacts cybersecurity outcomes, the results will not be a one-size-fits-all prescriptive model for cybersecurity. Rather, the results will demonstrate how particular design elements in the IT organization yield cybersecurity program benefits, and these insights will contribute to the understanding of how firms can make IT and cybersecurity design decisions within the context of their own strategic objectives. Furthermore, by exploring this relationship, I also want to contribute to the underexamined cyber risk area of management research and in this way, make a case for a higher level of integration between business and cyber risk functions. The results suggest that three components significantly impact cyber risk management maturity: the degree of IT outsourcing, decision rights allocation, and financial resource allocation within the IT organization. In the following subsection, I outline the problem area. This includes the state of cybersecurity in Denmark and the role of cybersecurity in organizations, which leads to the research question that guides this thesis.

1.1 The state of cybersecurity in Denmark

In recent years, a growing number of companies in Denmark have suffered at the hands of cyberattackers. Mærsk’s security breach during the global NotPetya incident in 2017 totaled around 1.9 billion DKK in business disruptions and subsequent recovery (Quass, 2017). Two years later, a Ryuk ransomware attack on hearing aid manufacturer Demant had an estimated cost of up to 650 million DKK (Jensen, 2019). Similarly, it was the Ryuk ransomware that facility services company ISS fell victim to in early 2020, an attack that caused up to 800 million DKK in business damage (Mirzaei-Fard & Moltke, 2020). According to one survey, half of the responding Danish companies reported being the victim of at least one cybersecurity incident in 2018 (PwC, 2019). While the high-profile cyberattacks on big companies such as Mærsk, Demant and ISS receive the most attention in the news media, an estimated 58 percent of cyber incidents internationally occur in small businesses (Verizon, 2018). With the mounting risk of being targeted by malicious hackers, organizations that would have never considered themselves potential targets are forced to face their own vulnerability. For example, out of the 98 Danish municipalities, 86 reported experiencing cyberattacks in the period between 2015 and 2018 (Riber-Sellebjerg & Okholm, 2018). And it is not just outside hackers that create cyber risks for these institutions – one incident that was reported in the media involved a municipal employee accidentally e-mailing confidential personal information to a local newspaper (Larsen, 2020). Local businesses are also being forced to rethink their approach to cybersecurity, as when a small supplier of automobile paint from Aalborg lost a million DKK recovering from a cyberattack, and later warned other small businesses "not to think that it won't happen to you" (Kildebogaard, 2015).

In addition to the risks posed by opportunistic cybercriminals and employee mistakes, organizations also need to be wary of the threat of cyberwarfare, where foreign state-sponsored agents target other nations in criminal and espionage activities. Typically, the intent is to cause disruption to the victim's economy or public services through cyberattacks, or to access sensitive confidential information through cyberespionage (Center for Cybersecurity, 2019). The Center for Cybersecurity under the Danish Ministry of Defense considers the cyberthreat against Denmark to be very high, particularly the risk of cyberespionage and cybercrime targeting Denmark (Center for Cybersecurity, 2019). Cyberwarfare is typically associated with a public sector victim, and targets are often agencies involved in foreign, defense, and military policy (Center for Cybersecurity, 2019). However, private sector entities can also become victims of cyberwarfare, either as the direct target or as collateral damage. Many of the international organizations that were affected by the NotPetya malware in the summer of 2017 are suspected to be collateral damage of the Russian government's cyberwarfare in Ukraine (Marsh, 2018). In another example, Danish biotech company Novozymes was directly targeted in an espionage incident which lasted for at least two months and where the likely culprit was thought to be the Chinese government (Lund & Fastrup, 2014). The private sector targets of state-sponsored cyberattacks and cyberespionage are rarely able to allocate the same amount of funding for defense as their adversaries have for offense, creating a hopelessly uneven playing field.

As illustrated by this brief overview of the cyber risk landscape in Denmark, the importance of cybersecurity in both public and private organizations cannot be overstated. Complex, globally intertwined processes create a wealth of potential security weaknesses, causing problems for the organizations and security technicians who must race to discover the holes in their defenses before potential adversaries do. Firms must learn to navigate this hectic realm of cyberthreats or face the consequences, and this has led to cybersecurity becoming an important part of the executive management's agenda in the last few years (KPMG, 2019, p. 8; PwC, 2019). Traditionally, cybersecurity tasks have been allocated within the IT department of an organization (Deloitte, 2019b; Div, 2015; Hooper & McKissack, 2016), but now these activities are increasingly receiving independent funding in response to the persistence and sophistication of cyberattackers (Allen et al., 2015; EY, 2019; PwC, 2019). Despite the growing cyber risk management budgets, Deloitte warns that cybersecurity is still dangerously underfunded in Denmark, and that the increased funding may give managers a false sense of complacency about their defenses (Deloitte, 2019a).

For the time being, it appears that ransomware, phishing, and all the other tools in the hacker's toolkit are an unavoidable part of doing business in a digitalized society. Accordingly, it is vitally important that cybersecurity activities are coordinated within and aligned with the remaining organization in a way that protects the critical business processes and information, i.e. the 'crown jewels' (Lobel, 2015). The coordination of cybersecurity activities is inextricably interlinked with the IT organization (Diamantopoulou et al., 2017; Liu et al., 2018), as this is the place in the organization where the cyber domain that creates cyber risks ultimately originates. The IT organization comprises all IT-related activities, from IT infrastructure such as hardware and software, to IT capabilities and guiding principles (Weill & Ross, 2004). If there were no servers storing business data, there would be no ransomware, and if there were no online applications, there would be no phishing. This link between the IT and cybersecurity organizational domains leads me to the research question that will guide this study:

RQ: How does the IT organization design impact cyber risk management maturity?

In section 2, I describe the theoretical basis for the thesis, including the cyber risk management framework used for the study's outcome variable and the IT organization literature used to develop the four predictor constructs. This review leads to the development of five main hypotheses that will guide me in answering my research question. Four of these hypotheses are examined along two dimensions, IT and cybersecurity, in order to account for the differences between these two functions. Next, in section 3, I explain the methodological considerations that have gone into the quantitative data collection process and subsequent statistical analysis. The data collection strategy uses a survey design to collect primary data about participants' organizational IT and cybersecurity activities. The data analysis uses this data in the creation of a multiple linear regression model that predicts the effect of the IT organization on cyber risk management maturity. The results of the data analysis are then detailed in section 4, where I report both the results of the regression model, the diagnostic tests used to assess the model, as well as the limitations of the study. The implications of the results are discussed in section 5, both for the hypotheses that were supported in the findings and the ones that were not. The thesis concludes with suggestions for research and practice.

2. Theory and hypothesis development

The term 'cybersecurity' refers to "the set of technologies and processes designed to protect computers, networks, programs, and data from attack, unauthorized access, change, or destruction" (Buczak & Guven, 2016). 'Cyber risk management' refers more specifically to the "development and implementation of [a] cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight" (FFIEC, 2017b). Accordingly, cyber risk management is a subset of the greater cybersecurity field, but for the sake of simplicity and linguistic variation, 'cybersecurity' and 'cyber risk management' are used somewhat interchangeably in reference to the latter throughout this thesis. Both cybersecurity technologies and procedures make up a crucial line of defense for organizations wanting to avoid the financial and reputational damage that comes with a cyberattack. This study seeks to address the gap in the literature between management of cybersecurity, IT, and the general business. It does so by examining key components of the IT organization's design, as identified through the management research, and putting them in the context of cybersecurity risk management practice. In the next sections, I begin by describing the cyber risk management field and the framework that will be used to assess participating organizations' cyber risk management program maturity. Afterwards, I present the academic and practitioner insights on the four domains of the IT organization and their connection to cyber risk management. Finally, I briefly describe the research model derived from the theory and literature examined in the section.

2.1. Cyber risk management

Cyber risk management programs typically center on the continuous monitoring, analysis, and reporting of cyber risks (FFIEC, 2015b). One of the features that differentiates cyber risks from other organizational risks is that they often involve an adversary who can operate in an adaptive, unpredictable manner (Marotta & McShane, 2018), although this is not always the case, such as with technical failures and external events (Kosub, 2015). Whatever the risk at hand, for organizations that seriously aspire to protect their information assets, a technical defense composed of firewalls and protective software – while still important – is not sufficient on its own (Gaudenzi & Siciliano, 2017; Kosub, 2015; Marotta & McShane, 2018). Increasing business process complexities within both IT and non-IT domains create the need for a holistic perspective on cyber risk, requiring for example the secure configuration of the IT infrastructure (Leuprecht et al., 2016; Richter et al., 2015), an organizational culture of security awareness (Bakhshi, 2018; Parsons et al., 2015), and a constant wary eye on the evolving cyber threat landscape outside the organization (Kruse et al., 2017; Nam, 2019). Organizations tackle cybersecurity issues in vastly different ways: some are mostly concerned with achieving an acceptable level of regulatory compliance, whereas others approach the matter proactively with the inclusion of new technologies and methods. Such strategic differences cannot necessarily be evaluated on a "good versus bad" basis, and will depend entirely on the organization in question (NIST, 2018). Accordingly, the level of cybersecurity that an organization aspires for should be aligned with the its risk tolerance and profile (Rodewald, 2005). Such an alignment perspective means that a local bakery with few critical information assets will likely have less use for an innovative cybersecurity strategy than an IT-intensive firm with many business-critical digital connections.

Cybersecurity frameworks are a popular tool to guide organizations' approach to cyber risk management. As of 2016, 84 percent of the responding companies in a US survey reported using at least one cybersecurity framework to guide their strategy (Tenable Network Security, 2016). The US National Institute of Standards and Technology (NIST) is behind one of the most popular publicly available strategic frameworks, the Framework for Improving Critical Infrastructure Cybersecurity, which was used by 43 percent of respondents in the same survey and is widely considered ‘best practice’ for cybersecurity (Tenable Network Security, 2016). However, the NIST framework is intended as a strategic guidance for companies (NIST, 2018), and for the purposes of this study, a more evaluative framework that allows for comparison is needed. Different levels of cybersecurity skill and ambition can be explained in terms of organizational maturity, which involves an assessment of a given organization’s cybersecurity sophistication and formalization (FFIEC, 2017b). Such an assessment framework has been developed by the FFIEC[1], a US government agency that establishes standards and procedures for financial institutions operating in the US. The FFIEC’s Cybersecurity Assessment Tool (CAT) maps directly to the widely used NIST framework (FFIEC, 2015a), thus ensuring that its assessment is relevant and appropriate for the types of cybersecurity strategies used among most practitioners. Furthermore, the FFIEC documents include direct instructions on how to assess cybersecurity across a variety of organizational domains and expertise levels (FFIEC, 2017a), making it readily adaptable for its intended use in this study.

The CAT consists of two parts: determining the inherent risk profile for the organization as a whole as well as for its activities, and establishing the cybersecurity maturity level of the organization across five domains. The five domains span both managerial, technical, internal, and external activities. In this thesis, I will focus only on one facet of the maturity assessment: the ‘risk management’ component nested in the first domain, which pertains to cyber risk management and oversight activities (see figure 1). I have decided to focus on this part of the cybersecurity framework because it relates directly to the research question I am pursuing, whereas the inherent risk profile and the remaining domains of cybersecurity outlined in the FFIEC’s model are less central to the subject investigated in this study. The risk management component of the framework involves an assessment of an organization’s cyber risk management program, risk assessment processes, and audit functions. In the CAT framework, each component is evaluated using a written guideline with declarative statements, each of which will determine whether an organization’s cybersecurity practices correspond with those of a given maturity level (FFIEC, 2017a). These declarative statements are used directly in the creation of questions to assess the cybersecurity maturity level, which I describe in more detail in section 3.1.1 on the questionnaire. There are five maturity levels: (1) baseline, (2) evolving, (3) intermediate, (4) advanced, and (5) innovative. The five maturity levels

[1] Federal Financial Institutions Examination Council

differ in terms of cybersecurity objectives, procedural formalization, control structures, and innovation (FFIEC, 2017b). At the baseline maturity level, the organization achieves the minimum requirements stipulated by law and strives to meet compliance-based objectives in their cybersecurity strategy. On the other end of the maturity spectrum, the organizations at the innovative maturity level are characterized by a holistic and proactive approach to the development of new procedures and knowledge to manage cyber risks.

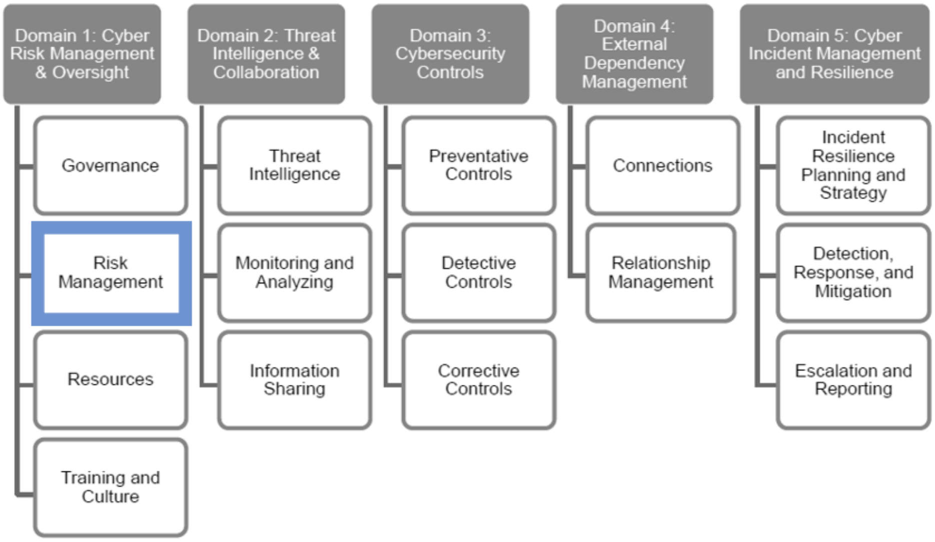

Domain 1: Cyber Risk Management & Oversight
Governance
Risk Management
Resources
Training and Culture
Domain 2: Threat Intelligence & Collaboration
Threat Intelligence
Monitoring and Analyzing
Information Sharing
Domain 3: Cybersecurity Controls
Preventative Controls
Detective Controls
Corrective Controls
Domain 4: External Dependency Management
Connections
Relationship Management
Domain 5: Cyber Incident Management and Resilience
Incident Resilience Planning and Strategy
Detection, Response, and Mitigation
Escalation and Reporting

Figure 1. The full range of cybersecurity domains and their components. The component investigated in this study is marked in blue (FFIEC, 2015b, p. 3).

Implementing a cybersecurity program helps to both mitigate the impact of a cyber incident and improve organizational resilience to cyber threats (ENISA, 2019; IBM Security, 2019, p. 66). Common motivations for cybersecurity framework adoption include requirements set by governmental contracts (28 percent) or business partners (29 percent), as well as simply wanting to follow best practice for securing the organization (70 percent) (Tenable Network Security, 2016, p. 7). However, many companies neglect to implement or maintain comprehensive cyber risk programs, and one survey found that up to 53 percent of respondents reported at least one crucial program deficiency (EY, 2019, p. 10). In a similar vein, another survey found that on average, cybersecurity programs only protect 67 percent of the entire organization (Accenture, 2019), thus leaving almost a third of the organization at risk. Using an established cybersecurity framework such as the CAT can help organizations close the gaps in their security coverage by providing guidelines to identify risk factors, assess incident preparedness, evaluate the potential for improvement, and provide support in the development of a cybersecurity strategy (FFIEC, 2015b).

2.2. The IT organization

The IT organization is the "collectivity of human resources that perform IT-related tasks, such as planning, building, and operating IT applications and their underlying [infrastructures], relationships, practices, norms, and capabilities" (Winkler & Brown, 2014, p. 56). The IT organization can be characterized along two primary dimensions: decision-making rights and resource allocation (C. V. Brown & Magill, 1994; Winkler & Brown, 2014). Decision-making structures describe the relative level of control exerted over matters concerning IT, for example the principles that guide the strategic role of IT in the business (Weill & Ross, 2004; Winkler & Brown, 2014). The allocation of resources refers to the "inputs into the production process" that are deployed across the organization to create strategic advantages (Grant, 1991). These two dimensions span the divisional and corporate levels, i.e. decentralization versus centralization (Peppard, 2018; Van Grembergen & De Haes, 2004; Weill & Ross, 2004; Winkler & Brown, 2014). In addition to these two internal design dimensions, outsourcing provides an element of market coordination by enabling firms to source external capabilities (Holcomb & Hitt, 2007; Lacity et al., 2010). Finally, knowledge-sharing processes facilitate the effective coordination of all IT activities across functional departments within the organization, enabling the firm to realize both employee-related and performance benefits (Ahmad & Karim, 2019; Kearns & Lederer, 2003; S. P.-J. Wu et al., 2015). Together, these four components make up the organizational structures that govern the IT organization's internal rulesets and external boundaries. An effective and business-aligned configuration of the IT organization drives both improved financial performance and a diverse array of IT outcomes, such as growth, business flexibility, or increased asset utilization (Bowen et al., 2007; Simonsson et al., 2010; Weill & Ross, 2004; S. P.-J. Wu et al., 2015). Furthermore, the IT organization's design can impact the overall organization in terms of for instance IT investment performance and firm profitability, thereby contributing to the achievement of strategic business objectives (Banker et al., 2011; Gu et al., 2008; Lunardi et al., 2014).

Furthermore, the IT competences that are concentrated within the IT organization drive cybersecurity implementation through norm-building, awareness, and effective leadership (S. E. Chang & Ho, 2006; Tu & Yuan, 2014). Aligning and integrating cybersecurity activities with both the IT organization and the remaining enterprise is critical to successful cyber risk management (Yaokumah & Brown, 2015; Young & Windsor, 2010). Achieving such alignment between business, IT, and cybersecurity is associated with the configuration of the four IT organization design elements outlined previously, i.e. governance decisions about cybersecurity and IT such as decision rights allocation (Liu et al., 2018; Xue et al., 2011) and executive responsibility (Hooper & McKissack, 2016; Karanja, 2017), the appropriate allocation of resources (Diamantopoulou et al., 2017; Srinidhi et al., 2015), interdepartmental communication (Gaudenzi & Siciliano, 2017; Herath & Rao, 2009), and the trade-off between in-house capabilities and outsourcing (Dahlberg & Lahdelma, 2007; Niranjan et al., 2007).

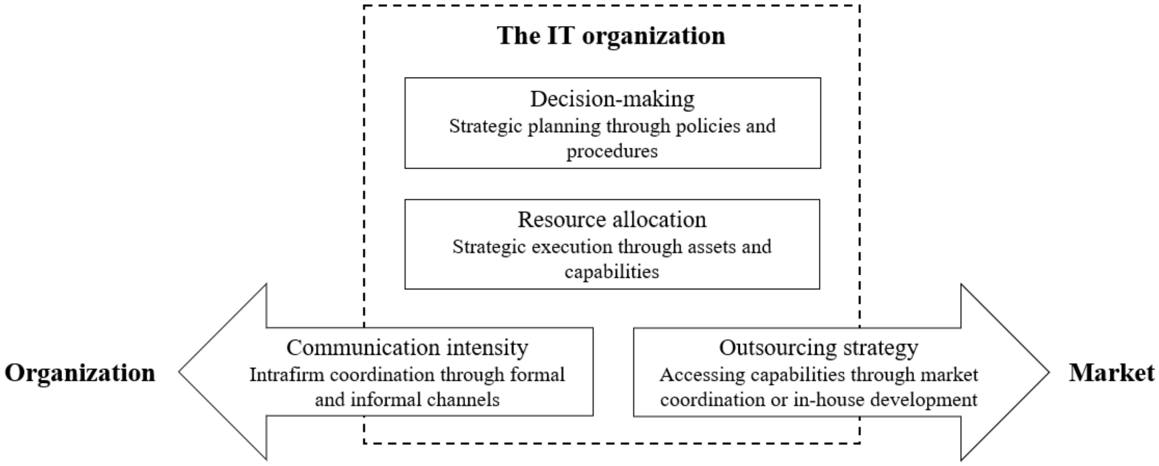

The IT organization
Decision-making
Strategic planning through policies and procedures
Resource allocation
Strategic execution through assets and capabilities
Organization
Communication intensity
Intrafirm coordination through formal and informal channels
Outsourcing strategy
Accessing capabilities through market coordination or in-house development
Market

Figure 2. Conceptualization of the IT organization and its interactions.

Figure 2 shows a conceptualization of the IT organization as described through these four components. Broadly speaking, the decision-making rights make up the policy and strategic planning within the IT organization, and the allocation of resources enables the execution of these strategic activities through investments and deployment of assets. Through coordination with internal stakeholders, IT knowledge is disseminated throughout the organization, while coordination with the market allows the IT organization to access external capabilities to complement or replace internal capabilities. The next sections review the academic literature focusing on these four domains of the IT organization, describing their contribution to the organization in general as well as their impact on cyber risk management. Furthermore, the four IT organization design elements will be contextualized through practitioner reports and surveys outlining the current management practices in order to provide a practice-oriented perspective to supplement the insights from academia. The review of each component leads to the development of hypotheses that predict its concrete impact on an organization's cyber risk management maturity.

2.2.1. Decision-making structures

There have been several attempts in the IT governance literature to characterize organizational decision-making structures (e.g. Hitt & Brynjolfsson, 1997; Sambamurthy & Zmud, 1999; Weill & Ross, 2004). A common feature of these characterizations is that they often define decision-making rights along an axis of centralization and decentralization, i.e. whether decisions about IT are made at a corporate or divisional level, respectively (Sambamurthy & Zmud, 1999; Van Grembergen & De Haes, 2004; Weill & Ross, 2005; Winkler & Brown, 2014). At the center of this spectrum is the federal or hybrid IT decision structure, where certain responsibilities are centralized at the corporate IT function and others are delegated to the individual departments in a more decentralized manner (A. E. Brown & Grant, 2005; Sambamurthy & Zmud, 1999; Weill & Ross, 2004). These general models for decision rights allocation each have their own distinct advantages for the organization. When decision rights are centralized at the corporate level, the potential benefits include a higher degree of interdepartmental coordination, operational efficiency and firm-wide procedural standardization (A. E. Brown & Grant, 2005; Sambamurthy & Zmud, 1999). Conversely, decentralization confers innovation benefits and improved responsiveness to changes (A. E. Brown & Grant, 2005; Sambamurthy & Zmud, 1999). The hybrid structure in the middle of the spectrum attempts to reconcile the benefits of centralization and decentralization to attain a balanced blend (Sambamurthy & Zmud, 1999; Weill & Ross, 2004).

Generally, a centralized governance is associated with improved profitability, whereas a decentralized approach encourages firm growth, and the federal model strikes an asset utilization balance between the two extremes (Weill & Ross, 2005). Similarly, decision rights pertaining to cybersecurity should be organized with the strategic or operational objectives of an IT practice in mind (Y. A. Wu & Saunders, 2005). Some research suggests that complex, uncertain business environments such as the one characteristic of the cyber threat landscape might make firms more likely to centralize IT decision rights (Xue et al., 2011). Other centralization outcomes such as greater organizational coordination and improved efficiency might also translate into greater security policy enforcement and a better ability to holistically address cybersecurity threats, leading to greater cyber risk protection (Liu et al., 2018). Decentralization benefits such as faster response time and local flexibility may be useful in the execution of cybersecurity (see section 2.2.2 on resource allocation), but at the policy level, a centralized, long-term orientation driven by corporate leaders enables greater alignment and efficiency benefits (Y. A. Wu & Saunders, 2005).

Decision rights structures are closely tied to the reporting structures and executive responsibilities within the organization (Banker et al., 2011; Weill & Ross, 2004). The executives sitting atop the corporate throne are usually known by a family of 'CXO' labels. The IT function is often overseen by the Chief Information Officer (CIO), who has also come to assume significant responsibility for the strategic direction of organizational technology in general (Banker et al., 2011; Marchand, 2008). The Chief Digital Officer (CDO) and the Chief Technology Officer (CTO) are two related roles, the former often emphasizing digital innovation, whereas the latter focuses on technological implementation (Centric Digital, 2017). However, the CIO label is most commonly used to describe the executive with responsibility for the digital strategy and execution (Deloitte, 2018, p. 11). On the security side, the Chief Information Security Officer (CISO) is often tasked with responsibility for the protection of IT assets (Hooper & McKissack, 2016). The Chief Security Officer (CSO) differs from the CISO in being responsible for business asset security in general (Fruhlinger, 2018), whereas the Chief Risk Officer (CRO) addresses business risk management (Burgess, 2014). These CXO labels may have overlapping responsibilities, but for the sake of simplicity, in this thesis CIO will be used in reference to the general IT executive, and CISO is used for the cybersecurity executive. However, the other four labels will be included in the questionnaire, which will be described in more detail in section 3.1.1.

The allocation of executive responsibility establishes leadership within a given domain and impacts its strategic function and direction (Bottger, 2008). Specifically, the role of IT within the organization is shaped by the presence of a leader with high IT competences (Bassellier et al., 2003). Furthermore, the decision-making authority of the CIO is affected by a range of organizational factors such as the climate of assertiveness, structural power, and political partnerships with other members of top management (Preston et al., 2008). In this political power play, other executives' acknowledgement of and support for the importance of IT in the organization is crucial to the empowerment of the CIO (Banker et al., 2011; Preston et al., 2008; Turedi & Zhu, 2019; Van

Grembergen & De Haes, 2004). Similarly, the role of the CISO should receive support to carry out their duties from the rest of the top management team (Karanja, 2017). CISOs still face challenges in fulfilling their role in the organization, and communicating security issues to members of the top management team remains a challenge both in terms of the content and frequency of their reports (Hooper & McKissack, 2016) as well as credibility and organizational power (Karanja, 2017). Until the CISO can secure a favorable organizational climate, support for cybersecurity, structural power, and political influence with the remaining members of top management, the cybersecurity function risks suffering as a consequence (Preston et al., 2008).

The need for increased decision-making authority for the CISO and the cyber risk function is reflected in practitioner reports. According to one survey, 79 percent of Danish firms have designated responsibility for cybersecurity to someone within the firm – however, only 47 percent of these individuals are part of the top management team (Deloitte, 2019a, p. 4), suggesting that this responsibility might not come with complete decision-making authority. In another survey, 40 percent of the responding firms indicated that the CIO was responsible for cybersecurity (EY, 2019, p. 25), which is a potentially problematic decision hierarchy that can cause conflicts of interest between IT service delivery and cybersecurity activities (Div, 2015; Doan, 2019; Overby, 2018; Zutshi, 2018). Furthermore, only 39 percent of firms' executive teams and boards are reported to have a solid understanding of cybersecurity, risks, and prevention (EY, 2019, p. 24), meaning that the remaining 71 percent of firms would stand to gain from adding a cybersecurity-specific executive to the roster. This issue is also reflected in a report that finds that a lack of management alignment was the top cybersecurity management challenge for 14 percent of the respondents (Deloitte, 2019b, p. 6), another indication that governance issues create significant obstacles for cybersecurity professionals.

As the literature on decision-making structures shows, reporting responsibilities and decision authority must be carefully organized so as to reflect the broader strategic objectives of the firm. The allocation of decision-making rights influences the strategic planning and policy development for the cybersecurity domain. Because of the benefits associated with centralized decision structures, such as firm-wide coordination and efficiency, this leads to the first hypothesis regarding the impact of the IT organization on cybersecurity:

H1: Centralized decision rights structures within the IT organization improves cybersecurity risk management program maturity.

Furthermore, governance structures shape the role and legitimacy of an organizational function, and a competent executive can be pivotal in developing and expanding this role to achieve firm goals. However, both the literature and practitioner reports reveal that too often, this logic is not applied to cybersecurity governance. When cybersecurity activities are underprioritized, part of the explanation can be found in the lack of political power and legitimacy of cyber risk functions. Consequently, the importance of the independence, authority, and competent leadership of the cyber risk function leads to the second hypothesis:

H2: Separate executive responsibility improves cybersecurity risk management program maturity.

2.2.2. Resource allocation

Aral and Weill (2007) distinguish between two types of IT resources: IT assets and IT capabilities. IT assets include IT investments such as infrastructure and strategic investments, whereas IT capabilities include intangible resources such as skills and work routines (Aral & Weill, 2007). The manner in which these distinct resources are allocated within the IT organization and prioritized across various projects and programs is a key component of IT execution, and it should be coordinated in alignment with the firm's strategic objectives (Aral & Weill, 2007; Mårtensson, 2006). Like decision-making rights, resource allocation can be described in terms of its centralization at the corporate level, or decentralization at the divisional level (Winkler & Brown, 2014). Centralized resource allocation may align better with long-term and growth-oriented strategic objectives because it provides for a wider distribution of risk across the organization (Jarzabkowski, 2002). Conversely, a decentralized resource allocation model is more likely to support the unique strengths and capabilities that exist across individual departments (Jarzabkowski, 2002).

The resource allocation model is thus at the heart of the organization's strategy execution, enabling the firm to make strategic decisions about IT investments, employee selection and training, and overall organizational alignment efforts (Chen, 2012; Mårtensson, 2006). IT investments are associated with the performance of the organization's IT infrastructure and physical IT assets, but do not necessarily predict the performance of human IT assets (Huang et al., 2006). For this reason, the two resource types will be considered separately, thus building on Aral and Weill's two IT resource constructs (2007). Instead, these two resources are interdependent within the IT organization, working together to create sustained competitive advantage for the firm (Diamantopoulou et al., 2017). Both financial and human IT resources are necessary to maintain the quality of IT assets and to confer IT competences to the organization, thus enabling a greater realization of IT business value (J. Crawford et al., 2011; Magnusson et al., 2018).

Furthermore, the prioritization of human resources and infrastructure investments is important to achieve a strong cyber defense (K. C. Chang & Wang, 2011; Tu & Yuan, 2014). The strategic allocation of organizational resources helps to mitigate the financial impact of a cybersecurity incident and prevent future incidents (Diamantopoulou et al., 2017; Srinidhi et al., 2015). By decentralizing human and investment resources for activities such as security awareness training and technical defense mechanisms within the appropriate local knowledge centers, the organization can benefit from divisional expertise and a more context-based execution (Y. A. Wu & Saunders, 2005). An example of the importance of IT investments is the poor management of technical debt and the consequent 'zombie systems' that hinder the strategic utilization of IT assets and create cyber risks for the firm (Kruchten et al., 2012; Magnusson et al., 2018; Winkler, 2016a). Similarly, the growing sophistication of cyber attackers calls for equally sophisticated cybersecurity capabilities, making human resources an important component of the cyber defense (Diamantopoulou et al., 2017). To reflect the expanding role of cybersecurity, talent is being recruited from a variety of disciplines, enabling a wide array of roles that range from technical specialists to business governance or legal compliance (Dawson & Thomson, 2018; Furnell & Bishop, 2020).

Generally, cybersecurity investments are increasing (Accenture, 2019, p. 12; EY, 2019; PwC, 2019), and their key performance indicators have come to include meaningful outcomes such as cyber resilience (Accenture, 2019) and strategic alignment with the business (Deloitte, 2019a, p. 9). Overall, this signals a positive development for cyber risk management. However, it also creates a new risk of complacency among those managing the cybersecurity budgets. For example, Deloitte reports that 61 percent of respondent firms are comfortable with their current cybersecurity budgets, noting also that this finding contrasts the still-pervasive systematic underinvestment in cybersecurity (Deloitte, 2019a, p. 9). Another report also indicates that the cybersecurity function benefits from budgetary independence from IT (Deloitte, 2019b, p. 6). In fact, inadequate funding for security initiatives is one of the top concerns for a quarter of cybersecurity employees ((ISC)2, 2019, p. 9). Furthermore, 65 percent of the organizations in one survey have a shortage of personnel dedicated to cybersecurity ((ISC)2, 2019, p. 9), a finding that is illustrative of the wider global skills shortage within cybersecurity (McAfee, 2016). The skills shortage should be seen in the light that 39 percent of respondent firms have dedicated less than 2 percent of their IT capabilities fulltime to cybersecurity (EY, 2019). This lack of access to cybersecurity capabilities increases the risk of lasting reputational and financial damage from cyberattacks (McAfee, 2016, p. 4).

To summarize, research on organizational resource allocation shows that IT assets and capabilities are instrumental in the execution of the overall business strategy and should be configured to align with strategic objectives. These resources affect cybersecurity execution in areas such as technical debt, incident impact, and cyber skills development. By deploying financial and human resources in a way that creates the flexibility to respond to issues such as system life cycles and talent recruitment locally, the organization benefits from a wider range of input to cyber risk management. Accordingly, a divisional strategic execution through assets and capabilities allows the organization to benefit from adaptability and local expertise, which leads to my third hypothesis:

> *H3: Decentralized human and financial resources improves cybersecurity risk management program maturity.*

2.2.3. Interdepartmental communication

Organizational communication facilitates the coordination of tasks across both horizontal and vertical levels (Ahmad & Karim, 2019; Grant, 1996; Hansen, 2002). Mechanisms for coordinating tasks across departments can be either formal or informal, depending on whether they are intended or emerge on their own (Dessne, 2013; Schlosser et al., 2015). Informal mechanisms often rely on integration with the corporate cultural identity through norm maintenance and the feeling of unity (Schlosser et al., 2015). Such mechanisms include office space colocation, social events, cross-functional teams (C. V. Brown, 1999; Coradi et al., 2015; Ghobadi & D'Ambra, 2012). Formal mechanisms create a social environment that is conducive to collaboration (Schlosser et al., 2015), including formal working groups, job rotations and knowledge networks (C. V. Brown, 1999; Hansen, 2002). Most knowledge-sharing and relational integration activities in organizations occur through informal channels, which are more difficult for managers to control and direct (Dessne, 2013; Schlosser et al., 2015). Nevertheless, a diversity of both formal and informal communication paths is conducive to organizational performance, affecting interdepartmental collaboration and the benefits derived from it (Hansen et al., 2005)

Effective management of the flow of organizational knowledge and information impacts organizational performance, innovation, and business process efficiency (Ahmad & Karim, 2019). Within an IT context, knowledge-sharing and communication are important to IT project success and business alignment (McKay & Ellis, 2015; Schlosser et al., 2015). The organization benefits from both formal and informal networks between its members, and these employee connections facilitate the coordination of tasks and knowledge across organizational functions (Diamantopoulou et al., 2017; Hansen et al., 2005; Schlosser et al., 2015). Employee relations enable the dissemination of specialized knowledge and increase creativity, performance efficiency, and workplace satisfaction (Ahmad & Karim, 2019; Grant, 1996). For these relational networks, the number of relations and the frequency of interaction are important indicators of their ability to facilitate knowledge sharing and cross-departmental collaboration (Hansen et al., 2005). Frequent and intense communication with diverse others drives reciprocal learning and consequent performance improvement, whereas a high communication intensity with similar others can yield the opposite results, i.e. decreased performance and excessive uniformity (Frigotto & Rossi, 2012). Communication frequency among business and IT management also fosters mutual understanding and enhances IT's strategic role within the organization (Johnson & Lederer, 2003). Accordingly, facilitating the frequency and multiplicity of both formal and informal communication paths position the organization to reap the benefits of intrafirm cooperation and an increased IT business value (C. V. Brown, 1999; Grant, 1996; Hansen et al., 2005; Schlosser et al., 2015).

In cybersecurity, humans are often the weakest link in the security chain (Puhakainen & Siponen, 2010). Accordingly, knowledge of the cyber risk management strategy must transcend departmental boundaries and be understood and incorporated across all employee groups in order to be effective (Gaudenzi & Siciliano, 2017; Hooper & McKissack, 2016). Cybersecurity awareness training is a popular method for broadcasting general cybersecurity guidelines, but on its own it can be a challenging medium for sustained behavioral change (Stewart & Lacey, 2012). Cyber risk management programs benefit from a broad internal stakeholder involvement, which helps both the implementation process as well as security analysis and design activities (Belsis et al., 2005).

This involvement is not only fostered through explicit communication structures, such as formal cyber awareness seminars, but also through tacit structures (Belsis et al., 2005; Hsu et al., 2015). The tacit social structures enable the development and maintenance of a cybersecurity culture where information and insights are shared and reproduced among organizational members (ENISA, 2017; Parsons et al., 2015). Perceptions of coworkers' behavior and compliance with security policies nudges other employees to behave in a secure and responsible manner (Herath & Rao, 2009). Accordingly, fostering a culture of cross-functional communication and information sharing makes up an integral part of the non-technical cybersecurity strategy (Gaudenzi & Siciliano, 2017).

The importance of broad employee involvement in cybersecurity is underlined in the findings of a report from PwC, where phishing attacks and social engineering made up 68 percent and 28 percent, respectively, of the cyber incidents reported by firms in 2019 (PwC, 2019, p. 20). These results illustrate how employees across all organizational levels make up the first line of defense against malicious outsiders. Some of the biggest growing cyberthreats are user-targeted attacks, for example digital extortion scams and Office 365-specific phishing (Cisco, 2019). Managers are well aware of the threat that a lack of security awareness poses to the firm, and employees' unsafe behavior is considered to be the single biggest threat to organizational cybersecurity (EY, 2019, p. 10; PwC, 2019, p. 21). Integrating cyber personnel within the business and increasing their interaction with other functions helps to mitigate these internal cybersecurity threats and increases interdepartmental collaboration (Deloitte, 2019b, p. 10), for example by having other staff members shadow cybersecurity personnel or through job rotations (Deloitte, 2019a, p. 11).

In sum, both informal and formal communication types drive performance efficiency, innovation, and critical knowledge sharing. Strong relational networks are characterized by communication path diversity and frequency, features that create better conditions for reciprocal learning and collaboration within the organization. Furthermore, strong interdepartmental networks enable the establishment of a culture of cybersecurity, ultimately creating an organization where cybersecurity is more embedded and where employees are more primed to resist human-targeted cyberattacks. These considerations about the role of communication and culture in creating cybersecurity awareness lead me to the next hypothesis:

H4: Strong interdepartmental communication improves cybersecurity risk management program maturity.

2.2.4. Outsourcing extent

Through outsourcing, organizations can access external capabilities to be deployed for their own benefit (Holcomb & Hitt, 2007). The purpose of strategic outsourcing is to use these external capabilities to achieve business objectives, and this involves carefully assessing which activities should be delegated to an external service provider, and which should be kept in-house (Winkler & Brown, 2014). Maximizing outsourcing outcomes involves ensuring the constant alignment between the business strategy and outsourcing strategy, thus creating and maintaining a strategically informed balance of external capability sourcing and internal capability development (Kroes & Ghosh, 2010; J. N. Lee et al., 2004; Valorinta, 2011). Too much outsourcing can lead to firms losing out on strategically important internal capability development (Handley, 2012; Winkler, 2016b). Accordingly, the scope of outsourcing makes up a key consideration for strategic outsourcing (J. N. Lee et al., 2004).

IT outsourcing decisions influence the external boundaries of the IT organization, transferring operational responsibility for the outsourced IT assets, processes, or personnel to the external provider (Valorinta, 2011). Some of the common motivations behind outsourcing decisions include an access to expertise, quality improvements, and the ability to focus on core capabilities, indicating that many firms outsource strategically with the goal of complementing existing organizational capabilities or balancing out deficiencies (Lacity et al., 2016). By outsourcing processes that are less strategically important to manage in-house, the IT organization can focus on the coordination of business issues and IT-business alignment (Valorinta, 2011). Without this strategic focus, outsourcing can lead to ‘hollow corporations’, where key competencies and core activities have been removed from the organization (Jennings, 2002). Outsourcing strategic capabilities can lead to decreased outsourcing performance and can damage the firm’s competitive advantage in the market (Handley, 2012). Another prerequisite for outsourcing success is a shared understanding between client and provider of the outsourced processes (Lacity et al., 2016). Achieving this shared understanding involves clarifying the complexity and criticality of the processes, particularly for processes with a significant business risk (Niranjan et al., 2007; Saxena & Bharadwaj, 2009).

Cyber risk management typically involves processes that are both complex and critical, which places a high demand on the client-provider relationship in a cybersecurity outsourcing transaction (Niranjan, Saxena, & Bharadwaj, 2007). Furthermore, organizations are generally less inclined to outsource processes that are complex, critical, and imbued with an element of uncertainty (Lacity, Khan, & Yan, 2016; Lacity, Khan, Yan, & Willcocks, 2010). This disinclination to outsource business-critical processes aligns with the principle that resources and capabilities with strategic value should be kept in-house (Handley, 2012). Cybersecurity outsourcing may be motivated by cost reductions as well as access to expertise and high-quality security technology (Gupta & Zhdanov, 2012; Liu et al., 2018). A popular model of cybersecurity outsourcing involves using managed security service providers (MSSPs), which are outsourcing partners that provide a range of technical security services such as spam filters, firewalls, VPNs, and antivirus (C. H. Lee et al., 2013). Such services enable firms with low cybersecurity capabilities to access resources and expertise that would otherwise be unavailable to them (Gupta & Zhdanov, 2012). However, outsourcing cybersecurity also comes with its own set of risks, including information leakage (Feng et al., 2019) and risk interdependence (Zhao et al., 2013). By keeping activities in-house, the organization itself is forced to assume a higher degree of responsibility for IT and cybersecurity management, possibly prompting a greater internal awareness of the related risks and issues (Dahlberg & Lahdelma, 2007). While some sectors might generally benefit from the scale benefits of outsourcing cybersecurity to a MSSP (Liu et al., 2018), an overall assessment of the organization’s cybersecurity strategy and risk appetite should inform the decision to outsource cybersecurity activities (Feng et al., 2019).

Generally, cybersecurity functions that are either wholly outsourced or wholly in-house are rare – usually, a hybrid model is chosen (Deloitte, 2019b, p. 14). One survey reports that the most widely outsourced cybersecurity functions are vendor risk management, identity and access management, and data protection (EY, 2019, p. 18). Overall, both basic and advanced cyber defense capabilities are sought after in organizational outsourcing partners (Deloitte, 2019b, p. 18). In addition to the strategic motivations to outsource cybersecurity, organizations are also faced with a more practical incentive to outsource: a gap in the workforce that makes it difficult to recruit and develop in-house cybersecurity talent ((ISC)2, 2019; Deloitte, 2019b, pp. 12–13). Insufficient access to cybersecurity skills is an increasing problem globally, with one survey finding that 53 percent of the participating organizations reported a dire shortage of talent (Oltsik, 2019). The skills shortage has even been reported to be a direct motivation for companies to outsource cybersecurity functions (McAfee, 2016), which can potentially be problematic if it causes companies to outsource activities that strategically should have been kept in-house. Furthermore, special care should be exercised in selecting outsourcing vendors for IT, cybersecurity, as well as all other business activities, as third-party involvement has the potential to aggravate the cost of a security breach (IBM Security, 2019).

In conclusion, organizations must carefully weigh which business processes they should outsource, considering both their strategic importance, their unique characteristics, and the desired outcome of outsourcing these processes. Generally, businesses will be disinclined to outsource business-critical activities, instead opting to keep these activities in-house. On the assumption that organizations with a high level of cybersecurity maturity will be more prone to consider IT security a business-critical activity, these organizations may be more likely to retain IT and cybersecurity in-house. This enables the organization to retain the relevant competences within the organization, thus allowing for greater internal innovation and thus cyber program maturity. This leads me to the final hypothesis:

H5: Minimal outsourcing improves cyber risk management program maturity.

2.3. Research model

Based on the above review of theory and practice within both cybersecurity and the IT organization, a research model with five main hypotheses has been developed. Each hypothesis (except for H4) is defined along both an IT and a cybersecurity dimension in order to clarify any potential differences between these two domains. Examining the hypotheses from both an IT and cybersecurity angle will contribute to understanding the relationship between these distinct but interrelated areas of the IT organization. The research model shows how the configuration of the IT organization influences cyber risk management program maturity. This research model predicts that the organizations with a high cyber risk management maturity level will be characterized by five different features. Their decision rights will be centralized at a corporate level, allowing for a high degree of firm-wide standardization of IT and cybersecurity activities. The responsibility for IT and cybersecurity will be allocated with separate executive roles for whom there are no competing interests or business objectives. This enables the IT executive to focus on IT service efficiency goals, and the cybersecurity executive can devote their attention on security objectives. Financial and human resources will be organized at a decentralized level, enabling the individual departments to allocate investments and skills to achieve strategic goals. The organization's relational networks will be characterized by diverse and frequent interdepartmental communication which is conducive to knowledge-sharing, norm-building, and greater IT and cybersecurity coordination. Finally, the external boundaries of the IT organization will be fairly rigid, allowing for very little outsourcing in order to maintain and develop strategically important skills in-house. This conceptualization of an IT organization, which has been developed based on the literature review above, is theorized to be able to realize a high level of cyber risk management program maturity.

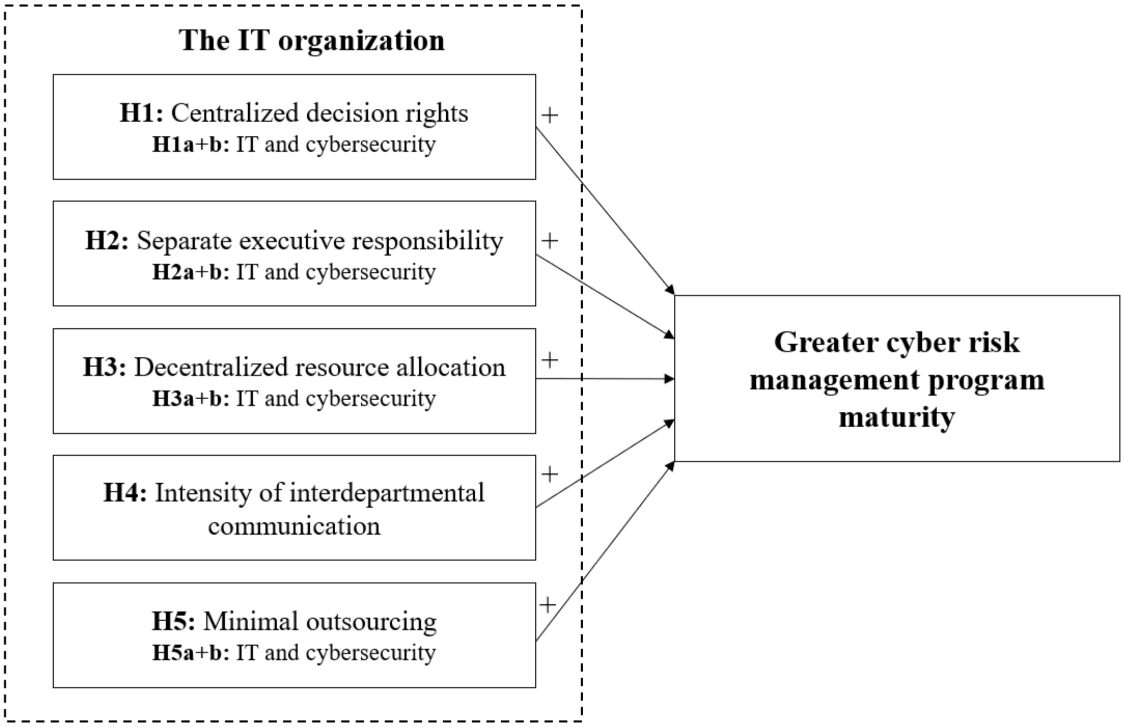

The IT organization
H1: Centralized decision rights
H1a+b: IT and cybersecurity
H2: Separate executive responsibility
H2a+b: IT and cybersecurity
H3: Decentralized resource allocation
H3a+b: IT and cybersecurity
H4: Intensity of interdepartmental communication
H5: Minimal outsourcing
H5a+b: IT and cybersecurity
+
+
+
+
+
Greater cyber risk management program maturity

Figure 3. Research model describing the hypothesized influence of the IT organization on cybersecurity maturity.

3. Methodology

This study has a quantitative research design based on a positivist ontological orientation. The positivist emphasis on testing phenomena from an objective, fact-based perspective aligns with the hypothetico-deductive research model that is used in this thesis (Saunders et al., 2016). In order to answer the research question posed at the beginning of this paper, the respondent organizations' cyber risk management maturity levels are measured as a quantifiable construct. It is then subsequently contextualized through the impact of the four predictor constructs describing the IT organization. This approach reflects the positivist commitment to explain phenomena (and reality in general) through predictive and generalizable models (Presskorn-Thygesen, 2012). Through a research design that emphasizes these positivist virtues, I aim to generate empirical insights that accurately describe the study's subject matter, and which can inform IT organization design in a useful and reliable manner. In the literature review, the IT organization was described through four constructs that were used to generate hypotheses: decision rights structures (H1-2), resource allocation (H3), interdepartmental communication (H4), and outsourcing strategy (H5). Using these constructs from the literature review, a survey has been developed that uses respondent self-reports to map the participating firms' IT organizations and cyber risk management programs. The data collected with the survey were analyzed using multiple linear regression to develop a predictive model for the relationship between the IT organization's design and cybersecurity maturity, and to evaluate the validity of the hypotheses.

3.1. Data collection

Data was collected through a self-completed online questionnaire which gathered information from respondents about their firms' IT and cybersecurity structures, policies, and processes. The questionnaire was designed to solicit concrete information in an unambiguous manner by using only closed questions (Saunders et al., 2016); to be easily and quickly completed by the respondents in order to reduce drop-out rates (Evans & Mathur, 2005; Granello & Wheaton, 2004); and to be accessible to and doable by the specific target respondents (Saunders et al., 2016; Van Selm & Jankowski, 2006), particularly in terms of the question difficulty. The sampling strategy targeted employees across three organizational tiers who could provide accurate snapshots of their respective organizations with regards to IT and cybersecurity. This sampling strategy was necessary in order to generate reliable, generalizable data about the constructs being measured, but targeting professionals at this level as an external researcher can be challenging in terms of data access (Saunders et al., 2016). In the end, data access was facilitated primarily with the help of two partner firms who were credible and trusted by the target respondents, as well as secondarily with the help of my own network (Saunders et al., 2016). The next two subsections will describe (1) the questionnaire used for the survey, including the question development process, and (2) the sampling strategy and survey distribution process.

3.1.1. Questionnaire

The questionnaire consists of 21 questions in total. Five of these questions collect demographic data (Q1-5) in order to describe the respondents and their firms' profiles. Furthermore, the results of these questions will also be used as control variables in the regression analysis. Of the remaining 16 questions, four pertain to organizational decision-making structures (Q6-9), two to interdepartmental communication (Q10-11), four to resource allocations (Q12-15), and two to the extent of outsourcing in the firm (Q16-17). The final four questions collect data about the respondent firms' cyber risk management programs, program assessment procedures, risk assessment procedures, and the use of independent audits for the evaluation of cybersecurity (Q18-21). The 12 questions measuring the four predictor constructs, i.e. decision rights structures, resource allocation, interdepartmental communication, and outsourcing extent, were developed based on the findings of the literature review. The questions measuring the outcome variable, cyber risk management maturity, were adapted directly from the CAT guidelines (FFIEC, 2017a, pp. 23–26). Below is an overview of the questions from the questionnaire and the constructs they relate to, as well as the primary references from the literature review that they are based on. A detailed version of the questionnaire can be found in appendix A.

Constructs	**References**
Decision-making rights: Centralization (Q7+9)	A. E. Brown & Grant, 2005; Hitt & Brynjolfsson, 1997; Liu et al., 2018; Sambamurthy & Zmud, 1999; Turedi & Zhu, 2019; Weill & Ross, 2004; Y. A. Wu & Saunders, 2005; Xue et al., 2011
Decision-making rights: Executive responsibility (Q6+8)	Banker et al., 2011; Bassellier et al., 2003; Bottger, 2008; Doan, 2019; Hooper & McKissack, 2016; Karanja, 2017; Preston et al., 2008

Interdepartmental communication (Q10-11)	Ahmad & Karim, 2019; Belsis et al., 2005; C. V. Brown, 1999; Frigotto & Rossi, 2012; Gaudenzi & Siciliano, 2017; Grant, 1996; Hansen, 2002; Hansen et al., 2005; Herath & Rao, 2009; Johnson & Lederer, 2003; Parsons et al., 2015; Schlosser et al., 2015
Resource allocation (Q12-15)	Aral & Weill, 2007; K. C. Chang & Wang, 2011; Chen, 2012; J. Crawford et al., 2011; Diamantopoulou et al., 2017; Huang et al., 2006; Jarzabkowski, 2002; Srinidhi et al., 2015; Tu & Yuan, 2014; Y. A. Wu & Saunders, 2005
Outsourcing strategy (Q16-17)	Dahlberg & Lahdelma, 2007; Feng et al., 2019; Handley, 2012; Holcomb & Hitt, 2007; Jennings, 2002; Kroes & Ghosh, 2010; Lacity et al., 2016, 2010; J. N. Lee et al., 2004; Liu et al., 2018; Niranjan et al., 2007; Saxena & Bharadwaj, 2009; Valorinta, 2011; Winkler, 2016b
Cyber risk management (Q18-21)	FFIEC, 2015a, 2017b, 2017a; Kosub, 2015; Marotta & McShane, 2018; NIST, 2018

Table 1. Overview of the constructs, their associated questions, and the sources they are based on.

The questionnaire contained only closed questions in order to generate comparable responses and facilitate faster completion of the survey (Saunders et al., 2016). Since the data collected would be analyzed statistically, it was necessary that the datasets from different respondents were directly comparable so that they could be operationalized in a consistent and uniform way. The questions were designed to enable a self-typing assessment of the respondent firms' intended IT organization and cyber risk management strategies (Snow & Hambrick, 1980). The questions are a mix of list questions and category questions. List questions enable the respondents to select one or more appropriate responses whereas category questions are mutually exclusive (Saunders et al., 2016).

Both types of questions allow for a high degree of response control for the researcher while still generating relatively detailed data within a given frame of questions (Dillman et al., 2014). Since respondents' influence over their response is limited to a range of pre-defined choices, the quality of these response options needs to be high enough that participants can respond satisfactorily (Saunders et al., 2016). Furthermore, enabling respondents to finish the survey relatively quickly both increases the chance they will see the survey through to the end and shows a respect for their time (Dillman et al., 2014; Van Selm & Jankowski, 2006).

On the introductory page of the survey, the estimated completion time was set to ten minutes, purposely exaggerated a bit to avoid the increased drop-out rate associated with an underestimated questionnaire completion time (S. D. Crawford et al., 2001). The data shows that the actual average response time was seven minutes after adjusting for five outliers that were over 40 minutes. Each question was designed to be as short and concise as possible in order to improve comprehensibility, both in terms of question length and number of response options. Furthermore, questions were grouped together according to their construct category from table 1 in order to create a logical question sequence (Dillman et al., 1998; Granello & Wheaton, 2004), i.e. questions about decision-making structures were presented to respondents on the same page, and likewise for the other constructs. The final version of the questionnaire was translated from English to Danish to reduce the risk that a language barrier would deter respondents from participating, or that the respondents would not be able to understand some of the specialist foreign-language words (Dillman et al., 2014). A purpose-oriented translation was pursued in order to convey the meaning from the source language in a manner that was easily decodable in the target language (Ditlevsen, 2007). The translation emphasized idiomatic adaptation and the experiential meaning of the questions' wording in order to maximize the translation's comprehensibility (Askehave & Norlyk, 2006; Saunders et al., 2016, p. 464). In the end, 81.13 percent (*n* = 43) of respondents opted for the Danish translation of the survey, and the remaining 18.87 percent (*n* = 10) completed it in the source language, English.

For the four predictor constructs, questions were developed in the form of declarative statements based on the literature review in section 2.2 on the IT organization. The declarative format was inspired by the FFIEC CAT maturity guideline, which outlines the maturity assessment criteria through a series of statements about the organization (FFIEC, 2017a). For the decision rights structure construct, there are two question types: one type measures the allocation of decision rights within the organization (H1), and the other measures the executive responsibility (H2). The decision rights questions were based on the concept of decision hierarchies, using the spectrum of centralization to decentralization as its measurement (Sambamurthy & Zmud, 1999; Weill & Ross, 2004). For the executive responsibility, questions were based on the literature that describes the role of the C-level executives with specific IT or cybersecurity capabilities, and the question wording adopted these CXO labels (Karanja, 2017; Turedi & Zhu, 2019). Questions about the resource allocation construct were also measured along a centralization dimension for both financial and human resources (Aral & Weill, 2007; Winkler & Brown, 2014).

The interdepartmental communication construct is the product of two variables, communication frequency and communication variety (Hansen et al., 2005). Communication frequency is measured on a five-point scale ranging from daily interaction to never having interaction, and communication variety is a categorical list of six different communication paths identified through the literature review. The outsourcing construct measures the extent of outsourcing on a three-point scale ranging from minimal to extensive, adapted from the scale used in Lee et al. (2004). Finally, the cyber risk management maturity level consists of four questions representing the three category subsets covered in the CAT's risk management assessment factor (FFIEC, 2017a, pp. 23–26): the first two questions are developed from the risk management program subset, the third is from the risk assessment subset, and the last is based on the audit subset. The four questions contain a mixed range of response options to cover the maturity levels from evolving to innovative. Baseline maturity level indicators have been omitted based on the assumption that all respondents live up to the minimum legal requirements for cybersecurity.

The validity and reliability of the research instrument were ensured by using the questionnaire development and evaluation framework developed by O'Brien and McCay-Peet (2017). The validity was established through the extensive review of the literature and subsequent evaluative tests to ensure that the questionnaire adequately covered the content being measured (O'Brien & McCay-Peet, 2017). The questionnaire's reliability was ensured by continually refining and assessing its ability to generate consistent results until a final, acceptable instrument was achieved

(O’Brien & McCay-Peet, 2017). The initial phase of the questionnaire development involved exploring the constructs that were going to be included in the questionnaire through a literature review. Once the constructs had been identified and their measurement dimensions defined, they were developed into questions. In order to assess the validity and reliability of the questions, two volunteers were recruited to provide an outsider perspective on the questionnaire (O’Brien & McCay-Peet, 2017; Saunders et al., 2016). One volunteer had limited insight into IT and cybersecurity but had a good grasp of language and clarity (person A), and the other had good insight into IT and cybersecurity from professional experience (person B). Person A was chosen in order to get an assessment of the sentence construction, readability, survey layout, and overall impression of the questionnaire. Person B was able to provide feedback on the constructs themselves, including whether the intended meaning of the constructs came across, and whether the questions could be answered by a technical professional.

Each volunteer completed the questionnaire independently and was then asked to paraphrase the questions in order to check their individual understanding. In doing so, the two volunteers provided feedback on the comprehensibility and wording of the questions in order to improve the reliability of the questionnaire (O’Brien & McCay-Peet, 2017). Furthermore, the response option ‘don’t know’ was included where appropriate (i.e. in questions that required factual knowledge of organizational procedures) in order to reduce the risk of non-attitude responses, also improving reliability (Alwin & Krosnick, 1991). The two volunteers also provided sparring about the questions’ ability to confer insight about the constructs and about the elimination of unnecessary questionnaire items (O’Brien & McCay-Peet, 2017; Saunders et al., 2016). Finally, an overall assessment of the questionnaire was made together with the supervisor of this thesis. Questionnaire elements such as question wording and presentation were adjusted to reflect the feedback given during the evaluation process.

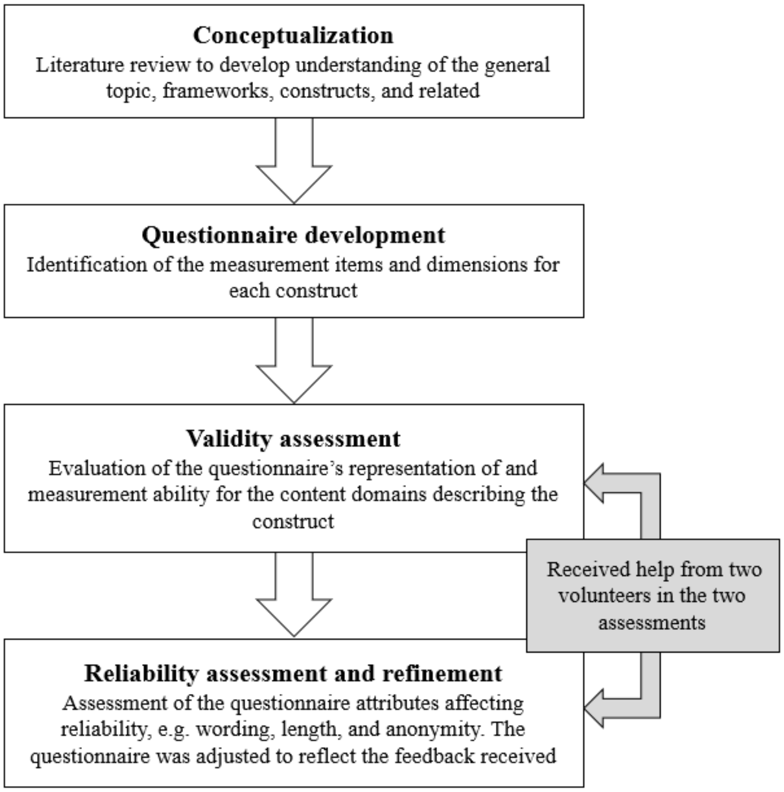

Conceptualization
Literature review to develop understanding of the general topic, frameworks, constructs, and related
Questionnaire development
Identification of the measurement items and dimensions for each construct
Validity assessment
Evaluation of the questionnaire's representation of and measurement ability for the content domains describing the construct
Received help from two volunteers in the two assessments
Reliability assessment and refinement
Assessment of the questionnaire attributes affecting reliability, e.g. wording, length, and anonymity. The questionnaire was adjusted to reflect the feedback received

Figure 4. Questionnaire development process, adapted from O'Brien and McCay-Peet (2017).

The questionnaire itself was then built and distributed through the online survey tool Qualtrics. A web-based survey was selected because of its many positive attributes: accessibility for both the data collector and the respondents, scalability, wide geographical reach, shareability, and a high degree of standardization (Atif et al., 2012; Evans & Mathur, 2005; Saunders et al., 2016; Van Selm & Jankowski, 2006). Furthermore, it is assumed that the target population will be familiar and comfortable with web-based questionnaires, which should enable them to complete the survey in a shorter timeframe (Yan & Tourangeau, 2008). Additionally, in a non-face-to-face format such as an online survey, respondents are more likely to provide answers that are honest and unaffected by ideas of socially desirable behavior (Dillman et al., 2014). Participants self-editing their responses to comply with socially desirable behavior can be a particular challenge for sensitive subjects (Ong & Weiss, 2000). In the case of cybersecurity, respondents may be motivated to avoid the negative feelings associated with responses that show a low cybersecurity maturity, but this risk of social desirability bias is reduced in web-based surveys (Kreuter et al., 2008).

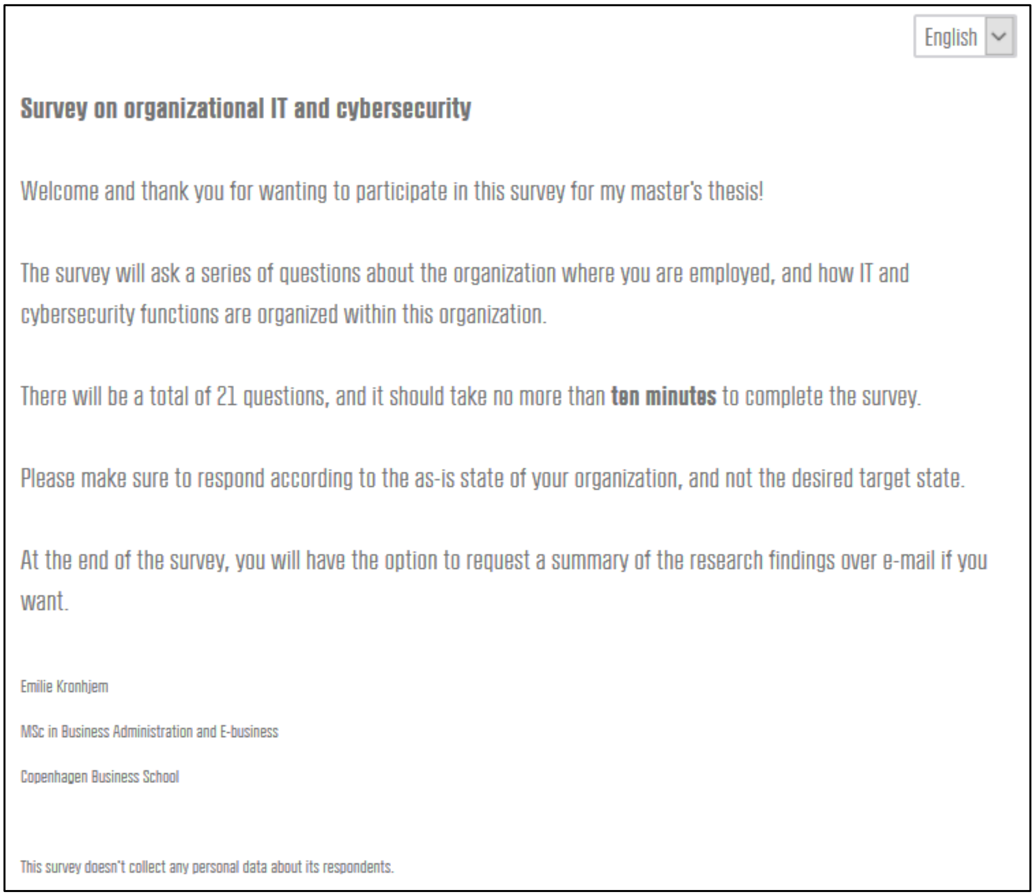
However, a web-based survey format also has inherent problems that must be addressed. A main challenge with online questionnaires is the generally low response rate (Dillman et al., 2014; Evans & Mathur, 2005; Granello & Wheaton, 2004; Van Selm & Jankowski, 2006). Members of the target population might consider requests to respond to a questionnaire as irrelevant to them or may simply get too many similar requests (Atif et al., 2012). In this study, the challenge was addressed by using partners that could broker data access to establish trust and legitimacy in the eyes of potential respondents (Saunders et al., 2016), a tactic that will be explained in more detail in section 3.1.2 below. Question ambiguity is another risk in online surveys, as the online format leaves respondents unable to ask the researcher for clarification on the questions, which could create misunderstandings or frustration (Evans & Mathur, 2005). This risk was addressed through the process outlined earlier in figure 4, where two volunteers helped evaluate and fine-tune the clarity and comprehensibility of the questionnaire.

3.1.2. Sampling strategy

As this study investigates the design of the IT organization, this naturally limits the target population to firms with an IT organization, excluding for example some small local stores with an ad hoc approach to IT. Additionally, the target population is geographically restricted to organizations operating in Denmark. Limiting the survey to a confined social, economic, and cultural sphere in this manner is practically motivated. By investigating the subject within a single country, it removes the need to control for the impact of complex broad socioeconomic factors, e.g. national economy, political security, or culture. For example, some cultures generally have a higher degree of deference to authority (Gladwell, 2008; Ting-Toomey, 1999), and may thus be more inclined to adhere to corporate cybersecurity policies, which could impact the survey results. While it would be interesting to study what the impact of different national or cultural characteristics on cyber risk management might be, it is a very complex topic that falls outside the scope of this thesis. Furthermore, the survey targets executives, managers, and employees with insight into both the organizational IT and cybersecurity, as the questionnaire requires a deeper knowledge of these areas than the average employee is likely to have. It is important to gain access to this particular segment of specialists in order to generate high quality data, and the survey distribution efforts thus specifically target these employees. For a hard-to-reach professional population such as this, obtaining a sampling frame is unfeasible (Goodman, 2011). Accordingly, a non-probability sampling strategy was used to generate data access, i.e. a respondent-driven and self-selection sampling strategy, which involves recruiting cases within the target population to help identify further cases (Goodman, 2011; Saunders et al., 2016).

Two partner firms agreed to distribute the survey within their networks (i.e. clients, business contacts, etc.), using both direct e-mails, social media (LinkedIn), and other miscellaneous channels. Using a trusted authority to establish contact with potential respondents in this manner helps to overcome initial hesitation towards participation (Dillman et al., 2014). In addition to these two partner firms, individual members of the target population with relevant networks were also recruited on a convenience basis to help generate responses. Together, these access brokers made up the driving force of the respondent-driven sampling tactic. This approach was selected because it is well-suited for hard-to-reach populations that are generally difficult to access as an external researcher (Goodman, 2011; Sadler et al., 2010). However, it should be noted that the chosen target population does somewhat limit the sample size that is realistically achievable for this study. The trade-off between a smaller sample of specialist respondents and a larger sample of respondents from the general population (e.g. other students) was considered in the light of the topic being investigated (Saunders et al., 2016). While a larger sample is generally desirable in statistical analyses, broadening the target population at the expense of the data quality would reduce the reliability of the study. Furthermore, respondents from the general population would likely have been unable to answer some parts of the questionnaire. Accordingly, widening the pool of potential respondents would have possibly diminished the data quality, and this option was rejected in favor of a smaller, high-quality sample.

Both of the partner firms recruited as access brokers specialize in information security, data privacy audits and independent certification. This does create a risk of participation bias in the data (Saunders et al., 2016), as partner firms' business contacts potentially have a higher level of cybersecurity sophistication than the average firm. However, both firms are involved at all stages of the audit and certification process, meaning that some contacts in their networks will be in the early stages of development for their cyber risk management programs. The questionnaire itself was distributed using an anonymized link provided through Qualtrics. Clicking this link brought the participant directly to the survey's welcome page, which was designed to provide a brief introductory overview of the survey (Dillman et al., 1998). The welcome screen contained a short description of the questionnaire's subject, an estimate of the questionnaire's duration, and an instruction on how to respond to the questions. The introduction page was intentionally written in a manner that only superficially describes the research in order to avoid potential contamination of participants' responses (Saunders et al., 2016). Furthermore, the welcome page was signed off by me as the sender, including my name, line of study, and university in order to make the introduction more personal (Saunders et al., 2016). The English version of the welcome page can be seen in figure 5.



Survey on organizational IT and cybersecurity

Welcome and thank you for wanting to participate in this survey for my master's thesis!

The survey will ask a series of questions about the organization where you are employed, and how IT and cybersecurity functions are organized within this organization.

There will be a total of 21 questions, and it should take no more than **ten minutes** to complete the survey.

Please make sure to respond according to the as-is state of your organization, and not the desired target state.

At the end of the survey, you will have the option to request a summary of the research findings over e-mail if you want.

Emilie Kronhjem

MSc in Business Administration and E-business

Copenhagen Business School

This survey doesn't collect any personal data about its respondents.

Figure 5. Survey welcome page.

Respondent privacy was a high priority, as information about IT and cybersecurity strategy might be considered confidential by the respondents and their firms, and privacy issues with the survey would then risk compromising this confidentiality (Saunders et al., 2016). Furthermore, obvious privacy issues would reduce the credibility of the survey and possibly deter respondents from participating (Evans & Mathur, 2005). Respondent anonymity was ensured by not collecting identifying metadata, not knowing to whom the survey had been distributed through the partner firms, and not asking questions in the survey that could give away information about the respondent's firm. However, it should be noted that at the end of the survey, respondents were offered the opportunity to voluntarily sign up for a summary of the final thesis as a thank you. To sign up, respondents were asked to send an e-mail to me to indicate interest, which of course breaches the anonymity somewhat. While this solution does not directly relate a respondent to a given response, it does allow for some inference of this relationship. However, this solution was chosen in order to provide a voluntary reward to participants (Dillman et al., 2014), and there were no other practically viable options to offer respondents the summary than to ask for a personal contact. This compromise is not taken lightly, and each e-mail address was treated with complete confidentiality, was used only for the given purpose, and was removed from the host server immediately upon completion of this purpose.

The final sample consists of 53 individual survey responses collected over a two-week period, with an additional subsequent collection period lasting one week. The sample is relatively small, which can create some difficulties in the data analysis. The normal distribution and confidence level of the mean usually improves with a larger sample size in accordance with the central limit theorem (Stutely, 2003). However, estimating what constitutes an ideal or sufficient sample size can be tricky. For instance, one method involves multiplying the number of predictor variables with a factor of five (Field et al., 2012, pp. 273–274), whereas another rule of thumb simply suggests having a minimum of 30 sample items (Stutely, 2003, p. 117). The minimum sample size should also be considered in the light of the effect size that is measured, and even small samples can show an effect if the effect is strong enough (Field et al., 2012, p. 274). Accordingly, the significant effects discovered in this small sample must be highly significant to appear at all. However, the small sample does limit how much we can rely on the non-significant relationships. Having a small sample will artificially inflate the standard deviations in the data, which makes it harder for significant relationships to emerge through the regression model. The implications of this will be discussed in more detail in section 3.2 on the data analysis. Due to the sampling design, it is difficult to pinpoint exactly how many potential respondents have been provided the opportunity to participate in the survey, either by receiving it over e-mail or seeing it on social media. The survey tool informs us that the survey link has been accessed a total of 91 times, meaning that 38 potential participants (41.76%) accessed the survey and decided at some point to abandon it again. The vast majority (*n* = 29, 76.32%) of the people who dropped the survey did so without answering a single question.

3.2. Data analysis

The quantitative data collected through the questionnaire was analyzed using multiple linear regression in the statistics software R, executed in the RStudio environment (R Core Team, 2020; RStudio Team, 2019). The purpose of the linear regression model is to assess the predictive value of the IT organization constructs on the participant firms' cybersecurity maturity levels. The survey data is measured in two different variable types: ordinal and binary. The ordinal variables reflect a score from low to high, and the binary variables are operationalized as dummy variables to divide the responses into 'true' and 'false'. Table 2 describes the predictor variables and how they were operationalized.

Construct and variables	Variable type	Operationalization
H1: Decision rights structures: Centralization ITSTRDEC CYBRSTRDEC	Ordinal	Creates a scale of IT and cybersecurity decision rights centralization that ranges from decentralized (1) to centralized (3).
H2: Decision rights structures: Executive responsibility ITEXEC CYBREXEC	Binary	For IT, CIO, CTO and CDO = 'true' and for cybersecurity, CISO, CRO, and CSO = 'true', all others are 'false.'
H3: Resource allocation ITFIN ITSKILLS CYBRFIN CYBRSKILLS	Ordinal	Creates a scale of IT and cybersecurity financial and human resource allocations that ranges from decentralized (1) to centralized (3).
H4: Interdepartmental communication COMINT	Ordinal	Determines an aggregate score for the frequency and variety of interdepartmental communication ranging from low (0) to high (10)

H5: Outsourcing strategy ITOUTSRC CYBROUTSRC	Ordinal	Creates a scale of IT and cybersecurity outsourcing extent that ranges from extensive (1) to minimal outsourcing (3).
Cyber risk management maturity CYBRSCORE	Ordinal	An aggregate score composed of the variables measuring the cyber program, evaluation efforts, and auditing practices.

Table 2. Overview of the variables and their operationalization.

The variable measuring the executive responsibility divides response options into true or false in order to determine whether the respondent's firm has a dedicated IT or cybersecurity executive. The IT executive variable checks for the technical executive roles, i.e. CIO, CTO, and CDO, which focus on technical aspects such as technological innovation and digitalization (Centric Digital, 2017; Deloitte, 2018). The cybersecurity executive variable checks for the security or risk mitigation executive roles, i.e. CISO, CRO or CSO, which all focus on facets of the business operations that relate to cyber risk management (Burgess, 2014; Fruhlinger, 2018). For the variables measuring decision rights centralization, resource allocation, and outsourcing degree, three-point scales were used that measure the construct on a basis of low control to high control. In practice, this means that decentralization is operationalized as a low degree of corporate control. The outsourcing extent is operationalized as the level of firm control, i.e. extensive outsourcing involves low firm control. Interdepartmental communication is an aggregate score that shows the relative intensity of communication. It is composed of two variables: communication frequency, a five-point scale ranging from 'daily' to 'never', and communication variety, a measurement of the different types of communication paths indicated by the respondent.

The outcome variable is composed of four weighted scoring variables that were each assigned a score based on the risk management assessment factor in the CAT framework (FFIEC, 2015b, 2017a, pp. 23–26). The scores assigned either correspond to the maturity levels evolving (for a score of '1'), intermediate (for a score of '2'), advanced (for a score of '3'), and innovative (for a score of '4'). If a respondent did not indicate that their organization's cybersecurity practices matched any of these levels, their maturity level is assumed to be baseline, i.e. the minimum level of cybersecurity permissible in accordance with the law, and they get a score of zero. The resulting variable determines the respondent firm's cyber risk management maturity based on the assessment provided in the FFIEC's CAT framework (FFIEC, 2017b). It combines the cyber risk management program observations in the dataset in order to create an aggregate score within the range zero to 38. A score of zero indicates that the respondent firm has achieved the 'baseline' maturity, demonstrating a compliance-based approach to cybersecurity. Conversely, a score of 38 is given if the firm is in the 'innovative' maturity category, driven by a holistic and proactive approach to cybersecurity innovation (FFIEC, 2017b). Rather than using the stepwise maturity levels that are used by the FFIEC, for the purposes of this study, the maturity range is seen as a fluid spectrum with the baseline maturity level at one end and the innovative maturity level at the other.

The five demographic variables described in section 3.1.1 are also used as control variables in the regression model. These control variables are the organization's size, sector, whether it follows a cybersecurity accreditation, as well as the respondent's position and area of employment. Organization size has previously been found to have a positive impact on cybersecurity management outcomes (S. E. Chang & Ho, 2006; Diamantopoulou et al., 2017). For sector, I distinguish between the private and public sectors as well as NGOs. Generally, market competition is conducive to innovation (Aghion et al., 2005). Per definition, the private sector is characterized by market competition, whereas the public sector is not. The NGOs in Denmark compete with each other for donations, but the sector is also heavily subsidized by the government (Olwig & Schou, 2020). Cybersecurity accreditation schemes are designed to improve cybersecurity programs, and thus this variable must also be accounted for in the controls. Finally, the two respondent-oriented variables control for the effect of respondent perspectives on their self-reports of cybersecurity maturity. Respondents in different positions or employment areas may differ in terms of their knowledge of organizational security processes. For instance, managerial staff may perceive cybersecurity compliance measures differently than operational staff, and employees working in IT may have a different overview than risk-oriented employees.

The variables were added to the regression model using a forced entry approach (Field et al., 2012, p. 264). Since none of the variables have been previously established as predictors of cyber risk management maturity in the literature, all the variables have equal theoretical merit in the model.

Thus, the forced entry approach was chosen in order to avoid having to make a subjectively based decision about a stepwise, hierarchical inclusion of variables (Field et al., 2012, p. 264; Studenmund & Cassidy, 1987). In order to assess the model's predictive accuracy across different samples, it would have been good practice to cross-validate the model by running it on two versions of the dataset that had been randomly split 20/80 (Field et al., 2012, p. 273). However, due to the small sample size of 53 responses, this would be a futile exercise, as it would create two data sets consisting of 11 and 42 items each. Given the difficulty of generating significant results in a small sample, it is not likely such a cross-validation would yield useful results.

4. Results

In this section, the results of the data analysis are reported for both the control variables, the predictor variables, and the regression model. First, the respondent demographics are outlined, followed by the descriptive statistics for the dataset, both in order to provide a brief overview of the data that has been collected and used in the analysis. Then, the analysis and validation process for the linear regression model are described. The R markdown document detailing the data processing can be found in appendix B.

The respondents were asked to respond to five demographic questions: three questions relating to the organization in which they are employed and two questions relating to their position within that organization. Table 3 reports the results of these demographic questions. Note that some variables may not add up to 100 percent, as cases where respondents have skipped the question are not reported in the table.

	Overall (N=53)
Organization: External accreditation	
Yes	31 (58.5%)
No	22 (41.5%)
Organization: Sector	
Private	35 (66.0%)
Public	10 (18.9%)
NGO	5 (9.4%)

	Overall (N=53)
Organization: Number of employees	
Less than 10	7 (13.2%)
10 to 49	16 (30.2%)
50 to 249	17 (32.1%)
250 to 1,000	3 (5.7%)
Over 1,000	10 (18.9%)
Respondent: Position	
Executive	15 (28.3%)
Manager	19 (35.8%)
Employee	19 (35.8%)
Respondent: Area of employment[2]	
Risk	14 (26.4%)
Cybersecurity	16 (30.2%)
Business strategy	18 (34.0%)
IT	25 (47.2%)
Other	14 (26.4%)

Table 3. Overview of the demographic variables measured.

Based on table 3, the average profile among the respondents is that they are managers or employees within some domain of IT, who work in a private SME (i.e. below 250 employees) that follows an external cybersecurity accreditation. Table 4 is a summary of the descriptive statistics for the variables in the data set. All variables are operationalized from low to high (e.g. low control is a measure of decentralization). The descriptive statistics illustrate a few interesting points that are relevant to the hypotheses. For instance, there appears to be a tendency for the executive in charge of cybersecurity not to have a role that is specific to information security, security or risk, whereas for the IT executive there are more technical than non-technical executives. Another noteworthy observation is that the high mean and median scores for the decision rights and resource allocation variables indicate that the data set is skewed towards a high level of corporate control for these

[2] Respondents were able to select multiple employment areas to reflect multifaceted roles. The percentages indicate how many of the 53 respondents indicated the given employment area.

variables. Consequently, the opposite end of the spectrum is likely not well represented in the data. The only variables that do not seem to be skewed towards corporate control are the outsourcing strategy variables, which have mean and median scores around the middle of the range. It should also be noted that the generally large standard deviations reported for all the variables in table 4 are likely a consequence of the small sample used for the analysis, which will create a tendency for the standard deviation to become artificially bloated.

	Overall (N=53)
IT decision structures	
Mean (SD)	2.49 (0.669)
Median [Min, Max]	3.00 [0, 3.00]
Cybersecurity decision structures	
Mean (SD)	2.40 (0.793)
Median [Min, Max]	3.00 [0, 3.00]
IT executive	
Yes	30 (56.6%)
No	23 (43.4%)
Cybersecurity executive	
Yes	12 (22.6%)
No	41 (77.4%)
IT financial resources	
Mean (SD)	2.42 (0.969)
Median [Min, Max]	3.00 [0, 3.00]
IT human resources	
Mean (SD)	2.58 (0.842)
Median [Min, Max]	3.00 [0, 3.00]
Cybersecurity financial resources	
Mean (SD)	2.25 (1.12)
Median [Min, Max]	3.00 [0, 3.00]
Cybersecurity human resources	
Mean (SD)	2.09 (1.23)
Median [Min, Max]	3.00 [0, 3.00]
Interdepartmental communication	

	Overall (N=53)
Mean (SD)	5.79 (1.74)
Median [Min, Max]	6.00 [1.00, 10.0]
IT outsourcing	
Mean (SD)	2.00 (0.941)
Median [Min, Max]	2.00 [0, 3.00]
Cybersecurity outsourcing	
Mean (SD)	2.17 (0.914)
Median [Min, Max]	2.00 [0, 3.00]
Cyber risk management maturity score	
Mean (SD)	14.3 (9.38)
Median [Min, Max]	14.0 [0, 33.0]

Table 4. Descriptive statistics for the variables.

The outcome variable describing the cyber risk management maturity level has mean and median scores that are below the middle of the range, which would be 16.5. This tells us that the respondent firms are on average at the lower end of the cyber risk management maturity spectrum. This is a surprising result given that most of the participants reported that their firm follows an external cybersecurity accreditation. When a majority of the firms follow an external accreditation, it would be expected that the results would be biased towards the higher end of the maturity spectrum. It is further worth noting that the highest value of the range is 33, but the maximum possible score for cybersecurity maturity was 38, meaning that no respondent was able to achieve the highest maturity score for their cybersecurity program. A histogram (figure 6) reveals that the outcome variable has highly uneven distribution, with concentrations at the low end and an apparent lack of firms with scores in the middle. The relatively few firms at the center of the distribution curve could indicate that cybersecurity maturity is an “either-or” situation where firms either exhibit a low or high degree of program sophistication, which few opting for an intermediate path. The lack of normal distribution in the data could also be caused by the small sample size. A large sample will generally create a more normal distribution (Stutely, 2003) and with a sample of only 53 observations, it might explain why the cyber risk maturity scores in the histogram do not show a normal distribution.

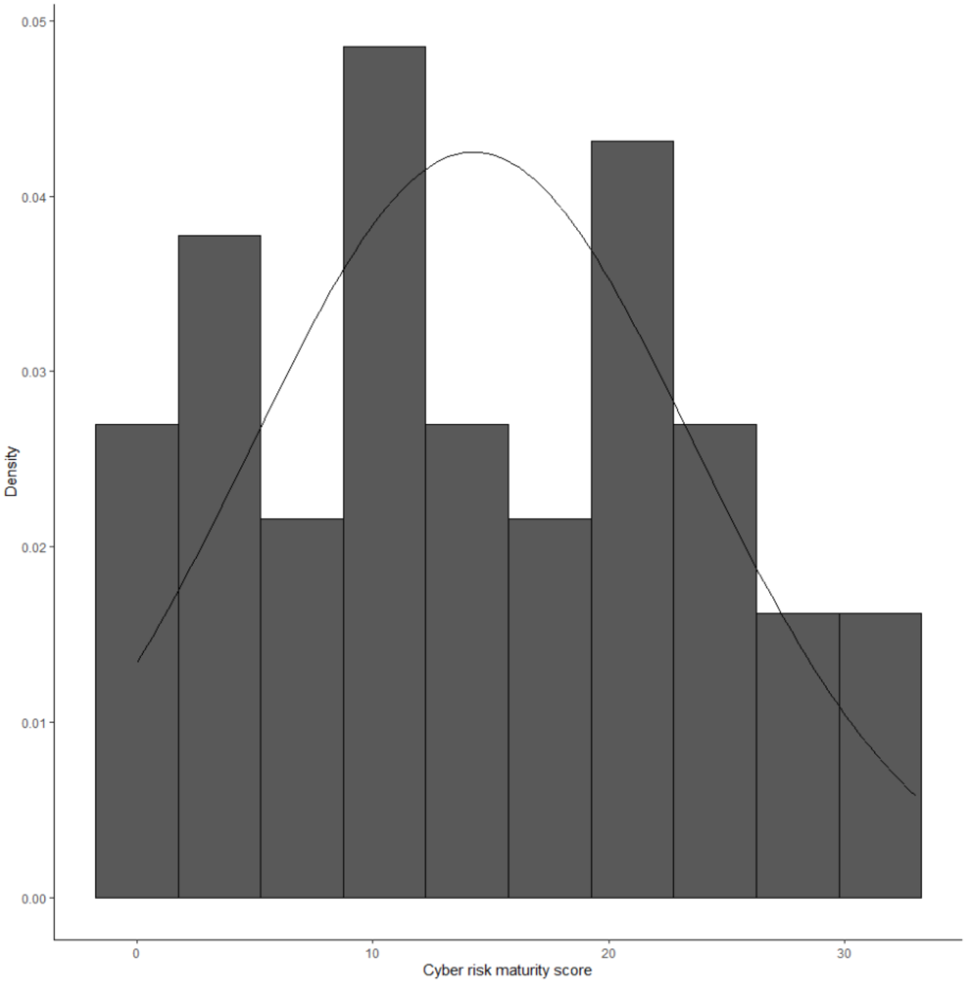


Figure 6. Cyber risk management maturity score distribution.

Both the control variables and the predictor variables are included in the linear regression model, which can be seen in table 5. Table 5 shows that there are five statistically significant predictor variables in the model: IT and cyber decision rights, IT and cyber financial resource allocation, and IT outsourcing. However, two of these variables (cyber decision rights and cyber financial resources) are significant in the opposite direction of the hypotheses' predictions. Furthermore, a number of the control variables also showed statistical significance in the model.

	Controls	**Model**
(Intercept)	-1.55 (6.06)	-17.86 (8.98)
Respondent: Position	1.16 (1.88)	-0.09 (1.68)
Respondent: Area of employment		
- Risk	1.89 (3.30)	-2.54 (3.19)
- Cybersecurity	1.46 (2.93)	6.91 (3.01)*
- Business strategy	3.69 (3.38)	11.92 (3.84)**
- Other	1.23 (2.83)	4.87 (2.78)
Organization: External accreditation (true)	7.16 (2.45)**	2.88 (2.65)
Organization: Number of employees	0.59 (1.12)	3.09 (1.15)*
Organization: Sector[3]	2.12 (1.22)	-0.49 (1.16)
IT executive (true)		-1.87 (2.43)
Cybersecurity executive (true)		-0.22 (2.73)
IT decision rights		8.36 (2.47)**
Cybersecurity decision rights		-4.58 (2.06)*
IT financial resources		-3.70 (1.61)*
IT human resources		1.60 (1.97)
Cybersecurity financial resources		4.37 (2.01)*
Cybersecurity human resources		-2.44 (1.36)
Interdepartmental communication		-0.57 (0.62)
IT outsourcing		3.64 (1.37)*
Cybersecurity outsourcing		1.65 (1.54)
R^2	0.33	0.66
Adj. R^2	0.20	0.47
Num. obs.	53	53
RMSE	8.37	6.84

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

Table 5. Overview of three linear regression models describing the data

The fact that the control variable measuring firm size is a significant predictor of the cybersecurity maturity is not surprising, given that studies have previously found a connection between organization size and greater cybersecurity (S. E. Chang & Ho, 2006; Diamantopoulou et al., 2017). Respondents employed within cybersecurity or business strategy functions were also significant predictors of a higher degree of cybersecurity maturity. However, the other employment areas,

[3] Defined on a spectrum of market coordination as described in section 3.2, i.e. private is high, NGO medium (due to partial market competition, partial public funding), public is low.

respondent position, sector and external accreditation were not significant. Interestingly, the use of an external cybersecurity accreditation is a significant predictor in the control model, and it would also make inherent sense as a predictor of cyber risk program maturity. Note that for the categorical control variable describing the respondent's area of employment, the choice option 'IT' was used as the base reference for the other options within that variable, and thus does not appear in the table below. IT was chosen as the base reference because it was the area most respondents selected as one of their primary fields of employment.

The R^2 is 0.66, while the adjusted R^2 is 0.47, and there is a relatively large distance between the two, with the R^2 being approximately 28.78 percent larger than the adjusted R^2. This difference could indicate that the model is not entirely parsimonious, and that some of the variables included do not contribute significantly to the model's predictive potential in the general population (Field et al., 2012, p. 281). However, the R^2 tells us that the model explains about two thirds of the variation in the cybersecurity maturity levels measured in this sample, and this predictive potential is 47 percent in the general population according to the adjusted R^2 (Field et al., 2012, p. 273). Cook's distance does not exceed 1 on any of the observations, indicating that no disproportionate influence is exerted by any single case on the model (Cook & Weisberg, 1982; Field et al., 2012). However, 7.55 percent (n = 4) of the studentized residuals for the 53 observations appear to be outliers falling outside the 95 percent confidence interval of 1.96 and -1.96. As this is higher than the five percent which are allowed within this confidence interval, it could indicate that there is a problem with the fit of the model to the data (Field et al., 2012, pp. 43–49). However, the high effect of a small number of outliers should be considered in the light of the small sample, which makes it easier for a single outlier to throw off the entire confidence interval. Furthermore, all values fall within the 99 percent confidence interval of 2.58 and -2.58.

In order to assess the generalizability of the statistical model, its basic assumptions are checked (Berry, 1993, p. 12; Field et al., 2012, pp. 271–272). Some of the general assumptions can be inferred from the research design and execution. Namely, that all the variables are quantitative, that the observations have nonzero variance, that the data (to the best of my knowledge) comes from unique participants, and that the relationship being modeled in the regression analysis is linear (Berry, 1993). The assumptions about the lack of perfect multicollinearity, error independence, homoscedasticity, and the normal distribution of errors are checked statistically (Field et al., 2012, pp. 288–298). The variance inflation factor (VIF) and tolerance statistics are used to assess whether there is multicollinearity in the model. Collinearity between variables can make some significant variables appear non-significant, which reduces the reliability of the regression analysis (Akinwande et al., 2015). None of the VIF values calculated for the predictor variables are over ten, however the mean VIF exceeds 1 (mean VIF = 2.46). As this is over 1, it may indicate that a weak collinearity between some variables is influencing the model (Field et al., 2012, p. 276). However, the VIF is still far from the high collinearity interval, which begins when the VIF approaches 5 (Akinwande et al., 2015). While most of the tolerance values are over the conservative lower limit of 0.20, the cybersecurity financial resources variable has a tolerance value of 0.18, which could indicate that there might be a small collinearity issue with this variable (Field et al., 2012, p. 293). However, since the tolerance value is still over 0.10, it does not pose a significant problem (Stubager & Sønderskov, 2011). The next assumption, error independence, must be fulfilled in order to ensure that autocorrelation between the standard errors does not decrease the inferential potential of the regression model (Stubager & Sønderskov, 2011). Error independence is checked using the Durbin-Watson test, which returns a D-W statistic close to 2 (DW = 2.13) and p-value greater than 0.05 (*p* = 0.77), both indicators of independent errors (Field et al., 2012, p. 292). The assumption of homoscedasticity requires that there is a constant variance among the residual errors, otherwise the *p*-values may be unreliable (Stubager & Sønderskov, 2011). Visual inspection of the plots (figures 7-9) for the studentized residual errors show that the variance in the data appears to be homoscedastic and the errors are normally distributed.

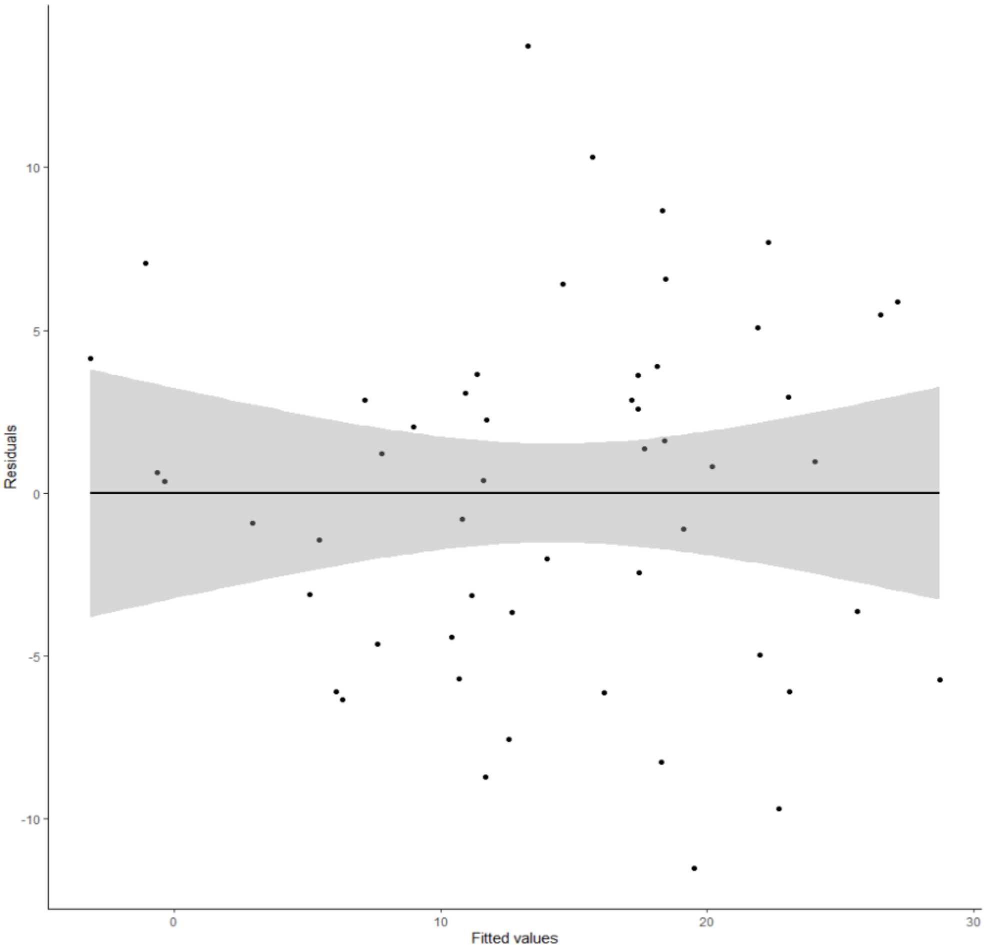


Figure 7. Scatterplot showing fitted values against residuals.

The plot of residuals versus fitted values (figure 7) has a generally random and evenly distributed pattern, albeit with some deviation at the low end of the graph. Particularly, the lower end of the fitted values seems to be more thinly populated, whereas the remainder of the graph has a more random scatter of values. This could point to some unequal variance across the data at the lower values, a tendency that might be exacerbated by the small sample size. However, overall the graph confirms that the assumption of homoscedasticity is not violated.

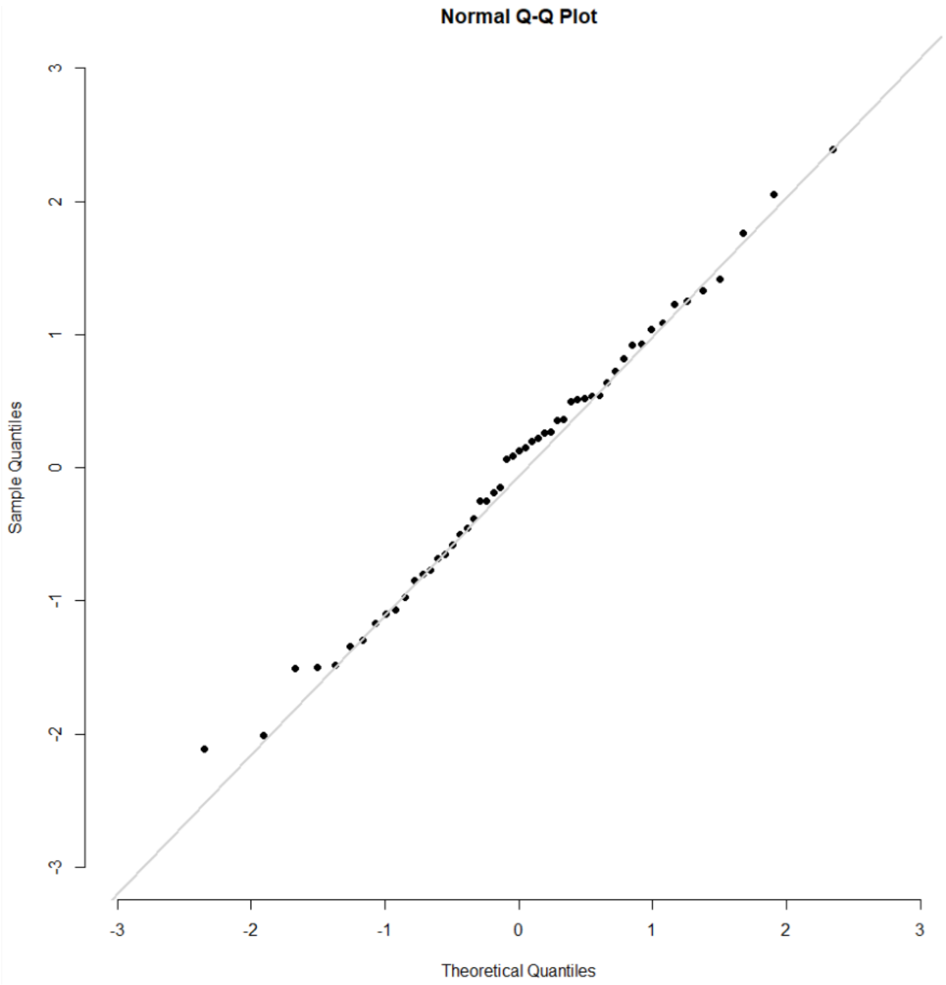


Figure 8. Q-Q plot showing the residual deviation from the mean.

Like the autocorrelation assumption, the assumption of normally distributed errors is important to ensure that reliable inferences can be made with the regression model (Stubager & Sønderskov, 2011). This assumption is checked by inspecting the Q-Q plot and histogram for the studentized residuals (Field et al., 2012, pp. 294–297). The Q-Q plot (figure 8) of the studentized residuals is generally normal looking, with the residuals fitting closely to the mean line across the graph. There are small deviations around the center and low end of the graph, which could indicate that there is a slight lack of normality in the studentized residuals around these parts of the normal distribution curve. However, a histogram (figure 9) showing the studentized residuals confirms that they have a mostly normal distribution. There is some abnormality in terms of the histogram's symmetry, which might cause the deviations in the Q-Q plot in figure 8. These abnormalities are not significant enough to cause concern and are a reflection of the fact that real data is likely to be somewhat imperfect.

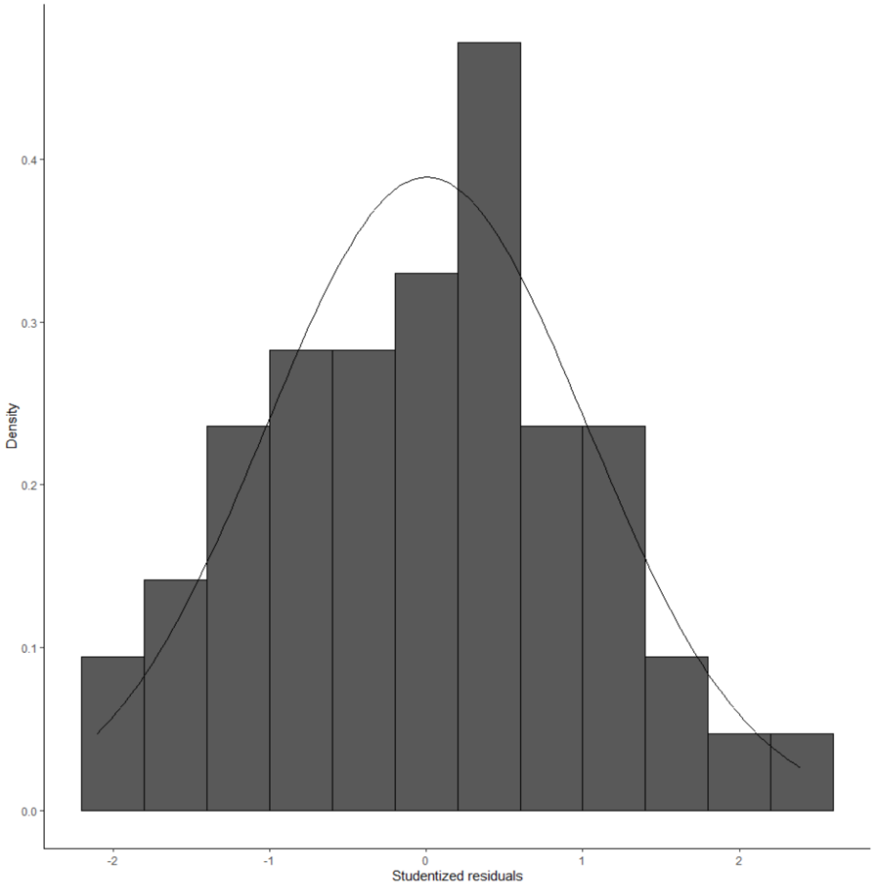


Figure 9. Histogram showing the distribution of the studentized residuals.

To summarize, the linear regression analysis revealed five significant variables among all the predictor variables: decision rights and financial resource allocation within both IT and cybersecurity, as well as IT outsourcing. The variables for IT decision rights and IT outsourcing were positive and significant, which supports hypotheses 1 and 5, respectively. IT financial resource allocation was negative and significant, thus providing support for H3. The cybersecurity decision rights variable was negative and significant, and the cybersecurity financial resource allocation variable was positive and significant. Accordingly, these two variables are directly contrary to hypotheses 1 and 5. The remaining predictor variables were not significant and could thus not be used to draw any definitive conclusions about the hypotheses. The control variables were mostly predictable with the notable exception of the external accreditation. It would seem natural for an external cybersecurity accreditation to improve cybersecurity maturity levels. While external accreditation was significant in the control model, this significance appeared to have been cancelled out in the main model. According to the R^2, the overall model explains 66 percent of the variation in cyber risk management maturity levels among the respondents in the sample, which is a sizeable predictive power. The regression diagnostics show that the model does not appear to violate any assumptions significantly. However, the cybersecurity financial resources variable had a tolerance value of 0.18, thus showing some signs of multicollinearity. The variable's tolerance level is below the conservative limit of 0.20, but still above the critical limit of 0.10. Furthermore, the diagnostic tests also revealed that four outliers may be affecting the fit of the model to the data. The results of these diagnostic tests may be exacerbated by the small sample size. Besides these two potential problems, overall the model seems to be a good fit for the data, and it has good predictive value. The limitations of the study will be discussed in more detail in the next section.

4.1. Limitations

The results of the study should be considered with some limitations in mind. Firstly, the lack of literature on the intersection between IT management and cybersecurity limited the study somewhat. Cybersecurity is still a relative newcomer to management research, and this limited my ability to draw on existing research connecting IT management and the IT organization to cybersecurity planning and outcomes. However, pursuing a relatively novel research direction also allowed me to exercise a higher degree of creativity in interpreting the connections between the various source materials and in developing a research instrument to illuminate these connections. The sparse literature does make it more challenging to formulate hypotheses, as these hypotheses will be based on a higher degree of inference based on the available knowledge. However, it also enabled me to make a greater contribution with this study by adding insight to a new research field.

Secondly, the target population for the questionnaire used in this study was difficult to gain access to, which proved problematic in terms of the sample size that could be achieved for the survey. An attempt was made to plan around the issue of data access by recruiting partners to help facilitate contact with members of the target population. Nevertheless, sample size still became a problem, and the small sample proved problematic to the data analysis, as statistical significance is more difficult to detect within a small sample. Furthermore, a larger sample would have provided greater certainty that the sample was representative of the target population, thus improving the generalizability of the study. Upon determining that the sample was too small after the initial planned round of data collection, another (unplanned) round was initiated in order to generate more data. This was somewhat successful, increasing the sample size by about 15 percent, but the sample was still much smaller than what is ideal for this type of study. While the small sample did not prevent some statistically significant results from appearing in the data, it does create a risk that other significant predictors remained undiscovered.

5. Discussion and conclusion

This study addresses the gap in management research between IT and cybersecurity management. It does so by exploring cyber risk management through four facets of the IT organization, i.e. the decision-making structures, resource allocation, interdepartmental communication, and outsourcing strategy. An examination of the existing literature lead to the development of five hypotheses that were tested empirically through a primary survey-based data collection and subsequent multiple linear regression analysis. Three of these variables were statistically significant in a way that provides partial support for three of the five hypotheses, while two variables were significant, but contrary to the hypotheses' predictions. The hypotheses were supported as reported in table 6.

Hypothesis	**a. IT**	**b. Cybersecurity**
H1: Decision rights: Centralization	✓	X
H2: Decision rights: Executive responsibility	NS	NS
H3: Resource allocation		
- Financial resources	✓	X
- Human resources	NS	NS
H4: Interdepartmental communication	NS	
H5: Outsourcing strategy	✓	NS

NS = Not significant, ✓ = Significant, X = Significant, but in opposite direction

Table 6. Overview of supported and unsupported hypotheses.

The IT decision structures were moderately significant (*p* < 0.01), while cybersecurity decision structures, the allocation of financial resources within both IT and cybersecurity, and IT outsourcing extent were all mildly significant (*p* < 0.05). The cyber decision rights and cyber financial resource allocation variables were significant in ways that were not predicted by the hypotheses. In the next section, I will discuss the five hypotheses in turn, combining the findings of the regression analysis with insights from the literature in order to shed light on why some hypotheses were supported while others were not. Finally, I will conclude by developing suggestions based on the findings, both for practitioners and for future directions for research.

5.1. Hypotheses

The first hypothesis proposed that centralized decision structures within the IT organization would improve cyber risk management maturity levels. This hypothesis was supported in the data along the IT dimension, which aligns with the findings of Liu et al. (2018) that centralized IT decision structures are associated with fewer cybersecurity incidents. The benefits of a centralized IT decision rights structure include improved enterprise-wide coordination and a higher degree of corporate control over standards and procedures (A. E. Brown & Grant, 2005; Sambamurthy & Zmud, 1999), and features such as these might create the foundation for a higher level of cyber risk management maturity. For example, 'shadow IT' describes the practice where employees throughout an organization install and use IT applications which are not officially sanctioned or integrated within the enterprise IT solution (Chua et al., 2014), and it is one of the main challenges of cybersecurity management (Deloitte, 2019b, p. 3). Because of its unmonitored and haphazard nature, shadow IT can pose a security and data privacy risk to the firm (Klotz et al., 2019). By centralizing the decision-making power over IT standards and removing that authority from the individual departments, organizations can more effectively manage the threat posed by dispersed practices such as shadow IT (Chua et al., 2014).

However, centralization of decision rights along the cybersecurity dimension showed the opposite pattern and was thus directly contrary to the hypothesis. Seemingly, decentralized cybersecurity decision rights are a predictor of superior cyber risk management program maturity. This finding indicates that while a large degree of corporate control over IT standards and procedures makes for better cybersecurity program maturity, control over the cybersecurity procedures should be allocated divisionally. A possible explanation for this finding could be that decentralized decision rights for cybersecurity enable the individual departments to make decisions about cyber risk management based on the specifications and needs of the local users. By allowing the risk management decisions to be made divisionally within a broader frame of central IT decisions, firms may be able to achieve an “embedded” decision rights structure. Such a structure might be able to draw on the efficiency and coordination benefits of centralization, while still allowing for the localization and flexibility benefits of decentralization (A. E. Brown & Grant, 2005; Sambamurthy & Zmud, 1999; Weill & Ross, 2004). However, this is merely a conjectural interpretation of the crude results, and such an idea would have to be further examined for its merit.

The second hypothesis stated that having distinct IT and cybersecurity executives would improve the cyber risk management maturity level. However, this hypothesis was not supported in the data, which is surprising given that both the academic literature and the practitioners within the field point to the importance of dedicated and competent IT and cybersecurity leadership (Deloitte, 2019a; Karanja, 2017; Preston et al., 2008). According to the literature, leadership characterized by IT competence and power to champion the IT strategy should improve the role and performance of IT in the organization (Bassellier et al., 2003; Bottger, 2008). This led to the hypothesis that having distinct, dedicated IT and cybersecurity leaders on the executive team would create a greater awareness and prioritization of these domains, thus yielding greater cybersecurity program maturity (Hooper & McKissack, 2016; Karanja, 2017). However, the results of the survey did not support this prediction. It should be noted first that one reason this hypothesis was not supported could be the small sample, which makes it difficult to trust the non-significant results, as previously explained. However, another explanation could be that a lack of these executives does not preclude the existence of other leadership structures with a similar effect. This study only examined such leadership structures at the executive level, but a more nuanced perspective on the role of leadership on the cyber risk management maturity may be required. For instance, it may be that the executive perspective on leadership encourages a managerial orthodoxy that is detrimental to the strategic development of IT and cybersecurity (King, 2011) and that these areas would benefit from distributed leadership structures instead (Mehra et al., 2006). Once again, such an interpretation of the results would have to be investigated in a future study.

The third hypothesis proposed that a divisional allocation of human and financial resources would improve cyber risk management maturity. Based on the literature review, resource allocation was described in terms of either financial or human resources, i.e. assets or capabilities (Aral & Weill, 2007; Grant, 1991). The results of the regression analysis indicated that while financial resources for both IT and cybersecurity are significant predictors of cybersecurity maturity, human resources are not. In the literature, skilled cyber personnel is reported to be one of the most important factors in a strong cyber defense (Dawson & Thomson, 2018; Diamantopoulou et al., 2017; Y. A. Wu & Saunders, 2005), but the findings of this study do not indicate that centralization or decentralization of the personnel plays a part in this importance. However, as hypothesized, IT financial resource decentralization is found to be a significant predictor of cyber risk management maturity. Allocating financial resources for IT throughout the functional units may create innovation and flexibility benefits by enabling the decentralized staff to tailor investments to the individual departments (Jarzabkowski, 2002; Liu et al., 2018). Through these investments, organizations can pursue the execution of strategic IT goals at the divisional level, such as infrastructure capability and productivity (Huang et al., 2006; Turedi & Zhu, 2019). Contrary to the hypothesis, the cybersecurity financial resources were found to be a significant predictor of cybersecurity maturity when they are centralized. This finding replicates the pattern from decision rights allocation, where the IT and cybersecurity dimensions were also inversely related to cybersecurity program maturity. In terms of affecting cybersecurity maturity, it is possible that cybersecurity investments benefit more from the standardization and efficiency outcomes associated with centralization than decentralization outcomes such as flexibility and responsiveness (Aral & Weill, 2007). When the cybersecurity function faces an adversary, adaptability and a fast response can be essential qualities, but it may be that this is not reflected in the maturity of the cyber risk management program itself. Further studies into the impact of cybersecurity investments on both cyber risk management programs and other cybersecurity outcomes are needed to better understand this relationship.

The hypothesis that interdepartmental communication intensity – the combination of communication frequency and variety (Hansen et al., 2005) – would predict a greater cyber risk management program maturity through norm-building and cyber awareness was not supported in the data. One explanation could be that interdepartmental communication does not influence the program maturity in itself as much as it influences program execution. Accordingly, while the communication intensity between departments may still impact the cyber culture and compliance among employees, this might not translate directly to the cyber risk management program, which focuses on formalized procedures and activities. The cyber-mature organization might still be characterized by a high degree of communication between functional departments, but the relationship with the cybersecurity program could be indirect and thus, communication intensity might be harder to use as a predictor for program maturity. Rather, communication may be more closely tied to an outcome such as the ‘training and culture’ component in the CAT (FFIEC, 2015b). Accordingly, future studies might have to find another measurement for cybersecurity success than the risk management program maturity in order to assess the impact of interdepartmental communication.

The fifth and last hypothesis stated that an outsourcing strategy based on minimal outsourcing would allow the organization to maintain more in-house control and talent development (Dahlberg & Lahdelma, 2007), which would consequently lead to a higher cyber risk management maturity level. This hypothesis was supported for IT, but not for cybersecurity. Retaining IT competence in-house may confer an improved capacity to perform certain cyber risk management processes, such as cybersecurity controls and implementation success (S. E. Chang & Ho, 2006; Tu & Yuan, 2014). Losing capabilities can result in a dependence on the external provider that reduces the internal understanding of the outsourced processes (Handley, 2012). While such a dependence is not necessarily bad for non-core business activities, in the case of cyber risk management capability, it may put the organization at a disadvantage, for example when it comes to the continuous assessment of IT asset risk (FFIEC, 2017a). It is surprising that cybersecurity outsourcing was not found to be a significant predictor of cybersecurity maturity at any level. It may be that a lack of cybersecurity competence does not handicap the organization as much as IT capability loss does, resulting in a lesser effect on the cyber risk management program maturity. Another possible explanation is that cybersecurity competences in general are still fairly low ((ISC)2, 2019; Furnell & Bishop, 2020; McAfee, 2016), making the organizational consequences of losing these capabilities more challenging to quantify at this point in time.

In conclusion, the study illuminates interesting – and unexpected – points about the relationship between the IT organization and cyber risk management maturity, as well as the effect of the separation between IT and cybersecurity activities on this relationship. That some of the hypotheses were unsupported in the data is unfortunate but given the small sample size used for the study, it is not surprising. These non-significant results should be interpreted with caution, as a survey with a larger sample might yield more significant results. The most surprising finding is perhaps that the financial resource allocation and decision rights allocation were found to be related in an inverse configuration for the IT and cybersecurity domains. For IT functions, cyber program maturity was associated with a top-down approach involving decision-making power at the corporate level and strategic execution through investments at the divisional level. Cybersecurity functions seem to impact the program maturity through a bottom-up approach instead, where divisional units decide the strategic direction, and then a corporate unit allocates investment resources. While hypothesizing about such an inverse relationship was not possible based on the existing literature, it illustrates the need for greater distinction between IT and cybersecurity both in the academic literature and in practice. The findings on IT outsourcing indicate that these complex internal structures should be encased by a rigid extraorganizational boundary marked by little outsourcing, thus retaining IT competence in-house.

Additionally, the conclusion to the research question that was asked at the outset of this paper must be that the impact of the IT organization on the cyber risk management program is multifaceted. IT and cybersecurity functions appear to differ fundamentally, apparently benefitting from different design configurations within the IT organization. These findings support the notion that IT and cybersecurity activities and objectives have diverged to the point of functional separation (Deloitte, 2019b; Doan, 2019; Hooper & McKissack, 2016; Karanja, 2017). Furthermore, the results provide actionable insights that can be used by business leaders to improve cyber risk management through organizational design. The next and final section will suggest some future courses of action for researchers and practitioners based on the results of the study.

5.2. Suggestions for research and practice

This study contributes to the academic literature by providing empirical evidence for the IT organization’s impact on cyber risk management program maturity. I find that IT decision rights centralization, IT financial resource decentralization, and a minimal degree of IT outsourcing all predict a high cybersecurity program maturity level. Furthermore, contrary to the hypotheses, cyber decision rights decentralization and cyber financial resource source centralization were also predictors of cybersecurity maturity. Future research might examine this relationship between cybersecurity and IT in more depth, for instance by examining whether this inverse effect is also found for other organizational design elements or other cybersecurity outcomes. Researchers could also build on the insights from this study by delving into the way mechanisms within the predictor constructs impact cybersecurity. For example, researchers could investigate the manner in which specific mechanisms within a centralized IT decision rights structure, such as greater procedural standardization and coordination, affect the maturity of a cybersecurity program. Another possible direction could be to examine the differences in the IT organization's influence on cybersecurity program development, implementation, and evaluation, thus taking a stepwise approach to the cyber risk program itself. The other domains and components within the FFIEC's CAT – for example cybersecurity controls or training and culture – may also be used as outcome variables in order to contribute to the holistic understanding of organizational cybersecurity management. Such studies would be able to shed more light on the effect that specific IT organization design elements have on the various stages and elements of the cybersecurity program. Furthermore, due to the small sample size used for this study, the non-significant results from the regression model may not be trustworthy, and an examination of these variables with a larger sample might yield other results. Additionally, this study was conducted within a Danish context and was distributed to firms based in Denmark, meaning that studies carried out in different countries could produce different results. Studies performed with larger sample sizes and in different cultural and economic contexts would also contribute to a more generalizable understanding of cybersecurity management.

The results of this thesis also contribute to practitioners' ability to make informed decisions about their IT organization and cyber risk management programs. It should be noted again that this study was not meant to produce a blueprint for an IT organization that produces a guaranteed stronger cybersecurity program. Instead, the study enables practitioners to consider these findings in the light of their own strategy. While a centralized IT decision rights structure might generally yield a greater program maturity, that does not mean that a decentralized structure cannot yield good results, nor that a centralized structure always will. However, it does mean that the relative strengths of the centralized governance model should be considered by organizations with a decentralized structure. For example, companies with a decentralized IT decision rights allocation should take extra care to mitigate the threats of shadow IT and user autonomy, because these are risk management concerns that are more inherently covered by a centralized structure. Similarly, companies with a high degree of IT outsourcing may still be able to achieve the cybersecurity maturity level that is appropriate for their organization. However, the findings of this study suggest that these organizations should be aware of the potential pitfalls of extensive outsourcing, including for example capability loss. Practitioners should also note the differences between IT and cybersecurity components in the IT organization. Since there appears to be an inverse relationship between these two components in the findings of this study, practitioners should integrate this perspective in the design of their IT organization and avoid lumping the two together unless there is a good reason to do so.

6. References

(ISC)2. (2019). Strategies for Building and Growing Strong Cybersecurity Teams. *(ISC)2 Cybersecurity Workforce Study*, *2019*, 1–37.

Accenture. (2019). *Securing the Digital Economy: Reinventing the Internet for Trust*. https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy

Aghion, P., Bloom, N., Blundell, R., Griffith, R., & Howitt, P. (2005). Competition and Innovation: An Inverted-U Relationship. *The Quarterly Journal of Economics*, *120*(2), 701–728. http://www.jstor.org/stable/25098750

Ahmad, F., & Karim, M. (2019). Impacts of knowledge sharing: a review and directions for future research. *Journal of Workplace Learning*, *31*(3), 207–230. https://doi.org/10.1108/JWL-07-2018-0096

Akinwande, M. O., Dikko, H. G., & Samson, A. (2015). Variance Inflation Factor: As a Condition for the Inclusion of Suppressor Variable(s) in Regression Analysis. *Open Journal of Statistics*, *05*(07), 754–767. https://doi.org/10.4236/ojs.2015.57075

Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Determining a Structure for the Chief Information Security Officer (CISO) Organization. *Carnegie Mellon SEI*, *September*, 48. https://doi.org/10.13140/RG.2.1.1242.6967

Alwin, D. F., & Krosnick, J. A. (1991). The Reliability of Survey Attitude Measurement. *Sociological Methods & Research*, *20*(1), 139–181. https://doi.org/10.1177/0049124191020001005

Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance: How resource allocations and organizational differences explain performance variation. *Organization Science*, *18*(5), 763–780. https://doi.org/10.1287/orsc.1070.0306

Askehave, I., & Norlyk, B. (2006). *Meanings and messages: Intercultural business communication*. Academia.

Atif, A., Richards, D., & Bilgin, A. (2012). Estimating non-response bias in a web-based survey of technology acceptance: A case study of unit guide information systems. *ACIS 2012: Proceedings of the 23rd Australasian Conference on Information Systems*.

Bakhshi, T. (2018). Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. *Proceedings - 2017 13th International Conference on Emerging Technologies, ICET2017, 2018-Janua*, 1–6. https://doi.org/10.1109/ICET.2017.8281653

Banker, R. D., Hu, N., Pavlou, P. A., & Luftman, J. (2011). CIO reporting structure, strategic positioning, and firm performance. *MIS Quarterly: Management Information Systems*, *35*(2), 487–504. https://doi.org/10.2307/23044053

Bassellier, G., Benbasat, I., & Reich, B. H. (2003). The Influence of Business Managers' IT Competence on Championing IT. *Information Systems Research*, *14*(4), 317–336. https://doi.org/10.1287/isre.14.4.317.24899

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management and Computer Security*, *13*(3), 189–202. https://doi.org/10.1108/09685220510602013

Berry, W. D. (1993). *Understanding Regression Assumptions*. SAGE Publications, Inc. https://doi.org/10.4135/9781412986427

Bottger, P. (2008). *Leading in the Top Team: The CXO Challenge*. Cambridge University Press. https://doi.org/10.1017/CBO9780511497636

Bowen, P. L., Cheung, M. Y. D., & Rohde, F. H. (2007). Enhancing IT governance practices: A model and case study of an organization's efforts. *International Journal of Accounting Information Systems*, *8*(3), 191–221. https://doi.org/10.1016/j.accinf.2007.07.002

Brown, A. E., & Grant, G. G. (2005). Framing the Frameworks: A Review of IT Governance Research. *Communications of the Association for Information Systems*, *15*(May). https://doi.org/10.17705/1cais.01538

Brown, C. V. (1999). Horizontal mechanisms under differing is organization contexts. *MIS Quarterly: Management Information Systems*, *23*(3), 421–454. https://doi.org/10.2307/249470

Brown, C. V., & Magill, S. L. (1994). Alignment of the IS functions with the enterprise: Toward a model of antecedents. *MIS Quarterly: Management Information Systems*, *18*(4), 371–395. https://doi.org/10.2307/249521

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys and Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Burgess, C. (2014, August 19). *CISO vs. CRO: What's the Difference?* Security Intelligence. https://securityintelligence.com/ciso-vs-cro-whats-the-difference/

Center for Cybersecurity. (2019). *Trusselsvurdering: Cybertruslen mod Danmark*. www.cfcs.dk

Centric Digital. (2017, September 6). *Too Many Chiefs? How CDOs, CIOs, CTOs, and CMOs Must Work Together | Centric Digital*. https://centricdigital.com/blog/digital-strategy/cdos-cio-cto-cmo/

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors’ behavior. *Decision Support Systems*, *50*(4), 651–661. https://doi.org/10.1016/j.dss.2010.08.017

Chang, K. C., & Wang, C. P. (2011). Information systems resources and information security. *Information Systems Frontiers*, *13*(4), 579–593. https://doi.org/10.1007/s10796-010-9232-6

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management and Data Systems*, *106*(3), 345–361. https://doi.org/10.1108/02635570610653498

Chen, J. L. (2012). The synergistic effects of IT-enabled resources on organizational capabilities and firm performance. *Information and Management*, *49*(3–4), 142–150. https://doi.org/10.1016/j.im.2012.01.005

Chua, C. E. H., Storey, V. C., & Chen, L. (2014). Central IT or Shadow IT? Factors shaping users’ decision to go rogue with IT. *35th International Conference on Information Systems “Building a Better World Through Information Systems”, ICIS 2014*.

Cisco. (2019). *Cisco Cybersecurity Series 2019: Threats of the Year* (Issue December).

Cook, R. D., & Weisberg, S. (1982). Residuals and Influence in Regression. In D. R. Cox & D. V. Hinkley (Eds.), *Journal of the Royal Statistical Society. Series A (General)*. Chapman and Hall. https://doi.org/10.2307/2981746

Coradi, A., Heinzen, M., & Boutellier, R. (2015). Designing workspaces for cross-functional knowledge-sharing in R&D: The “co-location pilot” of novartis. *Journal of Knowledge Management*, *19*(2), 236–256. https://doi.org/10.1108/JKM-06-2014-0234

Crawford, J., Leonard, L. N. k., & Jones, K. (2011). The human resource’s influence in shaping IT competence. *Industrial Management & Data Systems*, *111*(2), 164–183. https://doi.org/10.1108/02635571111115128

Crawford, S. D., Couper, M. P., & Lamias, M. J. (2001). Web Surveys: Perceptions of Burden. *Social Science Computer Review*, *19*(2), 146–162. https://doi.org/10.1177/089443930201900202

Dahlberg, T., & Lahdelma, P. (2007). IT governance maturity and IT outsourcing degree: An exploratory study. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *June*. https://doi.org/10.1109/HICSS.2007.306

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*(JUN), 1–12. https://doi.org/10.3389/fpsyg.2018.00744

Deloitte. (2018). *2018 global CIO survey*. https://www2.deloitte.com/insights/us/en/topics/leadership/global-cio-survey.html

Deloitte. (2019a). *Cyber Risk Landscape Report 2019*.

Deloitte. (2019b). *The future of cyber survey 2019*.

Dessne, K. (2013). Formality and Informality: Learning in Relationships in an Organisation. *International Journal of Knowledge Management*, *9*(4), 17–32.

https://doi.org/10.4018/ijkm.2013100102

Diamantopoulou, V., Loukis, E., Tsohou, A., & Gritzalis, S. (2017). Does the development of information systems resources lead to the development of information security resources? An empirical investigation. *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, *2017-Augus*, 1–10.

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method* (4. ed.).

Dillman, D. A., Tortora, R. D., & Bowker, D. (1998). Principles for Constructing Web Surveys. *Joint Meetings of the American Statistical Association*, *December*, 1–16. https://doi.org/10.1017/CBO9781107415324.004

Ditlevsen, M. G. (2007). *Sprog på arbejde: Kommunikation i faglige tekster* (2. ed.).

Div, L. (2015). *Why It's Worth Divorcing Information Security From IT*. https://www.forbes.com/sites/frontline/2015/06/22/why-its-worth-divorcing-information-security-from-it/

Doan, M. (2019). *Companies Need to Rethink What Cybersecurity Leadership Is*. https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is

ENISA. (2017). *Cyber security culture in organisations* (Issue November). https://doi.org/10.2824/10543

ENISA. (2019). ENISA Threat Landscape Report 2018. In *European Union Agency For Network and Information Security* (Issue January). https://doi.org/10.2824/622757

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research*, *15*(2), 195–219. https://doi.org/10.1108/10662240510590360

EY. (2019). *EY Global Information Security Survey 2018-19*. https://www.ey.com/en_gl/advisory/global-information-security-survey-2018-2019

Feng, N., Chen, Y., Feng, H., Li, D., & Li, M. (2019). To outsource or not: The impact of information leakage risk on information security strategy. *Information and Management,* 103215. https://doi.org/10.1016/j.im.2019.103215

FFIEC. (2015a). *Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework* (Issue June). https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf

FFIEC. (2015b). *Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors* (Issue June).

FFIEC. (2017a). *Cybersecurity Assessment Tool: Cybersecurity Maturity*. *May*. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Cybersecurity_Maturity.pdf

FFIEC. (2017b). *FFIEC Cybersecurity Assessment Tool: User's Guide* (Issue May).

Field, A., Miles, J., & Field, Z. (2012). *Discovering statistics using R*.

Frigotto, M. L., & Rossi, A. (2012). Diversity and Communication in Teams: Improving Problem-Solving or Creating Confusion? *Group Decision and Negotiation*, *21*(6), 791–820. https://doi.org/10.1007/s10726-011-9250-x

Fruhlinger, J. (2018, May 8). *What is a CSO? Understanding the critical chief security officer role | CSO Online*. CSO. https://www.csoonline.com/article/2122505/what-is-a-cso-understanding-the-critical-chief-security-officer-role.html

Furnell, S., & Bishop, M. (2020). Addressing cyber security skills: the spectrum, not the silo. *Computer Fraud and Security*. https://doi.org/10.1016/S1361-3723(20)30017-8

Gaudenzi, B., & Siciliano, G. (2017). Just do it: Managing IT and Cyber Risks to Protect the Value Creation. *Journal of Promotion Management*, *23*(3), 372–385. https://doi.org/10.1080/10496491.2017.1294875

Ghobadi, S., & D'Ambra, J. (2012). Knowledge sharing in cross-functional teams: A coopetitive model. *Journal of Knowledge Management*, *16*(2), 285–301. https://doi.org/10.1108/13673271211218889

Gladwell, M. (2008). *Outliers: The Story of Success*.

Goodman, L. A. (2011). Comment: On Respondent-Driven Sampling and Snowball Sampling in Hard-to-Reach Populations and Snowball Sampling Not in Hard-to-Reach Populations. *Sociological Methodology*, *41*(1), 347–353. https://doi.org/10.1111/j.1467-9531.2011.01242.x

Granello, D. H., & Wheaton, J. E. (2004). Online data collection: Strategies for research. *Journal of Counseling and Development*, *82*(4), 387–393. https://doi.org/10.1002/j.1556-6678.2004.tb00325.x

Grant, R. M. (1991). The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation. *California Management Review*, *33*(3), 114–135. https://doi.org/10.2307/41166664

Grant, R. M. (1996). Towards a knowledge-based theory of the firm. *Strategic Management Journal*, *17*, 5–9.

Gu, B., Xue, L., & Ray, G. (2008). IT Governance and IT Investment Performance: An Empirical Analysis. *McCombs Research Paper Series, July*. https://doi.org/10.2139/ssrn.1145102

Gupta, A., & Zhdanov, D. (2012). Growth and sustainability of managed security services networks: An economic perspective. *MIS Quarterly: Management Information Systems*, *36*(4). https://doi.org/10.2307/41703500

Handley, S. M. (2012). The perilous effects of capability loss on outsourcing management and performance. *Journal of Operations Management*, *30*(1–2), 152–165. https://doi.org/10.1016/j.jom.2011.10.003

Hansen, M. T. (2002). Knowledge networks: Explaining effective knowledge sharing in multiunit companies. *Organization Science*, *13*(3), 232–248. https://doi.org/10.1287/orsc.13.3.232.2771

Hansen, M. T., Mors, M. L., & Løvås, B. (2005). Knowledge Sharing in Organizations: Multiple Networks, Multiple Phases. *The Academy of Management Journal*, *48*(5), 776–793. https://doi.org/10.5465/AMJ.2005.18803922

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Hitt, L. M., & Brynjolfsson, E. (1997). Information Technology and Internal Firm Organization: An Exploratory Analysis. *Journal of Management Information Systems*, *14*(2), 81–101. https://doi.org/10.1080/07421222.1997.11518166

Holcomb, T. R., & Hitt, M. A. (2007). Toward a model of strategic outsourcing. *Journal of Operations Management*, *25*(2), 464–481. https://doi.org/10.1016/j.jom.2006.05.003

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585–591. https://doi.org/10.1016/j.bushor.2016.07.004

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282–300. https://doi.org/10.1287/isre.2015.0569

Huang, S. M., Ou, C. S., Chen, C. M., & Lin, B. (2006). An empirical study of relationship between IT investment and firm performance: A resource-based perspective. *European Journal of Operational Research*, *173*(3), 984–999. https://doi.org/10.1016/j.ejor.2005.06.013

IBM Security. (2019). *Cost of a data breach report*. https://www.ibm.com/downloads/cas/ZBZLY7KL

Jarzabkowski, P. (2002). Centralised or Decentralised? Strategic Implications of Resource Allocation Models. *Higher Education Quarterly*, *56*(1), 5–32. https://doi.org/10.1111/1468-2273.00200

Jennings, D. (2002). Strategic sourcing: benefits, problems and a contextual model. *Management Decision*, *40*(1), 26–34. https://doi.org/10.1108/00251740210413334

Jensen, D. (2019). *Demant efter hackerangreb: Situationen er nu normaliseret - men det kommer til at koste dyrt*. https://www.computerworld.dk/art/249703/demant-efter-hackerangreb-situationen-er-nu-normaliseret-men-det-kommer-til-at-koste-dyrt

Johnson, A. M., & Lederer, A. L. (2003). Two Predictors of CEO/CIO Convergence. *Proceedings of the ACM SIGMIS CPR Conference*, 162–167. https://doi.org/10.1145/761849.761881

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information and Computer Security*, *25*(3), 300–329. https://doi.org/10.1108/ICS-02-2016-0013

Kearns, G. S., & Lederer, A. L. (2003). A resource-based view of strategic IT alignment: How knowledge sharing creates competitive advantage. *Decision Sciences*, *34*(1), 1–29. https://doi.org/10.1111/1540-5915.02289

Kildebogaard, J. (2015, May 5). Lammet af hackerangreb: »Tro ikke, at det ikke sker for dig«. *Finans*. https://finans.dk/live/it/ECE7680572/Lammet-af-hackerangreb-»Tro-ikke-at-det-ikke-sker-for-dig«/?ctxref=ext

King, J. L. (2011). CIO: Concept is Over. *Journal of Information Technology*, *26*(2), 129–138. https://doi.org/10.1057/jit.2011.4

Klotz, S., Kopper, A., Westner, M., & Strahringer, S. (2019). Causing factors, outcomes, and governance of shadow IT and business-managed IT: A systematic literature review. *International Journal of Information Systems and Project Management*, *7*(1), 15–43. https://doi.org/10.12821/ijispm070102

Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift Fur Die Gesamte Versicherungswissenschaft*, *104*(5), 615–634. https://doi.org/10.1007/s12297-015-0316-8

KPMG. (2019). *2019 Global CEO Outlook: Nordic Executive Summary* (Issue June). https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/kpmg-global-ceo-outlook-2019.pdf

Kreuter, F., Presser, S., & Tourangeau, R. (2008). Social Desirability Bias in CATI, IVR, and Web Surveys: The Effects of Mode and Question Sensitivity. *Public Opinion Quarterly*, *72*(5), 847–865. https://doi.org/10.1093/poq

Kroes, J. R., & Ghosh, S. (2010). Outsourcing congruence with competitive priorities: Impact on supply chain and firm performance. *Journal of Operations Management*, *28*(2), 124–143. https://doi.org/10.1016/j.jom.2009.09.004

Kruchten, P., Nord, R. L., & Ozkaya, I. (2012). Technical Debt: From Metaphor to Theory and Practice. *IEEE Software*, 18–22.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263

Lacity, M. C., Khan, S. A., & Yan, A. (2016). Review of the empirical business services sourcing literature: An update and future directions ra. *Journal of Information Technology*, *31*(3), 269–328. https://doi.org/10.1057/jit.2016.2

Lacity, M. C., Khan, S., Yan, A., & Willcocks, L. P. (2010). A review of the IT outsourcing empirical literature and future research directions. *Journal of Information Technology*, *25*(4), 395–433. https://doi.org/10.1057/jit.2010.21

Larsen, H. (2020, February 28). *Alle taler om cybersikkerhed - men det vigtige er og bliver stadig informations-sikkerhed*. Computerworld. https://www.computerworld.dk/art/250914/alle-taler-om-cybersikkerhed-men-det-vigtige-er-og-bliver-stadig-informations-sikkerhed

Lee, C. H., Geng, X., & Raghunathan, S. (2013). Contracting information security in the presence of double moral hazard. *Information Systems Research*, *24*(2), 295–311. https://doi.org/10.1287/isre.1120.0447

Lee, J. N., Miranda, S. M., & Kim, Y. M. (2004). IT outsourcing strategies: Universalistic, contingency, and configurational explanations of success. *Information Systems Research*, *15*(2), 110–131. https://doi.org/10.1287/isre.1040.0013

Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, *33*(2), 250–257. https://doi.org/10.1016/j.giq.2016.01.012

Liu, C. W., Huang, P., & Lucas, H. C. (2018). IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education. *ICIS 2017: Transforming Society with Digital Innovation*, 0–18.

Lobel, M. (2015, February 3). *Cybersecurity: keeping the 'crown jewels' safe online is everyone's business - CEO insights*. PwC CEO Insights. https://pwc.blogs.com/ceoinsights/2015/02/cybersecurity-keeping-the-crown-jewels-safe-online-is-everyones-business-.html

Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. *International Journal of Accounting Information Systems*, *15*(1), 66–81. https://doi.org/10.1016/j.accinf.2013.02.001

Lund, M., & Fastrup, N. (2014). *Stor dansk virksomhed udsat for cyberspionage*. https://www.dr.dk/nyheder/penge/stor-dansk-virksomhed-udsat-cyberspionage

Magnusson, J., Juiz, C., Gómez, B., & Bermejo, B. (2018). Governing technology debt: Beyond technical debt. *Proceedings - International Conference on Software Engineering*, 76–84. https://doi.org/10.1145/3194164.3194169

Marchand, D. A. (2008). The Chief Information Officer – Achieving credibility, relevance and business impact. In P. Bottger (Ed.), *Leading in the Top Team: The CXO Challenge* (pp. 204–222). Cambridge University Press. https://doi.org/DOI: 10.1017/CBO9780511497636.011

Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, *21*(3), 435–452. https://doi.org/10.1111/rmir.12109

Marsh, S. (2018). *US joins UK in blaming Russia for NotPetya cyber-attack*. https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine

Mårtensson, A. (2006). A resource allocation matrix approach to IT management. *Information Technology and Management*, *7*(1), 21–34. https://doi.org/10.1007/s10799-006-5727-8

McAfee. (2016). *Hacking the skills shortage*. http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

McKay, D. S., & Ellis, T. J. (2015). Measuring knowledge enablers and project success in IT organizations. *International Journal of Knowledge Management*, *11*(1), 66–83. https://doi.org/10.4018/IJKM.2015010104

Mehra, A., Smith, B. R., Dixon, A. L., & Robertson, B. (2006). Distributed leadership in teams: The network of leadership perceptions and team performance. *Leadership Quarterly*, *17*(3), 232–245. https://doi.org/10.1016/j.leaqua.2006.02.003

Mirzaei-Fard, M., & Moltke, H. (2020, March 5). *ISS ramt af hackerangreb: Formålet var afpresning*. DR Nyheder. https://www.dr.dk/nyheder/penge/iss-ramt-af-hackerangreb-formaalet-var-afpresning

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*. https://doi.org/10.1016/j.techsoc.2019.03.005

Niranjan, T. T., Saxena, K. B. C., & Bharadwaj, S. S. (2007). Process-oriented taxonomy of BPOs: an exploratory study. *Business Process Management Journal*, *13*(4), 588–606. https://doi.org/10.1108/14637150710763595

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*.

O’Brien, H. L., & McCay-Peet, L. (2017). Asking “good” questions: Questionnaire design and analysis in interactive information retrieval research. *CHIIR 2017 - Proceedings of the 2017 Conference Human Information Interaction and Retrieval*, 27–36. https://doi.org/10.1145/3020165.3020167

OECD. (2017). *Digital Economy Outlook 2017*. OECD. https://doi.org/10.1787/9789264276284-en

Oltsik, J. (2019, January 10). *The Cybersecurity Skills Shortage Is Getting Worse*. ESG. https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse

Olwig, M. F., & Schou, J. A. (2020). *Saving the world by doing business? A background paper on the role of the private sector in Danish aid* (CBDS Working Paper Series).

Ong, A. D., & Weiss, D. J. (2000). The Impact of Anonymity on Responses to Sensitive Questions. *Journal of Applied Social Psychology*, *30*(8), 1691–1708. https://doi.org/10.1111/j.1559-1816.2000.tb02462.x

Overby, S. (2018). *What’s The Best Reporting Structure for the CISO?* Security Roundtable. https://www.securityroundtable.org/whats-the-best-reporting-structure-for-the-ciso/

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129. https://doi.org/10.1177/1555343415575152

Peppard, J. (2018). Rethinking the concept of the IS organization. *Information Systems Journal*, *28*(1), 76–103. https://doi.org/10.1111/isj.12122

Presskorn-Thygesen, T. (2012). Samfundsvidenskabelige paradigmer: Fire grundlæggende metodiske tendenser i moderne samfundsvidenskab. In *Samfundsvidenskabelige analysemetoder, Claus Nygaard (red.)*.

Preston, D. S., Chen, D., & Leidner, D. E. (2008). Examining the antecedents and consequences of CIO strategic decision-making authority: An empirical study. *Decision Sciences*, *39*(4), 605–642. https://doi.org/10.1111/j.1540-5915.2008.00206.x

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly: Management Information Systems*, *34*(4), 757–778. https://doi.org/10.2307/25750704

PwC. (2019). Cybercrime Survey 2018. *Cybercrime Survey*.

Quass, L. (2017). *Hackerangreb koster Mærsk milliardbeløb*. https://www.dr.dk/nyheder/penge/hackerangreb-koster-maersk-milliardbeloeb

R Core Team. (2020). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing. http://www.r-project.org/

Riber-Sellebjerg, T., & Okholm, M. M. (2018, September 18). Afsløring: 86 kommuner hacket. *Ekstra Bladet*. https://ekstrabladet.dk/nyheder/samfund/article7221664.ece

Richter, W., Bossert, O., & Weinberg, A. (2015). Protecting the enterprise with cybersecure IT architecture. *McKinsey & Company*, 1–6.

Rodewald, G. (2005). Aligning information security investments with a firm's risk tolerance. *Proceedings of the 2005 Information Security Curriculum Development Conference, InfoSecCD '05*, 139–141. https://doi.org/10.1145/1107622.1107654

RStudio Team. (2019). *RStudio: Integrated Development for R* (1.2.5033). RStudio, Inc. http://www.rstudio.com/

Sadler, G. R., Lee, H.-C., Lim, R. S.-H., & Fullerton, J. (2010). Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing & Health Sciences*, *12*(3), 369–374. https://doi.org/10.1111/j.1442-2018.2010.00541.x

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly: Management Information Systems*, *23*(2), 261–290. https://doi.org/10.2307/249754

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7. ed.).

Saxena, K. B. C., & Bharadwaj, S. S. (2009). Managing business processes through outsourcing: A strategic partnering perspective. *Business Process Management Journal*, *15*(5), 687–715. https://doi.org/10.1108/14637150910987919

Schlosser, F., Beimborn, D., Weitzel, T., & Wagner, H. T. (2015). Achieving social alignment between business and IT - An empirical evaluation of the efficacy of IT governance mechanisms. *Journal of Information Technology*, *30*(2), 119–135. https://doi.org/10.1057/jit.2015.2

Simonsson, M., Johnson, P., & Ekstedt, M. (2010). The effect of IT governance maturity on IT governance performance. *Information Systems Management*, *27*(1), 10–24. https://doi.org/10.1080/10580530903455106

Snow, C. C., & Hambrick, D. C. (1980). Measuring Organizational Strategies: Some Theoretical and Methodological Problems. *The Academy of Management Review*, *5*(4), 527. https://doi.org/10.2307/257458

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, *75*, 49–62. https://doi.org/10.1016/j.dss.2015.04.011

Stewart, G., & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management and Computer Security*, *20*(1), 29–38. https://doi.org/10.1108/09685221211219182

Stubager, R., & Sønderskov, K. M. (2011). Forudsætninger for Lineær Regression og Variansanalyse. *Aarhus Universitet*, 1–50.

Studenmund, A. H., & Cassidy, H. J. (1987). *Using econometrics: A practical guide*. Little Brown.

Stutely, R. (2003). *Numbers guide: The essentials of business numeracy* (5th ed.). Economist.

Tenable Network Security. (2016). *Trends in Security Framework Adoption Trends in Security Framework Adoption*. *March*. http://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901

Ting-Toomey, S. (1999). *Communicating across cultures*. The Guilford Press.

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. *20th Americas Conference on Information Systems, AMCIS 2014*, 1–13.

Turedi, S., & Zhu, H. (2019). How to generate more value from IT: The interplay of it investment, decision making structure, and senior management involvement in IT governance. *Communications of the Association for Information Systems*, *44*(1), 511–536. https://doi.org/10.17705/1CAIS.04426

UN. (2018). *E-Government Survey 2018*. https://doi.org/e-ISBN: 978-92-1-055353-7

Valorinta, M. (2011). IT Alignment and the Boundaries of the IT Function. *Journal of Information Technology*, *26*(1), 46–59. https://doi.org/10.1057/jit.2010.28

Van Grembergen, W., & De Haes, S. (2004). IT governance and its mechanisms. *Information Systems Control Journal*, *1*. https://doi.org/10.1109/HICSS.2006.322

Van Selm, M., & Jankowski, N. W. (2006). Conducting online surveys. *Quality and Quantity*, *40*(3), 435–456. https://doi.org/10.1007/s11135-005-8081-8

Venkatraman, N. (1997). Beyond Outsourcing: Managing IT Resources as a Value Center. *Sloan Management Review*, *38*(3), 51–64.

Verizon. (2018). *2018 Data breach investigations report*. http://rp_data-breach-investigations-report-2013_en_xg.pdf

Weill, P., & Ross, J. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Review Press.

http://web.b.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzY3NTA3N19fQU41?sid=f1ef50c5-fced-437c-a3d7-3ab94088a3aa@pdc-v-sessmgr02&vid=0&format=EK&rid=1

Weill, P., & Ross, J. (2005). A matrixed approach to designing IT governance. *MIT Sloan Management Review*, *46*(2), 26–34.

Winkler, T. (2016a). *Interview Part 1: IT organization and governance at Chr. Hansen*. https://cbs.cloud.panopto.eu/Panopto/Pages/Viewer.aspx?id=69540873-daa2-4ad0-96c1-a87a00eb56ab

Winkler, T. (2016b). *How to Make a Business-Focused IT Strategy while Ensuring Operational Stability: Arla Foods* (pp. 95–104).

Winkler, T., & Brown, C. (2014). Organizing and Configuring the IT Function. *Computing Handbook, Third Edition*, 57-1-57–14. https://doi.org/10.1201/b16768-66

Wu, S. P.-J., Straub, D. W., & Liang, T.-P. (2015). How IT governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *MIS Quarterly*, *39*(2), 497–518.

Wu, Y. A., & Saunders, C. S. (2005). Decision making, IT governance, and information systems security. *Association for Information Systems - 11th Americas Conference on Information Systems, AMCIS 2005: A Conference on a Human Scale*, *7*, 3239–3247.

Xue, L., Ray, G., & Gu, B. (2011). Environmental uncertainty and IT infrastructure governance: A curvilinear relationship. *Information Systems Research*, *22*(2), 389–399. https://doi.org/10.1287/isre.1090.0269

Yan, T., & Tourangeau, R. (2008). Fast times and easy questions: The effects of age, experience and question complexity on web survey response times. *Applied Cognitive Psychology*, *22*(1), 51–68. https://doi.org/10.1002/acp.1331

Yaokumah, W., & Brown, S. (2015). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Law and Governance*, *9*(2). https://doi.org/10.15209/jbsge.v9i2.718

Young, R. F., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems*, *26*(1), 245–266. https://doi.org/10.17705/1cais.02613

Zhao, X., Xue, L., & Whinston, A. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems*, *30*(1), 123–152. https://doi.org/10.2753/MIS0742-1222300104

Zutshi, N. (2018). *The Evolving Relationship Between the CIO and CISO*. Security Roundtable. https://www.securityroundtable.org/the-evolving-relationship-between-the-cio-and-ciso/

Appendix A: Survey (English and Danish versions)

Note: This print contains only the survey text, not the formatting and layout.

Start of Block: Intro to survey

Q0
Survey on organizational IT and cybersecurity

Welcome and thank you for wanting to participate in this survey for my master's thesis!

The survey will ask a series of questions about the organization where you are employed, and how IT and cybersecurity functions are organized within this organization.

There will be a total of 21 questions, and it should take no more than **ten minutes** to complete the survey.

Please make sure to respond according to the as-is state of your organization, and not the desired target state.

At the end of the survey, you will have the option to request a summary of the research findings over e-mail if you want.

Emilie Kronhjem
MSc in Business Administration and E-business
Copenhagen Business School

This survey doesn't collect any personal data about its respondents.

Q0
Spørgeskema om IT og cybersikkerhed i organisationer

Velkommen, og tak fordi du vil deltage i denne undersøgelse til mit speciale!

Spørgeskemaet indeholder en række spørgsmål omkring den organisation du arbejder i, samt om hvordan IT og cybersikkerhed organiseres inden for denne organisation.

Der er 21 spørgsmål som i alt tager cirka **ti minutter** at besvare.

Du bedes besvare spørgsmålene i forhold til din organisations nuværende forhold og ikke i forhold til eventuelle målsætninger, som ligger ude i fremtiden.

Efter spørgeskemaet er udfyldt har du mulighed for at skrive dig op til at modtage et resumé af specialets resultatet via e-mail hvis du har lyst.

Emilie Kronhjem
Erhvervsøkonomi og e-business (cand.merc.ebuss)
Copenhagen Business School

Dette spørgeskema indsamler ikke nogen personlige data om dig som deltager.

End of Block: Intro to survey

Start of Block: Decision-making structures

Q6 The executive in charge of IT is...[4]

▼ Chief executive officer (CEO) ... Don't know

Q6 Direktøren, der har ansvar for IT er...

▼ Den administrerende direktør (CEO) ... Ved ikke

[4] The full range of options in the dropdown list is: CEO, CIO, CISO, CDO, CRO, CSO, CTO, COO, None of the above, Don’t know

Q7 Strategic decisions about IT are usually made... (select one)

○ At the corporate level

○ At the divisonal level

○ Partially at both levels

○ Don't know

Q7 Strategiske beslutninger omkring IT træffes typisk... (vælg en)

○ På koncernniveau

○ På afdelingsniveau

○ Delvist på begge niveauer

○ Ved ikke

Q8 The executive in charge of cybersecurity is...[5]

▼ Chief executive officer (CEO) ... Don't know

Q8 Direktøren, der har ansvar for cybersikkerhed er...

▼ Den administrerende direktør (CEO) ... Ved ikke

[5] The full range of options in the dropdown list is the same as in Q6.

Q9 Strategic decisions about cybersecurity are usually made... (select one)

○ At the corporate level

○ At the divisional level

○ Partially at both levels

○ Don't know

Q9 Strategiske beslutninger omkring cybersikkerhed træffes typisk... (vælg en)

○ På koncernniveau

○ På afdelingsniveau

○ Delvist på begge niveauer

○ Ved ikke

End of Block: Decision-making structures

Start of Block: Relations and collaboration

Q10 My interactions (work-related or otherwise) with coworkers outside my own department occur... (select one)

○ Daily

○ Weekly

○ Monthly

○ Rarer than monthly

○ Never

Q10 Jeg har omgang (arbejdsrelateret eller ej) med kollegaer uden for min egen afdeling... (vælg en)

○ Dagligt

○ Ugentligt

○ Månedligt

○ Sjældnere end månedligt

○ Aldrig

Q11 I typically engage with new coworkers from other departments through... (select all that apply)

□ Cross-functional teams

□ Formal projects

□ Job rotations

□ Workspace proximity

□ Social events at work

□ Internal networks

□ None of the above

Q11 Jeg møder typisk nye kollegaer fra andre afdelinger gennem... (vælg alle der passer)

□ Tværfaglige arbejdsgrupper

□ Formelt projektarbejde

□ Arbejdsrotationer

□ Kontorpladser, som er tæt på hinanden

□ Sociale arrangementer på arbejdet

□ Netværk på firmaets intranet

□ Ingen af de ovenstående

End of Block: Relations and collaboration

Start of Block: Resources and skills

Q12 Financial resources for IT are allocated primarily in... (select one)

○ A corporate IT department

○ The individual functional departments

○ Partially at both levels

○ Don't know

Q12 De finansielle ressourcer til IT er primært placeret ved... (vælg en)

○ Koncernens IT-afdeling

○ De individuelle afdelinger i virksomheden

○ Delvist på begge niveauer

○ Ved ikke

Q13 Technical skills for IT are allocated primarily in... (select one)

○ A corporate IT department

○ The individual functional departments

○ Partially at both levels

○ Don't know

Q13 De tekniske IT-færdigheder er primært placeret ved... (vælg en)

○ Koncernens IT-afdeling

○ De individuelle afdelinger i virksomheden

○ Delvist på begge niveauer

○ Ved ikke

Q14 Financial resources for cybersecurity are allocated primarily in... (select one)

○ A corporate IT department

○ The individual functional departments

○ Partially at both levels

○ Don't know

Q14 De finansielle ressourcer til cybersikkerhed er primært placeret ved... (vælg en)

○ Koncernens IT-afdeling

○ De individuelle afdelinger i virksomheden

○ Delvist på begge niveauer

○ Ved ikke

Q15 Technical skills for cybersecurity are allocated primarily in... (select one)

○ A corporate IT department

○ The individual functional departments

○ Partially at both levels

○ Don't know

Q15 De tekniske cybersikkerhedsfærdigheder er primært placeret ved... (vælg en)

○ Koncernens IT-afdeling

○ De individuelle afdelinger i virksomheden

○ Delvist på begge niveauer

○ Ved ikke

End of Block: Resources and skills

Start of Block: IT and cybersecurity sourcing

Q16
The extent of IT outsourcing in my firm is... (select one)

○ Minimal

○ Selective

○ Comprehensive

○ Don't know

Q16 Omfanget af IT-outsourcing i min virksomhed er... (vælg en)

○ Minimalt

○ Selektivt

○ Omfattende

○ Ved ikke

Q17 The extent of cybersecurity outsourcing in my firm is... (select one)

○ Minimal

○ Selective

○ Comprehensive

○ Don't know

Q17 Omfanget af outsourcing af cybersikkerhed i mit firma er... (vælg en)

○ Minimalt

○ Selektivt

○ Omfattende

○ Ved ikke

End of Block: IT and cybersecurity sourcing

Start of Block: Cyber risk

Q18 Our cybersecurity program addresses... (select all that apply)

□ Risk identification, mitigation, and monitoring

□ Non-technological impacts for the firm (e.g. regulatory)

□ Financial losses and other expenses

□ Risk appetite for individual business units

□ Threat trend identification and analysis

□ None of the above

□ Don't know

Q18 Vores handleplan for cybersikkerhed adresserer... (vælg alle der passer)

□ Identificering, begrænsning og overvågning af ricisi

□ Ikke-teknologiske konsekvenser for virksomheden (f.eks. lovgivningsmæssige)

□ Finansielle tab og andre omkostninger

□ Risikoappetit for individuelle afdelinger

□ Identificering og analyse af udviklinger i trusselsbilledet

□ Ingen af de ovenstående

□ Ved ikke

Q19 Cybersecurity program performance is assessed through... (select all that apply)

□ External reviews

□ Internal audits

□ Target performance metrics

□ None of the above

□ Don't know

Q19 Vores handleplan for cybersikkerhed evalueres på baggrund af... (vælg alle der passer)

□ Eksterne eftersyn

□ Interne revisioner

□ Målbaserede evalueringer

□ Ingen af de ovenstående

□ Ved ikke

Q20 Our cyber risk assessments address... (select all that apply)

- □ Risks posed to all firm information assets (for example software or computers)
- □ Management or employee practices
- □ Immediate changes to the firm's risk profile
- □ Threat predictions as preemptive security measures
- □ None of the above
- □ Don't know

Q20 Vores risikovurderinger for cybersikkerhed adresserer... (vælg alle der passer)

- □ Risici for alle informationsaktiver (f.eks. software eller computere)
- □ Ledelses- og medarbejderadfærd
- □ Umiddelbare ændringer i virksomhedens risikoprofil
- □ Trusselsprognoser til brug som forebyggende sikkerhedsinitiativer
- □ Ingen af de ovenstående
- □ Ved ikke

Q21
An independent audit is used to validate the adequacy of the firm's... (select all that apply)

□ Procedures to identify security gaps

□ Adaptation to an evolving threat landscape

□ Cybersecurity controls

□ Incident response program

□ Cyber risk appetite statement

□ None of the above

□ Don't know

Q21 Uvildige eftersyn bruges til at godkende virksomhedens... (vælg alle der passer)

□ Procedurer til at identificere sikkerhedshuller

□ Tilpasning til et foranderligt trusselsbillede

□ Cybersikkerhedskontroller

□ Handleplan for sikkerhedsbrud

□ Erklæring om risikoappetit for cybersikkerhed

□ Ingen af de ovenstående

□ Ved ikke

End of Block: Cyber risk

Start of Block: Demographic questions

Q1 What best describes your current position? (select one)

○ Executive

○ Manager

○ Employee

Q1 Hvad beskriver bedst din nuværende stilling? (vælg en)

○ Direktør

○ Leder

○ Medarbejder

Q2 What best describes your primary area of employment? (select all that apply)

□ Risk

□ Cybersecurity

□ Business strategy

□ IT

□ Other

Q2 Hvad beskriver bedst dit primære arbejdsområde? (vælg alle der passer)

□ Risiko

□ Cybersikkerhed

□ Ledelsesstrategi

□ IT

□ Andet

Q3 How many people are employed at your firm? (select one)

○ Fewer than 10

○ 10 to 49

○ 50 to 249

○ 250 to 1,000

○ More than 1,000

Q3 Hvor mange ansatte har din virksomhed? (vælg en)

○ Færre end 10

○ 10 til 49

○ 50 til 249

○ 250 til 1.000

○ Flere end 1.000

Q4 Which sector are you currently employed in?

○ Private sector

○ Public sector

○ Non-profit sector

Q4 Hvilken sektor er du ansat i?

○ Privat sektor

○ Offentlig sektor

○ Non-profit sektor

Q5 Does your organization currently follow an external accreditation standard for its cybersecurity, for example ISO 27000 series or equivalent?

○ Yes

○ No

○ Don't know

Q5 Følger din virksomhed en uvildig akkrediteringsstandard inden for cybersikkerhed, f.eks. ISO 27000-serien?

○ Ja

○ Nej

○ Ved ikke

End of Block: Demographic questions

Appendix B: R Markdown document

Demographics

```
#Q1 - Current position
surveyData$DGPOSexe <- grepl("1", surveyData$Q1)
surveyData$DGPOSman <- grepl("2", surveyData$Q1)
surveyData$DGPOSemp <- grepl("3", surveyData$Q1)
DGPOS <- surveyData$DGPOSexe * 3 + surveyData$DGPOSman * 2 + surveyData$DGPOSemp * 1
DGPOSf <- factor(surveyData$Q1, levels = c(1,2,3), labels = c("Executive", "Manager", "Employe
e"))

#Q2 - Area of employment
DGAREArisk <- grepl(2, surveyData$Q2)
DGAREAcybr <- grepl(3, surveyData$Q2)
DGAREAbizniz <- grepl(4, surveyData$Q2)
DGAREAit <- grepl(5, surveyData$Q2)
DGAREAother <- grepl(9, surveyData$Q2)

#Q3 - Number of employees
surveyData$DGNOEMP.9 <- grepl("1", surveyData$Q3)
surveyData$DGNOEMP.49 <- grepl("2", surveyData$Q3)
surveyData$DGNOEMP.249 <- grepl("3", surveyData$Q3)
surveyData$DGNOEMP.999 <- grepl("4", surveyData$Q3)
surveyData$DGNOEMP.1000 <- grepl("5", surveyData$Q3)
DGNOEMP <- surveyData$DGNOEMP.9 * 1 + surveyData$DGNOEMP.49 * 2 + surveyData$DGNOEMP.249 * 3 +
surveyData$DGNOEMP.999 * 4 + surveyData$DGNOEMP.1000 * 5
DGNOEMPf <- factor(surveyData$Q3, levels = c(1,2,3,4,5), labels = c("Less than 10", "10 to 49"
, "50 to 249", "250 to 1,000", "Over 1,000"))

#Q4 - sector
surveyData$Q4[is.na(surveyData$Q4)] <- 0
surveyData$DGSECpri <- grepl("1", surveyData$Q4)
surveyData$DGSECpub <- grepl("2", surveyData$Q4)
surveyData$DGSECngo <- grepl("3", surveyData$Q4)
DGSEC <- surveyData$DGSECpri * 3 + surveyData$DGSECpub * 1 + surveyData$DGSECngo * 2
DGSECf <- factor(surveyData$Q4, levels = c(1,2,23), labels = c("Private", "Public", "NGO"))

#Q5 - External accreditation
surveyData$Q5[is.na(surveyData$Q5)] <- 0
DGEXTACC <- surveyData$Q5 == 1
```

H1 and H2: Decision rights

```
#Q6 - IT executive
surveyData$ITEXECf <- factor(surveyData$Q6, levels = c(1,2,3,4,5,6,7,8,9), labels = c("CEO", "
CIO", "CISO", "CDO", "CRO", "CSO", "CTO", "COO", "None of above"))
ITEXEC <- surveyData$ITEXECf %in% c("CIO", "CDO", "CTO")

#Q7 - Strategic decisions about IT
surveyData$ITSTRDECa <- grepl("1", surveyData$Q7)
surveyData$ITSTRDECb <- grepl("2", surveyData$Q7)
surveyData$ITSTRDECc <- grepl("3", surveyData$Q7)
ITSTRDEC <- surveyData$ITSTRDECa * 3 + surveyData$ITSTRDECb * 1 + surveyData$ITSTRDECc * 2
```

```
#Q8 - Cybersecurity executive
surveyData$CYBREXECf <- factor(surveyData$Q8, levels = c(1,2,3,4,5,6,7,8,9), labels = c("CEO", 
"CIO", "CISO", "CDO", "CRO", "CSO", "CTO", "COO", "None of above"))
CYBREXEC <- surveyData$CYBREXECf %in% c("CISO", "CRO", "CSO")

#Q9 - Strategic decisions about cybersecurity
surveyData$CYBRSTRDECa <- grepl("1", surveyData$Q9)
surveyData$CYBRSTRDECb <- grepl("2", surveyData$Q9)
surveyData$CYBRSTRDECc <- grepl("3", surveyData$Q9)
CYBRSTRDEC <- surveyData$CYBRSTRDECa * 3 + surveyData$CYBRSTRDECb * 1 + surveyData$CYBRSTRDECc 
* 2
```

H3: Resource allocation

```
#Q12 - financial resources for IT
surveyData$ITFINa <- grepl("1", surveyData$Q12)
surveyData$ITFINb <- grepl("2", surveyData$Q12)
surveyData$ITFINc <- grepl("3", surveyData$Q12)
ITFIN <- surveyData$ITFINa * 3 + surveyData$ITFINb * 1 + surveyData$ITFINc * 2

#Q13 - human resources for IT
surveyData$ITSKILLSa <- grepl("1", surveyData$Q13)
surveyData$ITSKILLSb <- grepl("2", surveyData$Q13)
surveyData$ITSKILLSc <- grepl("3", surveyData$Q13)
ITSKILLS <- surveyData$ITSKILLSa * 3 + surveyData$ITSKILLSb * 1 + surveyData$ITSKILLSc * 2

#Q14 - financial resources for cyber
surveyData$CYBRFINa <- grepl("1", surveyData$Q14)
surveyData$CYBRFINb <- grepl("2", surveyData$Q14)
surveyData$CYBRFINc <- grepl("3", surveyData$Q14)
CYBRFIN <- surveyData$CYBRFINa * 3 + surveyData$CYBRFINb * 1 + surveyData$CYBRFINc * 2

#Q15 - human resources for cyber
surveyData$CYBRSKILLSa <- grepl("1", surveyData$Q15)
surveyData$CYBRSKILLSb <- grepl("2", surveyData$Q15)
surveyData$CYBRSKILLSc <- grepl("3", surveyData$Q15)
CYBRSKILLS <- surveyData$CYBRSKILLSa * 3 + surveyData$CYBRSKILLSb * 1 + surveyData$CYBRSKILLSc 
* 2
```

H4: Interdepartmental communication

```
#Q10 - communication frequency
surveyData$COMFREday <- grepl("1", surveyData$Q10)
surveyData$COMFREweek <- grepl("2", surveyData$Q10)
surveyData$COMFREmonth <- grepl("3", surveyData$Q10)
surveyData$COMFRErare <- grepl("4", surveyData$Q10)
surveyData$COMFREnever <- grepl("5", surveyData$Q10)
COMFRE <- surveyData$COMFREday * 4 + surveyData$COMFREweek * 3 + surveyData$COMFREmonth * 2 + 
surveyData$COMFRErare * 1 + surveyData$COMFREnever * 0

#Q11 - communication type
COMTYP <- unlist(lapply(surveyData$Q11, FUN = myScore))
str_remove(COMTYP, ",None of the above")

#interdepartmental communication intensity score
COMINT <- COMTYP + COMFRE
```

H5: Outsourcing strategy

```
#Q16 - IT outsourcing extent
surveyData$ITOUTSRCmin <- grepl("1", surveyData$Q16)
surveyData$ITOUTSRCsel <- grepl("2", surveyData$Q16)
surveyData$ITOUTSRCext <- grepl("3", surveyData$Q16)
ITOUTSRC <- surveyData$ITOUTSRCmin * 3 + surveyData$ITOUTSRCsel * 2 + surveyData$ITOUTSRCext *
1

#Q17 - cyber outsourcing extent
surveyData$CYBROUTSRCmin <- grepl("1", surveyData$Q17)
surveyData$CYBROUTSRCsel <- grepl("2", surveyData$Q17)
surveyData$CYBROUTSRCext <- grepl("3", surveyData$Q17)
CYBROUTSRC <- surveyData$CYBROUTSRCmin * 3 + surveyData$CYBROUTSRCsel * 2 + surveyData$CYBROUT
SRCext * 1
```

Cyber risk management maturity score

```
#Q18 - cyber program
surveyData$CYBRPROa <- grepl("1", surveyData$Q18)
surveyData$CYBRPROb <- grepl("2", surveyData$Q18)
surveyData$CYBRPROc <- grepl("3", surveyData$Q18)
surveyData$CYBRPROd <- grepl("4", surveyData$Q18)
surveyData$CYBRPROe <- grepl("5", surveyData$Q18)
CYBRPRO <- surveyData$CYBRPROa * 1 + surveyData$CYBRPROb * 2 + surveyData$CYBRPROc * 2 + surve
yData$CYBRPROd * 3 + surveyData$CYBRPROe * 4

#Q19 - cyber program performance
surveyData$CYBRPERa <- grepl("1", surveyData$Q19)
surveyData$CYBRPERb <- grepl("2", surveyData$Q19)
surveyData$CYBRPERc <- grepl("3", surveyData$Q19)
CYBRPER <- surveyData$CYBRPERa * 3 + surveyData$CYBRPERb * 1 + surveyData$CYBRPERc * 2

#Q20 - cyber risk assessments
surveyData$CYBRASa <- grepl("1", surveyData$Q20)
surveyData$CYBRASb <- grepl("2", surveyData$Q20)
surveyData$CYBRASc <- grepl("3", surveyData$Q20)
surveyData$CYBRASd <- grepl("4", surveyData$Q20)
CYBRAS <- surveyData$CYBRASa * 1 + surveyData$CYBRASb * 2 + surveyData$CYBRASc * 4 + surveyDat
a$CYBRASd * 4

#Q21- independent audit
surveyData$CYBRAUDa <- grepl("1", surveyData$Q21)
surveyData$CYBRAUDb <- grepl("2", surveyData$Q21)
surveyData$CYBRAUDc <- grepl("3", surveyData$Q21)
surveyData$CYBRAUDd <- grepl("4", surveyData$Q21)
surveyData$CYBRAUDe <- grepl("5", surveyData$Q21)
CYBRAUD <- surveyData$CYBRAUDa * 2 + surveyData$CYBRAUDb * 3 + surveyData$CYBRAUDc * 1 + surve
yData$CYBRAUDd * 1 + surveyData$CYBRAUDe * 2

CYBRSCORE <- CYBRPRO + CYBRPER + CYBRAS + CYBRAUD
```

Regression model

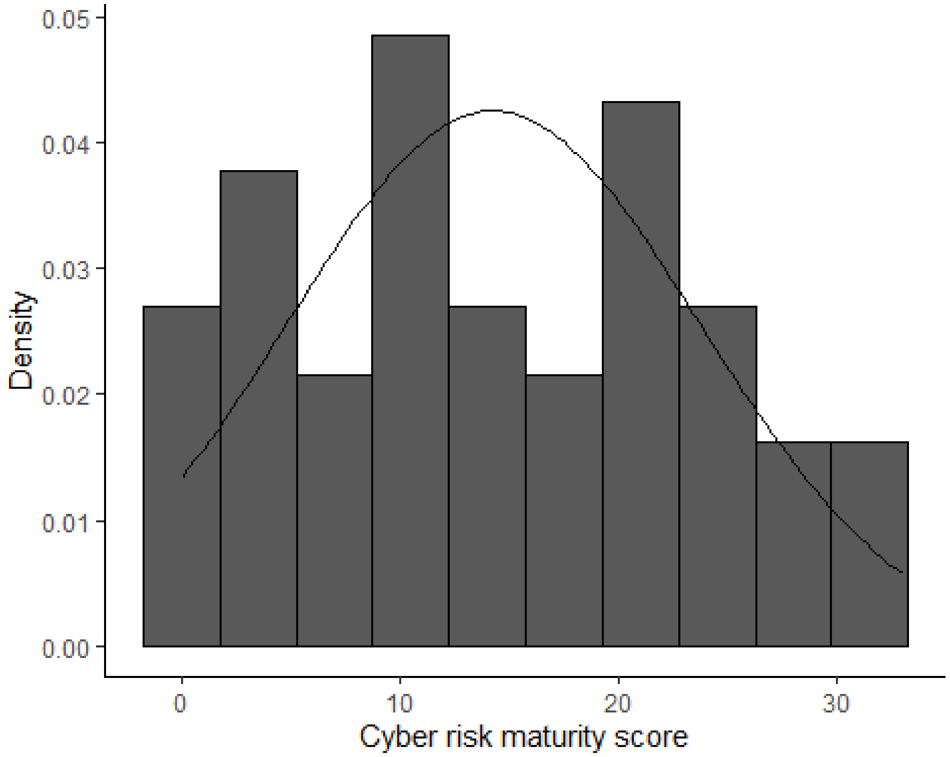
```
cybrMatModel.control <- lm(CYBRSCORE ~ DGPOS + DGAREArisk + DGAREAcybr + DGAREAbizniz + DGAREA
other + DGEXTACC + DGNOEMP + DGSEC)
summary(cybrMatModel.control)

##
## Call:
## lm(formula = CYBRSCORE ~ DGPOS + DGAREArisk + DGAREAcybr + DGAREAbizniz +
##     DGAREAother + DGEXTACC + DGNOEMP + DGSEC)
##
## Residuals:
##      Min       1Q   Median       3Q      Max
## -23.1005  -5.1848   0.8592   5.1172  13.8611
##
## Coefficients:
##                  Estimate Std. Error t value Pr(>|t|)
## (Intercept)       -1.5477     6.0560  -0.256   0.7995
## DGPOS              1.1563     1.8754   0.617   0.5407
## DGAREAriskTRUE     1.8877     3.3025   0.572   0.5705
## DGAREAcybrTRUE     1.4605     2.9256   0.499   0.6201
## DGAREAbiznizTRUE   3.6891     3.3815   1.091   0.2812
## DGAREAotherTRUE    1.2317     2.8322   0.435   0.6658
## DGEXTACCTRUE       7.1581     2.4516   2.920   0.0055 **
## DGNOEMP            0.5893     1.1188   0.527   0.6010
## DGSEC              2.1167     1.2202   1.735   0.0898 .
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## Residual standard error: 8.371 on 44 degrees of freedom
## Multiple R-squared:  0.3263, Adjusted R-squared:  0.2038
## F-statistic: 2.664 on 8 and 44 DF,  p-value: 0.01776
```

```
cybrMatModel.all <- lm(CYBRSCORE ~ DGPOS + DGAREArisk + DGAREAcybr + DGAREAbizniz + DGAREAothe
r + DGEXTACC + DGNOEMP + DGSEC + ITEXEC + CYBREXEC + ITSTRDEC + CYBRSTRDEC + ITFIN + ITSKILLS
+ CYBRFIN + CYBRSKILLS + COMINT + ITOUTSRC + CYBROUTSRC)
summary(cybrMatModel.all)
```

```
##
## Call:
## lm(formula = CYBRSCORE ~ DGPOS + DGAREArisk + DGAREAcybr + DGAREAbizniz +
##     DGAREAother + DGEXTACC + DGNOEMP + DGSEC + ITEXEC + CYBREXEC +
##     ITSTRDEC + CYBRSTRDEC + ITFIN + ITSKILLS + CYBRFIN + CYBRSKILLS +
##     COMINT + ITOUTSRC + CYBROUTSRC)
##
## Residuals:
##      Min       1Q   Median       3Q      Max
## -11.5025  -4.4236   0.6432   3.6059  13.7176
##
## Coefficients:
##                   Estimate Std. Error t value Pr(>|t|)
## (Intercept)      -17.85900    8.97661  -1.990  0.05499 .
## DGPOS             -0.08669    1.68332  -0.051  0.95924
## DGAREAriskTRUE    -2.53548    3.19142  -0.794  0.43260
## DGAREAcybrTRUE     6.91225    3.01202   2.295  0.02823 *
## DGAREAbiznizTRUE  11.92045    3.83837   3.106  0.00389 **
## DGAREAotherTRUE    4.86907    2.78387   1.749  0.08958 .
## DGEXTACCTRUE       2.87817    2.65423   1.084  0.28606
## DGNOEMP            3.09166    1.15341   2.680  0.01138 *
## DGSEC             -0.49257    1.15554  -0.426  0.67268
## ITEXECTRUE        -1.86769    2.42905  -0.769  0.44742
## CYBREXECTRUE      -0.22358    2.73119  -0.082  0.93525
## ITSTRDEC           8.36499    2.46500   3.394  0.00181 **
## CYBRSTRDEC        -4.58020    2.06142  -2.222  0.03326 *
## ITFIN             -3.69947    1.61433  -2.292  0.02844 *
## ITSKILLS           1.60302    1.97394   0.812  0.42256
## CYBRFIN            4.36849    2.00548   2.178  0.03663 *
## CYBRSKILLS        -2.44145    1.36180  -1.793  0.08218 .
## COMINT            -0.57082    0.61630  -0.926  0.36106
## ITOUTSRC           3.63604    1.37324   2.648  0.01233 *
## CYBROUTSRC          1.64802    1.54228   1.069  0.29302
## ---
## Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
##
## Residual standard error: 6.836 on 33 degrees of freedom
## Multiple R-squared:  0.663,  Adjusted R-squared:  0.4689
## F-statistic: 3.417 on 19 and 33 DF,  p-value: 0.0009705
```

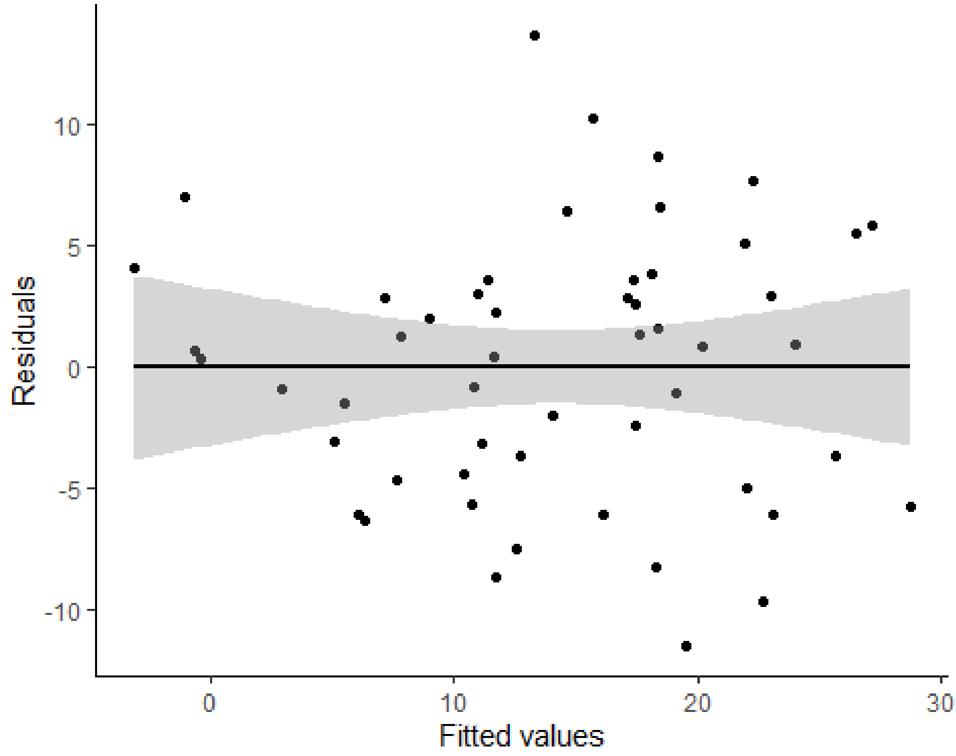
Regression diagnostics

```
#Cyber score histogram for normal distribution
ggplot(surveyData, aes(CYBRSCORE)) + geom_histogram(aes(y = ..density..), binwidth = 3.5, colo
ur = "black") + theme_classic() + stat_function(fun = dnorm, args = list(mean = mean(CYBRSCORE
, na.rm = TRUE), sd = sd(CYBRSCORE, na.rm = TRUE)), colour = "black", size = 0.5) + labs(x = "
Cyber risk maturity score", y = "Density")
```

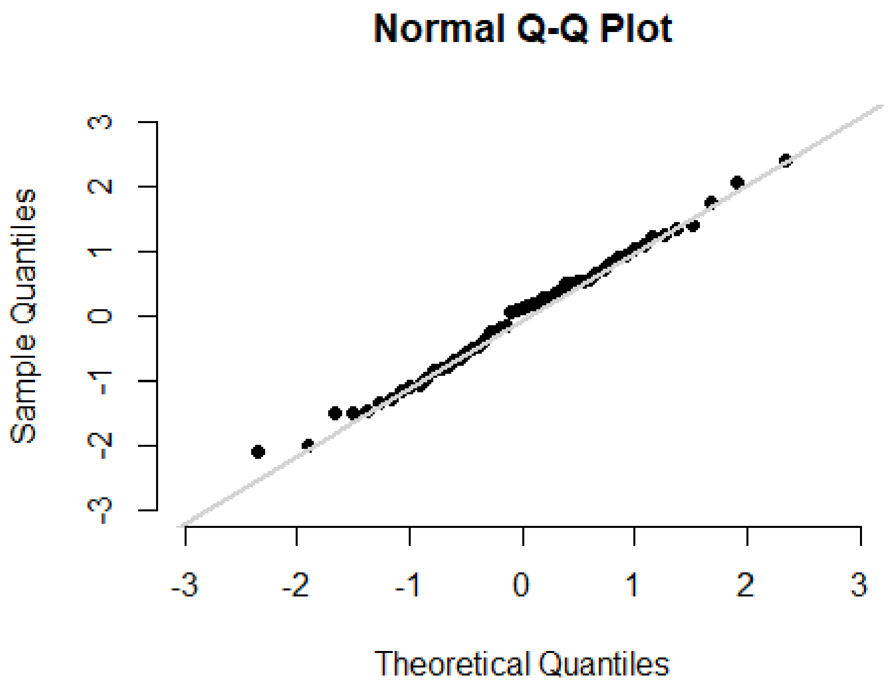


```
#Cook's distance
table((cooks.distance(cybrMatModel.all)) < 1)

##
## TRUE
##   53

#Studentized residuals
rsCybrMatModel <- rstudent(cybrMatModel.all)

#Confidence intervals
table(rsCybrMatModel < 1.96 & rsCybrMatModel > -1.96)

##
## FALSE  TRUE
##     4    49
```

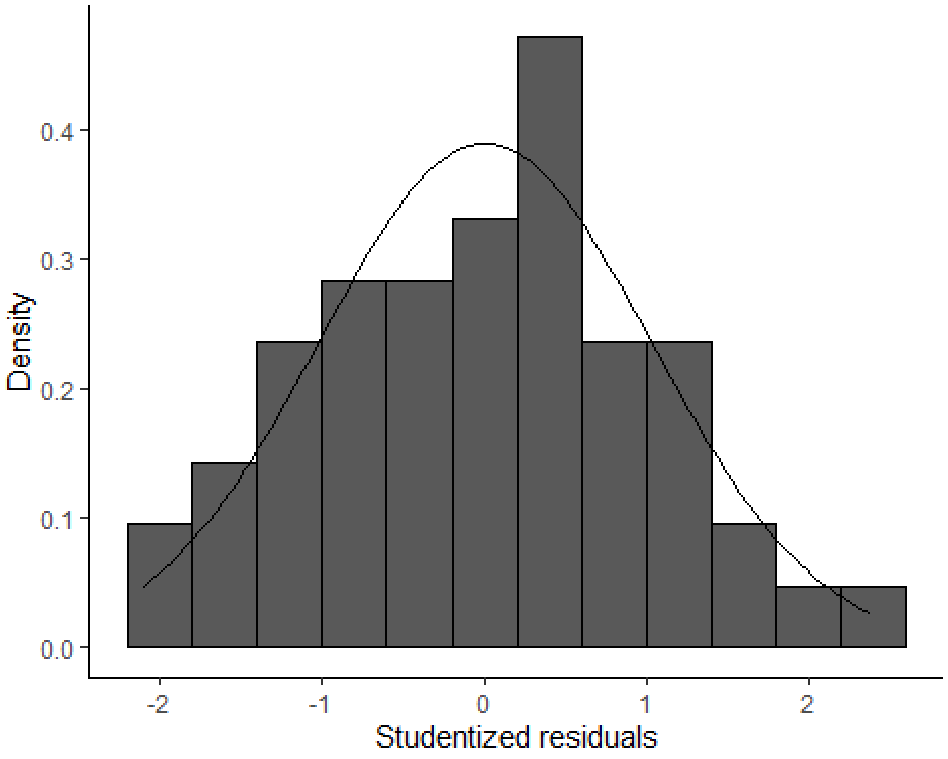
```
table(rsCybrMatModel < 2.58 & rsCybrMatModel > -2.58)

##
## TRUE
##   53

#Variance inflation factor
vifCybrMatModel <- vif(cybrMatModel.all)
vifCybrMatModel > 10

##        DGPOS   DGAREArisk   DGAREAcybr DGAREAbizniz  DGAREAother     DGEXTACC
##        FALSE        FALSE        FALSE        FALSE        FALSE        FALSE
##      DGNOEMP        DGSEC       ITEXEC     CYBREXEC     ITSTRDEC   CYBRSTRDEC
##        FALSE        FALSE        FALSE        FALSE        FALSE        FALSE
##        ITFIN     ITSKILLS      CYBRFIN   CYBRSKILLS       COMINT     ITOUTSRC
##        FALSE        FALSE        FALSE        FALSE        FALSE        FALSE
##   CYBROUTSRC
##        FALSE

mean(vifCybrMatModel)

## [1] 2.463205

1/vifCybrMatModel

##        DGPOS   DGAREArisk   DGAREAcybr DGAREAbizniz  DGAREAother     DGEXTACC
##    0.4894617    0.4454269    0.4612101    0.2668712    0.5853891    0.5155545
##      DGNOEMP        DGSEC       ITEXEC     CYBREXEC     ITSTRDEC   CYBRSTRDEC
##    0.4081460    0.6845355    0.6084364    0.6749413    0.3308958    0.3365544
##        ITFIN     ITSKILLS      CYBRFIN   CYBRSKILLS       COMINT     ITOUTSRC
##    0.3669871    0.3253437    0.1765728    0.3209266    0.7851737    0.5387737
##   CYBROUTSRC
##    0.4519887

#Durbin-Watson test
dwt(cybrMatModel.all)

##  lag Autocorrelation D-W Statistic p-value
##    1     -0.06758311      2.125674   0.766
##  Alternative hypothesis: rho != 0

#Residuals vs fitted plot
ggplot(cybrMatModel.all, aes(x = .fitted, y = .resid)) + geom_point() + theme_classic() + geom
_smooth(method = "lm", colour = "Black") + labs(x = "Fitted values", y = "Residuals")

## `geom_smooth()` using formula 'y ~ x'
```



```r
#Q-Q plot
qqnorm(rsCybrMatModel, pch = 19, frame = FALSE, xlim = c(-3,3), ylim = c(-3,3)); qqline(rsCybr
MatModel, col = "light grey", lwd = 2)
```



```r
#Histogram showing the normal distribution of the studentized residuals
ggplot(surveyData, aes(rsCybrMatModel)) + geom_histogram(aes(y = ..density..), binwidth = 0.4,
colour = "black") + theme_classic() + stat_function(fun = dnorm, args = list(mean = mean(rsCyb
rMatModel, na.rm = TRUE), sd = sd(rsCybrMatModel, na.rm = TRUE)), colour = "black", size = 0.5
) + labs(x = "Studentized residuals", y = "Density")
```


Density
Studentized residuals