LUND UNIVERSITY

SCHOOL OF ECONOMICS AND MANAGEMENT

The Role of Organisational Culture in Shaping and Ensuring Information Security Compliance

Bachelor Thesis

Alisa Ilina

Michael Jenka

June 2020

Bachelor's Program in International Business

Supervisor: Olof Hallonsten

Abstract

Course: IBUH19, Degree Project in International Business, 15HP

Seminar Date: June 2nd, 2020

Word Count: 24576

Purpose: This bachelor thesis examines the impact of organisational culture on the adherence to Information Security (hereinafter IS) protocols (IS compliance) and the crucial factors leading to varying levels of consistency in information security awareness (hereinafter ISA) between organisational departments while considering the unique Swedish cultural qualities.

Methodology: This thesis reaches its conclusion through a series of primary and secondary data collection procedures. Primary data relies on semi-structured interviews with experts from different departments influential in IS compliance decision-making in order to understand how existing practices influence organisation culture by changing incentives and attitudes change with regards to adherence to security practices.

Theoretical Background: The thesis breaks down the socio-technical research question into manageable chunks that can be explored through research, and consequently allows for proper questions to be framed in order to achieve findings within the outline of this thesis. IS compliance is broken down to its basic nature, investigating both the human factors that affect compliance with IS (based on existing research), as well as the technical elements and governance principles. Lastly, proper models are selected to identify ways through which to interpret the role of organisational culture (Schein's Iceberg Model) and national culture (Hofstede's Cultural Dimensions) with regards to compliance intention.

Empirical Findings: The compliance intention factors revealed varying values of the departments, however, transparency, accountability, and the nature of the data were deemed the most essential elements in identifying information security practices. Compliance is

shaped by the implied incentives from actions taken by the departments. The CS experts are the primary agents who act as a source of ISA, however, the tensions and nuance in responses between them, IT department and top management result in the lowering of their potential to affect the organisational culture in the desired way. The IT department is generally undertaking a mediating role in ISA, yet specifics of their jobs implied their prime focus in technicalities, which resulted in lower levels of proper interdepartmental communication. Overall, transparency and dynamic learning were the pivotal elements mentioned by fairly all respondents.

Analysis: Incentives and actions of different departments are projecting the leadership priorities and craft the general behaviour within organisational culture. It is crucial for the organisations to analyse ISA and IS compliance as a cultural component which shall be organically absorbed through dynamic learning. Moreover, compliance intention factors and maturity levels provide a certain prism of perception through which to determine proper levels of security compliance and governance. Such emphasis shall act as a tool for the cognition of actionable principles to be taken to reflect the cultural preferences of employees and cultivate proper interdepartmental practices.

Conclusion: With regards to the Swedish cultural maxim, greater transparency would be warranted to increase intra-organizational learning, and contribute to optimized solutions, as opposed to solutions oriented around top-management's objectives. In doing so, ISA and IS compliance are likely to become a more crucial aspect of workers' perceptions, by allowing workers more control over decisions, due to greater knowledge.

Keywords: cybersecurity, corporate culture, information security awareness, information security compliance, digital maturity, compliance intention factors, parochialism

Definitions and Concepts

A few notations shall be identified that will become a leitmotif in the further chapters. A proper comprehension of cybersecurity terms is the key for proper evaluation of cybersecurity performance.

Cybersecurity – a set of protective measures safeguarding information, data, systems, servers, networks from malicious attacks (Kaspersky, 2020)

Cybersecurity threat – a potential for engendering harm to security, asset loss and its possible impact (NIST, SP 800-160). It does not infer a security problem, however, it exists with the circumstance that might violate information safety. Nevertheless, there are certain countermeasures that may decrease the probability of exploitation of cybersecurity threats (Hell, 2019a)

Cybersecurity risk – expected loss defined as a function of the probability of an event of a threat and the impact of the consequences (RFC 4949, IETF). Majority of the companies nowadays are exposed to a myriad of cybersecurity risks and bifurcating attack vectors. Risk assessment, a component of risk management, is crucial in prioritised risk mitigation and control (Hell, 2020)

Compliance intention – the extent to which an individual is willing to follow orders/protocols willingly (Chen, Ramamurthy & Wen, 2013)

Cybersecurity weakness – a failure, for instance in the code, that is likely to lead to a vulnerability (Hell, 2019)

Cybersecurity vulnerability – an exploited weakness (Hell, 2019b)

Information leakage – a revelation of sensitive information to an unauthorised party which can be used in the cyberattack (The Web Application Security Consortium, 2020)

Parochialism – the limited nature in which different workers see their task, and fail to understand the aim of individuals who in turn rely on their own contribution to the final group effort (Gluesing, 2013)

Abbreviations

CDF – Cultural Dimensions Framework

CIF – Compliance Intention Factor

CML – Cyber Maturity Level

CS – Cybersecurity

GDT – General Deterrence Theory

IS – Information Security

ISA – Information Security Awareness

IT – Information Technology

LoC – Level of Control

WCL – Work Locus of Control

Acknowledgements

We would like to express our sincere gratitude to our supervisor Olof Hallonsten for aspiring guidance and constructive criticism. We are grateful to all our participants; their advice and insightful remarks have helped us tremendously in unravelling this complex issue. Moreover, we are deeply thankful to everyone who has responded to our interviews for their motivation and immense knowledge.

Lund, 27 May 2020

Michael Jenka Alisa Ilina

Table of Contents

Abstract **1**

Definitions and Concepts 3

Abbreviations 4

Acknowledgements **5**

Table of Contents **6**

1 Introduction **1**

1.1 Problem Discussion 2

1.2 Research Purpose and Research Question 4

1.3 Delimitations 4

1.4 Outline of the Thesis 5

2 Literature/Theoretical Review **6**

2.1 Societal Theoretical Aspects 6

2.1.1 Organisational Culture 6

2.1.2 Sweden's National Culture - Hofstede's Cultural Dimensions 8

2.1.3 Parochialism within Business Organisations 11

2.1.4 Compliance Intention Factors 12

2.1.4.1 Stress and Resilience 13

2.1.4.2 Punishment and Reward Systems 14

2.1.4.3 Worker's Perceived Level of Control 15

2.1.4.4 Risk Assessment 16

2.2 Technical Theoretical Aspects 18

2.2.1 Information Security Awareness (ISA) 18
2.2.2 Data Breaches and Information Leakages 19
2.2.3 Digital Maturity 20
2.3 Key CS/IS Governance Principles - Linking Societal and Technical Segments 22
3 Methodology 26
3.1 Research Approach: General Information 26
3.1.1 Research Design 27
3.1.2 Sampling 29
3.1.3 Data Collection Method 31
3.1.3.1 Primary Data 31
3.1.3.2 Secondary Data 32
3.2 Empirical Data 33
3.3 Validity and Reliability 34
3.4 Limitations 35
3.4.1 Impact of COVID-19 on Data Gathering 37
4 Analysis and Discussion 39
4.1 Analysis: Cybersecurity Department 39
4.1.1 Stress and Resilience 40
4.1.2 Punishment and Reward Systems 42
4.1.3 Worker's Perceived Level of Control 44
4.1.4 Risk Assessment 45
4.1.5 Digital Maturity 46
4.2 Analysis: IT Department 48
4.2.1 Stress and Resilience 48
4.2.2 Punishment and Reward Systems 49
4.2.3 Worker's Perceived Locus of Control 50

4.2.4 Risk assessment 51

4.2.5 Digital maturity 53

4.3 Final Discussion 54

5 Conclusion 59

5.1 Research Aims 59

5.2 Research Objectives 59

5.3 Conclusion/Findings 60

5.4 Practical Implications/Contribution 61

5.5 Future Research 62

References 65

Appendix 71

A. Interview Questionnaire Sample 71

1 Introduction

The cyber domain represents an eclectic discipline encompassing aspects of computer science, psychology, economics, and culture. Such multidimensional nature is taking a quantum leap in complexity with the number of potential vulnerabilities. Cybersecurity is, therefore, a young, complex field, where new challenges emerge regularly, but ultimately organisations will need to take an interest in cybersecurity to maintain their competitiveness in the future (Dawson & Thomson, 2018).

It is estimated that by 2021, cybercrime will account for approximately $6 trillion globally (Cybercrime Magazine, 2020). Global cybersecurity expenses are expected to reach $133.7 billion in 2022 (Moore & Keen, 2019). Moreover, with ever-increasing digitalisation, new sophisticated risks evolve, as novel technologies (e.g. 5G, cloud computing, AI) penetrate more areas of business. Therefore, new agile and adaptive frameworks become needed to insure the organisational assets against potential theft by encouraging greater IS awareness. With the increasing importance of proprietary knowledge, global competition, and ever-shorter product life cycles, the need to guard knowledge becomes highly salient. The complexity of cybersecurity addresses a unique challenge in the definition of models, specifically the cultural attributes due to their diverse nature, as the culture will always be an eternal residual in business.

The majority of the published literature prioritises technical approaches, however, it is the social and cultural influence that is highly underestimated in cyber settings. Indeed, the majority of research into IS takes a technical approach, with many researchers neglecting the importance of people in ensuring proper information security compliance within organisations (McEvoy & Kowalski, 2019). It is no surprise, therefore, that human-based cyber attacks, such as social engineering, are some of the most commonly experienced attack methods, with 62% of companies facing such attacks in 2018 (Milkovich, 2019). Furthermore, McEvoy and Kowalksi (2019) claim that in 2019, phishing, which is based on the exploitation of people's

behaviour, was the most prevalent attack vector. Such an observation emphasises the relevance of this thesis in the light of cultural dimensions. Corporate culture plays a pivotal role in cybersecurity management, and awareness among workers and clients becomes critical in raising the levels of security. Incentives greatly determine the IS compliance decisions and, therefore, the relevance of CIF becomes pivotal in this examination of human factors' relationship with security strength levels. The role and peculiarities of organisational and national culture shape the behaviour patterns/attitudes of the employees, who, in turn, ultimately decide whether or not to follow IS protocols – putting the organisation in potential danger.

Given the nature of the issue and the somewhat counterproductive research focus on technical factors, it becomes increasingly more salient to understand the nature of this socio-technical problem in a managerial sense. It is therefore needed to address this complex topic by investigating the particular conditions and reasons for why workers act in a deviant way. Since the behaviour is managed through the organisational culture and the nature of contracts within an organisational context, compelling insights could be gained by breaking down the topic along the aforementioned lines. Consequently, a cultural approach is warranted for sensemaking purposes to understand the conditions for willful compliance of IS protocols. Therefore, the thesis is of a behavioural nature and will deal with the compliance intention factors and their effect on IS compliance from a cultural perspective.

1.1 Problem Discussion

Firstly, it is important to understand what aspect of information security this thesis seeks to understand. Fundamentally, this thesis is tackling the management of people's behaviours. Accepting the fact that the primary reason for large IS leakages has been linked not to the failure of IT infrastructures, but to human behaviours within an organisational context (Gcaza, von Solms, Grobler and van Vuuren, 2015), the purpose changes from understanding IS as a technical field to understanding workers attitudes towards IS, from an organisational perspective.

If the primary reason for these costly mistakes is people, then there are two potential options that can be taken: 1) limit the extent to which people interact with IT equipment owned by the company, thus reducing the likelihood of IS breach/leakage, or 2) understand the underlying reasons for the persistence of deviant behaviour and address the root cause. Naturally, as implied from previous sections, the authors of this thesis advocate for the latter, as IT will become increasingly more important in the coming years. Moreover, reducing access to information by offering greater oversight of data movement will reduce the flexibility of the workforce itself. In a hypercompetitive market, such as the modern interdependent economy, that would be an immensely counterproductive measure in most organisational contexts.

The question, therefore, becomes how does one best understand this problem, and more importantly, through which theoretical frameworks can this problem be best explored. It is of no surprise, due to the subjective nature of the issue that no commonly used "framework" has been fully accepted (Wiley, McCormac & Calic, 2019). Instead, what most research points to is that there are apparent fundamental qualitative factors that overlap in the works of various researchers. These factors seem to have different effects on the compliance of workers with regards to IS protocols. Therefore, compliance intention can be assumed to be a crucial aspect of this issue. The problem, therefore, can be broken down into three manageable parts.

Firstly, how do we best understand why some people want to follow rules and protocols of IS, while others do not? This is a matter of understanding the compliance intention of individuals. People will naturally have different roles within an organisation as given by their job description and contract — but how does this affect their decision to follow guidelines or exhibit potentially costly deviant behaviour?

Secondly, how does the organisation influence the intention of an individual to follow ISA protocols? Organisational culture is widely believed to be a major contributing factor to the overall ability of an organisation to maintain organic capabilities to defend against malicious agents with regards to information security (Ioannou, Stavra & Bada, 2017).

Finally, research constraints that the authors are faced with in an effort to avoid generalization require an understanding of the underlying beliefs of influential entities (in this case, specific departments). How are these beliefs shaped, and what effect do they have on organisational

culture as a whole? Aside from that, there is the question of national paradigms, since culture, as such also leads to a preference of particular behaviours and beliefs (as will be explained later). Indeed, studies show that national culture itself has a major influence on actions that are less observable — such as communication, protection motivation, knowledge sharing, and overall team dynamics (Gcaza, von Solms, Grobler & van Vuuren, 2015).

1.2 Research Purpose and Research Question

Breaking down the nature of the posed socio-technical problem, this thesis seeks to aid in sensemaking of the role of organisational culture within the context of Information Security management and enforcement. It is expected that by the end of this study several actionable factors and observations will be identified. Those can be used as a bedrock for a culture-based framework that can be applied to Swedish firms to improve the overall levels of Information Security Awareness (ISA) The thesis seeks to identify the most actionable aspects of cybersecurity compliance, thus facilitating the quintessence of the socio-technical problem of Information Security management. Further to be studied in an extensive overview of the literature available to help in understanding the role of human factors within the domain of CS/IS, the following research question is identified:

What role does organizational culture play in influencing the information security compliance of Swedish employees?

1.3 Delimitations

Delimitations will offer a way through which to shape this study, thus increasing the quality of the potential theoretical contribution by defining the context in which the conclusions can be applied (Bryman & Bell, 2011). Firstly, it is important to understand what this study is and what it is not. Given the managerial educational background of the authors, while there is a

technical aspect to this research area as outlined in forthcoming sections, they merely serve as contextual guides to allow readers to better grasp the principles behind CS/IS.

Firstly, this study has been conducted with the notion of the peculiarities of Swedish culture as an area of interest. Consequently, as will be explained later, the findings of this study are only applicable to Swedish people or people of similar cultures. The presentation of other cultures serves only to contrast Swedish attitudes — the thesis will not consider the qualities of different cultures for any other purpose, nor will this thesis comment on culture as such, in so far suggesting how to best harness distinct cultural qualities of Sweden to increase security compliance.

The nature of data collection mandates that in order to get access to important information, skilled specialists need to be contacted as they can offer valuable insight through which to corroborate our preliminary beliefs and further elaborate on the contextual viability of the information present in *Chapter 2*. Under optimal conditions, only a specific niche of workers would be selected to get data that can be adequately applied within a specific context, however, given the difficulty in collecting data, sampling was impacted. Nevertheless, Bryman and Bell do highlight in their textbook that when it comes to qualitative research, a certain diversity may bring new exciting views and attitudes to light, from which compelling conclusions can be drawn (2011).

1.4 Outline of the Thesis

This thesis will be presented in five chapters. *Chapter 1* highlights the theoretical foundation, background, and importance of the research question. Subsequently, *Chapter 2* is a literature review that will focus on the relevant topics and insights to help deepen the understanding of the relationship between culture and cybersecurity. *Chapter 3* covers methodology, the description of data collection, and the nature of the analysis. *Chapter 4* summarizes the empirical findings and discusses analytical findings. Lastly, *Chapter 5* is the culmination of the research outcomes, presents the potential limitations, highlights the contribution, and suggests the potential further research avenues.

2 Literature/Theoretical Review

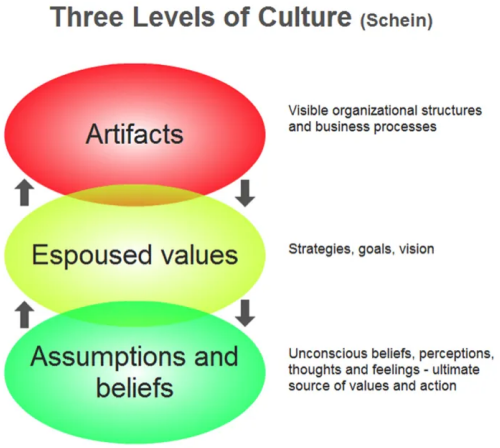
In this chapter the overview of the literature relevant to the thesis topic will be provided: specifically, the areas of interest that pertain to understanding the basic models which contribute to exploring the chosen socio-technical topic. The literature review will, firstly, elaborate on the societal aspects, assisting in comprehension of the fundamental relationships that link the areas of national/organisational culture and CS/IS, as well as the definition and significance of parochialism. The presented sections deal with the choice of the cultural model and the organisational context factors (which have the potential to reveal the relationships between culture and the resultant ISA). Compliance factors are particularly highlighted since they present the linkages to success or failure of CS policies as a result of national/organisational cultural influence. Consequently, the technical elements will be brought up, those will investigate the essence of breaches and leakages, the foundational assumption about the nature of CS/IS failure and external environmental factors which account for the general level of computer ability within a nation. The literature review will prioritise the ISA since it will further penetrate all other sections of the thesis. Digital maturity is brought up as a contextual element to denote the reference to Swedish level of digitalisation. Lastly, governance principles are introduced, alluding to the interconnection and application of societal and technical segments. The provided literature will be symmetrically reflected upon in the analysis of data in *Chapter 4*.

2.1 Societal Theoretical Aspects

2.1.1 Organisational Culture

Given the managerial nature of the issue at hand, it is important to understand and establish a particular theoretical paradigm through which to understand organisational culture. According to Edgar Schein who pioneered one of the most common organisational culture models, a

firm's organisational culture is one of the most important qualitative resources that can be cultivated due to its spillover effects with regards to corporate activities, communication, team cohesion, and internal information flow (1996). Ideally, each corporation has a unique organisational culture that is adopted through explicit and implicit means, giving a certain level of oversight over how things will be done within the workplace during the working hours. Hofstede defined organisational culture as ‘‘the manifestation of practices or behaviours evolving from the shared values in the organisation’’ (1991, p.3), while Schein defines culture as “a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration...to be taught to new members as the correct way to perceive, think, and feel in relation to those problems” (Schein, 1992, p.12). In addition, Schein has identified the Iceberg Model which succinctly describes the manner in which organisational culture manifests itself within a corporate environment. The model stipulates that ultimately there are three levels of organisational culture ranked from the most superficial and obvious to the most impactful and covert *(image sourced from Schein,1996, p.229)*:



- *Artefacts:* according to Schein, artefacts represent the most readily observable factors of organisational culture, such as the usage of uniforms, physical elements of the company and readily available documentation regarding conduct, communication and virtually all available resources that employees have to make sense of — what is expected of them during the working hours (1996).
- *Espoused Values:* this part of the organisational culture deals with less visible yet commonly used motifs, beliefs and practices that are perpetuated through interaction between management and employees. However, unlike basic assumptions, this part of the organisational culture still needs to be managed in order to be maintained and enforced (Schein, 1996).

- *Underlying/Basic Assumptions:* these are composed of unconscious thoughts, beliefs, perceptions and feelings (Schein, 1996). Since assumptions are not discussed or dealt with openly, they cannot easily be addressed or changed. As a result, organisational problems may arise, signifying that change is needed. The connection between underlying assumptions and national culture is tenuous. However, it is observed by researchers such as Hofstede that elements of underlying assumption are dictated by the nationality of the workers (1991).

The Iceberg Model has the ability to explain and illustrate the prevalence of ideas and the relative importance of certain modes of thinking of the workers, therefore yielding it being an ideal framework for the purposes of this thesis. Whenever the organisational culture aspect of our partner company will be discussed, Schein's work will be used for exploratory and explanatory purposes.

2.1.2 Sweden's National Culture - Hofstede's Cultural Dimensions

Culture is a fleeting idea of our modern society: we all experience it in nuanced ways, and in turn, our culture influences the ways in which we view the world around us and establishes our own behaviours and preferences for behaviour. According to Tung and Stahl (2017), who have made an extensive literature review on the topic of culture within International Business, few researchers have been as influential in defining culture as Geert Hofstede. It follows then according to Tung and Stahl, that during a highly turbulent business environment in the latter half of the 20th century, it became painfully apparent that there was a need to focus attention on nuances in the culture that could then be leveraged to increase learning and consequently improve the quality of cross-cultural communication between foreign nations. According to Hofstede, culture can be understood as the "programming of the mind" of a particular nation (1993, p.89). Given its simplicity, Hofstede's Cultural Dimensions Framework (CDF) emerged as the championed framework to understand different cultures around the world. Its simplistic six dimensions allow most individuals to understand how a culture differentiates from another, and more importantly how these differences affect the individuals of the same culture. Hofstede's culture dimensions are presented below:

Power Distance Index (PDI): This dimension deals with the expectations and acceptance of the distribution of power (Hofstede, 1993). High PDI countries are ruled by hierarchies and these hierarchies are widely accepted. Consequently, decision-making in high PDI countries is characterized by the concentration of decision-making power in a few individuals, while low PDI countries experience decision-making by incorporating several individuals.

Individualism/Collectivism (IDV): This dimension measures the way individuals position themselves in their society (Hofstede, 1993). In individualistic societies, the individual is considered to be responsible for their own actions, while in collectivist societies the group is considered to be the key.

Uncertainty Avoidance (UAI): This dimension concerns the way in which individuals deal with the unknown (Hofstede, 1993). High UAI suggests a profound fear of the unknown and consequently greater preference for clarity of actions which necessitates the usage of plans and other observable decision-making instruments. Low UAI cultures embrace risk and the unknown instead demonstrating a level of flexibility with regards to emergent strategies.

Long-term vs. Short-term Orientation (LvS): This dimension measures the way in which a nation determines the chronological aspect of gratification (Hofstede, 1993). That is to say, long-term oriented countries, which is usually the case with eastern nations, will tend to favour long-term solutions as opposed to western countries, such as the USA, where there is an emphasis on short-term successes.

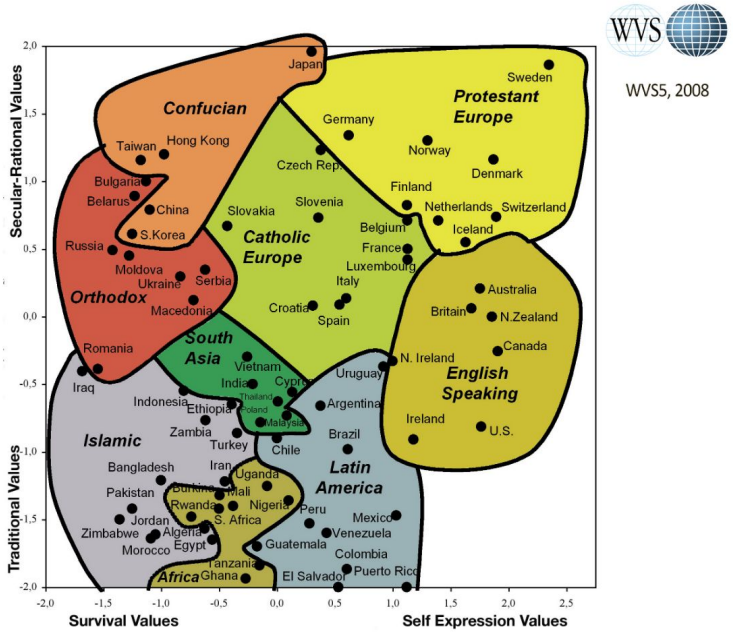
Indulgence vs. Restraint (IvR): This is sometimes colloquially known as the happiness dimension (Hofstede, 1993). This dimension refers to the way in which a culture controls the gratification versus control of basic human desires related to enjoying life. Aside from being associated with cultural looseness vs. tightness, Hofstede observed correlations between indulgence and humanities, and restraint and preferences for science and mathematics as opposed to humanities.

Masculinity vs. Femininity (MvF): This dimension deals with the way gender roles are distributed within society (Hofstede, 1993). A highly masculine society will have firm gender barriers and expectations towards the way men and women will act (aggressive, assertive, and controlling), while a feminine society will blur the distinction between masculine/feminine roles and personal traits resulting in a society where the emphasis is placed on sympathy and understanding. Masculine cultures are deemed to be performance-oriented, while feminine societies are deemed to be cooperation-oriented.

However, it should be noted that many authors, including Tung and Stahl, are critical of dimension-based frameworks when it comes to culture (2017). Best illustrated through Shenkar and Yeshekels' theoretical contribution (2008), where it is argued that such an approach, as used by Hofstede, reduces the nuances of culture and leads to broad generalizations that may not even be true as time goes on, due to the fact that culture evolves over time. Indeed, as it could be expected, Hofstede's framework exhibits what could be referred to as western-centrism, which is to say that foreign cultures are viewed from the perspective of a westerner, and thus potentially offer a skewed interpretation of what foreign cultures are really like and the degree to which each of the six dimensions is relevant.

Despite these criticisms, CDF is to this day being used as a framework in IS research, which, in turn, suggests that CDF may still have its value as an exploratory and explanatory tool. Indeed, Wiley et al rely on aspects of the CDF framework to highlight their views on the importance of culture for ISA, just as much as Henshel, Cains, Hoffman and Sample (2016) depend on using the CDF framework to explain their insights regarding operational learning and how national culture can at times act as a medium for the formation of in-groups and out-groups, which consequently influence ISA development, as learning and flow of information is stunted. This idea is further corroborated by the work of Waldo, who confirms that aspects of national culture, such as IvC and MvF, are determinant for the development of ISA due to them shaping the level of worker interaction within organizations (2018). Consequently, CDF is of high value for the purposes of this thesis.

Sweden is universally acknowledged to be a unique culture from the point of view of the CDF framework. While Sweden is still considered to be a part of the west, unlike many western countries, Sweden ranks lowest in the world on the MvF dimension and also is proportionately less individualistic than most western countries (Hofstede Insights, 2015). Consequently, Sweden can be culturally described as a highly feminist society with greater emphasis on collectivism than most other countries in Europe. This gives Swedish workers a unique fundamental existing paradigm that will impact the way they view interaction in their private lives and in the workplace. To further elaborate on this uniqueness, one may turn to the Ingelhart-Welzel cultural map (figure to the right; WVS 2008), created by the World Value Survey. According to research by the WVS, Swedish culture is one that espouses primarily "secular-rational" and self-expression values (2008). In simple terms, the focus on secular-rational values expresses the desire of culture to "[place] *less emphasis on religion, traditional family values and authority"*, instead, trying to identify ways through which to empower their citizens such as by accepting progressive political and socio-economic initiatives that offer greater self-determination to individuals (WVS, 2008). The emphasis on self-expression "*give high priority to environmental protection, growing tolerance of foreigners, gays and lesbians and gender equality, and rising demands for participation in decision-making in economic and political life"* (WVS, 2008). In short, Sweden is a highly progressive country that appears to favour initiatives that empower individuals in private and professional spheres.



2.1.3 Parochialism within Business Organisations

Parochialism as such is not commonly studied in business, given the fact that it forms a core part of the modern way of doing business. Division of labour, and subsequently departmentalization of corporations has been a major source of economic and business growth in the latter part of the 20th century and allowed many industries to increase their output enough to reach even the most price-sensitive customers (Wang, 2019). This purposeful limitation allows managers to monitor workers in a far easier manner and reduces the potential for workers to make mistakes. However, this action alone determines the level of the worker's commitment to the task itself, as decision-making power is removed, and therefore self-perceived responsibility is reduced (Wang, 2019). The closest way to describe this idea is that of parochialism, or specifically, the limited nature in which different workers see their task, as well as the empathetic inflexibility which diminishes the overall group effort due to different perspectives on the nature and goal of the work itself (Gluesing, 2013).

After an extensive survey of CS/IS literature, there appears to be a major emphasis on internal factors such as worker commitment or organisational commitment (McEvoy & Kowalski, 2019). However, there is little focus on the notion of interdepartmental barriers that arise as a result of limited intention to focus or observe rules and regulations outside of one's immediate job specification. Indeed, these barriers may contribute to lower observation of proper practices with regards to certain mandated protocols, as they may be viewed as unimportant or even intrusive to specific workers' daily goals and tasks (Hadlington, Popovac, Janicke & Jones 2018).

Consequently, the notion of parochialism as such can shed light on understanding the nature of the identified socio-technical problem and can offer an explorative lens that can help in making sense of the studied relationships and gathered data.

2.1.4 Compliance Intention Factors

Compliance intention refers to a workers ability and willingness to take a particular action, even if the action itself is not in the best interest of the worker from their own interpretive paradigm (Chen, Ramamurthy & Wen, 2013). Given the nature of this issue and the desire to understand why workers can deviate from predetermined rules, it is logical to see what factors

play a major role in shaping compliance intention. In the next section, after an extensive literature review, the most common, and therefore, likely factors will be defined and explored.

Compliance intention factors can shape the way in which workers interact due to the way things are handled within an organisation and where the organisation as a unit places emphasis — thus shaping attitudes pertaining to work (Chen et al, 2013). It is important to understand that these factors are not isolated occurrences but are in fact key aspects of an organisation's culture. Consequently, departments with key decision-making power can influence these aspects of culture, which can, in turn, affect the attitudes of people that work within the organisation, as would Schein's Iceberg model suggest (Chen et al, 2013). Based on the literature review the most common factors discussed are Stress/Resilience, Punishment/Reward Systems, Risk Assessment, and Locus of Control.

2.1.4.1 Stress and Resilience

Stress and resilience are features that have been identified as being linked to self-efficacy with regard to avoiding improper CS/IS behaviour (McCormac et al, 2018). In terms of definitions, *resilience* is defined by McCormac et al as *"the process of adapting well in the face of adversity, trauma, tragedy, threats or even significant sources of stress"* (2018, p.2). *Stress*, on the other hand, is not given a full definition by McCormac; the author is instead opting to describe it as the tension that can arise as a result of a mismatch between organisational expectations and applicable ability of allocated human resources for a given project (2018). In addition, McCormac et al identify stress as being crucial in the development of ISA (2018). This is mainly because it is believed that with lower job stress there is a lower chance of CS/IS protocols getting in the way of work being done, thus leading to higher voluntary compliance with protocols (2018). Resilience is understood as having a moderating effect on stress in the same study done by McCormac (2018). Indeed, Waldo confirmed that resilience can be viewed as a shared capability of an organisational entity, which is further distributed through knowledge sharing abilities (2013). However, the role of stress is less concrete in the sense that studies in CS/IS literature have not fully isolated stress as being solely personality-based or culture-based, instead, most studies seem to agree that both personality (such as higher levels of neuroticism or agreeableness) and culture (such as high UAI) can

lead to greater anxiety associated with damage to one's own job security in certain cultures, e.g. the United States (McCormac et al, 2018) (Zhang & Yang, 2018).

2.1.4.2 Punishment and Reward Systems

Individuals who are not directly responsible for failures and operate with capital that they do not directly own are at risk of acting against the interest of the actual capital owner. Jensen and Meckling (1976) called these types of problems *"principal-agent"* problems and explained why many organisations espouse punishment and rewards systems as a way to shape appropriate behaviour through negative or positive reinforcement, respectively. Consequently, in the grand scheme of IS non-compliance, it is important to understand how incentives are shaped within organisations through punishments and rewards.

Research suggests that punishments are a substantially greater motivational factor that affects behaviour with regards to ISA. According to Chen et al, *punishment* is defined as *"the application of negative consequences to or withdrawal of positive consequences from employees"* (2015, p. 402). A study by Parsons, Young, Butavicious, Pattinson and Jerram, that dealt with this particular issue found conflicting findings (2015). Supposedly, punishment systems are substantially more effective at shaping ISA and IS compliance (Parsons et al, 2015) seeing that more workers become aware of negative outcomes, as opposed to aware of potential benefits.

Punishment systems must be easy to understand, and more importantly easy to align with for knowledge reasons. Indeed, Proctor and Chen confirm that punishments are greatest motivators for otherwise disinterested parties, however, they argue that for such a system to be truly effective, it needs to be designed with an explanatory aspect in its design (2015). Specifically, ISA initiatives need to be qualitatively and appropriately explained in order to offer worker knowledge benefits and reduce principal-agent problems (Proctor & Chen, 2015). Indeed, this idea is further confirmed by a study of cybersecurity campaigns by Bada et al, in which they advise against fear campaigns as these do not contribute to behaviour changing processes, instead, instilling anxiety and feelings of powerlessness, thus reducing the feasibility of CS/IS practices for individuals and corporations (2015).

2.1.4.3 Worker's Perceived Level of Control

The ability to make decisions for oneself and actually influence the external environment is a great motivational factor for many, however, unfortunately, this luxury is seldom available to all workers (Hadlington et al, 2018). In their recent literature review on the matter, Hadlington et al stress that LoC is an old concept, yet one that is becoming increasingly salient in modern management practices (2018). With regards to LoC, there is an external or internal orientation of LoC, which is used to describe situations in which workers feel powerless to take actions (because they cannot due to organisational reasons) or situations in which a worker is given a higher level of trust and therefore ability to influence organisational outcomes, respectively (Hadlington et al, 2018).

An internal LoC is believed to be needed for good ISA and IS compliance. In more recent articles, such as the study by Hadlington et al, LoC is viewed as being important with regards to IS compliance and, consequently, SA (2018). Indeed, according to this study, an external LoC allows individuals to devote more time to IS principles and, consequently, is believed to be able to influence an individual's/organisation's likelihood of IS compliance (2018). Hadlington and her co-researchers believe that the internal reasoning for this is that with a greater level of direct accountability, workers will make sure to fulfil the working requirements, as failure to comply will be directly linked to them, as opposed to their manager.

On the other hand, researchers argue that an external LoC leads to neutralization behaviours that workers ultimately use to justify decisions against directives. Neutralization refers to the idea commonly used in criminology, which explains internal thought processes. Those are ultimately used to justify a worker's decision to act against the expected norms, i.e. to be deviant (Hindelang, 1973). Aside from indirectly corroborating Hadlington et al's research, other researchers such as Willison and Warkentin attempted to better understand neutralization behaviours in 2013, and have ultimately found that neutralization behaviours are prevalent within the context of ISA and IS compliance (2013). Subsequent work by Barlow, Warkentin, Orlow and Dennis identified *defence of necessity* as the most prevalent neutralization behaviour (2015). According to Siponen and Vance, type of behaviour

essentially represents the internal reasoning that given the context of work, a worker will prioritize direct orders, as opposed to secondary ones that may get in the way (2010).

2.1.4.4 Risk Assessment

This section describes how people generally perceive risk with regards to the General Deterrence Theory (GDT), followed by the application of ISO27001 (International Organisation for Standardization) standard onto risk assessment. Knowledge on risk assessment practices and risk perception attitudes will assist in determining the factors promoting ISA of the organisation. GDT attempts to explain how people make connections between their beliefs regarding the severity of punishment. It states that people rationally assess the risk of consequences when deciding whether to commit crimes or violate rules. According to this theory, the risk of consequences is decomposed into severity, certainty and celerity of sanctions (Zhang & Yang, 2018). If an individual feels that the severity, certainty and/or celerity of a possible negative consequence are high, the associated behaviour is judged to be risky. Risk assessment in this particular case refers to the way individuals evaluate the potential negative consequences of improper action or the failure stemming from willingness or reluctance to comply with mandated rules.

IS policy derives the framework for the extensive information resource use of the enterprise. According to a research review by Wong, Tan, Tan & Tsen, GDT proposes that illegitimate behaviour may be regulated by sanctions. It is accentuating the disincentives against crimes and the influence of those on preventing others from deviancy (2018). The classic theoretical framework implies that in the context of a strict determinant punishment, rational individuals would respond to efficient policy and evaluate the gains and loss of committing a deviant act. Assuming that the employees would be deterred from risky and abusing security behaviour patterns under appropriate organisational policies, this theory has been commonly applied in the IS safety landscape.

The theoretical framework has been improved with the extension of modern policies. Under an assumption of security education and technical controls to be decreasing information misuse, GDT became linked to these control measures. It is commonly suggested that password safety, anti-virus systems, and educational awareness training can aid in preventing

risky behaviour. Security policies comply with the deterrence theory and leverage similar principles, i.e. shaping the definition of illegitimate behaviour patterns in relation to the perceived punishment for it (Wong et al, 2018).

ISO27001 provides an essential departmental way to operationalise the GDT principles in organisational practice. To validate the analysis of the performance of cyber protective measures, the adherence to risk assessment processes shall be monitored. One of the key pillars of IS management is the ISO27001 international standard which evaluates the interdependencies of people, technologies, and processes in information management (IT Governance Ltd, 2020).

ISO27001 risk assessment sets a sound foundation for organisational information security. The IS objectives should be following the risk assessment and be promoted within the organisation. The risk treatment plan is implemented based on the risk assessment and objectives, according to ISO 27001 section 6. A common way of managing risks based on ISO 27001 involves the following sections (Kosutic, 2020):

1. *Definition of risk assessment methodology:* In order for the whole organisation to perform in the same way, the types of risk assessments, scales, and risk levels shall be defined, since the majority of challenges within risk assessments render from improper communication between the organisational departments.

2. *Implementation:* This phase involves identification of the assets and possible vulnerabilities associated with them, as well as estimation of potential risks.

3. *Risk treatment*: Mitigation of the risks might imply transfers to third parties, application of security controls, avoidance, acceptance in case of higher mitigation costs than expected damage. The company shall derive plans for risk cuts with the least investments.

4. *Reporting for dynamic checks and auditing*

5. *Statement of applicability*: Document envisioning the current security profile based on risk planning, which is utilized by certification auditors.

6. *Risk treatment plan:* Active planning accounting for timeframes, scope, budgets, and stuff which requires leadership commitment and approval (Kosutic, 2020).

Following the general deterrence theory and its practical application in the essence of the risk assessment principles will aid in investigating the risk perception in the analysis chapter, as a component of compliance intention factors effects.

2.2 Technical Theoretical Aspects

2.2.1 Information Security Awareness (ISA)

Naturally, for people to be able to comply with IS policies of an organisation they, first of all, need to be aware of the necessary limitations, in order to appropriately act according to these principles. This is the idea behind Information Security Awareness. Information Security Awareness (ISA) refers to the manner in which employees understand and apply organisational policies on IS/CS, following available policies, rules, and guidelines (McCormac, Calic, Parsons, Butaviciu, Pattinson & Lillie, 2018). Researchers, therefore, believe that ISA is considered a part of organisational culture, as per the definitions of Schein (Wiley, McCormac & Calic, 2019).

General levels of ISA are believed to be good predictors of not only the general ability to deter cyber attacks on an organisation, but also help in reinforcing appropriate behaviour. Indeed, according to research by Parsons, Young, Butavicious, McCormac, Pattinson, and Jeram, a good ISA level within an organisation increases the likelihood of workers being able to follow through the IS protocols they are subjected to, due to internalization mechanisms and mutual learning (2015). Consequently, it becomes crucial for top management to find ways through which to increase and monitor ISA levels within organisations to reduce the propensity of an organisation to make errors with regards to IS enforcement (Parsons et al, 2015).

Consequently, ISA as such is an excellent proxy through which to assess IS compliance, yet it is limited by the fact that ISA by nature is difficult to gauge in an organisational context.

Parsons has attempted to make a case for the HAIS-Q, a scenario and point-based questionnaire that gives workers theoretical scenarios and scores them based on a selection of potential courses of action (Parsons et al, 2015). However, researchers tend to agree that these frameworks are self-serving in nature, as they do not realistically assess the knowledge of workers, rather their ability to effectively reason on the test (Wiley, McCormac & Calic, 2019). Researchers like Wiley, McCormac, and Calic instead opted to quantitatively assess which qualities of workers are the best predictors with regards to their ISA (2019). In their research, it was concluded that age, gender, and personality are some of the greatest predictors (or are the most statistically significant in their model). Unfortunately, gender and personality can rarely be controlled by management, but the fact that *age* is of consequence is of interest.

This confirms the fact that ISA is cultivated on a long-term basis and further reaffirms that managerial practices can be improved to reduce the statistical significance of greater age in ISA and IS compliance, for example, through greater interaction and encouragement of learning processes. Indeed, a comprehensive overview of ISA by Jeong, Mihelcic, Oliver, and Rudolph (2019) has identified that aside from the general culture of the nation, age is an ISA predictor due to learning, experience, and possibly also due to the fact that older individuals may have problems with new technologies. Therefore, ISA is an important aspect to consider when it comes to assessing the impact of organizational culture on compliance.

2.2.2 Data Breaches and Information Leakages

For the purposes of this study, it is not entirely important to understand the nature of information leakages from a technical side, but it is crucial to understand what these terms mean within the context of the chosen departments for clarifying purposes, and more importantly to explain how these mistakes can be handled from a managerial perspective.

To match the goals of this thesis, only unintentional leakages are considered, given the fact that only those can be prevented through managerial practices. Wong, Tan & Tseng in their literature review outline leakages as generally being *intentional* or *unintentional* (2018). *Unintentional leakage* is described as an occurrence in which an insider reveals critical business information not meant to be shared with third parties unintentionally (Ritala,

Olander, Michailova & Husted, 2015). *Intentional leakage* is an occurrence in which an insider reveals critical business information for selfish purposes ranging from basic grudge to incentivized corporate espionage (Ritala et al, 2015). As could be expected by now, most companies will not openly discuss intentional leakages, as it represents a crucial managerial failure, and more importantly, it is not an aspect of the small mistakes that have been described in previous sections — intentional leakages cannot be fully prevented, but unintentional can be minimized given their nature.

Unintentional leakages that have not been exploited can be used as a platform for adaptation of managerial practices within an organisation. As outlined by Wong, Tan and Tseng, unintentional leakage is the result of human conditions pertaining to cognition, including but not limited to: lack of clarity of protocols, poor general knowledge of required protocols, weak situational awareness, professional pride (as an impediment to crucial information sharing), and poor cognitive processes of workers (2018). Therefore, certain organisational factors (such as knowledge, motivation, and dedication) can lead to poor decisions which may endanger the company's CS/IS (2018). Consequently, this type of leakage is far more likely to be influenced by proper management practices. Hence, the decision has been made to focus only on unintentional leakages and their reasons.

2.2.3 Digital Maturity

Since the research is performed in Sweden, its digital maturity has to be taken into consideration for a comprehensive view onto its infrastructure facilitation, technological environment, and knowledge communication. Digital maturity corresponds to the performance and competency within disruptive technology across culture, processes, and innovation. According to the IMD World Digital Competitiveness Ranking 2019, Sweden is the top third most digitally mature nation as it promotes a balanced pattern in the knowledge generation, developing supportive technology environments and nurturing systems for innovation adoption, implying relatively common collective effort in addressing cybersecurity (2020).

A sequence of academic findings corresponds to the linkage between the levels of digital and cyber maturity with the national culture which is quite relevant in the domain of this thesis and, therefore, will be elaborated in further detail. For instance, the study by Jeong, Grobler, Chamikara, & Rudolph, C. (2019) analyses the impact of the variables of national culture (HCD) and cybersecurity maturity on identifying the relationship with riskier cybersecurity behaviours. The research substantiates that there is a significant influence of the cultural elements of Power Distance, Long-term Orientation and Individualism on cyber maturity level (CML), implying that the national culture must be taken into consideration when deriving frameworks and regulations within cybersecurity growth.

Application of HCD indicates that short-term orientation is related to lower CML since individuals often neglect to pay attention to their long-term security preferences which may deem weaker initial security strength. High individualism index is associated with stronger CML since societies of cultures strong in this dimension prioritise secure and private online identity. Moreover, low power distance is also related to higher CML, because cultures with high power distance, in contrast, are usually more dependent on authorities actions, therefore are not fully aware of the risks on their own. The implication of HCD on CML overall signifies strong levels of cyber maturity in Sweden since it has a quite low power distance, high individualism and relatively strong long-term orientation dimensions (Hofstede Insights, 2015). High CML may explain somewhat less strict digital policies supported by the higher trust in digital maturity.

Transitioning from national to organisation dimension, a key component to consider when measuring digital maturity of an organisation is leveraging the BSIMM, which will also further expand the maintenance of ISA. BSIMM (Building Security in Maturity Model) is a security maturity model which organises the initiatives for estimating the level of maturity and recommending practises for the development of security in an organisation (BSIMM, 2020). It includes several categories - governance, intelligence, architecture analysis, and deployment, with the first being most salient for the purposes of this thesis. The governance domain highlights such activities as awareness training, translation of compliance needs, and security leadership communication. One of the critical elements of BSIMM metrics in terms of information security awareness is the notation of satellites [SM2.3: 52]. Satellite is a group

of people with a high-security awareness which assists in shaping a network which accelerates the absorption of security knowledge within the organisation. Satellites can be chosen during training or volunteering activities. Strong satellites signal high maturity and strong interdepartmental links of awareness, while digital advancement normally enhances the strength of satellites. The presence of satellites indicates and refers to high levels of ISA and will be taken into account in the investigation of the organisational IS compliance (BSIMM, 2020).

Taking into consideration the overall digital maturity of Sweden, specific security maturity levels of the organisation, the strength of governance activities, and satellites will play a major role in estimating the interdepartmental ISA and compliance with IS practices.

2.3 Key CS/IS Governance Principles - Linking Societal and Technical Segments

In order to properly highlight the subsequent section dealing with adherence to governance and policies and connect the societal and cultural theory with technical aspects, an overview of research on most prominent governance elements is provided in the following paragraphs. A summary of the governance factors will further allow evaluating the viability of an organisation's CS policy and attitude to ISA of the employees.

Institutions and governments are undertaking various cybersecurity initiatives, including standardisation, guidance, and regulations, in order to deal with cyber threats. According to the ISO/IEC 27001 standard (International Organisation for Standardization and International Electrotechnical Commission), IT governance is stated as “the system by which an organisation directs and controls security governance, specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks”. Security professionals are challenged with governing and maintaining cyber arrangements. Guidance principles are crucial in exhibiting the cybersecurity value for a company and play a crucial role in balancing the risks

(Binwal, 2015). These principles encompass the foundation for cybersecurity as an essential component of information safety:

Principle 1. Estimating the potential effect of the cybercrime

The notation of cybersecurity is often utilized in the context of the effects of cyberwarfare. In order to efficiently study the levels of risk and impacts on the organisation, in-depth information on the damage on end-users shall be obtained.

Principle 2. Evaluation of organisational and personal culture and the cyber behaviour patterns

Despite the reinforcements of preventive procedures in information infrastructures, human fact prevails as the key threat to cybersecurity. Situational and behavioural patterns shall be considered (Dreibelbis, 2016). In accordance with the growing literature emphasising the importance of conscientiousness predictive to cybersecurity behaviour, the study supports the assumption of personality being essential in relationship to cybersecurity behaviour patterns (Shappie, Dawson & Debb, 2019). People often behave not aligned with their initial intentions, therefore it is not surprising that many still violate security practises (Ajzen, Brown, & Carvajal, 2004). Traditional personality assessments can be leveraged as a tool screening the employees for the likelihood of expected cyber behaviour. Based on the diversity of the spectrum of employee personalities, various training programs shall be developed. These measures convey a potential to decrease the inside threats. Governance principles account for cultural and individual factors integrating those into tactical security initiatives.

Principle 3. Identification of the context and risk aversion level

Expected return and tolerance to risks are pivotal in identifying the adoption of the cybersecurity strategies. These definitions have to be adopted by all organisational departments. Furthermore, cost-benefit, investments, values considerations shall be taken in relation to cybersecurity (Kriz, 2011).

Principle 4. Institute a set of governance measures

Cybersecurity governance provides a clear vector of development as well as limitations, adjusting for the transforming objectives of the enterprise (Kriz, 2011).

Principle 5. Assurance and objectives identification

Assurance infers the deploying efficient countermeasures and ensuring compliance with the relevant standards and plausible objectives (DNW GL, 2019).

Principle 6. Evolving cybersecurity systems

Cybercrime is targeting the weakest point of the organisational system. Optimized cybersecurity implies comprehension of the interdependencies of the elements and the dynamic performance of governance and management (Kriz, 2011).

Most companies possess a sufficient set of security regulations pertaining to their attitude to information security. Nevertheless, the diffusions of the policies signed by senior management throughout the organisation often engender governance challenges. Previous literature research suggests that one of such crucial challenges may be the fact of varying levels of ISA between different organisational departments, rendering systematic mismatches. Investigating and analysing those is essential for an effective cybersecurity performance. In the modern environment which proliferates with novel sophisticated threats, the enterprises often face difficulties with cybersecurity governance reinforcements. Diverse organisational assessments are used in the area: Cyber Resilience Reviews (CRRs), Information Security Continuous Monitoring Assessments (ISCMs), External Dependencies Management (EDM) Assessments. With regard to CS governance, the existing research has demonstrated that the majority of the organisations are commonly bewildered with the following complexities (Swinton, 2019):

1. *Cybersecurity Strategy and Vision*, which refer to identifying needs, KPIs, scope and continuity of CS practises.
2. *Standardization* is another complexity related to establishing repetitive tasks to ensure consistency.

3. Moreover, CS governance also has to be *accountable* – complied throughout all levels of the organisation. The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is advocating for the enforcement of safety into IS via system development life cycle (SDLC). Dynamic monitoring is performed to facilitate operations and situational awareness.
4. *Supportive leadership* engaging the entire enterprise and incorporating high-level standards is another vital element. According to ISO27001 section 5, the key pillars of plausible leadership features for outstanding cybersecurity governance include ensuring the integration of the requirements and resources into the organisational processes, communicating the goals and significance of efficient IS safety, supporting employee contributions and promoting dynamic updates. Cybersecurity policy shall be aligned with organisational purpose, available in a documented form to stakeholders, established within frameworks, communicated on all levels of the organisation. Leadership plays the pivotal role is diffusion and absorption of ISA throughout different organisational levels (ISMS, 2020).
5. *Availability of relevant resources* is required to meet cybersecurity governance compliance with prioritised allocation and fundings for training and tools (Swinton, 2019).

The above-described principles outline the general foundations of CS/IS governance which, in turn, can guide the reader in the comprehension of personnel behaviour in terms of IS compliance. The governance activities may highlight the risks of parochialism emergence and recommend ways of dealing with those, which is expected to be stressed in the analysis of employee behaviour patterns. The issue of a rather narrow corporate perspective remains salient limiting interdepartmental ISA. The governance principles will be referred to and serve as an outline for analysing the technical and non-technical employees attitudes to IS

3 Methodology

Briefly, this chapter is presenting the way in which the thesis has been carried out. Due to external constraints, convenience sampling was performed and varied quality data from Swedish respondents was obtained. This chapter comments on the choice of respondents, paying attention to a stigma of non-IT personnel failing to believe they can contribute to the security discussion. This chapter guides the reader through gradual decision-making of the authors regarding all information relevant to the research approach. Primary data collection methods are outlined, with a general wariness of the fact that any and all verbal communication is subjected to a qualitative nature which may impact interpretation, fuelled by the author's preconceived notions. Secondary data served as a way to familiarize oneself with the topic at hand. Credibility, transferability, dependability, and confirmability of the research were analysed. Given the constraints of information gathering during the pandemic, primary research had to be readjusted to ensure the validity and quality of data. Consequently, primary research has been carried out through lengthy semi-structured interviews, which address areas of interest outlined in *Chapter 2*. Data collection and process has been summarized, and limitations of this approach (a qualitative study) have been addressed to prove that the authors are aware of the constraints of this method, highlighting subjectivity, replication problems, generalization problems, and lack of transparency. Lastly, the authors provide a short section to outline the impact that the novel coronavirus outbreak had on the strained communication and consequently reduced the availability of knowledge leads and subsequent response rates.

3.1 Research Approach: General Information

With regards to the previous chapter, it becomes apparent that the studied research area cannot adequately be addressed through quantitative means unless it is a matter of

understanding the prevalence of behaviours or attitudes through statistical methods. However, that approach does not solve the underlying questions regarding the nature of the relationships of the previously highlighted socio-technical problem. Therefore, a qualitative approach had to be adopted.

A case study was found to be the most optimal format, as it allows for a qualitative approach. Bryman and Bell claim that *"what distinguishes a case study from other research designs is the focus on a bounded situation or system, an entity with a purpose and functioning parts"* (2011, p.60), which is ideal given our interests in understanding the nature of organizational culture and IS compliance in Sweden. Furthermore, Bryman and Bell (2011) reason that qualitative studies require greater intellectual flexibility due to the inherent fact that sensemaking depends on the understanding of the topic at hand and the general creativity in interpretation to reach appropriate conclusions. Needless to say, once again that is highly appropriate as it allows us to explore the data through an interpretative, hermeneutic paradigm.

The decision to adopt a qualitative approach, however, requires certain assumptions to be made, especially regarding the nature of truth. This study rests on the authors' acceptance of the interpretive paradigm also known as interpretivism, therefore, it is assumed that the world is socially constructed by interaction of individuals with their world and reality (Bryman & Bell, 2011, p.16). In the absence of a better alternative, our respondents' words are for the most part assumed to represent the truth, and consequently, the value of the conclusions will be dependent on this assumption.

3.1.1 Research Design

Having developed a greater understanding of the nature of this socio-technical issue, finding a way through which to adequately get insight into the views of Swedish workers was needed. Therefore, a question was brought up: whom to talk to and why?

Certain assumptions had to be made regarding the individuals of interest, who could adequately help the authors to contribute meaningfully to the final conclusions of this thesis. It is crucial to highlight that the stated problem refers to issues pertaining to the relationship

between people and IT infrastructures. Consequently, it makes sense that individuals from departments responsible for the management of human-IT interactions and individuals responsible for the IT infrastructures themselves are of key significance. Such an assumption is validated by the work of Bada, Nurse, and Sasse on the effectiveness of CS initiatives, which argues that information managers need to structure principles of IS in such a way to create perceivable practicality to encourage behavioural change (2015).

Consequently, IT managers/experts, and CS/IS managers/experts are certainly individuals that can help in the sensemaking this thesis sets out to accomplish. However, there is an additional entity — the people who will be subjected to the IS protocols established by the CS/IS and IT departments of the organisation. However, due to data gathering limitations (general paranoia and lack of willing information leads) outlined in following sections, it was ultimately decided not to include this group. This was based on the fact that the literature review portrays non-tech workers as disinterested, and ultimately unable to change the organisational paradigms regarding CS/IS protocols. That decision-making power and consequently ability to affect organisational culture (such as ISA) rests in the hands of the CS/IS and IT departments.

Following this decision, the proper information collection medium was needed. Out of necessity and practicality, the authors opted to conduct digital semi-structured interviews. According to Bryman and Bell, a semi-structured interview *"...typically refers to a context in which the interviewer has a series of questions that are in the general form of an interview schedule but is able to vary the sequence of questions"* (2011, p.246). Given the complex nature of IS compliance, this structure is appropriate as it allows researchers to pry further into the beliefs of contacted experts, should an interesting thought appear during the interviews themselves. Additionally, given the language constraints of the respondents and the usage of English as the lingua franca, the interviewers could clarify the questions if a language barrier appears. That is substantially stemmed from the fact that open-ended questions have been used as they represent the best way to avoid personal bias that could arise from knowledge gained during the literature review process (Bryman & Bell, 2011).

3.1.2 Sampling

Due to the outbreak of COVID-19, the sampling used in this thesis has been limited, yet rendered somewhat qualitatively flexible. In the initial stages of this thesis, it was decided that the best method to adopt would be to work with a single organisation to facilitate information gathering and to enable potential follow-up opportunities, should further information be needed. According to Bryman and Bell (2011), this is the most basic form of the case study and one that is the easiest to manage. Due to the authors' previous connections with experts in the field at a respectable consulting company, a viable research contact has been established, who demonstrated a great desire to aid the authors in their thesis work. This relationship has been maintained over a series of weeks and appeared increasingly more fruitful. However, as the impacts of COVID-19 have not been anticipated, the organisation itself eventually became unable to efficiently participate due to a spike in the workload, and alternative knowledge sources had to be sought out on fairly short notice.

Cold calling non-tech individuals has been fruitless, due to the paranoia regarding the topic. Initially, there was a desire to contact conventional workers (non-tech), but regardless of the persuasion methods used, almost all aside from a single contact eventually decided not to participate. The most common excuse being along the lines of the fact that ISA is not a concern of their department, and that IT departments should be contacted instead. Indeed, there appears to be a certain stigma regarding the discussion of Information Security, given its somewhat mysterious, but perceptibly important nature. Most workers believed they were not informed enough to be able to tell what they can say and what they cannot. Consequently, out of the necessity of the situation, but also surprisingly due to the low belief of their own potential to contribute, this category of knowledge sources has been removed from this thesis.

Although these unfortunate events were devastating given the time investment into the relationship, the situation allowed the authors to reach out to various experts to get a varied qualitative sample. The research focus of this thesis is experienced for the most part by all companies within Sweden to a varying degree; in the absence of a single anchoring company, and with limited options, the authors, unfortunately, relied on convenience sampling in the sense of seeking out "good samaritans" who sympathized with the intent of the authors (the

data gathered is illustrated in the table below). Furthermore, Bryman and Bell point out that the emphasis of the qualitative studies should, by the nature of the study itself, be placed on the quality and diversity of perspectives, as well as how they best serve to answer the research aims of the project (2011). Although a less than ideal situation, given the existing constraints, it is still believed by the authors that the samples gathered can and do contribute in answering the proposed research question.

Table A. Summary of Conducted Interviews

Pseudonym	**Role/Position**	**Department**	**Organisation**	**Length of the Interview**	**Interview Date**
Petra	Cybersecurity Lead	CS Expert	Multinational Consulting Firm	30 min	27 April 2020
Benjamin	Cybersecurity Lead	CS Expert	Multinational Consulting Firm	30 min	27 April 2020
Tyrell	Front-end Developer	IT	Database Engines Startup	50 min	2 May 2020
Angela	Fraud & AML Specialist	IT	Consumer Finance Bank	30 min	3 May 2020
Charles	IT Specialist	IT	Fast Fashion Multinational & Tech Consultancy	40 min	6 May 2020
Darlene	IT Manager	IT	Retail	30 min	6 May 2020
Stephan	Start-up CISO	CS Expert	Health Tech Startup	40 min	7 May 2020
Elliot	CS Senior Advisor	CS Expert	Cybersecurity Startup	35 min	7 May 2020
David	Risk & Compliance	CS Expert	Personal Finance Advisory	25 min	1 May 2020

	Consultant				
Gideon	Senior Backend Engineer	IT	Online Retail	40 min	16 May 2020

3.1.3 Data Collection Method

3.1.3.1 Primary Data

When it comes to qualitative studies, Bryman and Bell (2011) emphasize the practical importance of primary research. Hence, the most important knowledge asset of the thesis is the gathered responses from the interviews, which serve as the primary data. On a general level, Bryman and Bell (2011) argue that primary data offers fresh perspectives which cannot be often acquired through secondary research, and more importantly, the data itself can be gathered in such a manner that it can directly aid with answering potential research questions, as opposed to awkwardly trying to establish connections in support of the potential thesis. Such an approach is argued to be especially valuable when the point of the research is to expand on an existing knowledge paradigm and aid in sensemaking (Bryman & Bell, 2011).

Although a potentially problematic medium, e-communication platforms like GoogleMeet, Skype and Zoom have been used. After a respondent has confirmed their intent in participating, they have been given a choice between the three mediums. On the day of the interview, the research participant has been presented with the questions in Appendix A and given the freedom to express themselves. The interviewer transcribed the responses and engaged only to either hasten the interview (to prevent verbal tangents) or to potentially clarify the questions in the event that the neutral language was deemed to be difficult to understand due to language barriers.

According to Bryman and Bell (2011), the questions needed to be appropriate with regards to the research interest and had to enable the authors to be able to reflect on the gathered data, through the lenses presented in theoretical foundations. Consequently, general questions that dealt with ISA have been selected, and few department-specific questions have been adapted

to be suitable for either of the two departments (CS/IS or IT). The questions presented in the interview were limited to eight to ensure that a respondent would be able to adequately answer each question within a limited time-span. Indeed, it was found that emphasis on short-time investment has been a major reason for respondents to confirm their participation, though in most cases our respondents would discuss the material in greater detail. Consequently, the interviews were usually ten minutes longer than what was originally anticipated. All names of our respondents were assigned randomly to preserve their anonymity, and only relevant information is presented to prove their ability to contribute to the aims of this thesis.

3.1.3.2 Secondary Data

According to Bryman and Bell, in the absence of the first-hand experience with the subject matter, secondary data serves as an excellent way to generate a foundational understanding which can be used for primary-data gathering purposes (e.g.: interview question choice, research design or selection of interpretive frameworks) (2011). The researchers are fairly new to the topic specifics, which meant that a large general literature review had to be done to adequately develop the ability of the researchers to discern what is important and what is not — eventually leading to the material presented in *Chapter 2*. However, Bryman and Bell explain that when it comes to secondary data, it needs to be of a high quality so as to prevent false initial beliefs (2011). Indeed, the best method, in general, is believed to be gathering information from reputable sources such as academic journals, peer-reviewed scientific articles or even university-level academic work (Bryman & Bell, 2011).

Consequently, the choice of secondary data has been limited to accepted and used frameworks and peer-reviewed articles available through Lund University's LUB database. The choice of frameworks was flexible with regards to publishing dates, as it was based primarily on explanatory ability. Academic journals on ISA and IS compliance, on the other hand, were limited to a publishing date within 2009-2019 to prevent the adoption of outdated ideas that may have been disproved in recent years. This is generally due to the relatively recent nature of ISA as an area of academic interest (McEvoy & Kowalski, 2019). Majority of secondary data has been sourced from reputable journals such as Information & Computer Security, Computers & Security, IEEE Security & Privacy, among others. The key was for the articles

to be peer-reviewed to ensure theoretical and academic validity, as urged by Bryman & Bell (2011).

3.2 Empirical Data

The collection of empirical data, all things and circumstances considered, has been fairly straightforward, majority of limitations have been discussed in previous sections, however, what has to be addressed is the nature of the data itself and the feasibility of analysis, which is the point of the current section.

Given the nature of the research as qualitative semi-structured interviews, the authors have been offered a unique way to look into the minds of the research participants, and in doing so understand where their minds dwell on the presented issue. In essence, their focus on particular aspects of the questions highlight where their professional interests lie, and what they consider to be redundant, thus offering a perception prism through which to address the underlying secondary research on which this thesis has been based. This, in turn, allows the authors to gain the way the experts view their own role within the organisations and can serve as both a reflection of their own influence on the way things are done within an organisation, while also highlighting their own beliefs regarding how things could potentially be. Consequently, as outlined previously, the interpretive paradigm is assumed to be true, and that these views represent the participants' true views, thus giving gravity to the potential analysis with regards to the participants' beliefs and influence with regards to organisational culture. However, as Bryman and Bell point out, this assumption rests on the fact that the respondents are able to verbalize their beliefs efficiently to offer their true view, as opposed to a convenient response limited by the respondents' command of English.

Given the semi-structured nature of the interview, the authors have received useful material, but also material that is redundant to the purposes of this thesis. The most compelling thoughts from each respondent will be used in the analysis section, as it has been found difficult to separate discussing empirical data from the actual analysis.

3.3 Validity and Reliability

Without appropriate methods, the ultimate findings of the thesis (regardless of how compelling they may be) cannot be justified (Bryman & Bell, 2011). If that is the case, there are several identified qualities of studies/theses that increase the value of any bit of academic research by establishing the thesis as valid and reliable. Bryman and Bell identify four crucial qualities that aid in making sure that a thesis can be regarded as reliable and valid, namely: credibility, transferability, dependability and confirmability (2011, p.392).

In terms of credibility, the major importance lies in ensuring that a representative sample has been obtained. Indeed, *"stress on multiple accounts of social reality is especially evident in the trustworthiness criterion of credibility"* according to Bryman and Bell (2011, p.395). Consequently, it is important to obtain a sample that can adequately be considered to illustrate at least partially the reality of what it is that is studied. Multiple individuals have been approached, and their ideas, beliefs and attitudes will need to be cross-referenced in order to justify the potential conclusions that may be reached. Additionally, the chosen frameworks need to be of logical consequence. There is no point in attempting to reconcile the data, with something that cannot explain it. This part of credibility has been addressed through the justification presented in *Chapter 2*.

With regards to transferability, Bryman and Bell reason that in qualitative studies, the studied group needs to be at least somewhat defined, yet flexible enough to allow for findings to be able to be applied within different mediums (Bryman & Bell, 2011). As the authors put it, *"qualitative findings tend to be orientated to the contextual uniqueness and significance of the aspect of the social world being studied"* (2011, p.398). Simply put, the nature of the thesis needs to be flexible enough to allow for potential findings to be reasonably extrapolated to entities aside from those specifics that have been studied. Given the sensemaking purpose of this study, the findings can reasonably be considered transferable to other entities in Sweden aside from those that have been addressed in the empirical work.

Dependability and confirmability are linked to the fact that in qualitative research the material needs to be tracked and properly assigned, which is done through extensive note-taking, and more importantly, clear explanations regarding decisions made. Bryman and Bell, highlight that *"...problem formulation, selection of research participants, fieldwork notes, interview transcripts, data analysis decisions..."* all need to be justified and presented to allow for reliability to be confirmed (2011, p.398). Given this is the basic procedure, this quality should be self-explanatory.

3.4 Limitations

No matter the effort, there are always ways in which the study can be improved which can either be due to internal (e.g.: problematization, research approach, design or interview format) or external factors (e.g.: availability of previous research on which to build, access to primary data, general awareness of the issue). Bryman and Bell identify four primary types of limitations for qualitative research: subjectivity, replication problems, generalization problems, and lack of transparency (2011, p.408).

Indeed, subjectivity is a major issue, especially given the dependability of people to explain their own views. Everyone views the world through their own interpretative paradigm, including respondents and the authors themselves. This implies that no same response can be expected from a group of individuals. Sampling is of major concern as this is an approach that can help reduce bias in data through randomization in qualitative and quantitative studies (Bryman & Bell, 2011). Similarly, a crucial concern is the nature of the responses. In a sense we all desire honesty, but we also rarely appreciate it due to the potential social effects that the perceived truth may have on the opinions or actions of others. In a simple sense, we always wear a particular mask, that is given to us by our social context, and this, in turn, shapes the way we voice our opinions as those may have consequences. As Oscar Wilde puts it: *"Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth".* Unfortunately, the sampling issue could not be addressed, but the nature of the

interviews and their anonymity is believed to be able to coax out the true views of our respondents, and therefore offer a mask in its own way.

The replication problem refers to the fact that no single sample is the same. Conducting this study again with a different potentially more varied group could lead to different insights, given that these individuals will have a different unique way of viewing the world around them and the nature of the identified socio-technical problem of IS compliance. Since convenience sampling was performed with a limited number of people, it is not certain that the authors can infer the general trend that all companies follow a similar pattern shown in the analysis. Consequently, it has to be assumed that for the purposes of this study, the gathered responses represent a potential way of interpreting and answering the research question. Additionally, other researchers may opt to view the problem through different means. Bryman and Bell surmise that the best way to counter this issue is through transparency in explanation and data gathering (2011). While the authors understand the nature of this limitation, given the sensemaking purpose of this study it is concluded that general conclusions can still contribute effectively to answer the proposed research question.

According to Bryman and Bell, *"when participant observation is used or when unstructured interviews are conducted with a small number of individuals in a certain organization or locality, they argue that it is impossible to know how the findings can be generalized to other settings"* (2011, p.428). Indeed, if the research design is too constrictive and far too specific, the potential contribution is only and solely relevant to the research participants. In a practical example, in the study of a uniquely rare condition, general findings may not be applicable to others given the low prevalence of patients. In more specific terms, if the research interest of this thesis is too restrictive, the conclusions themselves are not very generalizable and offer a meagre contribution to the knowledge pool of the research area. This is a risk that needs to be considered, yet ultimately is one that is believed to be unlikely to occur given the nature of mankind's relationship with IT systems, and more importantly the fact that individuals from different companies have been approached in the fieldwork conducted for this thesis.

The issue of transparency is perhaps the most important limitation of this study, given the nature of the authors, the importance of interviews, and the reliance on the interpretation of

language. The authors act as interpreters and researchers alike, and base both on their background regarding the area of research, consequently although substantiated by the presented literature review and methodological overview. The presented approach may not be the best approach — though given the perspective of the authors it may be the most viable one. As Bryman and Bell point out the researchers in a qualitative study are subject to their own subjective nature (Bryman & Bell, 2011). Additionally, given the distribution of the work, each author focused on a particular aspect of the problem, essentially becoming specialized in different chunks that have been outlined in *Chapter 2.* Consequently, during the interviews, personal bias could manifest itself, in the sense that during clarification (which arises as a result of the language barrier) the authors coil inadvertently nudge the answer in a particular way. With the greater familiarity of the topic, the author (interviewer) gains a greater ability to express specific details in a neutral fashion but will be unable to do so on topics on which the author/interviewer is less informed. The creation of a standardized and mutually approved set of questions was designed to reduce the likelihood of such an occurrence, but as Bryman and Bell point out, these biases can accidentally express themselves in the most minute form (2011).

3.4.1 Impact of COVID-19 on Data Gathering

Although it is understood that the impact of COVID-19 on global society is likely well known, given the ongoing nature of the issue, a little more emphasis should be given to understand the limitations. The initial collaboration with the partner organisation was strained already from initial stages when authors needed to be introduced to the organisation and, given the nature of the studied material, had to clear several security protocols. Simply said, the authors needed to prove their intention, which required time but contributed to trust-building and the time expectation of higher quality data. Eventually, communication became even more strained as demand for the consulting company services skyrocketed in the first weeks of the pandemic. Unfortunately, priorities had to be made, and our partnership had to be altered. Though the contact person has shown apparent desire to help, ultimately, given limitations in communication and the fact that the CISO did not have enough time to provide to the authors for information gathering purposes, the relationship had to be abandoned

altogether. Due to such circumstances, the authors were left with little choice but to reach out to known contacts in Sweden and relied on cold-call, which, for the most part, were fruitless, aside from the presented individuals *(table A)* who provided excellent insights. Under ideal conditions, a more representative sample would be obtained, but the gathered sample is still believed to be of a decent size and meaningful to lead to viable conclusions on the research question.

4 Analysis and Discussion

The nature of this study made it difficult to separate analysis from discussion, which is why the two have been included in a single chapter. The analysis of the empirical data presented in this chapter will offer a proxy through which to assess the self-perceived ability of both the CS/IS and IT departments, and also assess the way in which these departments shape organisational culture with regards to the identified compliance intention factors. It should be noted the use of italics is purely a stylistic choice to differentiate respondents' beliefs from the analysis. Following the analysis of the empirical data is a discussion of findings which will offer a way through which to highlight primary ideas, and relate these to organisational and national culture.

By the end, the data will be presented in such a way to highlight which courses of action should be taken to increase IS compliance based on presented beliefs of CS/IS and IT departments, and the theoretical foundations presented in *chapter 2*. In doing so it is believed that the research question will be adequately answered with emphasis on the nuanced relationships between the departments, and the importance of transparency and collaboration between CS/IS and IT departments. Indeed, from the Swedish cultural paradigm, a greater level of collaboration/transparency would be beneficial in incorporating ISA as a fundamental part of organisational culture, by increasing perceived LoC, and in doing so encouraging higher levels of willful IS compliance.

4.1 Analysis: Cybersecurity Department

The role of CS/IS experts should be quite clear at this point in the thesis: as the primary agents who ensure that protocols are followed, known, and understood, they are the source of ISA within the organisation. However, it appears as though that their potential in influencing

the organisational culture with regards to previously identified factors, such as stress, LoC, and risk assessment seems to be stunted partially due to inherited directives from top management (which make their presence known through the nuance in responses), but more importantly due to a persistent grievance with the IT department, which is thought to perpetuate a false sense of security. Though our respondents have different beliefs regarding their own organisational cultures, they can agree that the nature of the data used and transparency matter the most in defining best practices. However, pressured by top management, there is an apparent trade-off between transparency and accountability. The potential impact of CS/IS experts will be explored based on the CIFs defined previously in the following subsections.

4.1.1 Stress and Resilience

Stress and the way we react to it can be an extremely advantageous proxy for ensuring proper behaviour. Certain organisations are prone to greater levels of stress due to the nature of the work itself, yet it also offers an opportunity for the organic development of resilience, which in turn reduces the propensity for workers to deviate from their directives. In short, having a culture which embraces stress, but has a way of dealing with it effectively, can be a crucial aspect in ensuring that workers will follow directives even if they feel as if these directives actually get in their way. Another point to consider is the nature of control. Stress, as defined earlier, occurs when the management requirements imposed on workers are greater than the self-perceived level of ability of the worker, which results in a situation of work struggles. Consequently, the issue is then how to bridge this gap, and therefore improve the management and, in tandem, the organisational culture.

Most of our CS/IS respondents, however, do not really consider the impact of stress, instead, their time is preoccupied with managing their own requirements. In case these requirements manage to reduce overall stress, the work can be deemed effective, yet in the opposite case, unfortunately, accountability seems to be of higher importance than an organically developed resilience stemming from sufficient levels of ISA. Our CS/IS respondents are torn between believing in the ability of other departments (especially non-administrative workers) and

presuming that stricter controls are required, which is due to the fact that the inherent beliefs of top management trickle down and manifest themselves as components of the organisational culture. As Benjamin points: "*You can't have KPIs [Key Performance Indicator] about trained staff [for ISA]... It is really hard to show ROI [Return on Investment] on this kind of topic*". Unfortunately, the very nature of modern-day business necessitates that decisions (especially in larger organisations) need to have some sort of data or some form of evidence to prove that present and future initiatives are worthwhile. Consequently, as Benjamin, David, and Stephan point out there appears to be an over-reliance on the use of technology on its own, without emphasis, and effort being put into organically developing users. Naturally, this is because of accountability. The parochialism within this department manifests itself in such a way that CS/IS experts are pressured to maintain a clear line of evidence to prove their efforts. As mentioned before, ISA cannot be measured the same way finance or click-through rate can be, and grim reality for CS/IS experts like Benjamin is that when it comes to ISA *"it is easier to measure the number of incidents (per minute, per year)"* than to measure how well the employees themselves are actually able to deter potential attacks or demonstrate enough self-reflection to understand when they've made a mistake. With such a situation, it is no wonder that top management makes specific requirements of CS/IS specialists. Consequently, all of our respondents emphasize the reliance of their departments on e-learning, with limited actual interaction. David, for example, claims: *"We usually measure ISA through the completed training module within our company's LMS [not sharing what LMS it is due to confidentiality] ...trainings are required for all employees"*. However, to what extent can a static, low-stake and "check-box" activity actually increase ISA on a meaningful level? Aside from David, who does claim that these matters work, all other CS/IS experts claim that it is not enough — more interaction is needed. However, David's deviation does bring up an important point that needs to be considered — the nature of the data itself.

In its own way, data is a reflection of the industry, and therefore, data from certain industries is undoubtedly more valuable than from others — to the right individual/organisation anyway. Data in such industries as pharmaceuticals, financial asset management and governments is without a doubt generally far more valuable than those of a small shipping company. David's team essentially works with financial information, and by the nature of the industry itself,

David confirms that people are on average more stressed, and perhaps more rigid when it comes to the discussion of clientele. As David puts it: *"We want our workers to feel proud about what they do, and we try to foster a sense of urgency, action and effectiveness"*. Indeed, David is right in saying that the nature of the job in itself will influence the organisational culture with regards to ISA and IS compliance. For instance, a banker or a consultant working with David will feel better about their position and will covet the social prestige that may come with the industry, aside from being subjected to more regulations, the workers will actively try to think about what they do. This approach additionally tries to leverage this fact to incorporate it organically into the organisation's culture by leveraging it's practical importance: *"Information Security means to properly protect yourself, your critical assets (your identity and sensitive information about yourself), protect your family, and protect the information associated with your job"*. Similarly, Stephan agrees with this sentiment, that the implied sensitivity of the data itself greatly contributes as a self-reinforcing mechanism, which guides principles within his health-care oriented start-up organisation: *"[We strive to]…always have people think about why you're handling data, and don't just do things; the actual motivations for why you are doing things… to have internal principles"*.

Consequently, when it comes to stress or resilience, CS/IS experts do not really occupy their thoughts with how lack of control can actually influence the decision-making abilities, instead opting for using proxies through which they aspire to "channel" (such as in the case of sensitive data) or divert stress through using the current practices available.

4.1.2 Punishment and Reward Systems

Within the grand scheme of things, punishment and rewards help with operationalizing and reinforcing the appropriate behaviour that is expected based on the existing contract between the principal and the agent, thus reducing the likelihood of principal-agent problems. Under normal circumstances, and given the previously presented literature review, the cultivation of ISA and IS compliance is no different. At least that was the assumption, yet Swedish CS/IS managers have shown an interesting level of lenience, where deviations from behaviour

(unless it is obviously due to gross negligence), will make excuses for individuals — and more importantly show a substantial level of empathy.

When questioned about the role of incentives, and, consequently, potential punishments, most if not all CS/IS experts almost visibly recoiled. Naturally, the idea was to use neutral language so as to better get more details and hence understanding of the mechanism's value to the organisational culture, but almost all, aside from David, would go out of their way to emphasize other aspects of the organisation as being substantially more valuable. For example, Benjamin and Petra emphasized changing strategic priorities: "*We need to consider cybersecurity as a strategic risk in the overall assessment no matter the type of business… we need to get more focus knowledge on the management and board level around these themes*". Stephan, on the other hand, could summarize his thoughts on the matter through his own words: *"It is relevant to why it happened, we can talk about individuals, this person was in charge, and then there was a miscommunication — so this says that this team should look more into their process".* The common deviation between these responses could be addressed as a difference in opinions due to the size of the companies. Benjamin's and Petra's consulting agency is substantially larger than Stephan's health-care startup. However, on both ends of the spectrum, we notice one key thing — even the one's in charge do not believe in the value of punishments, and instead would prefer to alter incentives based on values. This paradigm can be likely attributed to the uniqueness of the Swedish culture. The desire to learn, and more importantly to clearly explain the reasons for particular occurrences is something that is very conducive to a society which is based on equality and harmony as it facilitates greater levels of trust which is not only crucial for motivational reasons but also because it leads to greater speed of knowledge generation. Consequently, the views of our CS/IS Experts are in line with the attitudes outlined by Proctor and Chen, but simultaneously deny parts of their study — specifically the value of punishment systems.

In this sense, the presented analysis points towards the fact that the Swedish cultural paradigm does not emphasize reinforcement through positive or negative means as such, in so far as finding ways through which to establish relevance, and more importantly view failures, or

reasons for distributing punishment, to be more beneficially used as indicators that processes need to be changed.

4.1.3 Worker's Perceived Level of Control

The ability to decide for yourself how to handle matters has been highlighted in previous chapters as a means through which workers attain a greater level of commitment to IS compliance and cultivate ISA. However, compliance will be determined by the overall ability of individuals to actually use their directives and their ISA with regards to their end goal. When it comes to the influence of CS/IS experts, their efforts result in two opposing forces.

All CS/IS experts participating in this thesis tend to agree that the value of the data in question will dictate the individual's work commitment, but also shapes the nature of the IS policies that are adopted within the organisation. David, for example, highlights that the rigidity of communication is the result of the sensitive nature of the data and highlights that protocols are aimed at reducing the worker's ability to commit mistakes. As David puts it: *"It is everyone's responsibility to complete pieces of training annually. Then there are the actual contracts, periodical evaluations; people know what they should know"*, however, David still believes that: *"Most general (non-administrative) users will not notice a data breach occurring"*. It is a strange occurrence given the fact that David presents these solutions as a way to ensure compliance, he still presents the case that most people will not be able to tell if they have done something that can compromise the system. Logically, although espoused, these solutions appear to be less than ideal. Incidentally, it is also David who claims that there are attempts that are made to give ISA a practical quality within their organisation: *"We try to have our teams understand that this is just the way it is because it is the best way to ensure that even non-technical people will understand this complicated issue in a way that [they] can understand"*. In David's situation, the management appears to place emphasis on reducing the likelihood of issues given the potential damage as a result of reputational costs. Indeed, as David puts it: *"We've been doing well at keeping our data ours, and our clients trust us"*, — external trust within the industry is difficult to attain, leading to greater dependence on protocols, increase in paranoia, and lower flexibility. Ultimately, in large environments with

high-value data, flexibility is not favoured nearly as much as accountability in the potential event that reputational damage could be devastating to stakeholders.

In Stephan's start-up, he is faced with similar difficulties with the nature of the data his medical company works with, however, his leadership appears to be more progressive, which can be attributed to the fact that his organisation is not as departmentalized as David's. Indeed, Stephan claims: *"...[This is] conceptually how we look at these things...[there is] a general onboarding and some roles have specific other parts — software engineers will have additional onboarding, from both technical and medical staff for what they are working off. We frontload a lot of stuff during the onboarding process"*. Emphasis is placed on interdepartmental cooperation, especially early on in the lifecycle of the company, as this may be the best way to cement these issues. This is further corroborated through Stephan's common reference to the "process" or the teamwork dynamics. In Stephan's company, LoC is not solely external, instead, people are encouraged to learn from one another, and the lower emphasis on negative consequences of failure encourages learning. As he puts it, in the event of situations happening, at the end: *"We explain it so everyone is on the same page, and then if there is anything we could have done to prevent this, and if there are changes we could do and would these changes be reasonable"*. Transparency is encouraged in Stephan's organisation, which is bound to profound effects on the behaviour and beliefs of his fellow team members.

4.1.4 Risk Assessment

Risk assessment is best addressed by the actions that the CS/IS experts take to ensure that they can control the behaviour of the people, and thus negating the potential risk a company can endure during normal operations. However, as highlighted before, there appears to be an extra emphasis on the ability of these measures to be tracked, which is further evidenced by the fact that all CS/IS respondents accept the reality that conventional workers will not "care".

All the CS/IS respondents illustrate that there is a fundamental acceptance of the paradigm that the worker doesn't care, which in turn is fuelled by personal biases, and also business

conduct given by the nature of the data. Petra elaborates on the fact that this can be attributed to the way business is done in consulting. She claims that *"organisations are struggling with getting clients to stop focusing purely only on tech",* which incidentally also leads to the particular way that businesses shape their own demands when it comes to matters such as Information Security. In other words, although Petra agrees that *"you can have every system in the world designed properly but if you don't teach the people you can't have a 100% security against human error"*. So why is that the case? Surely, if the expert is aware of the importance of people using the systems being informed, then the said expert would ensure the methods and practices used would be adequate in solving the issue. David's insight offers a little more clarification, which is based on the data-context: *"We enforce ISA through the use of mandatory video/computer training as well as "Lunch and Learns" related to current event topics… [We] try our best to ensure that our teams are ready for each challenge given the nature of the data that we work with"*. David does not comment on the necessity that is also brought about due to the size of the company. As illustrated before, Stephan and David have opposite views, which can be potentially attributed due to the sheer size of the respective companies. As a company increases from a start-up (e.g. company Stephan works in) to a significant market player (e.g. company David works in), the cost of failure increases proportionately, and, consequently, leads to demands of top management for factors which indirectly enforce IS compliance and ensure oversight. This approach could explain the difference in both respondents' attitudes, while corroborating Petra's view.

In short, risk assessment systems will become increasingly inflexible as the organisation takes a more prominent market position and decisions of top management to ensure their own organisational objectives being met, and enough data being supplied will necessitate an overdependence on technological solutions that can be provided on a massive scale, as opposed to tailoring solutions based on the team.

4.1.5 Digital Maturity

The beliefs of CS/IS respondents regarding the importance of technology have been outlined in the previous section, but it is important to consider what these decisions and beliefs imply

about the organisation in general. A reliance on ensuring accountability, and the subsequent use of technological solutions to statically monitor "performance" of workers highlights that technology as such is far more important than the understanding of the subject matter among the general workers. Given Petra's views regarding technology, Benjamin's comment on the measurability of ISA and IS compliance, Elliot's view can give an even greater insight into why organisations set up their practices the way they do.

The nature of organisational culture reflects itself in a top-down manner, and in this regard, when it comes to digital maturity of organisations, management's perspectives ultimately shape the CS/IS department's actions. Elliot's long-standing experience with CS/IS has offered him a certain perspective that may be lacking from individuals working within extremely defined conditions (such as David) or individuals who had the luxury of interacting with different departments to shape their own understanding (such as Stephan). According to Elliot, compliance is not a matter of incentives — that is to say that punishment and reward systems can be used — but ultimately it is a matter of top management's position on the issue. Indeed, Elliot claims: *"It is challenging to work with the security if you don't have support from the leadership, therefore, it is critical for the board to communicate it to all levels of the organisation".* It is of consequence therefore to understand the top management's position on the nature of cybersecurity, which in turn would necessitate a greater general understanding of CS/IS through greater interaction with the CS department. Unfortunately, given Benjamin's, Petra's and David's views — this is unlikely due to the need for each individual to segment their time to fulfil their own purpose. Parochialism within the higher echelons of an organisation therefore greatly limits the feasibility of CS/IS practices throughout the organisation. In simple terms, if the company leaders believe that IT structures are easier to present to shareholders as a "solution" as opposed to "education", that will ultimately force the hands of the CS/IS experts.

4.2 Analysis: IT Department

This section is studying the insights provided by IT professionals and their application and adherence to the theoretical concepts. As inferred from the literature review, the IT department is expected to act as a mediator, a satellite, between the cybersecurity management and the non-IT departments, as their own goals are very much in line with those of cybersecurity department, albeit more focused on the technical aspect such as patching potential software- or hardware-related vulnerabilities, and ensuring that nobody gains access into the organisation's intranet through forceful means. What this implies is that a fairly high level of ISA is expected, but their particular work orientation and used jargon will likely result in low levels of fruitful interdepartmental interaction. The use of jargon alone used in a semi-structured interview may contribute to neutralization behaviours, reducing the non-IT WLC. In the case of the IT department, it can be expected that risk assessment will be fundamentally different and based on different values, which likely emphasize accomplishing their own task as opposed to ensuring full IS compliance, high awareness on data confidentiality and integrity. Their compliance with IS practises will be examined in the next paragraphs elaborating on the CIFs influences established earlier.

4.2.1 Stress and Resilience

Overall, interviews revealed that it is strongly believed that Swedish employees prefer to follow strict guidelines to avoid job-related stress. Low working stress is a crucial element in proper ISA development since in such an environment IS governance principles are assisting the workers and match their voluntary compliance. Resilience is widely adopted among IT employees and seems to act as a strong organisational capability shared among workers.

From Charles' international experience of working in a global consultancy company, he could comment and elaborate on certain cultural differences he encountered with a reflection on Swedish security attitudes, specifically with regard to rules and training diminishing the possibility of stress when working in such a sensitive field. As Charles said: *"If I compare*

countries, they are different…Swedes are very loyal to their processes. They are very [trusting], they could even be naïve, but they need rules to play with, they are especially loyal when it comes to enforcing processes and routine. That is why training is very valued in this type of work." Sufficient training allows proper adherence to rules, following the compliance factors, as well as lowers the stress levels. It seems that Swedish culture is assisting in effectively dealing with stress since it ensures the following of the top management governance, workers are loyal to the directives and rules and build resilience.

4.2.2 Punishment and Reward Systems

The type of data, level of risk, sensitivity, industry and culture seem to dictate the impact of punishment and reward factors. As Charles claimed: *"If you compare that with organisations, it is a different level with how much you invest on security. When people get classified like systems do for the information they hold...you are in a government [security] level, e.g. the military. In my opinion, that is the highest level of cybersecurity [application]. Many organisations which I have been working with aren't even close."* Organisations and industries with the highest levels of the system and human factor classification in terms of security are, due to highly sensitive data, those most relevant to accounting for punishment and reward systems as the necessities to tailor appropriate behaviour by incentivising positive or negative reactions become especially urgent. However, overall it seemed that the IT representatives did not have enough experience to comment on those.

Charles believes that the two main elements in shaping ISA adoption are knowledge and transparency in security practices. The first is achieved by training and accumulated experience, while the second assists in the rapid acceleration of security levels. *"Many times security departments within organisations do not have open transparency. If an incident occurs, it is often only the IT and security department that gains the knowledge and improves their own awareness, but do not allow this throughout the whole organisation. Even public companies do not share so much information about them...they try to hide incidents from the competitors".* As a result, the lack of information sharing only worsens security levels. The fear for punishment results in a certain level of parochialism when individuals are more

concerned for their own corporate interests compared to the overall goals of the organisation. The Swedish culture which adopts consistent training and dynamic learning, as well as the equalities laying in foundations of Swedish society are promoting an accelerated trust development, which in turn generates higher motivation intentions. An overview of the interview insights indicates that motivational factors in Sweden are forming a quite different approach, avoiding punishment and fear.

4.2.3 Worker's Perceived Locus of Control

The commitment to adherences to IS practices, as well as cultivation of ISA greatly depends on individual incentives on how to perform and use oneself's directives with the end goal in mind. It generally seems that the sensitivity of data and the internal motivation to contribute the levels of commitment as well as the organisational ISA. According to Gideon, *"information security is very important but often missed or even skipped on purpose due to its "unnecessary" complexity",* highlighting often parochial intentions of the organisation and the paradox of usable security, when the overcomplication of IS practices does not necessarily infer to better security, yet oftentimes to an even weaker one. In his opinion, prioritisation of customer data protection is key in maintaining trustworthiness and credibility in front of the customers. *"Defining the right ways to measure the health of the system is very important. Moreover, every developer in the company must know how to access monitoring tools and investigation tools...My strong belief is that every department in the company, no matter if it is technical or operational, should be concerned about security",* — Gideon is emphasizing the significance of the adoption of internal LoC among workers as that inner conscientiousness and high responsibility eventually results in improved awareness and self-efficacy.

"In order to reach higher levels of ISA, transparency is really important…[the organisation should] try to educate the employees so that they have that self-interest and feel like they have a certain degree of responsibility", — claimed Charles. Internal WLC has indeed deemed a crucial element in proper ISA adoption in the eyes of the IT department as it drives the

responsibility and genuine enthusiasm of workers onto such a level that internal intentions are fitting the overall vision.

However, during the security policy meetings, managers of different departments seem to prioritise their own goals and intentions. As noted by Darlene, *"as long as it does not directly affect their department or their statistics, they do not care enough about security policy"*. Such limited inflexible parochial mindset is negatively related to the overall organisational efforts. The workload division may result in imbalance and inefficiency in goals and vision achievement. Therefore, interdepartmental collaboration and team dynamics are crucial, throughout all stages, and training shall be consistent. Transparency and dynamic learning shall be encouraged, facilitating internal LoC. Charles claims one of the crucial responsibilities of the company shall be to inculcate the ISA through security governance on its all levels. Charles adds that regular and persistent consultancy with compliance managers and other personnel related to security governance is an efficient way to stimulate organisational ISA.

4.2.4 Risk assessment

Risk assessment is mainly investigated by the actions taken which may put the security of the company at risk. The values identifying risk assessment aspects among IT personnel are mostly tech-related, despite the shared vision for the importance of ISA adoption on all organisational levels, which may render certain interdepartmental adoption difficulties. Tyrell claims that *"security should always be a part of the company's mind",* implying that security should be employed on all organisational levels, in all its activities and all stages, yet it certainly shall be dynamically adjusted to the business and industry. From an IT department perspective, it seems that the security incentives are not uniform between the departments since there is a higher technical requirement from the IT team. In order to facilitate the awareness of any even unexploited failures, continuous penetration tests are performed by the IT team.

According to Charles, one of the greatest issues for organisations is to understand the principles of regulations, and, consequently, apply those on technical and human aspects of work. *"The managements' main focus is to report that you are fulfilling compliance", w*hat results in undervaluation of the main asset – the users, since "*when you reclassify the systems, you need to reclassify the users you let the workers work with to protect the information within an organization"*. Charles here is reflecting on the risk assessment and how GDT and associated behaviour to risks unravel in the organisation. The overall perspective of IT personnel seems to be closely reflecting the aspects of ISO27001 standard and specifically risk treatment plans.

Introductory awareness training generally does not suffice in the opinion of Angela: for instance, from her experience of working with fraud and money laundering, numerous employees tend to neglect certain practices without further systematic reminders and training, resulting in posing high risks. IT department is often relied upon in ISA communication yet the jargon may distort the comprehension and interdepartmental absorbing of the practices. The view on ISA of IT department representatives is evidently mostly reliant on technical elements and "facilitated integration of selected security solutions" as stated by Tyrell in one of the interviews. The IT department focuses on ensuring the selection of security solutions to be properly integrated. Throughout the interviews it has been specifically emphasised that any security failure is of the highest priority and the IT team undertakes a variety of alerting and monitoring tools if that occurs while simultaneously coordinating and signalling the issue to other units. More technical view on the IS compliance may decrease the pace and absorption of security knowledge among departments, resulting in the dissipation of overall organisational awareness. Summary of the responses by the IT team infers that most of the protective measures seem to form a habit however it has to be supervised and consistent. Oftentimes, according to Tyrell, IT personnel when handling low-risk data, are not concerned with security as much, yet even failures with non-sensitive data may yield significant dangers, as stated by cybersecurity expert Elliot. This is supported by the GDT on how individuals make connections between illegitimate behaviour and possible sanctions. In the case of low-risk data, IT personnel are less concerned with punishments on deviant behaviour, therefore are not paying much attention to security, putting the company at high risks.

According to Darlene, the organisation shall be more tech-oriented and they believe that putting sufficient safeguards *"will reduce user's error and negligence with the help of investments in powerful security tools (equipment and software) that allow controlling every single data passing through the network"*. This highlights the common issue of failing to take proper care of risk assessment and allocate sufficient investments to the human side of information security, resulting in asymmetric and weak ISA. Charles commented that *"[security] is about how much you invest. Swedish companies budget for security, they allocate resources and spend time on it. In other countries, they may not invest in security and you get what you pay for."* Yet, prioritisation done via risk assessment and treatment plans is crucial for enabling proper resource allocation which is one of the main elements of governance principles of IS. Investments, to be efficient in the long run, shall be taken under a clear understanding of asset values, associated costs and risks, in order to maintain a coherent cybersecurity strategy.

4.2.5 Digital maturity

A few interviewees have highlighted the issue of cooperation with the rest of the company as oftentimes trust becomes the critical point of reliability. Tyrell, who is an employee at a young yet accelerated in its growth technical Swedish startup, has highlighted the absence of a dedicated security team as the main problem in the coordination of IS measures. Lack of such specific focus implies missing supervision which is critical for any company. Absence of experienced cyber leadership is a foundational complexity weakening the levels of digital maturity and ISA, and shall at least be complemented by experienced IT individuals able to spread awareness.

However, Tyrell notes that the IT team is *"trying to enforce information security on all different levels and in all departments, because we think that the system is as secure as its weakest link"*, therefore acting as an agile group of satellites, yielding high digital maturity of the organisation and following the BSIMM principles. *"We see security as a continuous improvement process of our business...No single person is able to make some concerning decision just by oneself. It means that almost everything in the company goes through at least*

several people. Maybe that is slower, but it helps to cut some insecure solutions and to make the code more robust — it brings overall awareness." This proves the typically Swedish collectivist attitude and encouragement of transparency among workers. Nevertheless, the interviewee has also shown a slight lack of trust in ISA among departments which indicates varying trustworthiness in Swedish organisations, despite the generally high level of personal reliance.

Charles stated: *"I think that cybersecurity cannot be generalized and applied in one way to all companies, you need to know your organization and what your main goals are before you set the security requirements and the levels of security. I believe that flexibility is something that Swedes are good at. [They] are tired of [thinking within] the box, they aren't so hard on structures. Security should be just like IT - something supporting the organization, and it should be transparent, it shouldn't make the organizational growth slow down".* Flexibility and dynamism of adaptation and open-minded thinking determine the power of group effort, unifying the essence and the goal from multiple angles of view. Proliferating complexity of unique organisational vision is positively proportional to the ability of flexible security compliance.

Commenting on the relation of security to cultural mindset, Charles claimed that *"security and mentality go hand in hand many times because in the lack of training you fall back on your mentality. That is my philosophy...They [Swedes] are open in the way they think... This is in general quite similar to all Nordic countries. I'm half-Nordic/half-Arab, and it is completely opposite if you go to Tunisia: they do not trust you until you prove that. They have another mentality".* Indeed, the digital and cyber maturity level is dependent on cultural dimensions and peculiarities of the cultural mindset. IT personnel are observant of such aspects, proving the high cyber maturity of Sweden and its enabling cultural characteristics which project onto Swedish organisations.

4.3 Final Discussion

Answering the question of *"what is the role of organisational culture in shaping and ensuring ISA compliance"* is in its own regard easy. However, how do we substantiate this claim? This is best done by looking at how the different surveyed departments shape the organisational culture, which is analysed in the prior section. At this point of the thesis, it is crucial to understand the underlying factors that seem to come up during the analysis, but that need to be given a cultural context.

The role of organisational culture in shaping IS compliance is contingent on the initiatives taken by the CS/IS and IT departments due to their close connection to Information Security as a whole, but also because it is ultimately the initiatives, protocols, guidelines, and approaches that craft the resulting attitudes of the conventional non-tech worker within an organisation. The analysis presented in the previous section illustrates several crucial points that are currently important in shaping organisational culture through IS initiatives, but also several drawbacks that arise due to the tensions between the two departments, which in a tandem hint at the ideal situation. By focusing attention on these attitudes and on what is currently believed to be lacking, one can optimize the organisational culture in an effort to render ISA and IS compliance as a fundamental assumption of an organisation's culture (as per Schein's Iceberg Model).

Firstly, it is essential to understand the role of the Swedish peculiar way of thinking in shaping the presented attitudes in the previous section. Sweden's unique cultural paradigm, underscored by its extremely low MvF (high Femininity) and focus on collectivism, theoretically (and practically based on analyzed empirical material) places immense value on honesty and transparency. This is perhaps because for teams to work efficiently and harmoniously, a mutual understanding is needed to ensure trust, guide behaviour, and most importantly give knowledge a practical value to allow for greater organisational flexibility

and greater self-determination. Under ideal circumstances, these qualities would be attained — but if that was the case, there would be no point to this thesis.

Instead, it is apparent that a profound paradigm shift is needed at top management level to allow for existing ISA incentives to move from observable actions (artefacts) to more meaningful cultural schemas (underlying assumptions). Attitudes expressed by Benjamin, Petra, and Elliot demonstrate that the IT department is given a greater preference due to the rather new nature of ISA. For the majority of the time in which IT infrastructures have been used, these same systems have demonstrated that certain cultural qualities can be more easily measured, and in turn, top management gives preference to measurable initiatives as opposed to more abstract views. However, it should also be noted that this attitude depends on the nature of the data itself, recalling that different data types and quality will necessitate different levels of paranoia and work commitment. However, the context alludes that for some industries it is easy to understand why IS compliance is important. Internally, all workers will know that banking or medical information is associated with sensitivity and privacy, and, therefore, can empathize with individuals. As identified before this context acts as a self-reinforcing ISA mechanism, yet the question still pertains for low sensitive data. However, as inferred from the previous chapter, with regard to less sensitive data ISA is a matter of ensuring understanding, yet it is the belief of both CS/IS and IT departments that the general worker doesn't pay significant attention.

A greater level of communication and transparency is warranted to reconcile departmental bias and improve the placement of ISA within the organisational culture of a firm. This bias needs to be fixed within the Swedish context as it acts against the cultural norm: Swedes have the ability to understand the importance of data, if given the proper chance — reducing Swedish workers' WLC will not lead to any profound changes and will perpetuate the small mistakes that can eventually become costly for organisations. The persisting departmental and organisational boundaries prevent individuals from understanding other perspectives than their own, which in turn leads to tension and grievances. These grievances are the basis on which non-compliance and parochialism become self-reinforcing. The lack of perspective and ability to learn puts greater emphasis on what workers can control as opposed to trying to find

ways to control what they cannot. In a more specific manner, individuals will cling to that which is important to them, and will use that as a way to achieve their organisational goal; Should workers be uninformed on an expected aspect of their work (IS compliance), though this aspect is perceptibly secondary to *results* within the organisation, neutralization behaviours can be expected to persist. Simply said, the existing organisational paradigms prevent departments from encouraging an internal locus of control which would bring about positive change in terms of willing IS compliance.

As stated in an earlier section in *Chapter 3*, when the initial partnership with the collaborating organisation was unfortunately terminated, attempts to find non-tech (conventional) workers to get their insights on IS compliance was ultimately fruitless. Most commonly the excuse was either a lack of trust with regards to our intent or beliefs that the worker in question was incompetent to answer the questions since they presumed it does not directly concern their department. However, our inability to conduct interviews with non-technical personnel may be deemed as a result of itself. Whether the reason given was the former or the latter, this fact highlights the primary issue of lower ISA of conventional workers and their lack of knowledge of IS compliance to know what can be revealed and what cannot. Consequently, although taken at its value, this suggests that for most workers IS is still a topic they aren't familiar with, which in turn will be perpetuated by top management.

All of our CS/IS and IT respondents demonstrated a baseline of actions and initiatives taken, with most of them focusing more on accountability rather than on practical value, given the fact that the frequency of IS failures for companies, where the damage done is significant, is rare. There does not appear to be a learning opportunity for conventional workers to apply what CS/IS experts set out to do, and instead preferred organisational initiatives are those that remove control from the worker and give managers greater oversight — despite this approach being perceived as a weak proxy for actually assessing organisation's ISA.

Consequently, although hardly a cure-all for the presented socio-technical problem, this issue sheds light on greater coordination ability and greater self-determination of both the CS/IS and the IT department. Despite their parochial nature of the job, interviewed experts

demonstrate to be somewhat aware of the needs of the other departments, however, their skill sets complement one another and could benefit from greater collaboration. Each party affects the discussed factors in their own way, and for the most part, it is the enforced parochialism between the two departments that prevents the more tailored solutions. This parochialism, however, does not naturally originate from the departments themselves, yet from the top management (which is at least perceivably based on the responses from respondents). Therefore, a greater collaboration would allow for more consistent valuable information flows that could combine the skill sets of CS/IS and IT people to create properly crafted solutions. Notice that this idea closely resembles the thoughts of Stephan as presented before. For instance, unlike David's, Petra's, or Benjamin's company, Stephan's start-up is in its early stages of existence and, consequently, expresses greater cultural flexibility with regards to role boundaries, and the different departments interact on a greater scale, establishing a history of collaboration.

In summary, organisational culture is shaped according to the actions of the different departments, however, these actions themselves reflect where the heads of the company place their priority. It is important for managers of established as well as growing companies to view ISA and IS compliance as a cultural and not technical factor; hence, it needs to be cultivated through organic development. Additionally, certain organisational traits, such as attitudes pertaining to stress, WLC, risk assessment, and digital maturity, all offer an interpretive lens through which to assess how an organisation sets up its own compliance factors, and can, therefore, be used as a way of interpreting reasons for non-compliance. By focusing on these parts of the organisational culture, a manager can not only better understand the organisational culture with regards to ISA, but also comprehend what actions need to be taken to create an organisational culture that complements the cultural preferences of the workers themselves.

5 Conclusion

5.1 Research Aims

The purpose of this study was to aid in sensemaking of a complex socio-technical issue with regards to unravelling the key relationships and aspects of organisational culture that contribute to or prevent Information Security compliance. Distinct emphasis is placed on the nature of Swedish culture, as a unique maxim, that in turn shapes the ideal situations pertaining to interdepartmental communications, and offers a base-line of which to understand the cultural preference of the average Swedish worker. In doing so a greater understanding of the role of organisational culture is established. The expected end result was to contribute to the urgent sensemaking that is needed within the relatively new research area of the Human Factors of Information Security.

5.2 Research Objectives

The research objectives of this thesis were to gain a more detailed understanding of the perspectives held by crucial departments within organisations that theoretically have direct control over the way ISA is shaped within organisations. In doing so, differences can be highlighted, as well as common bridging points with regards to governance preferences, and consequently, a more nuanced understanding of how existing practices and beliefs of each department shape the degree to which workers comply with IS protocols mandated by the organisation.

As a secondary layer, the role of the Swedish cultural maxim is included to offer a perspective to existing and future employers within Sweden to reduce learning costs associated with

understanding how to cultivate a suitable and efficient ISA and IS compliant organisational culture.

5.3 Conclusion/Findings

The interviews and models used highlight that the Swedish culture is unique in the sense that it is a culture that values practical information flow. Hierarchies are tolerated but the heavy emphasis on segmentation without adequate cross-departmental interaction is observably detrimental to moving ISA and IS compliance deeper into the culture of an organisation.

Measures by CS/IS and IT departments are in a way marred thanks to their own parochialistic objectives, which can overlap but ultimately require contrasting approaches. Whereas one department favours limitations of access to data and in the optimum aspires for total information access segmentation, the other argues that ultimately what matters is ensuring accountability through mandated training. Participating respondents have voiced their concerns over the conventional worker's ability to effectively participate in the creation of IS compliant culture: it is apparent that greater coordination is needed, but this can only be encouraged by adjusting the role of ISA within an organisation and encouraging interdepartmental collaboration in order to kick-start learning processes that build up ISA organically, regardless of size or the industry.

After a lengthy analysis, the findings suggest that a single type of solution is not suitable given the context of the data itself. In certain industries, such as the financial or medical sectors, a perceived necessity of security will manifest itself due to the implied sensitivity of data used. However, what the research points out is that awareness of the value is brought on naturally. In less "stressful" environments, the value of information can be internally perceived as lower leading to carelessness, which in turn suggests that greater emphasis has to be placed on data value as such within less stressful industries to encourage compliance.

Consequently, with regards to organisational culture, and the peculiarity of the Swedish national culture, it is crucial to encourage greater information flow and transparency between departments to foster a sense of trust and increase workers' locus of control so that even

conventional workers will be able to discuss ISA and IS compliance with enough self-perceived ability to demonstrate actual knowledge.

5.4 Practical Implications/Contribution

As has been highlighted in the previous chapter, the analysis has allowed us to corroborate some aspects of research highlighted in *Chapter 2* of this thesis, while hinting at differences in certain perceptions. The practical implications of this being that, indeed, national and organisational culture have certain impacts on the compliance intention of workers, and these intentions are shaped according to the incentives created by CS/IS and IT departments, respectively.

The thesis has elaborated on the nature of the socio-technical problem and provided additional detail on the internal organisational dynamics that influence IS compliance. In the most basic terms, as has been emphasised by all interviewees, the personnel is aware of their parochial role, however, Sweden has the unique national advantage of their fairly collectivist attitudes, which does not appear to be adequately leveraged with regards to ISA cultivation. People do not compete with one another, and in fact, encourage each other to be fairly transparent with their own mistakes, and more importantly do not really promote punishment, neither formal nor informal. In the absence of emphasis on punishment and contextual stress (given by reputation of the firm or the industry), it is crucial that top management espouses ISA and IS compliance as equally important to attaining results. In doing so it can be expected that CS/IS and IT solutions will, in fact, reduce the propensity for non-tech workers' potential deviant behaviour, and reduce the likelihood of unintentional data breaches.

From the perspective of Swedish national culture, certain preferences for the organisational incentives can be derived, which have been additionally corroborated through empirical work. Transparency and the creation of a flexible organisational perspective appear to be the optimal conditions for many of the CS/IS experts and several of the IT experts. However, the parochial nature of the departments enforces solutions that both CS/IS and IT experts find ultimately unsatisfactory from the perspective of their professional goals, but that top

management appears to appreciate. Both departments lament that greater levels of transparency would facilitate the work as it would encourage learning within the organisation, and consequently lead to ISA becoming an espoused value within an organisation's culture. Learning as a mechanism is facilitated through semi-permanent departmental and job boundaries.

The authors of this thesis have demonstrated that in a collectivist nation such as Sweden, the best way to encourage ISA development and to increase the overall IS integrity is through the adoption of such values as managerial flexibility, transparency, interdepartmental communication, and most importantly through a required change in the strategic positioning of ISA by top management. In doing so, appropriate incentives would be shaped through the creation of greater interdepartmental cooperation,

In summary, the thesis has demonstrated that, indeed, many of the compliance factors discussed are significant in compliance intention, while some, such as punishment and reward systems are less important, given the greater national culture aspect of Sweden. In doing so, this thesis contributes to greater sensemaking and offers interested parties to better understand the tensions between the discussed departments. Therefore, this thesis can aid young organisations in understanding the importance of organisational incentives in shaping an organisational culture that espouses IS compliance.

5.5 Future Research

Given the nature of this research area, much of the existing literature is still fairly obscure due to the prevalent false belief that Information Security is a fundamentally technical problem. Naturally, for many, it is much easier to view it in such a way that it becomes a question of funding, rather than a question of management. However, given our fieldwork, contribution, and problem discussion it cannot be denied that IS management is at its core about people management. Consequently, many researchers have opted for various applications of theory, practical work, and bespoke assessment solutions (as described in the literature review).

However, this also offers a plethora of options, through which to explore the best practices to manage the human aspect of IS. Some of which will be addressed shortly.

The role of national culture is viewed as being important, but thus far there are no real qualitative case studies through which collectivism or individualism is adequately analysed to identify the trends among the workers, and, consequently, any current research can be deemed anecdotal at best. Furthermore, given the position of researchers and their views on the topic itself, there is not an attempt at identifying the effect of the industry itself on the way ISA is managed, and how this could differ from the general observations acquired in either collectivist or individualistic contexts.

Another possible consideration for future research could be to investigate and evaluate the linkages of presented findings to different types of organisational architectures and hierarchies. Such a study could find potential explanations behind compliance intention factors, willingness to adhere to IS protocols and varying interdepartmental levels of ISA. It would also offer a highly tangible practical contribution for organisational consideration. Since the organisational structure is oftentimes built with the cultural influence in mind, decisions regarding IS compliance might also reveal a significant relationship towards the firm's architecture. The communication flow and progressive evolution of the organisation may influence the emergence and variations of IS policies as those penetrate the structure and culture on multiple levels. Therefore, to avoid systematic mismatches between architecture, culture and ISA, such relationships could be studied.

Our research suggests that the best practices, much like education, require transparency. The findings, relevant to Swedish culture, suggest that this is best done through informal communication and mixing of departmental personnel to encourage dialogue and sharing of opinions. Will this, however, work for cultures that are fundamentally different from Sweden? Would companies themselves be willing to accept a practice of transparency if it meant that their stock could suffer as a result of lower shareholder trust? Trying to understand the role of a national culture through other models than the CDF model is bound to offer new and exciting ways, through which to isolate and understand the effects of national culture on the importance and feasibility of transparency.

The qualitative analysis performed in this thesis served as a sensemaking study, but the field of ISA from the perspective of international managers would greatly benefit from a combination of sectoral studies (e.g. identifying how compliance factors differ between industries). Industries could be segmented according to economic sectors or some other documented basis, such as revenue levels, to allow for greater diversity in understanding how the nature of the industry itself should shape ISA and IS compliance.

References

Ajzen, I., Brown, T. and Carvajal, F. (2004). Explaining the Discrepancy between Intentions and Actions: the case of hypothetical bias in contingent valuation. *Personality and Social Psychology Bulletin*, [e-journal] vol. 30, no. 9, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 5 April 2020]

Bada, Maria, et al (2015). Cyber Security Awareness Campaigns: why do they fail to change behaviour? I*nternational Conference on Cyber Security for Sustainable Society,* Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 10 April 2020]

Barlow, J.B., Warkentin, M., Ormond, D. & Dennis, A.R. (2013) Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation. *Computers & Security*, [e-journal] vol. 39, no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 5 April 2020]

Binwal, P. (2015). Creating A Cybersecurity Governance Framework. Security Intelligence., Available Online: : https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time /[Accessed 17 April 2020].

BSIMM. (2020). Software Security Metrics And Strategy | BSIMM, Available online: https://www.bsimm.com/framework/governance/software-security-metrics-strategy.html [Accessed 1 May 2020].

Chen, Y., Ramamurthy, K. & Kuang W. (2013) Organizations' Information Security Policy Compliance: stick or carrot approach? *Journal of Management Information Systems*, [e-journal] vol. 29, no. 3, 2012, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 6 April 2020]

Cybercrime Magazine. (2020). Cybercrime Damages $6 Trillion By 2021, Available Online: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [Accessed 9 May 2020]

Dawson, J. & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, [e-journal] vol. 9, no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 6 April 2020]

DNV GL. (2019). Cyber Security Assurance And Evaluation, Available Online: https://www.dnvgl.com/services/cyber-security-assurance-evaluation-and-certification-127269 [Accessed 16 April 2020]

Dreibelbis, R. (2016). It's More Than Just Changing Your Password: Exploring the nature and antecedents of cyber-security behaviors. *Graduate Theses and Dissertations*, Available Online: http://scholarcommons.usf.edu/etd/6083 [Accessed 10 April 2020]

Gcaza, N., von Solms, R., Grobler, M.M., van Vuren, J.J. (2017). A General Morphological Analysis: delineating a cyber-security culture. *Information and Computer Security*, [e-journal] vol. 25, no. 3, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 8 April 2020]

Gluesing, J.C. (2013). Qualitative Research Methods in International Organizational Change Research. *Journal of Organizational Change Management*, [e-journal] vol. 26, no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 6 April 2020]

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I. & Jones, K. (2019) Exploring the Role of Work Identity and Work Locus of Control in Information Security Awareness. *Computers & Security*, [e-journal] vol. 81, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 5 April 2020]

Hell, M. (2019a). What Is A Security Threat? - Debricked. Debricked, Available Online: https://debricked.com/blog/2019/05/29/what-is-a-security-threat/ [Accessed 25 April 2020]

Hell, M. (2019b). What Is A Security Vulnerability? - Debricked. Debricked, Available Online: https://debricked.com/blog/2019/05/29/what-is-a-security-vulnerability/ [Accessed 25 April 2020]

Hell, M. (2020). What Is A Cybersecurity Risk? - Debricked. Debricked, Available Online: https://debricked.com/blog/2020/02/06/what-is-a-cybersecurity-risk/ [Accessed 25 April 2020]

Henshel, D., Cains, M.C., Sample. C. & Hoffman, B. (2016). Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers. *Advances in Intelligent Systems and Computing Advances in Human Factors in Cybersecurity*, 2016, Available Online: https://www.researchgate.net/publication/305082004_Integrating_Cultural_Factors_into_Human_Factors_Framework_and_Ontology_for_Cyber_Attackers [Accessed 8 April 2020]

Hindelang, M.J. (1973) PERCEIVED LOCUS OF CONTROL AND GUILT AROUSAL FOLLOWING NORM TRANSGRESSIONS. *Criminology*, [e-journal] vol. 11, no. 1, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 9 April 2020]

Hofstede, G. (1993) Cultural Constraints in Management Theories. *The Executive*, [e-journal] vol. 7, no. 1, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 6 April 2020]

Hofstede Insights (2015). What about Sweden? Available Online: https://www.hofstede-insights.com/country-comparison/sweden/

IMD Business School. (2020). IMD World Digital Competitiveness Ranking 2019, Available Online: https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2019/ [Accessed 5 May 2020]

ISMS. (2020). ISO 27001 Policies And Controls Documentation, Available Online: https://www.isms.online/iso-27001/policies-and-controls/ [Accessed 1 May 2020].

Ioannou, M., Stavrou, E. & Bada M. (2019). Cybersecurity Culture in Computer Security Incident Response Teams: investigating difficulties in communication and coordination. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security),* Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 19 April 2020]

IT Governance Ltd. (2020). What Is ISO 27001?, Available Online: https://www.itgovernance.co.uk/iso27001 [Accessed 6 May 2020]

Jensen, M.C. & Meckling, W. H. (1976). Theory of the Firm: managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, [e-journal] vol. 3, no. 4, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 11 April 2020]

Jeong, J.J., Grobler, M., Chamikara, M., & Rudolph, C. (2019). Fuzzy Logic Application to Link National Culture and Cybersecurity Maturity. 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), 330-337, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 20 April 2020]

Jeong, J.J., Mihelcic, J., Gillian, O. & Carsten, R. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 20 April 2020]

Kaspersky. (2020). What Is Cyber Security?, Available Online: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security [Accessed 25 April 2020]

Kosutic, D. (2020). ISO 27001 Risk Assessment And Treatment: 6-Step Guide, Available Online: https://advisera.com/27001academy/knowledgebase/iso-27001-risk-assessment-treatment-6-basic-steps/ [Accessed 6 May 2020]

Kriz, D., (2011). Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity, Available Online: https://www.researchgate.net/publication/241188172_Cybersecurity_principles_for_industry_and_gov

ernment_A_useful_framework_for_efforts_globally_to_improve_cybersecurity/stats [Accessed 25 April 2020]

McCormac, A., Calic, D., Parsons, K., Butavicious, M., Pattinson, M. & Lillie, M. (2018) The Effect of Resilience and Job Stress on Information Security Awareness. *Information and Computer Security*, [e-journal] vol. 26, no. 3, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 10 April 2020]

McEvoy, T.R., & Kowalski S.J. (2019). Deriving Cyber Security Risks from Human and Organizational Factors: a socio-technical approach. *Complex Systems Informatics and Modeling Quarterly*,[e-journal] vol. 1, no. 18, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 11 April 2020]

Milkovich, D.. (2019). 15 Alarming Cyber Security Facts And Stats. Cybint, Available Online: https://www.cybintsolutions.com/cyber-security-facts-stats/ [Accessed 2 April 2020].

Moore, S., & Keen, E.. (2019). Gartner Forecasts Worldwide Information Security Spending To Exceed $124 Billion In 2019. Gartner, Available Online: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 [Accessed 9 May 2020]

Parsons, K.M., Young, E., Butavicius, M., 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*,[e-journal] vol. 9, no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 13 April 2020]

Pattinson, M., Butavicious, M., Lillie, M., Cicarello, B., Parsons, K., Calic, D. & McCormac, A. (2019). Matching Training to Individual Learning Styles Improves Information Security Awareness. *Information & Computer Security*, [e-journal] vol. 28, no. 1, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 15 April 2020]

Proctor, R.W. & Chen, J. (2015). The Role of Human Factors/Ergonomics in the Science of Security. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, [e-journal] vol. 57, no. 5, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 9 April 2020]

Ritala, P., Olander, H., Michailova, S. & Husted, K. (2015). Knowledge Sharing, Knowledge Leaking and Relative Innovation Performance: an empirical study. *Technovation*, [e-journal] vol. 35, no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 7 April 2020]

Ross, R., McEvilley, M. & Oren, J. (2018). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. csrc.nist.gov,

Available Online: https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final [Accessed 25 Apr. 2020]

Schein, E. (1992). Organizational Culture and Leadership, (2nd ed.) Jossey-Bass Business & Management Series, San Francisco, CA Available through EBSCO Library Database: https://search.ebscohost.com/login.aspx?direct=true&db=cat07147a&AN=lub.277225&site=eds-live&scope=site. [Accessed 16 April 2020]

Schein, E. (1996) Culture: The missing concept in organization studies. *Administrative Science Quarterly*, [e-journal] vol. 41 no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 16 April 2020]

Shappie, A., Dawson, C. & Debb, S. (2019). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, [e-journal] vol. 1, no. 1, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 7 April 2020]

Shenkar, O., Luo, Y. & Yeheskel, O. (2008). From "Distance" to "Friction": substituting metaphors and redirecting intercultural research. *The Academy of Management Review*, [e-journal] vol. 33, no. 4, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 6 April 2020]

Shirey, R. (2019). Internet Security Glossary, Version 2. The IETF Trust, Available Online: https://tools.ietf.org/html/rfc4949

Siponen M. & Vance A. (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* , [e-journal] vol. 34, no. 3, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 3 May 2020]

Swinton, S. (2019). Cybersecurity Governance, Part 1: 5 Fundamental Challenges. Carnegie Mellon University, Available Online: : https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html [Accessed 16 April 2020]

The Web Application Security Consortium. (2020). Information Leakage, Available Online: http://projects.webappsec.org/w/page/13246936/Information%20Leakage [Accessed 9 May 2020]

Waldo, R.F. (2013). Shaping information security behaviors related to social engineering attacks, PhD thesis, KTH, Elkraftteknik, Available Online: https://kth.diva-portal.org/smash/get/diva2:925493/FULLTEXT02.pdf

Wang, Y.J. (2019). The Dictions of Labour and its Alien Effects, *Symposium: Canadian Journal of Continental Philosophy / Revue Canadienne de Philosophie Continentale*, [e-journal] vol. 23 no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 1 May 2020]

Warkentin, M. & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*,[e-journal] vol. 18, no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 3 April 2020] .

Wiley, A., McCormac, A., Calic, D. (2020). More than the Individual: Examining the Relationship between Culture and Information Security Awareness. *Computers & Security*, [e-journal] vol. 88, 2020, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 7 April 2020]

World Value Survey. (2008). Findings and Insights, Available Online: http://www.worldvaluessurvey.org/WVSContents.jsp?CMSID=Findings [Accessed 10 May 2020]

Wong, W.P., Tan H.W., Tan, K.H. & Tseng, M. (2019). Human Factors in Information Leakage: mitigation strategies for information sharing integrity. *Industrial Management & Data Systems*, [e-journal] vol. 119, no. 6, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 12 April 2020]

Zhang, X. & Yang, H. (2019). Impact of Cross-Culture on Behavioral Information Security. *Journal of Integrated Design and Process Science*, [e-journal] vol. 22, no. 2, Available through: LUSEM Library website https://www.lusem.lu.se/library [Accessed 12 April 2020]

Appendix

A. Interview Questionnaire Sample

Note: the questionnaires are semi-structured, i.e. allowing for flexible discussion and open-ended questions

Questionnaire format: Cyber-security Expert/Head (CS/IS Expert)

Intro:

1) Would you kindly state your name, educational background and your tenure with the company? [These will be anonymised, but are needed for our purposes]
2) How would you describe your day-to-day activities at the company

The nature of Information Security Awareness (ISA):

1. How does the company enforce ISA? What sort of resources are available?
    a. When a person can be unsure of what to do, how do they find out what they should do in a situation?
2. How does the company measure ISA? Could you comment on the philosophy of the ISA culture at your company, if you are aware?
3. When there is a failure to comply with IS protocols, what is done? Could you give a general overview of the series of actions that occur, and in what succession?
4. Could you comment on the incentives for compliance with IS protocols for your department, if there are any?
    a. Rules
    b. Personal beliefs
    c. Other incentives?
5. Do you believe that the general incentives are uniform between different departments?
6. As an IS expert, when you find out that an IS breach has been committed due to some innocent reason (eg: negligence), who is the first person you talk to, and who is the last? Why is that so?
7. In terms of managing breaches, how often do you think that a breach is exploited? How often is an unknown breach exploited, and how often is a reported breach identified by the workers?
    a. What are the key factors in identifying an exploitable vulnerability, and are they attainable within the context of a departmentalized organization? Why or why not?
8. How often do you interact with different departments to create a mutual understanding of the importance of cyber-security? Do you think that the current way of interacting is enough, too much or too little? Why?

Questionnaire format: Tech-focused (IT Department)

Intro:

3) Would you kindly state your name, educational background and your tenure with the company? [These will be anonymised, but are needed for our purposes]
4) How would you describe your day-to-day activities at the company

The nature of Information Security Awareness (ISA):

9. What does information security mean to you? Is it important in your day-to-day tasks, in your opinion?
10. How does the company enforce ISA? What sort of resources are available?
    a. When a person can be unsure of what to do, how do they find out what they should do in a situation?
11. How does the company measure ISA? Could you comment on the philosophy of the ISA culture at your company, if you are aware?
12. When there is a failure to comply with IS protocols, what is done? Could you give a general overview of the series of actions that occur, and in what succession?
13. Could you comment on the incentives for compliance with IS protocols for your department, if there are any?
    a. Rules
    b. Personal beliefs
    c. Other incentives?
14. Do you believe that the general incentives are uniform between different departments?
15. How do you tell if you have accidentally committed a breach? Can you tell even if the breach remains unexploited?
16. How often do you interact with different departments to create a mutual understanding of the importance of cyber-security? Do you think that the current way of interacting is enough?