HELLENIC
OPEN
UNIVERSITY

School of Social Science

Master in Business Administration (MBA)

Postgraduate Dissertation

"The contribution of fostering a cyber security culture in organizations' cyber resilience."

Michail Michalos

Supervisor: Eleni Gaki

Patras, Greece, May 2021

HELLENIC OPEN UNIVERSITY

“The contribution of fostering a cyber security culture in organizations’ cyber resilience.”

Michail Michalos

Supervising Committee

Supervisor:	Co-Supervisor:
Eleni Gaki	Konstadinos Kutsikos
University of the Aegean	University of the Aegean

Patras, Greece, May 2021

"I would like to thank my supervisor Dr. Gaki, for her guidance during the past months while developing this research project. Her continuous encouragement and further questioning have made this journey an exciting and productive learning experience.

This dissertation is dedicated to my family. My wife Ariadni and our daughter, Ino. I would not have completed this project without Ariadni's patience, support, and constant encouragement. I am lucky and thankful for having you in my life."

Abstract

While cyber security awareness has become fundamental for organizations, the threat landscape indicates that adversaries constantly evolve their tools and techniques, delivering further sophisticated attacks. Given that the human factor remains a considerable threat, a holistic approach engaging organization members by cultivating a cyber security culture intensifies cyber resilience. Various commercial and research perspectives introduce frameworks on assessing the cyber security culture deployed alongside technical and administrative controls.

This dissertation aims to upraise the importance of cyber security culture and explore practical aspects of developing and deploying an assessment tool. Organizational culture is being elaborated first as there is common ground to examine, including some further considerable aspects such as subcultures and culture change. Subsequently, cyber security cultures are being analyzed by decomposing definitions, frameworks, and significant elements such as cultivating methods and functional practicalities. While delving into the literature, a new cyber security culture framework is introduced based on Schein's model.

The research segment has been endorsed by a questionnaire which 156 participants supported. Data has been analyzed with the help of IBM's SPSS and Amos. The findings indicate that cyber security culture is statistically related to the presence of Chief Information Security Officer (CISO), the organization's industry, and the cyber security resilience, as perceived by organization members. Considerable results have been derived from relevant factor analysis and confirmatory factor analysis, corroborating the questionnaire's reliability.

While an actual assessment of cyber resilience would require a time-consuming procedure for months or years, this study has provided theoretical supporting factors of resilience and a toolbox of practical elements to consider while developing a plan to assess and bring cyber security culture to a substance.

Keywords

Cyber security culture, information security culture, cyber security, organizational culture, cyber resilience, culture assessment.

"Η συμβολή της προώθησης μιας κουλτούρας κυβερνοασφάλειας στην ψηφιακή θωράκιση των οργανισμών"

Μιχαήλ Μίχαλος

Περίληψη

Παρόλο που η εκπαίδευση για την κυβερνοασφάλεια έχει πλέον εδραιωθεί για τους οργανισμούς, οι απειλές στον κυβερνοχώρο εξελίσσονται συνεχώς μέσα από εργαλεία και τεχνικές, κάνοντας έτσι τις επιθέσεις πολύ πιο περίπλοκες. Με δεδομένο πως ο ανθρώπινος παράγοντας εξακολουθεί να παραμένει μια σημαντική απειλή, μια ολιστική προσέγγιση για μέλη οργανισμών όπου συμμετέχουν σε μια διαδικασία καλλιέργειας μιας κουλτούρας κυβερνοασφάλειας, φαίνεται να είναι σε θέση να βελτιώσει την ψηφιακή θωράκιση του οργανισμού. Υπάρχουν πολλά εμπορικά και ερευνητικά μοντέλα διαθέσιμα για την εκτίμηση της κουλτούρας κυβερνοασφάλειας τα οποία μπορούν να χρησιμοποιηθούν παράλληλα με τεχνικά και διαχειριστικά μέσα.

Σκοπός αυτής της διπλωματικής εργασίας είναι να αναδείξει την σπουδαιότητα της κουλτούρας κυβερνοασφάλειας και να διερευνήσει τις πρακτικές πτυχές της αναπτύσσοντας και θέτοντας σε εφαρμογή ένα εργαλείο εκτίμησης. Αρχικά αναλύεται η έννοια της οργανωσιακής κουλτούρας καθώς υπάρχουν κοινά σημεία προς επεξεργασία, συμπεριλαμβανομένων σημαντικών πτυχών όπως οι υποκουλτούρες και η αλλαγή κουλτούρας. Στην συνέχεια αναλύεται η κουλτούρα κυβερνοασφάλειας μέσα από την μελέτη ορισμών, μοντέλων και άλλων σημαντικών στοιχείων όπως μεθόδων καλλιέργειας και πρακτικών θεμάτων. Μετά την ολοκλήρωση της βιβλιογραφικής ανασκόπησης, προτείνεται ένα νέο μοντέλο κουλτούρας κυβερνοασφάλειας το οποίο βασίζεται στο μοντέλο του Schein.

Το ερευνητικό μέρος της εργασίας υποστηρίζεται από ερωτηματολόγιο το οποίο απαντήθηκε από 156 συμμετέχοντες. Τα δεδομένα που συλλέχθηκαν αναλύονται με τις εφαρμογές SPSS και Amos της IBM. Τα αποτελέσματα της ανάλυσης υποδεικνύουν πως υπάρχει στατιστική σχέση μεταξύ της κουλτούρας κυβερνοασφάλειας και της παρουσίας επικεφαλής ασφάλειας πληροφοριών (CISO), τον τύπο δραστηριότητας του οργανισμού αλλά και της ψηφιακής ανθεκτικότητας όπως την αντιλαμβάνονται τα μέλη του οργανισμού. Σημαντικά είναι και τα αποτελέσματα της παραγοντικής ανάλυσης αλλά και της επιβεβαιωτικής ανάλυσης παραγόντων καθώς υποστηρίζουν την αξιοπιστία του ερωτηματολογίου.

Μια πραγματική εκτίμηση της ψηφιακής ανθεκτικότητας απαιτεί μια χρονοβόρα διαδικασία που μπορεί να διαρκέσει για μήνες ή και χρόνια. Η εργασία αυτή παρέχει τους θεωρητικούς παράγοντες που υποστηρίζουν την ψηφιακή θωράκιση με την παρουσία της κουλτούρας κυβερνοασφάλειας. Επίσης, παρέχει μια σειρά μεθόδων και εργαλείων που μπορούν να ληφθούν υπόψη, κατά τη διάρκεια δημιουργίας ενός σχεδίου για την εκτίμηση της κουλτούρας κυβερνοασφάλειας.

Λέξεις – Κλειδιά

Κουλτούρα κυβερνοασφάλειας, κουλτούρα ασφάλειας πληροφοριών, κυβερνοασφάλεια, οργανωσιακή κουλτούρα, ψηφιακή θωράκιση, εκτίμηση κουλτούρας.

Table of Contents

List of Figures

List of Tables

List of Abbreviations & Acronyms

APT	Advanced Persistent Threat
CFA	Confirmatory Factor Analysis
CIA	Confidentiality Integrity Authentication
CS	Cyber Security
CSC	Cyber Security Culture
CSIRT	Computer Security Incident Response Team
CSO	Chief Cybersecurity Officer
DPA	Data Protection Authority
ENISA	European Network Information Security Agency
EU	European Union
GDPR	General Data Protection Regulation
IR	Incident Response
IS	Information Security
MSSP	Managed Security Services Provider
MTTR	Mean Time to Recover
OC	Organizational Culture
SETA	Security Education, Training and Awareness
SMT	Senior Management Team
SOC	Security Operations Center

1. Introduction

While organizations tend to depend further on cyberspace, threat actors identify this fact as an opportunity to attack them. Within this context, organizations invest heavily in technical controls to protect their digital assets, including data considered the new gold (Shepherd, 2018). Be that as it may, security breaches continue to avalanche daily news, including Microsoft, FireEye, SolarWinds, and other well-established and respected technology vendors. In 2019, IBM reported that for Europe and Asia, insider threat remains in the top three notable attack activities (*X-Force Threat Intelligence Index 2020*, 2020). Organizations continue to put their money on technical controls and do not look after their weakest link, the human factor. Cyber resilience relies greatly upon human effort, knowledge, skills, behaviors, and norms, and hence a Cyber Security Culture (CSC) should be nourished to strengthen the organization's cyber defense.

The purpose of this dissertation is to upraise the importance of CSC in today's organizations cyber defense by exploring both theoretical and practical aspects that comprise and influence the CSC status and cyber resilience thereafter. Theoretically, aspects of OC are being elaborated first and pursuing, CSC prospects are discussed along with other manners, including cultivating considerations. Practically, apart from unfolding handy aspects of CSC and how it can be assessed, this study itself is an example of how to develop a tool from scratch based on solid scientific groundwork. Beyond theory and practice, further aspects are being explored that might affect CSC, including a CISO presence, industry, and more.

To meet this study's purpose, apart from the literature review required to be developed, as already discussed, a primary research has been elaborated using a questionnaire. Following an exploratory research design, this study incorporates the quantitative method to interpret collected data. A set of specific hypotheses help to unfold CSC status characteristics that support CSC's understanding and its practical aspect. The questionnaire is being further elaborated within the research area through factor analysis and a CFA, which helps understand the tool used better.

Throughout the course of this dissertation, some conclusions of high interest have been evolved. First and most significant, this dissertation introduces a CSC framework to be used for assessment which is primarily based on Schein's Organizational Culture (OC) model. This conceptual model is based on well-established foundations and has been used throughout the course of this study to carry out the primary research. Furthermore, given that during literature review the fact that CSC contributes to cyber resilience is established, this study has provided evidence about the organization's characteristics and if they affect CSC status. For example, data collected provided evidence that organizations with CISO have a strong correlation concerning CSC status.

Inevitably, coping with an exploratory study, a set of limitations has been recognized. Carrying out a research regarding Cyber Security (CS), inescapably led to constraints, given that CSC assesses an organization's status and could eventually publish information on vulnerabilities that threat actors could take advantage of. Hence, a broad approach has been incorporated, rather than narrowing it down to a specific organization. On the other hand, although supported by theory that CSC contributes to, cyber resilience could not be practically assessed as this would require the development of an upcycling process that would demand recurring assessments. The last limitation is that CFA might have been elaborated regarding the questionnaire tool in a primary manner; however, a competent analysis requires high qualifications and proficiency in this domain.

To achieve the objectives outlined formerly, the following structure has been cultivated. Chapter 2 constitutes the Literature Review, which is logically divided into two major parts: OC elaboration and the CSC. An effort to unfold all aspects is taking place, including concepts such as definitions, subcultures, and culture change to get a deep understanding of the OC primarily and the CSC thenceforth. Chapter 3 unfolds the Research Methodology, where the research structure is being contemplated along with all aspects involved in the data analysis process. Chapter 4 lays out all the data collection analysis while Chapter 5 summarizes the Conclusions, including all research answers and comments that are valuable developments of this study.

2. Literature review

2.1 Introduction

To build vital research around CSC, a company should inevitably have an OC instilled. Many definitions could describe culture, but the most predominant could be considered Daft's (2010) "*The set of key values, beliefs, understandings, and norms that members of an organization share*.". Although a managerial approach would require the deployment of a strategic framework to inculcate a corporate culture, a more simplistic approach would include the definition of far more plain statements such as "*the way we do things around here*," referring to the relevant organization (Lundy & Cowling, 1996).

OC has been studied since its first concept introduction by Elliott Jacques in 1951. In his book "*The Changing Culture of a Factory*," he elaborates research comprising group employees' social norms and behavioral analysis (Jaques, 2013). Culture's significance has clambered notably within the corporate environment; Peter Drucker's quote, "*Culture eats strategy for breakfast*," could support this purport (Hyken, 2015).

2.2 Organizational Culture

2.2.1 Organizational Culture definition

Throughout the course of OC research, many definitions have been attributed. Some of them are being referred to below.

Davis (1984) published his first book in 1970, and since then, he drew the attention of executives that showed interest in the term corporate culture. In his second book, he defined culture as "*The pattern of shared beliefs and values that give members of an institution meaning and provide them with the rules for behaviour in their organization*." (Davis, 1984).

O'Reilly and Chatman (1996) explored culture, and they focused mainly on its aspect in terms of shared values and norms and how this could define a system of social control. In their paper, they defined OC as "*a system of shared values and norms that define appropriate attitudes and behaviors for organizational members*." (O'Reilly & Chatman, 1996).

In his book, Brown (1998) elaborates on OC origins and how it has evolved to interact with human resources management and organization's members performance. He defined culture as "*the pattern of beliefs, values and learned ways of coping with experience that have developed during the course of an organization's history, and which tend to be manifested in its material arrangements and in the behaviours of its members*." (Brown, 1998).

Schein (2004) focused on psychological patterns of culture and acknowledged two dimensions; the first is a dynamic actuality being present within a group and the other, as a formality through rules and policies. Hence, he ascribed culture as "*a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems*." (Schein, 2004).

Most recent definitions can be drawn from institutions such as the Chartered Management Institute (CMI), a long-lived professional organization focusing on management and leadership. CMI's definition of culture is "*the way that things are done in an organization, the unwritten rules that influence individual and group behaviour and attitudes*." (*Understanding Organizational Culture*, 2016).

Having explored the definitions, it is evident that although OC has been studied through different prospects in terms of research domains such as psychology, the management, or human resources management, they all come down to a set of common elements. Tharp's visual representation is where culture can be found, presenting the common ground of cultures' various definitions, which is a strong example to take into consideration.

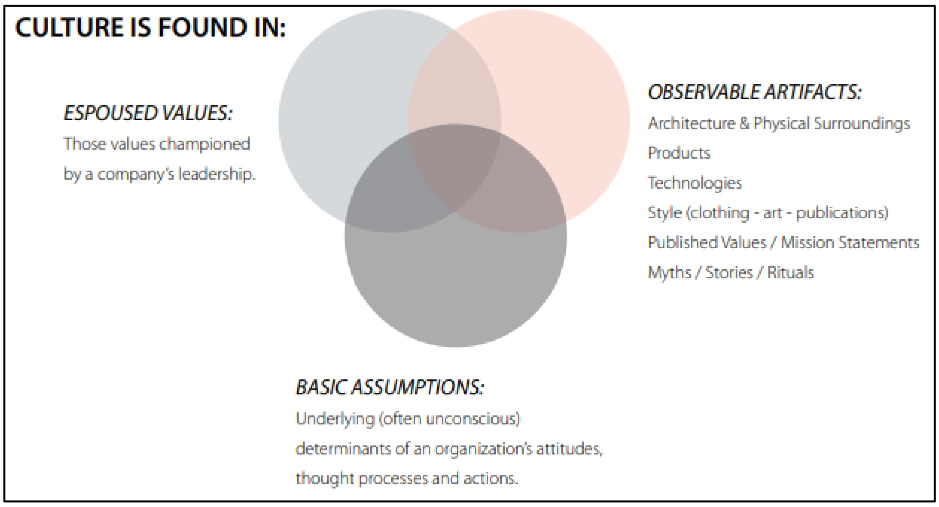

CULTURE IS FOUND IN:
ESPOUSED VALUES:
Those values championed by a company's leadership.
OBSERVABLE ARTIFACTS:
Architecture & Physical Surroundings
Products
Technologies
Style (clothing - art - publications)
Published Values / Mission Statements
Myths / Stories / Rituals
BASIC ASSUMPTIONS:
Underlying (often unconscious) determinants of an organization's attitudes, thought processes and actions.

Figure 2.1 Tharp's (2009) approach in defining organizational culture.

2.2.2 Organizational Culture models

Throughout the course of culture's examination and research, the notion of having one, comes fairly early within the 70s, with the groundwork of Turner, Handy, Hofstede and others (Allaire & Firsirotu, 1984). Since then, a lot of types, models and frameworks have been developed mainly to assess and identify the characteristics and ultimately define the culture of an organization. Some of the most notable models worth mentioning here, have been developed by Harisson (1972) and his Organization Ideologies, Dean and Kennedy's (2000) culture which first introduced forces outside the organization and Schneider's (1999) approach to bridge both aforementioned models into one. Schein, Hofstede and Cameron and Quinn's work is also considered as pioneering and their models on OC are elaborated on 2.2.2.1, 2.2.2.2 and 2.2.2.3 respectively. Further models are elaborated below as well to build a comprehensive understanding of OC and how it can be defined through various elements considered.

2.2.2.1 Schein's three levels in the organizational culture

Schein introduced the three levels of culture to provide means of analysis and differentiation regarding values that define an OC. These three levels are complementary to one another and can be described as follows (Schein, 2004).

- **Artifacts**: the first level represents all elements that can be seen, heard, or felt for an organization. This level embodies for example, the working environment, the offices, the products, ceremonies, dress code, and more.
- **Values**: the second level constitutes the mindset of the organization's members, which evidently comprise individuals' attitudes. Decisions made at this level are typified as values and beliefs.
- **Assumptions**: in the third and last level, when values and beliefs become granted and are perceived as shared knowledge or an established type of work that is ordinary, then values have become assumptions.

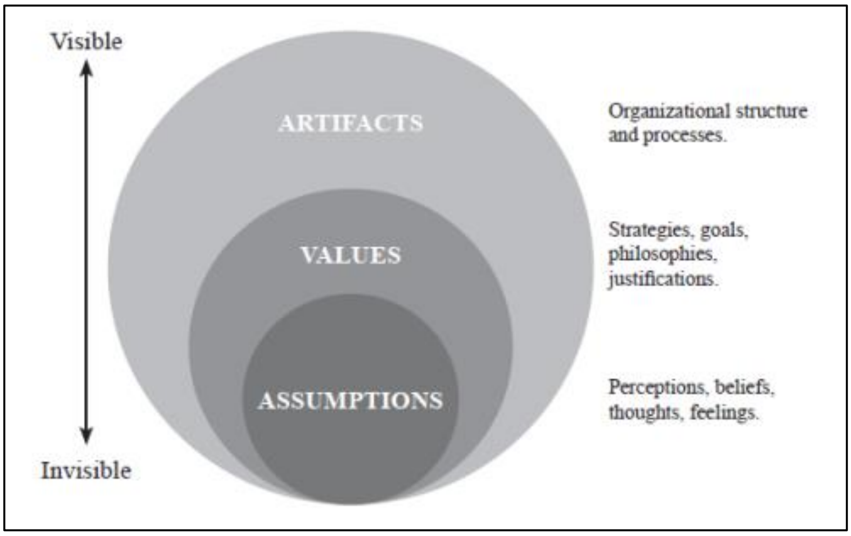

Visible
Invisible
ARTIFACTS
VALUES
ASSUMPTIONS
Organizational structure and processes.
Strategies, goals, philosophies, justifications.
Perceptions, beliefs, thoughts, feelings.

Figure 2.2 Schein's three levels of Organizational Culture (Morente et al., 2018).

Recently, Granter and Edgell (2020) introduced an additional level that dethrones artifacts from the upper level, the **superstructural/ideological** one. They supported that since organizations are not operating on an isolated island with no interference from the outside, national, societal, and economic adjustments and rulings affect culture and should be considered.

2.2.2.2 Hofstede's four culture themes & six dimensions

Hofstede has been a significant contributor to national and OC research. His findings provided the following four different cultures focused on the assessment step before committing to organizational change (Hofstede, 2019).

- **Optimal**: this type of culture focuses on aligning the organization towards its strategic goals. This is the type one should have primarily in mind. It is the first and utmost culture that should also consider any restriction such as specific legal or financial rules. To assess this type of culture, it is essential to identify any subcultures present within the organization's functions.
- **Actual**: This is where it begins; this is the initial assessment of where the organization stands. It is the outcome of the culture's evaluation before its change begins. Within this type, any functional subcultures must be identified. It is doubtful that the IT department has the same subculture as the Legal one.
- **Perceived**: this is the culture the organization members think that they have. This is not the actual culture, and when assessing the overall environment, it could be considered as it depicts what employees think their culture is.

- **Ideal work environment**: within this context, employees are requested to express how they think the optimal culture would be. Even though this type does not provide any insight into the current status, it could be of assistance as employees' explicit preferences could be taken into consideration.

Further to the above, Hofstede's approach to developing an OC is relied heavily on building a culture that is backing the corporate strategy. Hence, he introduced the Multi-Focus Model, with which he incorporates six independent dimensions, but at the same time and while aiming towards strategy, they all work collectively (Hofstede, n.d.).

- **Organizational effectiveness**: in a means-oriented culture, individuals are motivated by "how" work must be done, while in a goal-oriented culture, motivation lies on "what" and thus focus on bringing back to the organization specific results. Avoiding risks and restricted endeavors drive a means-oriented environment; taking risks and bringing back outcomes is what makes a goal-oriented culture.
- **Customer orientation**: on an internally driven culture, business integrity and fairness are of most importance while customer comes first. On the other hand, in an externally driven culture, the organization focuses on fulfilling the customer's expectations with a rational, rather ethical mindset.
- **Level of control**: within a calm environment, a flexible formation is present with little restraints and authority. On the other hand, a strict work environment reveals a relatively rigid job framework where individuals are precise and austere.
- **Focus**: local companies' individuals are being distinguished by the manager and/or the function they are members of, and they are being short-term led targeting internally. Contrariwise, professional companies distinguish their members by the function or expertise.
- **Approachability**: An open culture instantly accepts new employees, and it is an environment where everyone is assumed to fit into the organization. A very closed one, though, is the exact contradictory environment.
- **Management philosophy**: Management is closely tied with the OC. An employee-oriented organization provides caring and fosters for its members while a work-oriented one, constant compelling and significantly less caring for the employees are present.

Hofstede's Multi-Focus Model is used widely within the market to assess whether organizations focus on their desired strategy using a toolkit ready to evaluate culture.

2.2.2.3 Cameron and Quinn's four dimensions

Cameron and Quinn have developed the Organizational Culture Assessment Instrument (OCAI), a tool that assesses an OC status. As with Hofstede, four different types are being introduced (Cameron & Quinn, n.d.).

- **Adhocracy Culture**: this is the culture that has instilled a creative and highly dynamic setting. Further characteristics include experimenting, risk-taking, failing fast, and learning from mistakes, innovation, and this culture has entrepreneurs and visionaries present.
- **Clan Culture**: in this type, words like family and friendship matter. Values such as partnership, human development, and cooperation are significant to this culture. An organization's people are described by devotion and their customs, while managers are recognized as mentors.
- **Hierarchy Culture**: this is where values include formal practices, policies, result-driven long-term planning, reliability, and competency. Management in this culture is responsible for eliminating miscalculations and cautiously solving any problem to deliver rigorously and coherently.
- **Market Culture**: this is a result-driven environment, and priorities in this culture include directing resources towards goals, the insistence of prevailing, significance of achievements, and antagonism. Managers, in this case, are assertive, strict, and requesting.

When assessing these types of cultures together, OCAI provides a mapping depicting the Competing Values Framework (CVF), including Flexibility, Stability, Internal or External Orientation (Bremer, 2019).

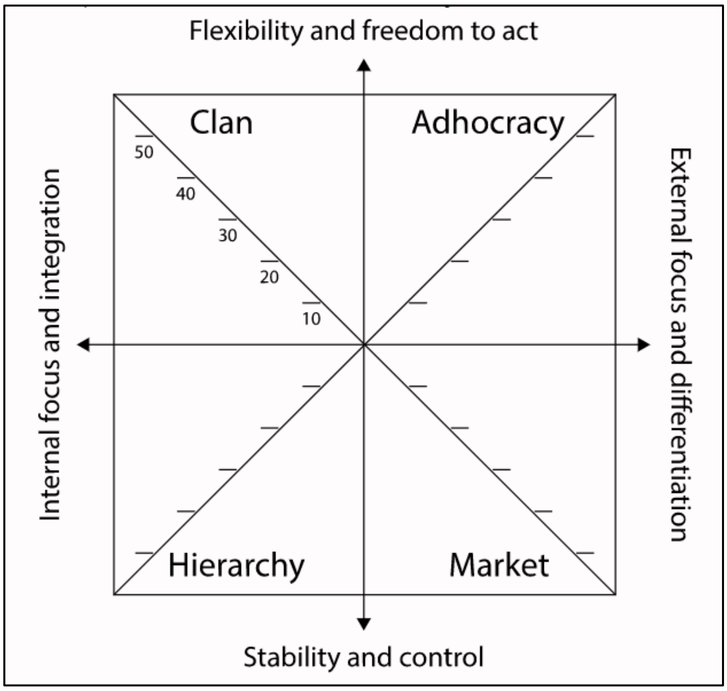

Flexibility and freedom to act
Clan
Adhocracy
50
40
30
20
10
Internal focus and integration
External focus and differentiation
Hierarchy
Market
Stability and control

Figure 2.3 The Competing Values Framework (Cameron & Quinn, n.d.).

2.2.2.4 The Organizational Culture Inventory by Cooke and Lafferty

Cooke and Lafferty introduced in 1987 the Organizational Culture Inventory (OCI) framework, an assessment tool that evaluated twelve behavioral patterns categorized, which are further sorted into three types of cultures as follows (Cooke & Rousseau, 1988).

- **Constructive Cultures' norms**
  - **Achievement**: members set ambitious yet achievable objectives, rely on relative plans, and engage with eagerness.
  - **Self-Actualizing**: members are encouraged to improve and undertake new and exciting assignments within a pleasant environment.
  - **Humanistic Encouraging**: this environment supports ancillarisation, motivation, and positivity within its members.
  - **Affiliative**: this is an affectionate environment where partnership and gratification of the group are essential.
- **Passive/Defensive Cultures' norms**
  - **Approval:** in this environment, obtaining acceptance and admittance with each other is crucial.
  - **Conventional:** this environment is about complying with policies, reconciling, and leaving a positive feeling.

- **Dependent:** nothing is being done without prior consideration with managers; the organization's members do not improvise; they do what they are being told.
- **Avoidance:** an environment where people tend to avoid being blamed by not accepting or either changeover responsibilities.

- **Aggressive/Defensive Cultures' norms**
  - **Oppositional**: an analytical and interpretative environment of interchanging and defending ideas where non-risk decisions are taken.
  - **Power**: Imposing of dynamism from managers on members which are menial and unpretentious.
  - **Competitive**: members operate in a constant race where they either win or lose, steadily in a rivalry position rather than collaborative.
  - **Perfectionism:** an antagonistic environment where members pay attention to details and are expected to put much effort into small tasks.

This framework's measurement is being represented through a circumplex where further results can be derived, which reflect whether the organization in question tends to mind tasks over people or security over satisfaction.

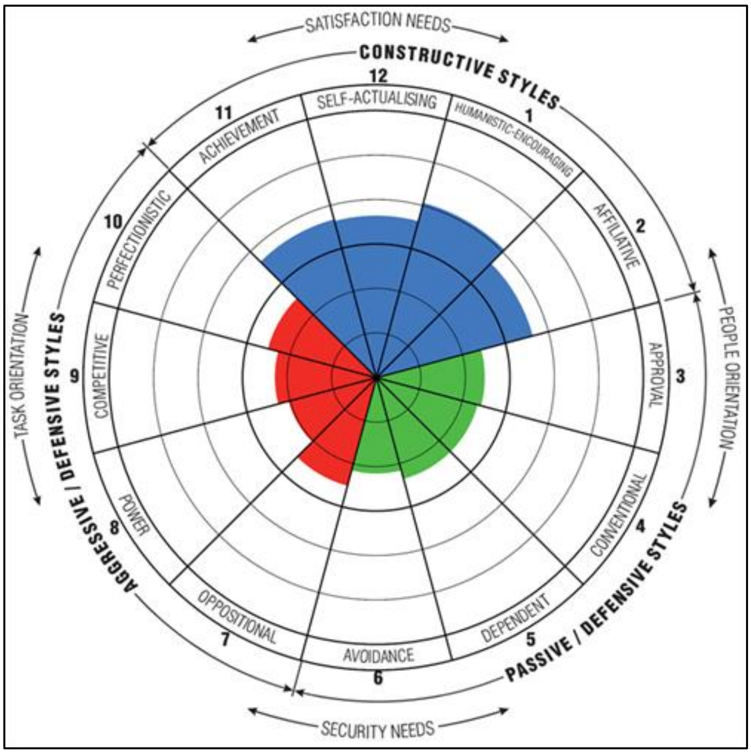


Figure 2.4 Organizational Culture Inventory Circumplex example (*The Circumplex*, n.d.)

2.2.2.5 Johnson and Scholes cultural web

Johnson and Scholes (1998) developed the cultural web. This tool is widely used to assess and analyze organizational culture, which consists of six elements that all come down to the paradigm, a blended mix of all elements that define the culture.

- **Stories and Myths**: descriptions and sayings that recite both organization's members as well as foreign people. Stories and myths represent values that the organization chooses both voluntarily and purposefully to deify.
- **Rituals and Routines**: this element represents the actual accustomed behaviors within the organization's environment, including the ones that derive from management decisions.
- **Symbols**: components that comprise the visual portrayal of the organization, which include logos and designs, advertisements, working environment, and dress code.
- **Control Systems**: this element includes structural processes by which the organization is run. Aspects like reporting, strictness, performance-based evaluation and quality are assessed here.
- **Organization Structures**: this is where hierarchy is being decomposed and analyzed in detail to determine where power and decision-making responsibilities lie on.
- **Power Structures:** this element examines where pure influence derives from within the organization and how authority flows from top to bottom.

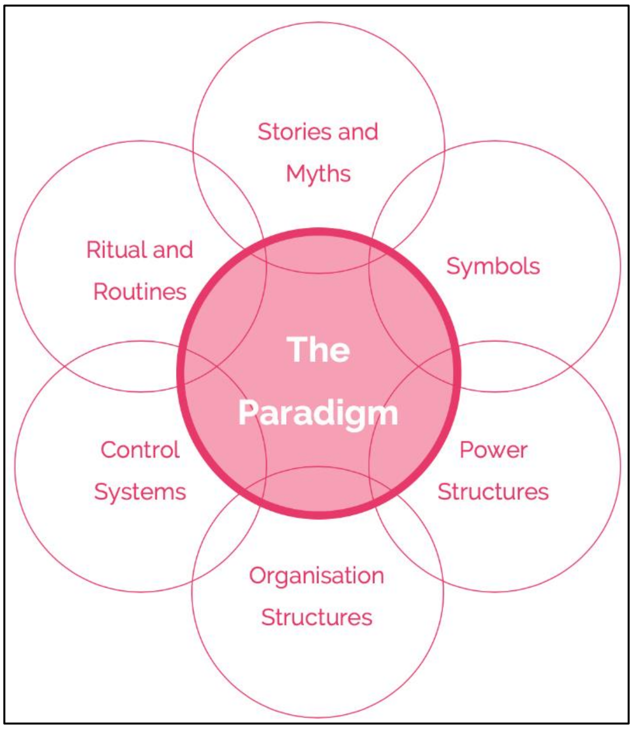


Figure 2.5 Johnson and Scholes cultural web (Johnson & Scholes, n.d.).

2.2.3 Further culture considerations

2.2.3.1 External Culture Environment

Until now, unfolding of models and types focus mostly on the internal environment of organizations, except from the introduction of superstructural level in Schein's model by Granter and Edgell. However, it is important for organizations to be able to keep up with the environment and consequently shift their course to face challenges or keep a consistent and safe operation route. Daft (2010) describes a relevant culture model that interprets environmental forces and how they affect the internal environment.

- **Adaptive**: undoubtedly, technology has provided the means for companies to transform over the past decade, and there is still more to come on this subject. Be that as it may, companies were challenged to either keep up with the competition or set a more conservative course. This culture describes organizations that respond quickly in challenges and can detect all relevant required warnings to do so.
- **Achievement**: organizations incorporate this culture when their products are addressed to a distinct set of customers. Members focus solely on providing their

distinct product and forbear the necessity to respond to the environment's challenges flexibly.

- **Involvement**: this culture describes organizations that emphasize on their members. Taking care of employees rather than putting the customer first no matter what fosters a corporate environment that can boost overall performance and thus make the relevant organization thrive at what it does.
- **Consistency**: this culture describes organizations that decide to operate in a disciplined, careful, and stable manner. Although this culture diverges from the current fast-paced landscape, organizations still decide to operate in a slow yet safe, to some extend, demeanor.

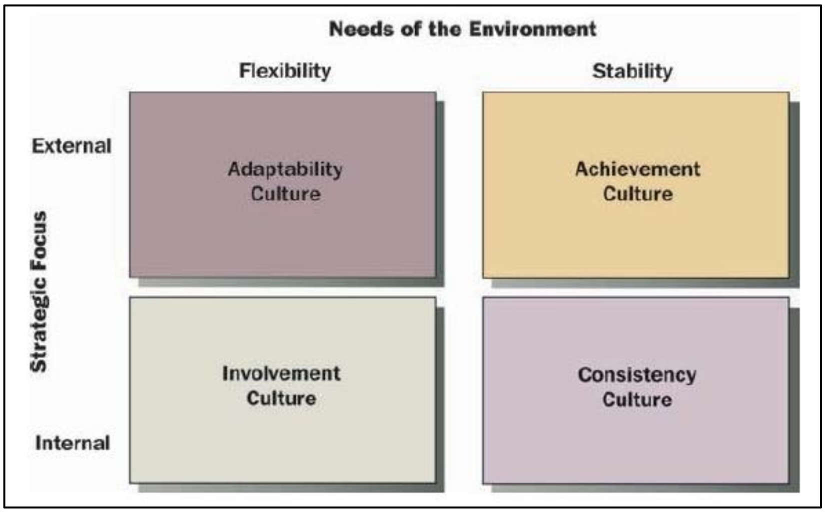


Figure 2.6 Four types of organizational culture (Daft, 2010).

Daft (2010) depicts this culture matrix in Figure 2.6. One can visually detect whether an organization, depending on the culture, focuses internally or externally and whether it incorporates an internal environment of flexibility or stability.

2.2.3.2 Innovation culture

The World Economic Forum (Kailash, 2020) has recently released the tool UpLink with which it anticipates connecting innovative ideas to address challenges that emerge from the United Nation's Sustainable Development Goals (SDGs). A well-fitted innovation strategy can create value that companies tame and deliver to their customers in the corporate landscape. Innovation's significance is in rise as it is perceived as a breakthrough to solve problems and offer new products and services. Within this context, the proper organizational environment should be fostered to be able to experiment and motivate for ideas.

A culture of innovation could support this environment, and Maher (2014) has described seven elements that organizations with high innovative practices have in place.

- Members of this culture should be allowed to make mistakes without the fear of negative consequences. Mistakes should be part of the learning process because there is further motivation for more ideas to be experimented with.
- Senior Management should back members both with means of resources but in a motivational and leadership way.
- As learning by doing is a key aspect of innovation, what has already been done should be well documented. An openly distributed and easily accessible knowledge base is essential.
- An organization's goals should be distinct and unequivocal, and leadership is responsible for this element. When the objective is comprehended, motivation for innovation can be significantly greater.
- Symbols and rituals are also enablers for motivation as they directly affect the behavioral aspect of the members.
- There is a practical aspect of developing innovative cultures, which refers to providing tools such as formal training and skills advancement.
- Member's interaction is also notable as it provides an environment of trust, teamwork, and praising each one's contribution.

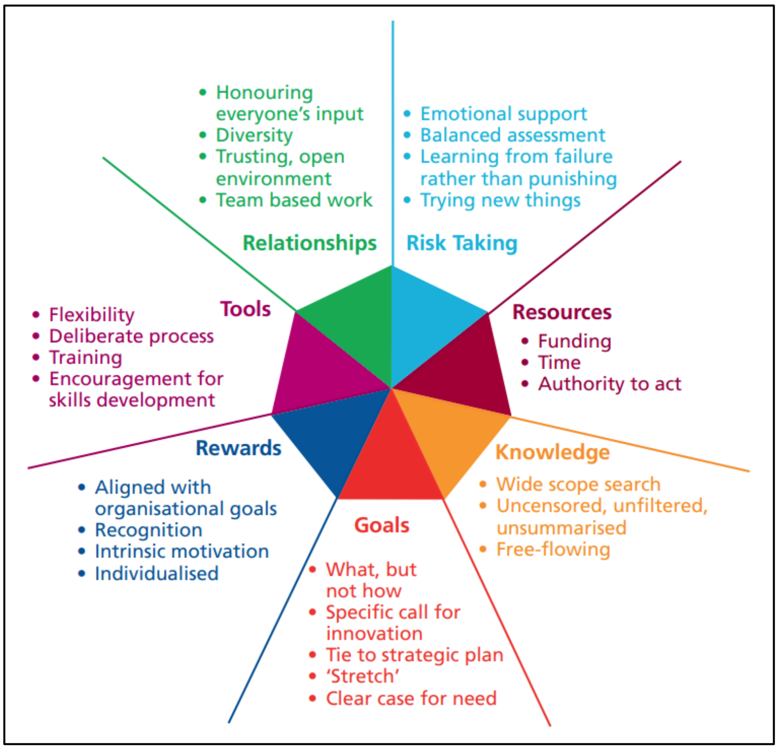


Figure 2.7 Elements of Culture of Innovation (Maher et al., 2010).

Having already discussed OC models, it is evident that innovation could find significant barriers in cultures that include aspects of the ruling, control, and procedures.

2.2.3.3 Subcultures

In large organizations that span across multiple geographic regions and involve a great number of functions, it is highly likely that subcultures are present. Although core culture values are present crosswise in an organization, subcultures incorporate behaviors and senses that emerge following members of distinct groups, working together (Khatib, 1999).

An example of this could be a technology company that, amongst other activities, incorporates a software development department that uses Agile and DevOps methodology. Frameworks that help these functions include distinct values to excel and thrive in performance, such as the Scaled Agile Framework (SAFe). SAFe distinguishes four core values required for the framework to succeed, Alignment, Built-In Quality, Transparency, and Program Execution (Leffingwell, 2019). It is highly unlikely that these values would be of any use for the organization's financial or legal department. However, the framework succeeds only when it is aligned with the organization's strategic goals, which means that an OC is present. This group follows the relevant core values, but it also consolidates its values as well.

The significance of the challenges mentioned above should not be left without confrontation and proper, delicate working. If subcultures prevail over the organization's core values, controversies between workgroups might rise; thus, culture and subcultures need to be aligned with the organization's strategic goals (Khatib, 1999).

2.2.3.4 Culture change

An essential aspect of OC is none other than to be instilled in benefit of the strategy and performance. Within this context, there are cases where strategies, plans, and goals need to change, and thus, culture must follow this new course. Khatib (1999) elaborates on some of the critical aspects to consider while contemplating culture change.

- Two main elements define the difficulty of culture change, how well established is the current culture and if there are any subcultures present. Difficulty rises when multiple and highly embedded subcultures are present.
- A significant challenge is being able to assess the current culture state. A distinct framework assessment must take place to understand fully where culture is, appraise findings, and set a course to the culture elements required.
- Indisputably, the organization's senior management team plays a substantial role within the change process as it defines the culture required and is responsible for carrying out the relevant transformation operation.

As member's participation, involvement, and understanding will define the culture change outcome, every member needs to be well informed and own this process's gravity. (Sinek, 2011) has developed a theory where "Why" is the main element of leaders that need to elaborate and as a consequence, to motivate. "Why" drives a force for members that consigns symbols, values, and beliefs and thus, strengthens the culture change process while dissociating the risk of an unwanted outcome.

2.3 Cybersecurity Culture

2.3.1 The importance of Cybersecurity Culture

According to Morgan (2018), the cost of cybercrime is projected to grow by approximately 15 percent every year until 2025. While in 2015, the cost of cybercrime was $3 trillion, by 2025, it will have skyrocketed to $10,5 trillion (Morgan, 2018). To understand the amount, cybercrime's cost is third to the world's largest economies, the US first, and China second. Ransomware, a malware category that infects workstations and sometimes all connected computers on the same network, could be considered a global epidemic. It is responsible for some of the well-known attacks in recent digital history, including the NotPetya attack on Maersk shipping company in 2017, which ended up costing the world shipping leader a total sum of almost $300 million (Lord, 2017).

Gartner reports that during 2020 the Internet of Things (IoT) devices connected to the internet will reach the astounding amount of almost 20,5 billion devices (van der Meulen, 2017). This number magnifies cyberspace to a new level where a global culture of people and devices are all interconnected in a digital environment. The National Institute of Standards and Technology (NIST) defines cyberspace as "*a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*." (Joint Task Force Interagency Working Group, 2020). Although cyberspace brings opportunities and potential for growth, it also comes with a set of risks that should not be neglected. Amongst the consequences of a malicious attack, apart from the profound financial losses for which some sizes have been discussed before, an organization's impairment of reputation and credibility is also significant (Da Veiga, 2016).

Within cyberspace, three categories are responsible for cybercrimes, cybercriminals, organization's insiders, and last, hackers (Da Veiga, 2016). A review of 7800 publicly disclosed security breaches from 2012 to 2017 indicated that half of the breaches had been attributed to insider threats (Tucker et al., 2018). Out of this portion, an astounding 44% was made by human neglectfulness, while 38%, had malicious intentions (Tucker et al., 2018). These numbers are alarming, given the fact that an organization might have invested significant capital in technical controls but still could not have prevented the human factor.

Having examined the above, it is evident that technical controls alone cannot cope with the CS requirements, but organizational means should be put in place. Hence, the human factor should not be overlooked but must be taken as a substantial element to consider (Reegård et al., 2019). If members of an organization are not trained or do not know how to use cyberspace in a safe, conscientious, and principled manner, they eventually become a peril for their organizations and themselves (Seyran et al., n.d.). Therefore, fostering a CSC is significant as eventually, it would provide a cyber-resilient environment for their organization.

2.3.2 Cybersecurity Culture Definition

As a concept, CSC is being explored over the last 15 years, where the internet has massively sprawled worldwide. However, it is essential to unfold that culture, in the essence of securing all things digital, is way older and included within IS culture. The concept behind both aspects of CS and IS is related but remains lightly comparable. IS considers information as an asset while CS considers everything and everyone connected to and reached by cyberspace as an asset (von Solms & van Niekerk, 2013). That aside, practically today, both domains are interchangeable and, in essence, are conceived as the same. Having sorted this out, some definitions follow from researchers and other organizations who have contributed to this domain.

Da Veiga (2016) supports that to define CSC, the OG should be discussed first and the fact that CSC is being defined by factors other than an individual or organizational, but from a national and international perspective. Da Veiga defines CSC as "*the intentional and unintentional manner in which cyberspace is utilized from an international, national, organizational or individual perspective in the context of the attitudes, assumptions, beliefs, values, and knowledge of the cyber user. The cybersecurity culture that emerges becomes the way things are done when interacting in cyberspace and it can either promote or inhibit the safety, security, privacy, and civil liberties of individuals, organizations or governments*" (Da Veiga, 2016).

ENISA is the par excellence European Agency that deals with CS and supports organizations within the EU to advance their security disciplines. According to ENISA, CSC "*refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies*" (*Cyber Security Culture in Organisations*, 2017).

Another approach comes from Tziarras (2014), whose research unfolds a common path for both CSC and strategic culture, including CSC's multi-leveled management elements. Tziarras defines CSC as "*a body of collective—i.e., non-state, sub-national, and national—attitudes, patterns of behavior, beliefs, as well as conceptions of (cyber)* *security, shaped based on the need to secure multiple referent objects against various cyberthreats, which would influence cybersecurity strategies*" (Tziarras, 2014).

Roer has been contributing to the CSC domain for over a decade and has commercialized his and his team's approach to measuring CSC. His definition might be explicit; however, it cannot be taken as simpleminded, and so far, it is the broader approach. Roer exemplifies CSC as "*the ideas, customs and social behaviours of a particular people or group that helps them be free from threat and danger*" (Roer, 2015).

2.3.3 Cultivating Cybersecurity Culture

Having underlined the importance of CSC and some prevailing definitions, a description of how one could approach CSC should occur. As this is a strategic decision that involves every member of an organization, from SMT members to internship employees, there are many ways to get involved. Be that as it may, it is essential to comprehend that each plan should be set based on many different variables, but it all comes down to strategic decision. A high-level synopsis of how cultivating CSC could take place can be given by combining Redi and van Niekerk's (2014) approach to Schein's model and ENISA's practical implementation guide for CSC.

Following relevant research review, Redi and van Niekerk (2014) supported that Schein's OC model, along with some adjustments, can provide a fostering environment for CSC. Their concept unfolds as follows:

- Artifacts: This element includes visible aspects of the organization, such as network security arrangements and formalized procedures.
- Espoused Values: This element documents the strategic point of view for both security and business, which in practice, fuels the Artifacts.
- Shared Tacit Assumptions: As with Schein's approach, this element includes the instinctive beliefs and instilled thoughts and perceptions amongst the organization's members that relate to security.
- Knowledge: The fundamental and mandatory security-focused knowledge as a requisite for daily operational excellence in a digitally protected manner.

Going through Schein's model, the adjustment included is the last element of Knowledge. However, by considering recent Granter and Edgell's addition of the Superstructural element as examined in 2.2.3.1, this could also be of assistance when considering CSC.

This element could include intelligence regarding adversaries known as APTs and collaboration frameworks with national and international agencies such as CSIRTs and DPAs. Considering the model mentioned above, a substantial number of aspects that directly influence CSC are being discussed and should be elaborated en route to establishing a competent CSC.

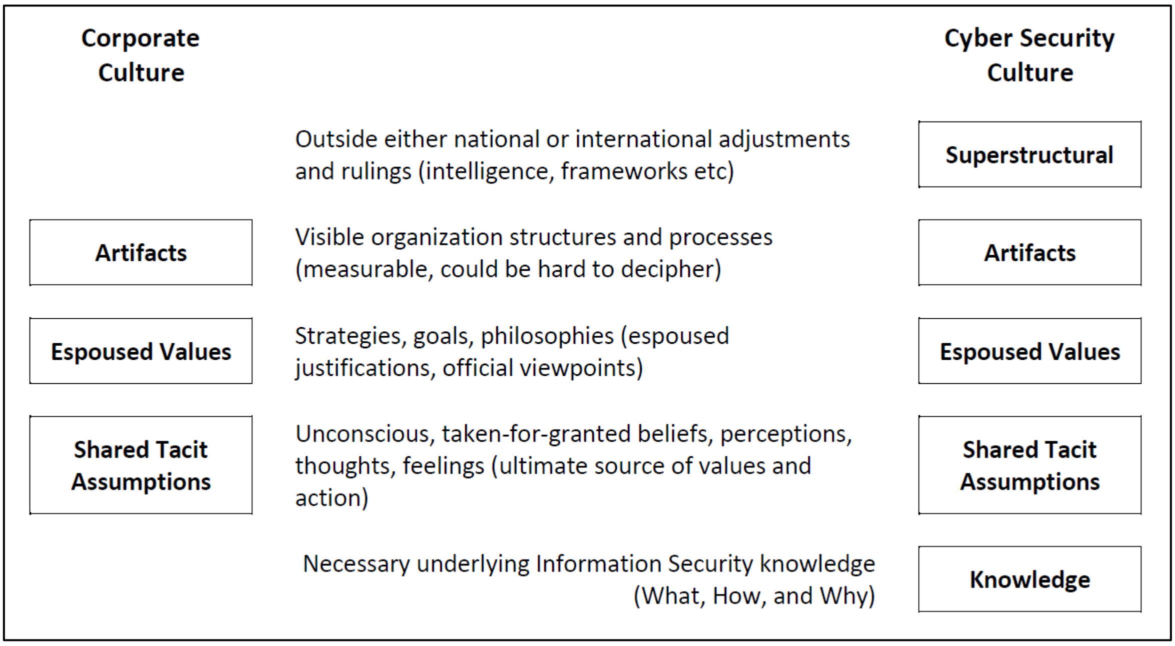

Corporate Culture
Cyber Security Culture
Outside either national or international adjustments and rulings (intelligence, frameworks etc)
Superstructural
Artifacts
Visible organization structures and processes (measurable, could be hard to decipher)
Artifacts
Espoused Values
Strategies, goals, philosophies (espoused justifications, official viewpoints)
Espoused Values
Shared Tacit Assumptions
Unconscious, taken-for-granted beliefs, perceptions, thoughts, feelings (ultimate source of values and action)
Shared Tacit Assumptions
Necessary underlying Information Security knowledge (What, How, and Why)
Knowledge

Figure 2.8 Schein's readjusted model including Redi and van Niekerk's approach (2014) and the Superstructural element adaptation.

Having elaborated a theoretical groundwork, ENISA defines a practical guide towards CSC by unraveling a step-by-step blueprint on preparing, executing, and recycling a CSC instrumentation plan. Going through this guide, the following eight steps are being specified (*Cyber Security Culture in Organisations*, 2017).

- Assembling a specific team of organization's members will be tasked to monitor the implementation of the CSC plan in terms of operations, policies, and strategy alignment. This team will be staffed by members of various functions, including legal, IT, HR, and different levels, including SMT supervision.
- Then, an outline of the business, along with the relevant risk assessment, must take place. This step comprises two elements; the first denotes that the current OC should be mapped to understand what the current stature is. The other requires a security assessment, which eventually, along with the mapped OC, will unfold synergies, compromises, or conflicts. The outcome of this exercise will provide tuned coordination between CSC and OC, without intensifying shortcomings.

- As with every plan, implementing a CSC needs specific, measurable goals. This is where objectives are defined either organization-wide or for specific functions or both, but with relevant weight.
- The fourth step is quantifying the difference between the CSC in place with the desired CSC as described from the goals set in the previous step. The idea behind this step is that one cannot reach its desired goal without a definite and straightforward starting point.
- The next step includes all the actions that need to be taken from the organization to implement the desired CSC. In this step, everything that needs to be done is documented in detail including policies, technical controls, awareness training, purchases etc.
- The sixth step is about executing what has been prepared so far by enacting the previous step's activities. This is a delicate step and needs close supervision, while it is wise to assess current conditions and decide whether activities should be set off as a whole or build a schedule of granular implementation.
- The next step is assessing the outcome of the activities completed and whether they have accomplished the relevant goals. This is an important step, and thus it should be fueled with all feedback that could be made available as for example, whether any unwanted consequence arise.
- The final step is the aftermath of the assessment conducted previously and evidently provides insight into further actions. These include reviewing elements between steps 2 to 5, which might need redefining and eventually reconsidering actions in Step 6.

ENISA also provides further insights to consider for the CSC program to succeed (*Cyber Security Culture in Organisations*, 2017).

- Instilling and maintaining a CSC within an organization should not be perceived as a one-off procedure but as a continuing operation. Be that as it may, there are different initiation paths to outset, including top-down, mid-level, and bottom-up approaches. Whatever the inauguration may be, it must be highlighted that SMT involvement lights a transcendent example to be followed for the rest of the organization.

- Without a doubt, the CSC establishment will emanate by fostering encouragement to endeavor the required activities for the goals to be met and, why not, even overmatch. However, it is important to keep in mind that changes of this scale and manner cannot be imposed forcefully. Consequently, engagement, motivation, rewarding, openness, adaptability, and communication are elements to look after while commencing a CSC program.

It is evident that elements described from Schein's model are the bedrock for ENISA's workable step-by-step guide. For example, Artifacts' structure could befall at Step 1, when choosing the relevant workgroup, Espoused Values, are beseemed in Step 3 where goals are being set, Shared Tacit Assumptions can be found in Step 4, where "how we do things around here" is being defined, then Knowledge could fit in Step 6, where activities are being documented and last but not least, Superstructural, can be found in Step 2, where operational business can be affected by factors outside of the organization.

One could conclude that rectifying the course of an OC while instilling a strong CSC is not an easy process. The guide examined demonstrates that CSC requires investment in a substantial effort to succeed as it involves people and working hours in a durable plan that might either succeed, require reformulation, or hopefully not, even fail. Nevertheless, the desired outcome would strengthen an organization's cyber existence, and thus outsetting an effort towards a CSC program should utterly be considered an advantage.

2.3.4 Cybersecurity Culture frameworks

While going through the literature review, some studies introduced frameworks that included a concrete scheme of assessment. Apart from the ones elaborated below, some others notable enough to mention here are, AlHogail's information security culture framework (2015), Tolah et al. comprehensive information security culture framework (2017), Nel and Drevin's identification of key elements for ISC (2019) and Alshaikh's research on developing CSC through employee behavior (2020). Furthermore, since organizations are most likely to obvert towards commercial solutions, a set of well documented, backed by scientific research, productized CSC assessment toolkits are elaborated. Again, some further commercial solutions are available to investigate, including CultureAI (*CultureAI | The Cyber Security Culture Management System*, n.d.)

and Security Awareness Radar by TreeSolution (*TreeSolution - Your Expert for Security Awareness*, n.d.).

2.3.4.1 Da Veiga's Information Security Culture Framework

Da Veiga (2010) has been a significant contributor to IS culture. She has developed the Information Security Culture Framework (ISCF), which has been the groundwork for further research regarding CSC. A brief description follows while Figure 2.9 unfolds the framework extensively.

- **Leadership and Governance**: This element includes the strategic approach of the organization with regards to security.
- **Security management and operations**: The aspects that contribute to effectively managing security including structure and regulations.
- **Security policies**: Any documented regulatory frameworks in place either internal or external that affect security.
- **Security program management**: This element is comprised by aspects that make sure security in place is effective such as auditing.
- **User security management**: This element defines behavioral aspects which need to be addressed for members to act in a secure manner.
- **Technology protection and operations**: Any technical or physical controls in place, are described in this element.

Da Veiga' s (2020) research has probably been the most extensive one regarding culture. She has proved that this framework is also flexible in rearranging and fitting further needs and industrial challenges.

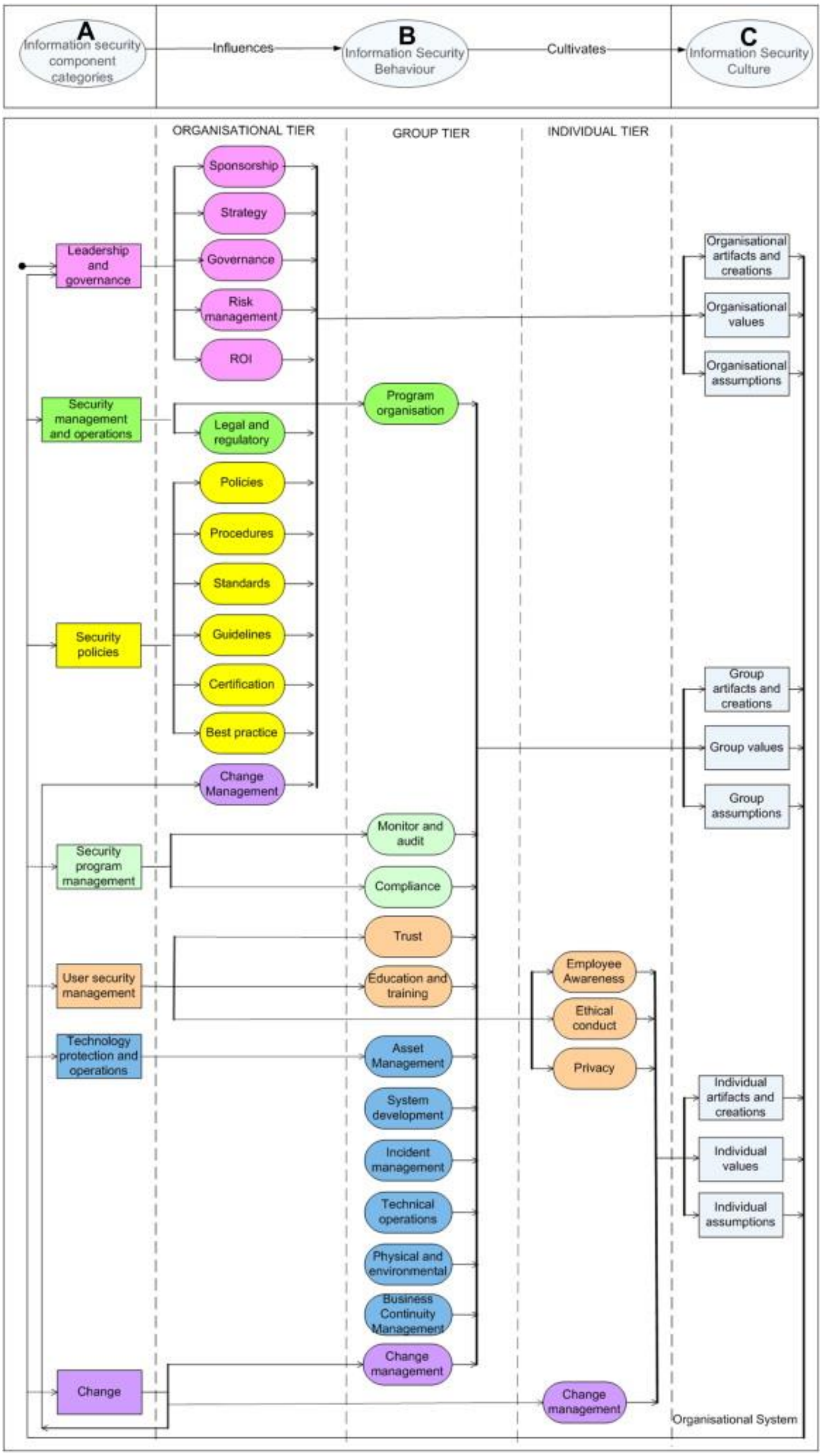


Figure 2.9 Da Veiga's (2010) Information Security Culture Framework.

2.3.4.2 Security Culture Framework by Georgiadou et al.

Recently, Georgiadou et al. (2020) introduced the security culture framework. In contrast to the dimension breakdown of the models introduced for CSC, their research indicated that a leveling should be introduced, as depicted in Figure 2.10. A brief study of the model follows.

Organizational Level

- **Assets**: everything tangible or intangible owned by the organization and its level of security attributed based on CIA controls.
- **Continuity**: ensuring the organization's continuous operations while defining levels of importance in terms of urgency (ie MTTR).
- **Access and Trust**: authorized handling of resources by organization members as defined by relevant policies.
- **Operations**: business defined procedures to ensure the organization's competence while adequately maintaining security.
- **Defense**: technical controls envisaging and deploying to ensure information security in practice.
- **Security Governance**: organization's administrative approach on how to manage information security.

Individual Level

- **Attitude**: how members feel or what they believe regarding security.
- **Awareness**: the level of realization of security related subjects.
- **Behavior**: how members react, and steps taken with regards to security.
- **Competency**: the level of education and relevant abilities that help ensure security.

Georgiadou et al. (2020) model also include a breakdown of each element into specific disciplines where indicators are being introduced to provide an accurate quantifiable assessment.

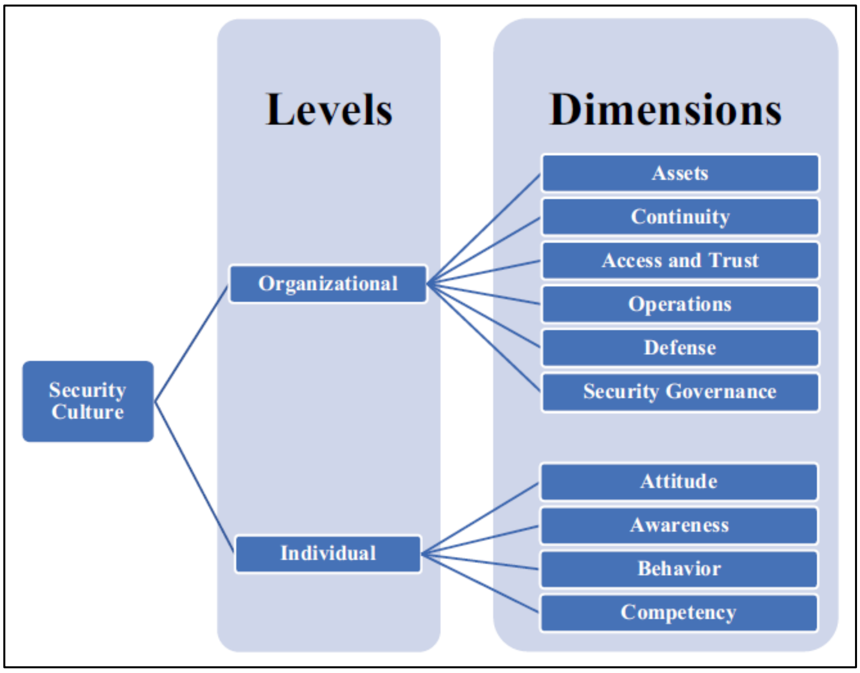


Figure 2.10 Security Culture Framework by Georgiadou et al. (2020).

2.3.4.3 Organizational Cybersecurity Culture Model

Huang and Pearlson (2019) of MIT's Sloan School of Management introduced the Organization Cybersecurity Culture Model, which covers a set of elements but explores further the managerial aspect of CSC. The framework is depicted in Figure 2.11, and an elaboration of their study follows.

- **External Influences**: This element describes factors that influence CSC but originate from outside the organization; this could be a legislative or regulatory framework such as GDPR.
- **Organization Mechanisms**: As depicted in Figure 2.11 below, management is expected to influence beliefs, values & attitudes directly. Thus, this element describes what aspects management can take advantage of towards this influence process.
- **Beliefs, Values & Attitudes**: This is where the tacit principles are being documented, what members of the organization know and do, but few of them can enunciate.
- **Behaviors**: This element responds to members' conduct that helps in prohibiting security incidents and ultimately protecting the organization effectively.

As Huang and Pearlson (2019) discuss in this study, this model is addressed primarily to perform relevant surveys and elicit conclusions that will help leadership-level members to understand where they stand with their CSC and take strategic decisions.

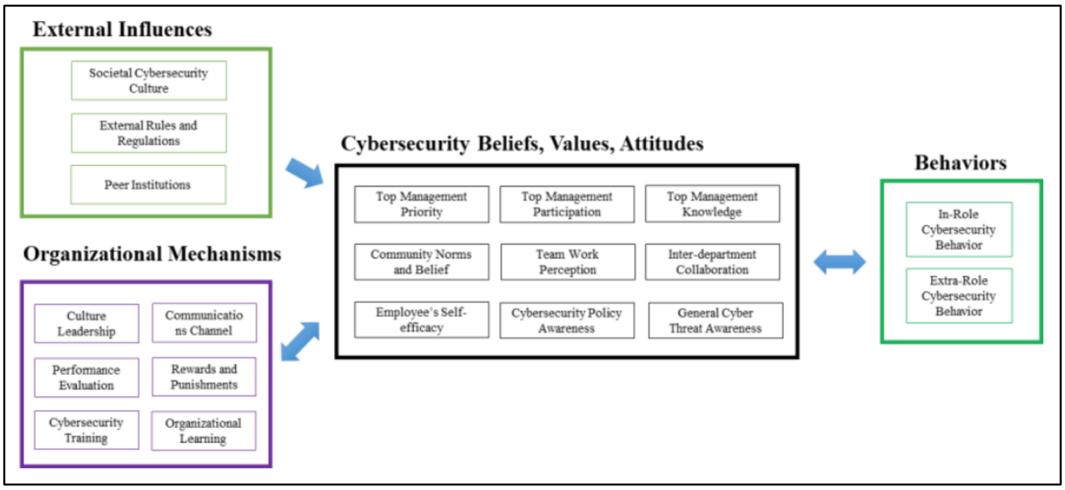

External Influences
Societal Cybersecurity Culture
External Rules and Regulations
Peer Institutions
Organizational Mechanisms
Culture Leadership
Communicatio ns Channel
Performance Evaluation
Rewards and Punishments
Cybersecurity Training
Organizational Learning
Cybersecurity Beliefs, Values, Attitudes
Top Management Priority
Top Management Participation
Top Management Knowledge
Community Norms and Belief
Team Work Perception
Inter-department Collaboration
Employee's Self-efficacy
Cybersecurity Policy Awareness
General Cyber Threat Awareness
Behaviors
In-Role Cybersecurity Behavior
Extra-Role Cybersecurity Behavior

Figure 2.11 The Organizational Cybersecurity Culture Model by Huang and Pearlson (2019).

2.3.4.4 CLTRe Security Culture Framework

As mentioned in 2.3.2, Roer and his team have developed the Security Culture Framework known as CLTRe (Laycock et al., 2019). While Roer introduced this framework as open-source and provided it publicly for free, it has been sold (and become commercial) to KnowBe4, the company partly owned by Kevin Mitnick, the first hacker in history. This framework is composed of seven elements as follows (Laycock et al., 2019).

- **Attitudes**: Referring in general to things members like or dislike, feel happy or not and whether they have favoritism to do something.
- **Behaviors**: This element describes acts and practices performed by members that influence the organization's security.
- **Cognition**: Member's perception, comprehension, and intelligence with regards to security concerns and tasks.
- **Communication**: Measuring the quality of communication channels to foster security, examine and review events and incidents.
- **Compliance**: This element includes all written regulatory frameworks and examines the degree to which members practice them.
- **Norms**: Referring to the compliance and insight demonstrated by members with tacit codes of conduct.

- **Responsibilities**: Measuring the extent to which members comprehend their part as a significant aspect when it comes to protecting the organization.

Laycock et al. (2019) support that when it comes to measuring the organization's security, the foundation is to comprehend the metrics, then justified and analyzed measurement will be provided.

2.3.4.5 CybSafe's Culture Assessment Tool

CybSafe is a London based private company that offers its tool commercially, CybSafe Culture Assessment Tool (C-CAT). C-CAT has been developed internally by a group of scientists and promotes a people-centric framework where vulnerabilities are detected (Blythe & Alashe, 2019). C-CAT is comprised of 7 elements, which are described below (Blythe & Alashe, 2019).

- **Trust**: this element describes the multifaceted confidence that needs to be present and strong amongst the people involved regarding CSC and the relevant mechanisms. This is also an aspect of motivation by having faith and trust to the members who actively practice CSC in terms of operations.
- **Just & Fair**: when a security incident occurs, the engagement of members is required, and as such, reliable documentation of what happened must take place. There is no space for blaming or trying to identify insubstantial presences; people should be encouraged and given the right environment to flourish as cyber citizens.
- **Responsibility**: fostering an individual's responsibility for CS is a significant aspect. This element supports that people should recognize CS as an individual and shared responsibility as well with the remark to own it, rather than quickly shifting it to someone else.
- **Resources & Communication**: this element includes the training material and all the commodities required for the organization's members to build strong awareness. It is important to mention that awareness should be suited according to one's role.
- **Productive security**: this element describes the importance of security policies in place at an organization and why it should be focused on people's operation and

relevant productivity rather than forcing members to skip policy controls just to do their job.

- **Ease & Choice**: people are more likely to repeat an assignment when they feel comfortable completing it easily. In CSC, this is substantial for related tasks such as reporting breaches and changing passwords.
- **Community**: this is where social norms can be described and when it comes to security. Leading by example from SMT and group behaviors is involved and should be elaborated so that all divergences are eradicated considering the shared goal, a highly effective CSC.

CybSafe supports that the ABC element can effectively contribute to cyber resilience where ABC stands for Awareness, Behaviour, and Culture. Although an underrated perspective of CS, culture should not be neglected but upraised and highly considered to invest in.

2.3.4.6 Kaspersky Lab's CyberSafety Culture Assessment

Kaspersky Lab (2018), one of the oldest and most renowned cybersecurity companies globally, has developed the CyberSafety Culture Assessment tool. Although focusing on four main prospects, the tool elicits information from further aspects as described below, providing a holistic overview of the CSC (*Cybersafety Culture Assessment*, 2018).

- **CyberSafety Mindset**
  - **Collaboration with IT**: Approachability from members of groups within an organization to IT when help is required.
  - **Policies Acceptance**: Members trust any regulatory frameworks in place and do not think of them as confining.
  - **Skills**: Members' competencies required to address and pinpoint CS threats must be contemporary.
- **Risk Management**
  - **Management Support**: Management members of any level are expected to support CSC within the organization.
  - **Lessons Learnt**: Knowledge is power, and hence, every time an incident occurs, new guidelines are distributed based on relevant event analysis.

- **Reporting Culture**: It is significant for CS to report events in a structured manner and instantaneously.

- **Business Impact**
  - **Implementation**: When regulatory frameworks are being deployed, a detailed justification takes place for every member to be aware.
  - **Trade-off**: When operations and security collude on daily operations, a concession should rise, considering satisfying corporate and safety goals.
  - **Security Recognition**: SMT appreciates CS and dignifies it as a significant element of an organization's operation.
- **Commitment to Security**
  - **Involvement**: Members of the organization are not indifferent when it comes to CS; contrariwise, they are actively engaged in activities or to learn.
  - **Personal Responsibility**: Members are expected to shoulder their accountability regarding CS and not think of IT as the sole undertaker of this domain.
  - **Impact – my actions matter**: members understand that every action might have a direct effect in terms of CS withing the whole organization.

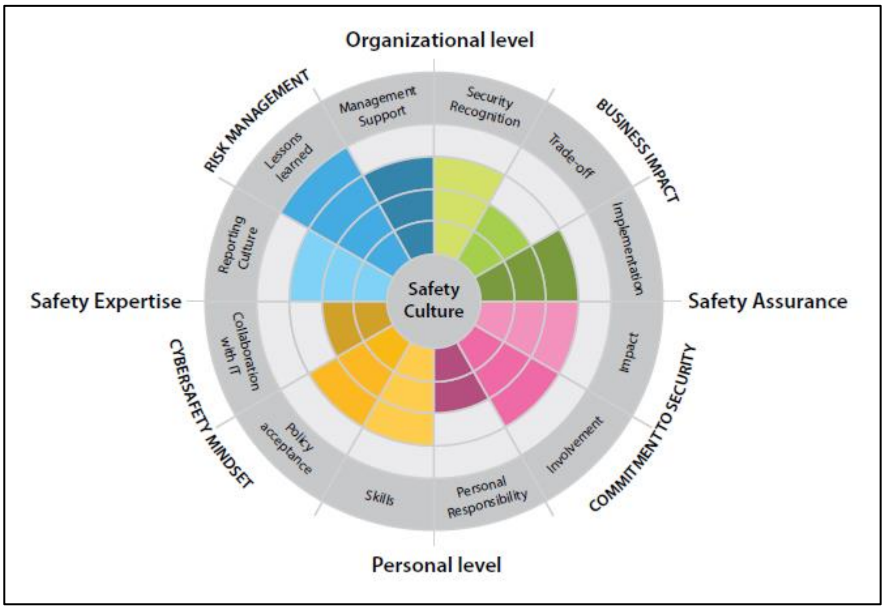


Figure 2.12 Kaspersky Lab's CyberSafety Culture Assessment tool representation (*Cybersafety Culture Assessment*, 2018).

Kaspersky Lab's tool apart from providing a CSC assessment also contributes to identifying strengths and weaknesses in a corporate plane by reaching out to Organization, Safety Expertise and Assurance and Personal level.

2.3.5 Considerations on CSC frameworks

Following the elaboration of cultivating CSC in 2.3.3 and the relevant exploration of CSC frameworks in 2.3.4, one can safely conclude that there is no incantation to approach CSC. However, by putting in place the principles of cultivating CSC and scrutinizing the available frameworks, one can either perform a first approach by uncovering some elemental weaknesses and then gradually add elements where assessments will lead to further and advanced rectifying actions. Commercial frameworks provide a rather holistic overview of CSC aspects that are ready to deploy, while academic approaches seem to be more flexible by focusing on assessing specific domains chosen. Be that as it may, as with every other activity, the CSC program should be developed in such way, to follow the organization's strategy and further enhance its competencies.

3. Research Methodology

Having compiled a theoretical establishment regarding CSC, it is imperative to explore its practical facet. By describing a framework alone does not provide a thorough insight into its impact and application. This chapter aims to elaborate the method followed to roll out a research study pursuant by describing the respective analysis of collected data.

3.1 Research Objective

The goal of this study is to explore CSC and its cyber resilience. Although it is implied that a strong CSC can serve as the driving force of furnishing organizations throughout the course of theoretical elaboration, its pragmatic and measurable impact with specific deliverables has not been described exceedingly. Furthermore, throughout the literature review, there were other challenges uncovered. Karyda (2017) has provided some perceptible aspects, some of which include organization's characteristics such as OC type, organization's size, type, and more. Consequently, cyber resilience might result from a well-designed CSC presence; however, the CSC is a prospect that might be induced from other factors. Having in mind the above, the following questions have been developed and need to be justified:

1. Is there a statistically significant relationship between the size of the organization with CSC status?
2. Is there a statistically significant relationship between the presence or not of a Chief Information Security Officer, with CSC status?
3. Is there a statistically significant relationship between the OC, with CSC status?
4. Is there a statistically significant relationship between the status of the security as perceived by organization members with CSC status?
5. Is there a statistically significant relationship between the organization industry/activity with CSC status?

If explored together, the above aspects will provide an overview of the survey, hence shed light on CSC, resilience perception, and other organizational factors.

3.2 Research Design

Blanche et al. (2006) define five distinctive steps which comprise a strategic framework to traverse research questions and the outcome of the study. These five steps are described as research question definition, design, data collection, analysis, and results elaboration

(Blanche et al., 2006). Having in mind this framework, the first step has been defined in 3.1, while the design will be discussed below. As these are the research design's planning steps, the execution and the report will comprise later chapters of this study, Chapter 4 and Chapter 5, respectively.

Research design falls into a typology that can be defined into four discrete categories, exploratory, descriptive, explanatory, and experimental (Akhtar, 2016). Starting from bottom to top, experimental design involves constant, controlled variables that are being tested to alternative hypotheses formulation. Explanatory refers to research that has not been done before, while descriptive interprets actual developments statistically. Exploratory type refers to research used to advance understanding of an aspect, and its purpose is to investigate a problem more rigorously. Hence, and by considering the research objective approach described in paragraph 3.1, **Exploratory** is the research type that fits best for this study.

While considering collecting data as part of the research framework, it is significant to choose between the available methods, quantitative, qualitative, and mixed methods (McCusker & Gunaydin, 2015). The quantitative method refers directly to interpreting figures and statistics. While this method could provide justification to loose statements, it shortfalls when it comes to extensive requirements. On the other hand, the qualitative method is more specific and is based upon phrases, expressions, perceptions, and attitudes. Loose statements do not fit in this method, and analysis is time-consuming. In mixed methods, the question in place requires both approaches to be answered. This study will incorporate the **quantitative method** to answer the involved research questions.

To explore the questions established for this study, primary data are required to be collected; hence, a questionnaire needs to be formed.

3.2.1 Questionnaire

The questionnaire is a conversation instrument between the researcher and the responder. The researcher sets a series of questions, to which he seeks answers, and responders through the questionnaire deliver their answers back to the researcher. A questionnaire aims to collect the information a researcher needs to support him respond to the research objectives (Brace, 2004). To succeed in that, one must keep in mind that collecting data is not enough. A questionnaire should be elaborated in a precise manner, to make the most out of the data collected and consequently respond to the research objective efficiently (Brace, 2004).

For this research, the questionnaire developed has been published in English. Throughout the course of the questionnaire, short explanatory texts have been provided to make sure that requirements are described thoroughly. The questionnaire consists of six distinct parts that are analyzed below.

- **Demographics**, where information about the participant could be acquired, including gender, age group, education, and residence.
- **Organization information,** where information about the organization could be acquired including seniority, industry, size, and national and international operation.
- **OC type**. Paragraph 2.2.2 provided a variety of assessment tools for OC to gain an understanding of the culture and the underlying elements present. Commercial tools do not come for free; however, Cameron and Quinn's OCAI framework provides its assessment design and life cycle for free online. Hence, this research method will be used in this survey to assess the OC. This method assesses six different categories through four questions A, B, C and D where 100 points are being appointed. Whichever of the four questions A, B, C or D of all six categories collects the most points, is interpreted to the relevant OC type.
- **General Security Questions,** where some fundamental security information can be acquired, including induction training, the presence of CISO/CSO, SOC presence and operation, information identification, and information security update channels. Answers here included yes/no and multiple-choice options.
- **CSC status**. As with OC, tools for CSC have been elaborated under paragraph 2.3.4, both academic and commercial. However, no commercial tool is available for free, but some academic questionnaires are available as part of the relevant theoretic groundwork. Having developed Schein's culture model as described in 2.3.5, a set of questions for each category, Superstructural, Artifacts, Espoused Values, Shared Tacit Assumptions and Knowledge have been collected from various questionnaires belonging to already reviewed contributors at literature review. These belong to Da Veiga (2008), Da Veiga et al. (2020), Huang & Pearlson (2019), and Alshaikh (2020). This part of the questionnaire was

developed using the 5-point Likert scale (1: Strongly Disagree, 2: Disagree, 3: Neutral, 4: Agree, and 5: Strongly Agree).

- **Perception on cyber resilience**. Other than Da Veiga et al. (2020), no other academic source provided a tool to assess resilience perception. Hence, a question from Da Veiga et al. (2020) was used along with two others developed by the author to identify the perception of the organization's members regarding their relevant environment's security resilience. The same 5-point Likert scale was used as with the CSC status assessment.

3.2.2 Preparatory questionnaire assessment

To make sure that the questionnaire flow is adequate, it was sent to three close people for preparatory assessment before setting it available in public. Within this context, feedback was received for typos and specific areas that raised questions and uncertainty which were afterwards rectified by adding further explanatory comments. Also, feedback was received on the average time for completion, and hence fifteen minutes are mentioned before the questionnaire begins for every responder to be aware of.

3.2.3 Sample

This study's objectives include a wide variety of potential responders with various backgrounds, current job status, and organization characteristics that are of significant research value. Be that as it may, there were three prerequisites for a potential responder to proceed further:

- Work/be a member of an organization of at least 20 people in size because there would be a better understanding and establishment of both OC characteristics and security administrative controls to explore.
- Work with a PC/laptop because questions in both CSC and general security matters imply that the responder should be working with a PC/laptop for its daily duties.
- Work in Greece, although the organization might be international because national superstructural factors of CSC would severely interfere with the research outcome.

Snowball technique has been incorporated for this questionnaire to reach potential responders starting from the author's social networks, friends, acquaintances, and close and corporate environment people. Snowball's potential to reveal facets of social experience, as well as its fast and cost-effective potential, has made this method most favored for this research's objectives and remainder methodology, as described through this chapter ("Non-Probability Sampling," 2018).

3.3 Software

To support the research objectives of this study, several applications have been used. Google Forms has been used to develop the questionnaire and distribute it to potential participants. Microsoft Excel supported the realization of demographics analysis through relevant graphics and table development. Finally, statistical analysis would not have been completed without the support of IBM SPSS Statistics for the Hypotheses tests and the factor analysis, while CFA has been materialized using IBM SPSS Amos.

4. Results

The survey has been accepting answers for eleven days, and a total of 162 participants have contributed to the questionnaire. After a review and inspection for relevant inconsistencies, 156 answers are valid and hence, were taken into consideration for the results.

4.1 Descriptive statistics

As discussed in part 3.2.1, the questionnaire has been divided into six specific domains. Four of them comprise the material for descriptive statistics that will be described below.

4.1.1 Demographics

Demographics comprise a substantial statistical part, as this is the area that participant factors such as gender and age are being explored. Broader characteristics of the contributing participants will be discussed below.

The participants who contributed to the questionnaire seem to be diverse as almost 60% comprise males and 40% females.

	Frequency	Percent
Female	64	41,03
Male	92	58,97
Total	156	100,00

Table 4.1. Participant's gender.

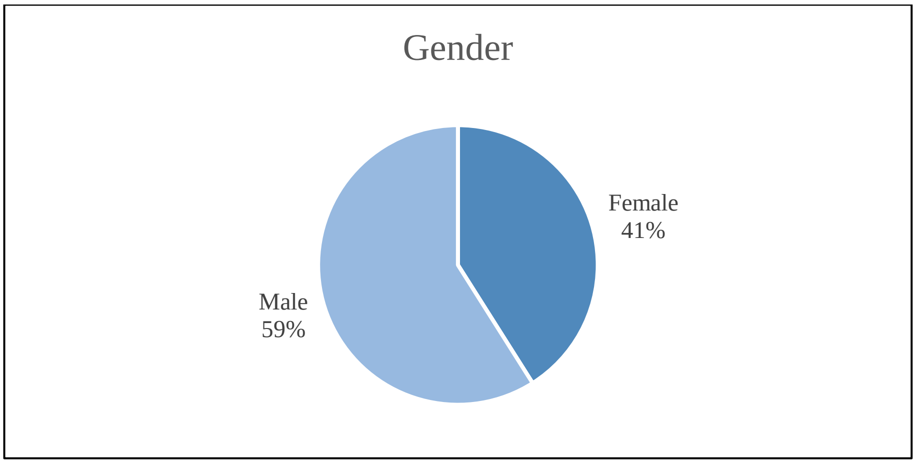


Figure 4.1. Participant's gender.

Regarding the age, the greater part with a 45% lies between 35-44 whereas almost 50% split in half is being sliced between 25-34 and 45-54. A smaller, almost 4,5% comprises 18-24 and over 55 age groups.

	Frequency	Percent
18-24	4	2,56
25-34	45	28,85
35-44	68	43,59
45-54	36	23,08
>55	3	1,92
Total	156	100,00

Table 4.2. Participant's age.

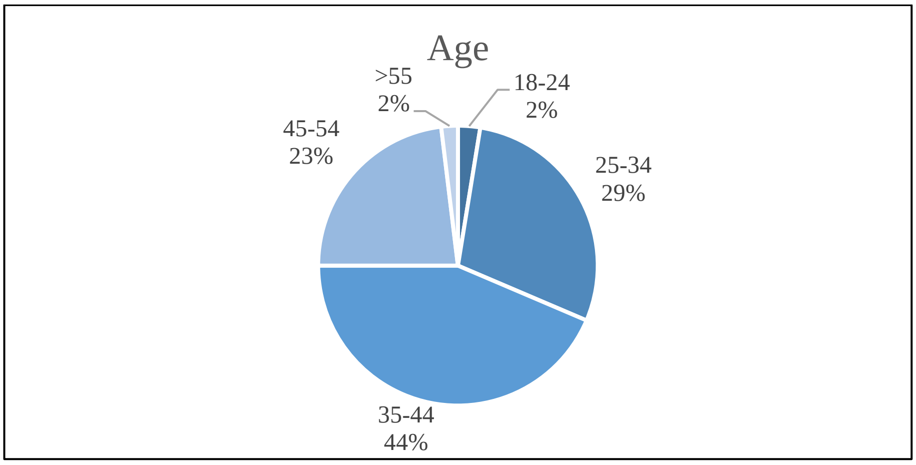


Figure 4.2. Participant's age.

Almost 95% of the participants hold a higher education degree of either Bachelor's, Master's or a Doctorate diploma. Out of the total, almost 60% hold a Master's degree.

	Frequency	Percent
High School diploma	7	4,49
Bachelor's degree (e.g. BA, BSc)	46	29,49
Master's degree (e.g. MA, MSc, MEd)	91	58,33
Doctorate (e.g. PhD, EdD)	12	7,69
Total	156	100,00

Table 4.3. Participant's education.

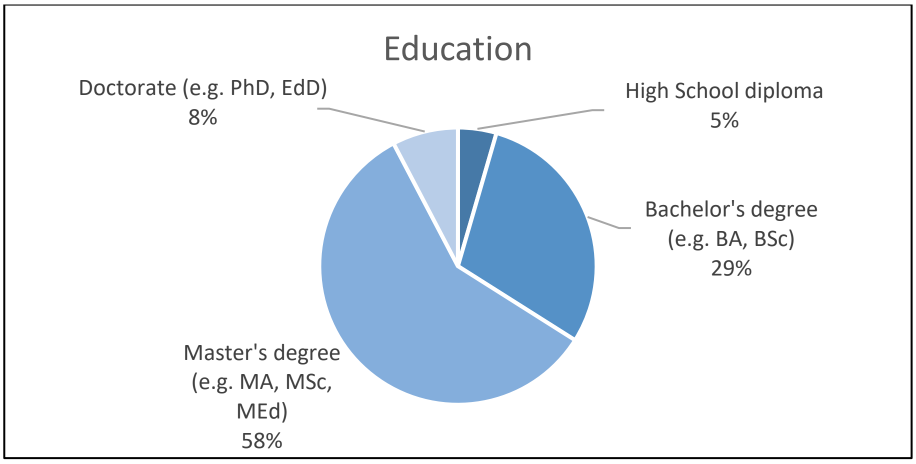


Figure 4.3. Participant's education.

Participants have been dispersed from all over Greece's regions; however, only Western Macedonia did not provide any. Attica has been the origin of almost 60% of the participant's total.

	Frequency	Total
Eastern Macedonia & Thrace	5	3,21
Central Macedonia	17	10,90
Western Macedonia	0	0,00
Epirus	2	1,28
Thessaly	15	9,62
Ionian Islands	4	2,56
Western Greece	4	2,56
Central Greece	4	2,56
Attica	90	57,69
Peloponnese	3	1,92
Northern Aegean	6	3,85
Southern Aegean	2	1,28
Crete	4	2,56
Total	156	100,00

Table 4.4. Participant's region.

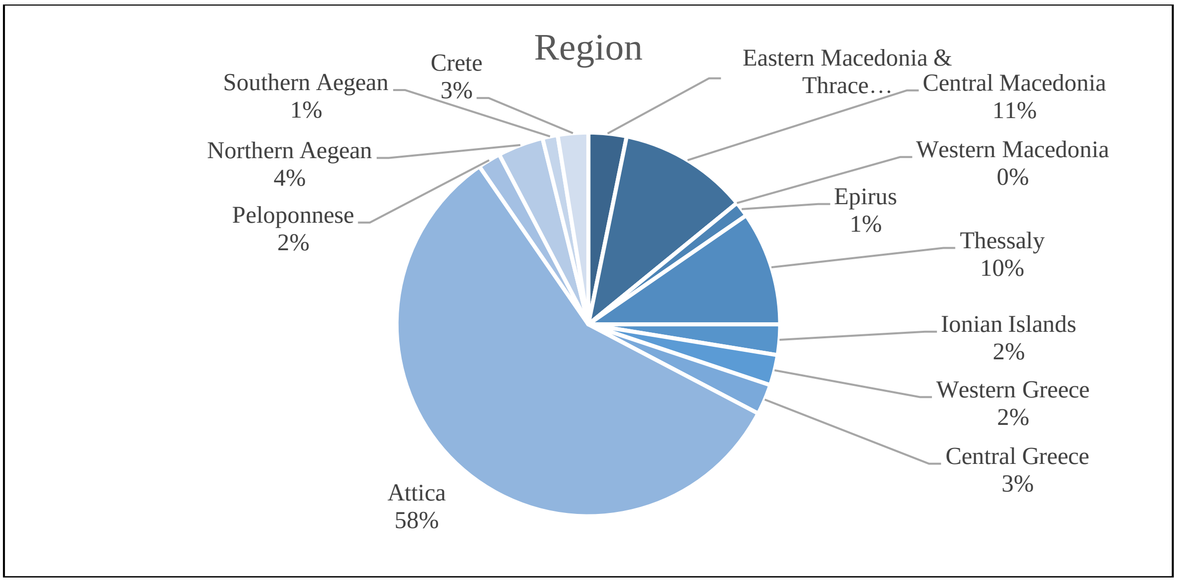


Figure 4.4. Participant's region.

4.1.2 Organization related questions

Participants' seniority is dispersed through all levels; however, Mid-Senior and Senior levels comprise almost 50% of the respondents constituting approximately 20% and 29%, respectively.

	Frequency	Percent
Intern	2	1,28
Junior	19	12,18
Mid-Senior	32	20,51
Senior	45	28,85
Supervisor	14	8,97
Manager	31	19,87
Director	9	5,77
Executive	4	2,56
Total	156	100,00

Table 4.5. Participant's seniority.

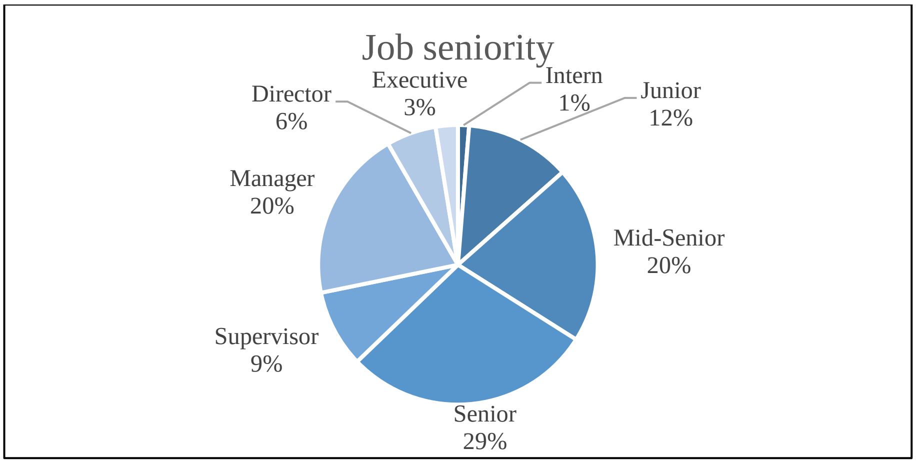


Figure 4.5. Participant's seniority.

Answers regarding participants' industry have been diverse; however, none has been received for Life Sciences. The larger amount is attracted to Data Infrastructure, Telecom with approximately 18,5% of the total and Public Sector with 16,5% of total answers.

	Frequency	Percent
Agriculture, Forestry, Mining	2	1,28
Industrial (Manufacturing, Constructions, etc.)	13	8,33
Energy, Utilities	5	3,21
Transport, Logistics	6	3,85
Media, Creative Industries	5	3,21
Data Infrastructure, Telecom	29	18,59
Healthcare	7	4,49
Education	12	7,69
Retail/E-commerce	11	7,05
Hospitality, Food, Leisure Travel	9	5,77
Financial Services	13	8,33
Professional Services (Law, Consulting, etc.)	11	7,05
Public Sector	26	16,67
Non-Government Organization (NGO)	7	4,49
	156	100,00

Figure 4.6. Participant's industry.

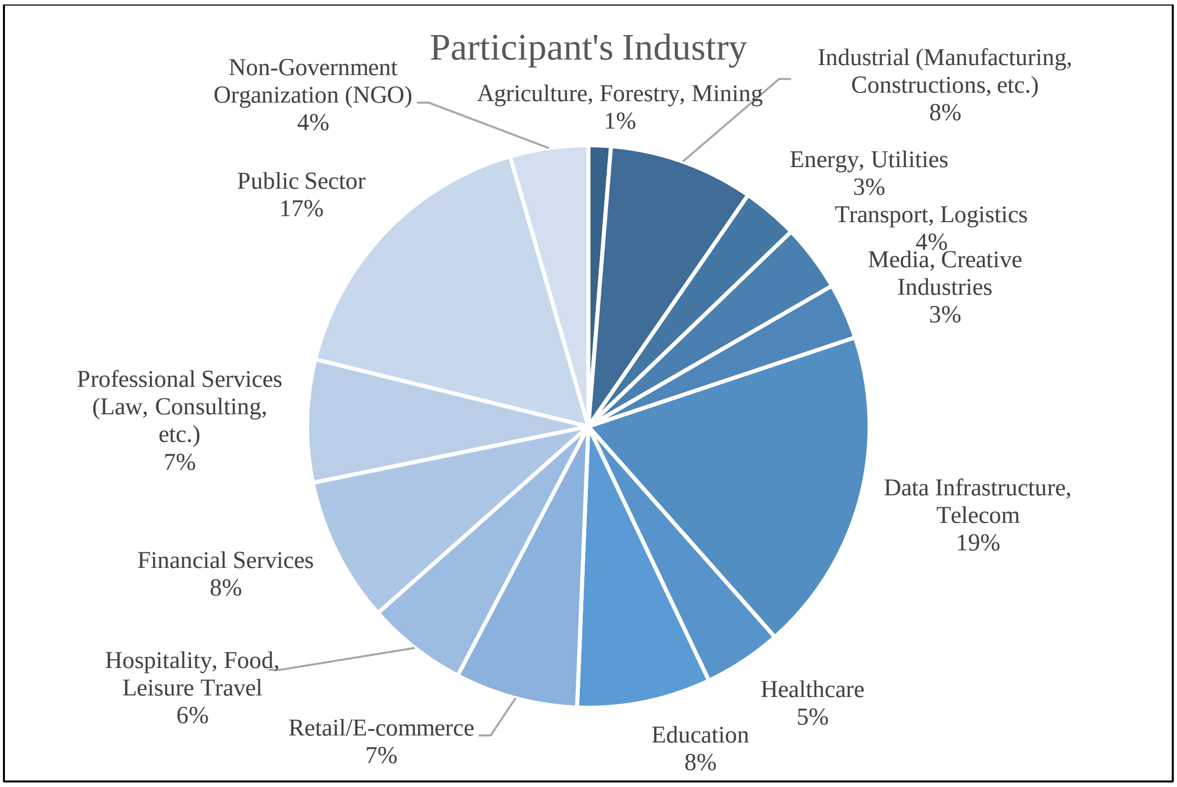


Figure 4.6. Participant's industry.

Organization size also demonstrates a diverse outcome as all sizes are present and dispersed through all levels.

	Frequency	Percent
20-49	35	22,44
50-249	31	19,87
250-1.499	43	27,56
1.500-9.999	35	22,44
>10.000	12	7,69
Total	156	100,00

Table 4.7. Organization size.

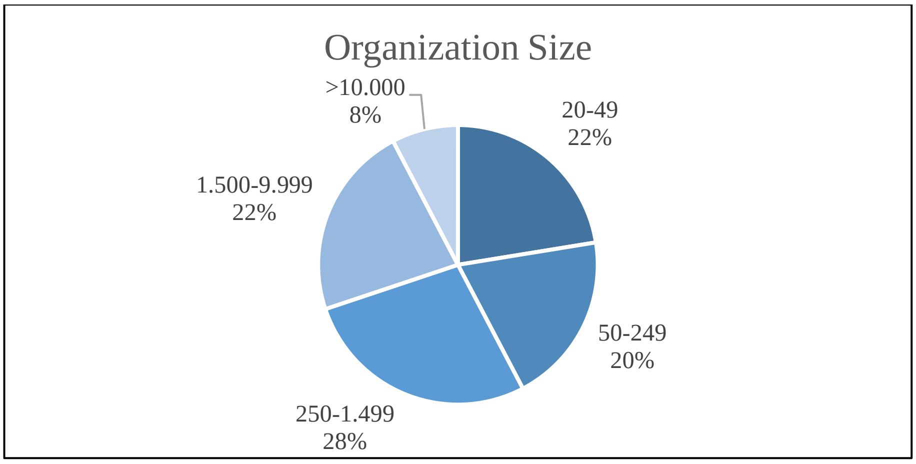


Figure 4.7. Organization size.

Out of all participants, 45% work in an organization that operates in Greece exclusively, while the rest, 55%, work for an international organization operating in Greece.

	Frequency	Percent
Only in Greece	71	45,51
In Greece & Abroad	85	54,49
Total	156	100,00

Table 4.8. Organization operation.

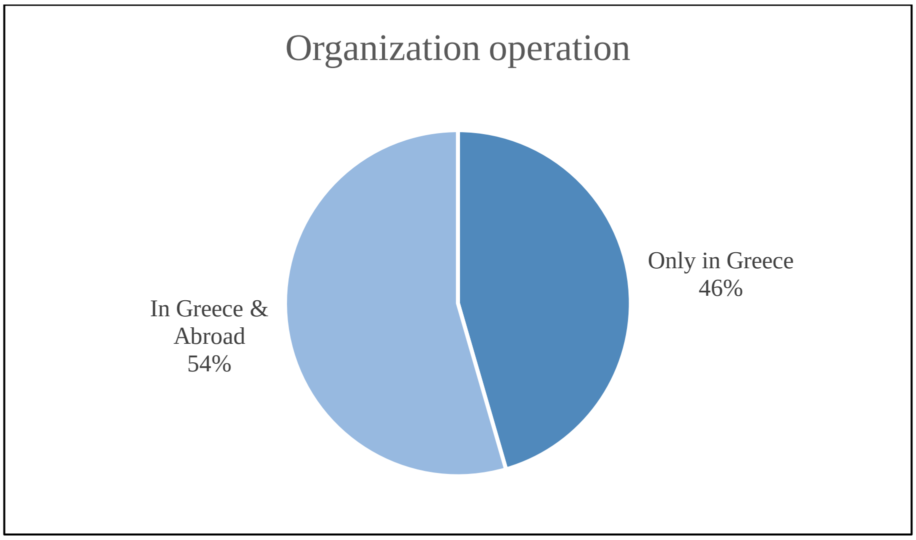


Figure 4.8. Organization operation.

4.1.3 Organizational Culture tool

The OCAI tool for assessing the OC, is based upon the A, B, C, and D answers given by the participants. Whichever sets of questions receive more points, this is what the dominant OC is. The average results of the dominant OC from each answer have been calculated and demonstrated in Figure 4.9.

Approximately 50% of the participants' OC has been pointed out to be Hierarchy, indicating that half of the participants' organizations represent an OC of control, processes, efficiency, and punctuality. The other half is split between Clan (Collaborative) with approximately 24%, Market (Compete) with approximately 18,5%, and finally, Adhocracy (Create) with the smallest percentage of approximately 5%.

	Frequency	Percent
Clan	37,00	23,72
Adhocracy	8,00	5,13
Market	29,00	18,59
Hierarchy	82,00	52,56
Total	156,00	100,00

Table 4.9. Average OC.

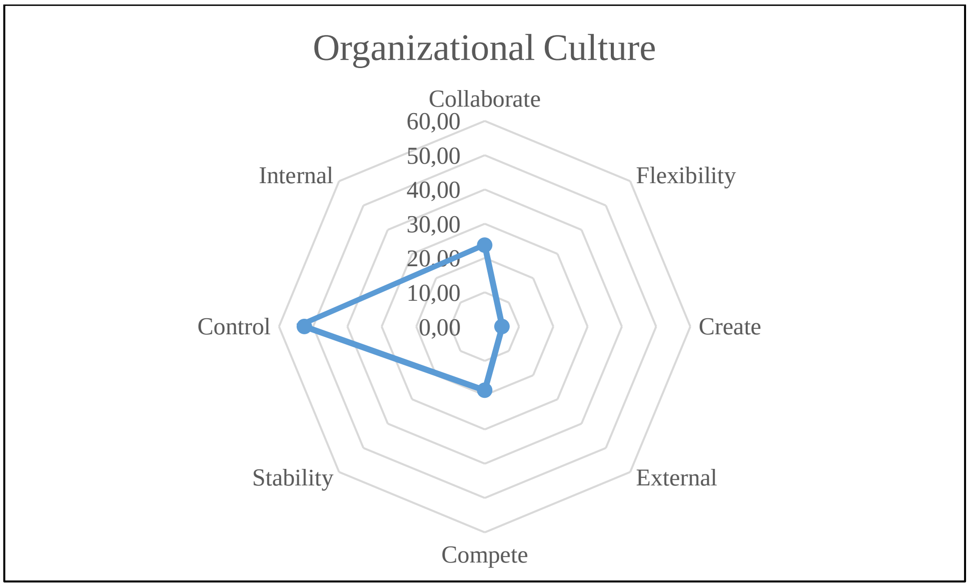


Figure 4.9. Average OC.

4.1.3 General security questions

Induction training is considered an industry standard to raise awareness for security and other aspects of the organization for new joiners. Approximately 55% of the participants answered that their organization offers induction training, while 45% do not.

	Frequency	Percent
Yes	86	55,13
No	70	44,87
Total	156	100,00

Table 4.10. The organization provides induction training.

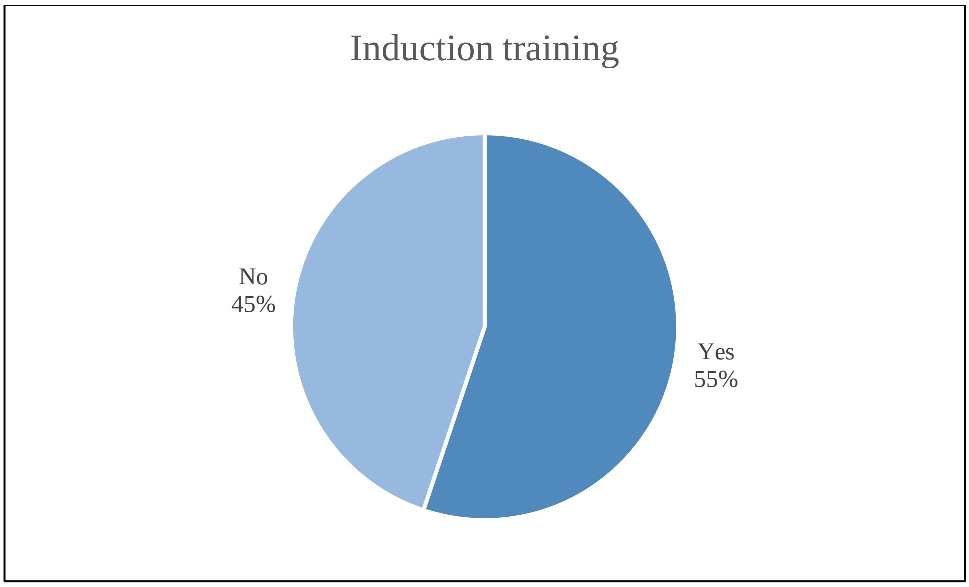


Figure 4.10. The organization provides induction training.

Even though data protection regulations require skilled professionals, it is significant to employ an executive tasked to overview its cyber security landscape. Approximately 56% replied that they have a CISO/CSO in their organization, while the rest 44% that do not have this sort of executive.

	Frequency	Percent
Yes	88	56,41
No	68	43,59
Total	156	100,00

Table 4.11. The organization has CISO/CSO.

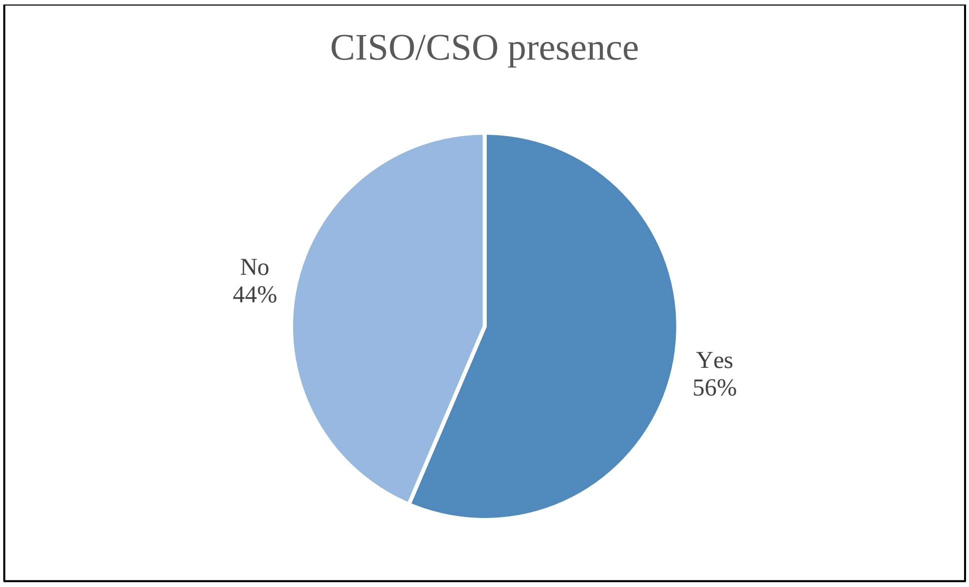


Figure 4.11. The organization has CISO/CSO.

As MSSP grow in the market, so is the need to deploy constant monitoring and IR systems. Participants provided an overwhelmingly result of 58% that their organizations have SOC while the rest 42% do not.

	Frequency	Percent
Yes	90	57,69
No	66	42,31
Total	156	100,00

Table 4.12. The organization has SOC.

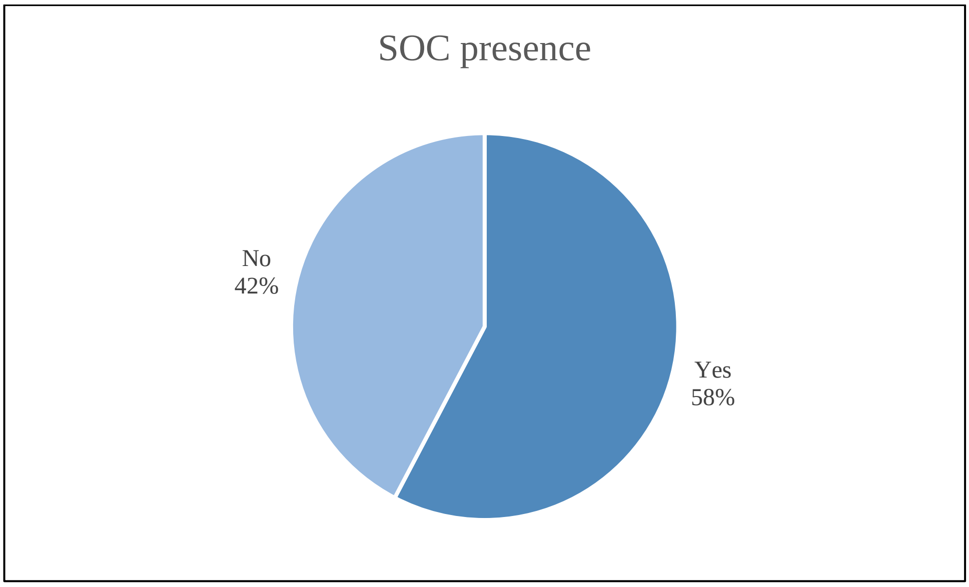


Figure 4.12. The organization has SOC.

Responders have provided insights into what they classify as information. 103 out of 156 responses have identified all given options as information. E-Electronic documents, E-mails, and Hard copy documents were the next prevailing options, with approximately 50 responders choosing them. Another interesting comparison lies between Faxes and Instant messaging where Faxes prevail. It is interesting because Fax seems to remain a ruling means of communication, while instant messaging, although used daily for business or socializing, received a low score.

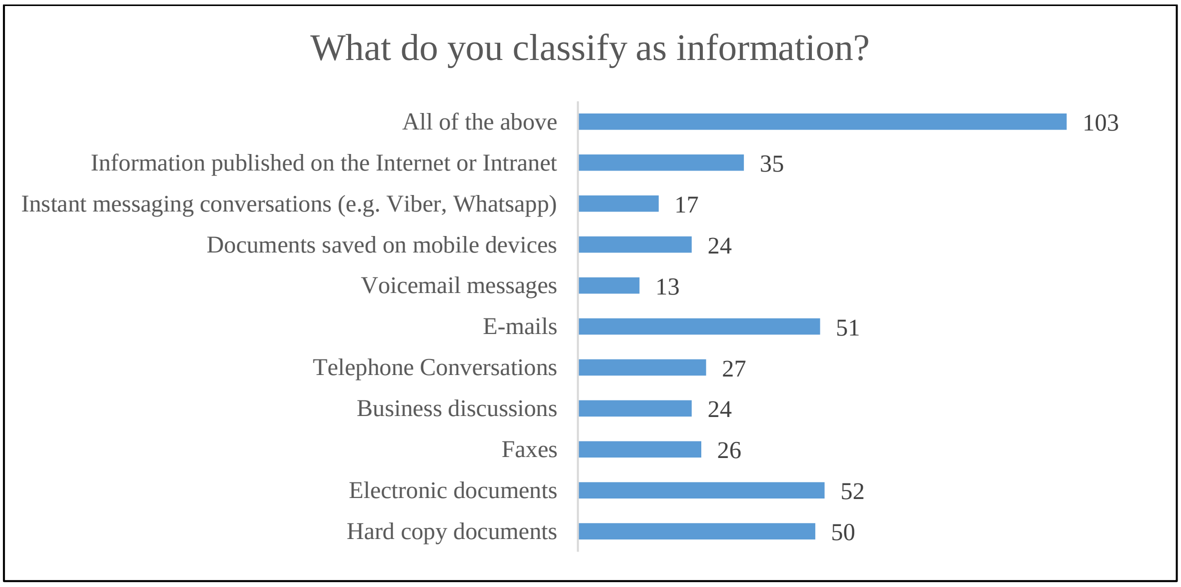


Figure 4.13. Classification of information.

Regarding how responders prefer to receive information security messages, results have provided a prevailing 108 out of 156 answers ascribed to E-mail messages. One would expect the following as runner-ups, Induction training, Web-based training, and the organization's intranet. Posters scored only 11 answers; this could be a sign of all things digital or the pandemic's outcome where work-from-home has prevailed.

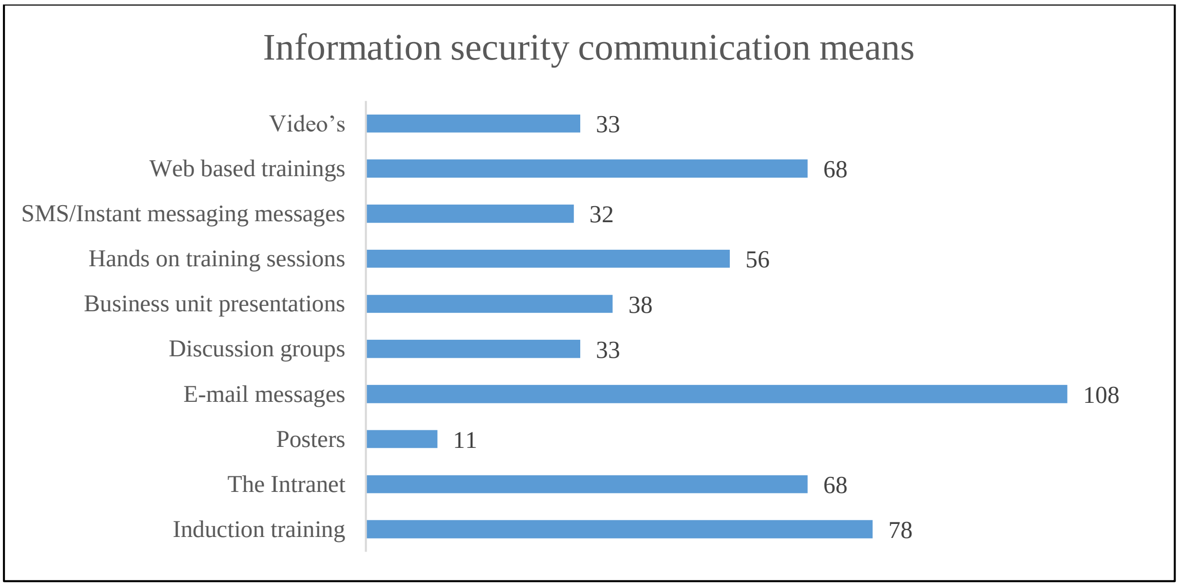


Figure 4.14. Information security communication means.

4.2 Statistical analysis

4.2.1 Reliability analysis

This questionnaire included two Likert sets of questions. The first one, comprised of fifteen questions and intended to measure the CSC, and the second, comprised three questions intended to measure the perception of CS's resilience. As both sets of questions have never been used before and were put together for this research, a reliability analysis is mandatory. Cronbach's alpha values that need to be taken into consideration are 0,7-0,79 acceptable, 0,8-0,89 good and 0,9-0,94 excellent.

Table 4.13 includes the Cronbach's alpha coefficient analysis results for the set of questions that comprise the CSC. The result is 0,858, indicating that the questionnaire in place has acceptable reliability. All items are worthy of retention since none of the variables' deletion would increase Cronbach's alpha result, as represented in Table 4.14.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0,858	0,855	15

Table 4.13. Reliability analysis for CSC.

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q1	53,9487	63,030	0,394	0,328	0,854
Q2	54,1795	60,922	0,460	0,483	0,851
Q3	54,9551	57,488	0,545	0,554	0,847
Q4	54,8462	58,996	0,522	0,532	0,848
Q5	54,3462	60,576	0,486	0,460	0,849
Q6	54,8205	58,032	0,580	0,607	0,844
Q7	54,7564	58,973	0,585	0,531	0,844
Q8	54,6346	59,124	0,586	0,492	0,844
Q9	54,8205	60,419	0,431	0,422	0,853
Q10	53,4359	66,106	0,263	0,589	0,858
Q11	53,4487	65,462	0,301	0,595	0,857
Q12	53,4936	64,987	0,353	0,652	0,855
Q13	54,2500	56,782	0,720	0,764	0,836
Q14	54,1603	58,277	0,687	0,757	0,839
Q15	53,6090	63,440	0,437	0,491	0,852

Table 4.14. Item total statistics for CSC.

Table 4.15 represents Cronbach’s alpha coefficient analysis for the set of questions that comprise the CS resilience perception. The result for the set of questions is 0,784, indicating that they have acceptable reliability. As with the CSC, all variables are significant, and hence any removal would not increase Cronbach’s alpha higher than the value in place now. The last statement is supported by Table 4.16.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0,784	0,786	3

Table 4.15. Reliability analysis for CS resilience perception.

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q1	7,4103	2,205	0,719	0,521	0,598
Q2	7,0192	2,625	0,586	0,395	0,746
Q3	7,8141	2,307	0,573	0,361	0,767

Table 4.16. Item total statistics for CS resilience perception.

4.2.2 Evaluation of CSC and CS Resilience

As both sets of questions have been developed for this research, the proper evaluation of the assessment should be put in place. As discussed in Chapter 2 regarding OC and CSC, there is no "bad" or "good" culture. Assessments are designed in such a way to uncover weak aspects of an organization that are important and need to be reconsidered. Be that as it may, in this research, a more straightforward approach needs to be implemented, and hence, CSC is evaluated based on three arrangements by summing all results from fifteen answers, 15-34,9 "Poor," 35-54,9 "Average" and 55-75 "Adequate." The same rationale has been used for the CS resilience perception set of questions, where the respective summing of results provided with three categories, 3-6,9 "Poor," 7-10,9 "Average" and 11-15 "Adequate."

4.2.3 Assumptions

As the Hypotheses will be elaborated with chi-square tests, the examination of relevant assumptions should be probed. First and utmost, as with any other non-parametric test, data are considered to have been collected inconstantly, rather than in a coherent and non-randomly manner. As already discussed in Paragraph 3.2.3, the sample had a set of prerequisites; however, it was not addressed or sent to a specific set of potential responders but was publicly shared throughout various communication channels; hence randomness can be supported. Further assumptions (McHugh, 2013) of the Chi-square test and the appropriate asymptotic method consist of:

1. Data are expected to consist a table of frequencies and not percentages or any other calculating or statistical variation.
2. Data comprised in categories are expected to fit one another solely.

3. Data comprised in categories are expected to contribute data to one cell exclusively and one-off in a matter of time. If data represent a second or third collection, the chi-square test is violated.
4. Data groups that are being examined should not be related.
5. Variables examined can be comprised of nominal, ordinal, interval, or ratio level and data. Within this context, there is no limit in cells considered; however, when the frequencies examined surpass twenty cells, this could violate the assumption below.
6. The expected frequencies should have a value higher than five in at least 80% of the cells examined.

Although all points up to 4 are being met by all Hypotheses examined, the following should be considered. H5, provided with a table of cells relatively more extensive than the level as denoted in point 5, and thus point 6 has been violated. A preliminary chi-square test has provided results that point 6 is being violated by all tests as described in Table 4.17.

Hypothesis	Violation result
H1	6 cells (40%) have expected count less than 5
H2	2 cells (33,3%) have expected count less than 5
H3	5 cells (41,7%) have expected count less than 5
H4	5 cells (55,6%) have expected count less than 5
H5	32 cells (76,2%) have expected count less than 5

Table 4.17. Preliminary chi-square tests violations.

These results, however, should not comprise a barrier to this research. The Exact and Monte Carlo methods accommodate solid results when point 6 of the asymptotic assumptions fail to be met (*Exact Tests*, n.d.), and hence, this practice will be followed on the following Chi-square tests.

4.2.4 Chi-square tests analysis

4.2.4.1 Hypothesis 1

The first Hypothesis examines the possible existence of a relationship between the CSC and the Organization's size. Large organizations tend to have broader structures and processes, including them. Respectively, the CS posture is more expansive, and one would expect that an appropriate CSC environment should be commonly adequate.

H1: There a statistically significant relationship between the size of the organization with the CSC status.

The relevant Chi-square test was performed, and the following results from tables 4.18 and 4.19 have been provided. Considering the Fisher-Freeman-Halton Exact Test result with a P-Value of 0,341 for a 2-sided test, the final P-Value to contemplate is 0,17. Since P-Value is larger than α (0,05), we fail to accept the Hypothesis, and hence, **there is no statistically significant relationship between the organization's size with the CSC status**. This means that regardless of the organization's size, CSC remains a challenge for all sorts of organizations.

			CSC			Total
			Poor	Moderate	Adequate	
Organization Size	20-49	Count	0	17	18	35
		Expected Count	0,4	11,4	23,1	35,0
	50-249	Count	0	9	22	31
		Expected Count	0,4	10,1	20,5	31,0
	250-1.499	Count	1	12	30	43
		Expected Count	0,6	14,1	28,4	43,0
	1.500-9.999	Count	1	11	23	35
		Expected Count	0,4	11,4	23,1	35,0
	>10.000	Count	0	2	10	12
		Expected Count	0,2	3,9	7,9	12,0
Total		Count	2	51	103	156
		Expected Count	2,0	51,0	103,0	156,0

Table 4.18. Observed and Expected frequencies for H1.

	Value	df	Asymptotic Significance (2-sided)	Monte Carlo Sig. (2-sided)		
				Significance	95% Confidence Interval	
					Lower Bound	Upper Bound
Pearson Chi-Square	8,010	8	0,432	0,454	0,444	0,464
Likelihood Ratio	8,684	8	0,370	0,362	0,353	0,372
Fisher-Freeman-Halton Exact Test	8,066			0,341	0,332	0,351
Linear-by-Linear Association	2,020	1	0,155	0,159	0,152	0,166
N of Valid Cases	156					

Table 4.19. Chi-square Exact test for H1.

4.2.4.2 Hypothesis 2

The second Hypothesis examines whether a relationship exists between the presence of a CISO within the organization and the relevant CSC status in place. CISO is usually a C-level executive responsible for the technical aspects of security and the holistic governance that reflects CS (Fruhlinger, 2019). One would imply that a CISO presence could support that IS would be much better organized and hence CSC would have better status.

H2. There is a statistically significant relationship between the presence of a CISO with the CSC status.

The Chi-square test performed provided with results depicted in tables 4.20 and 4.21. Again, considering the Fisher-Freeman-Halton Exact Test result with a P-Value of 0,0 would imply a much lower value from the α (0,05). Therefore, we accept the Hypothesis and hence, **there is a statistically significant relationship between the presence of a CISO with the CSC status**. This means that organizations with CISOs, have better CSC status.

			CSC			Total
			Poor	Moderate	Adequate	
CISO Presence	No	Count	1	37	30	68
		Expected Count	0,9	22,2	44,9	68,0
	Yes	Count	1	14	73	88
		Expected Count	1,1	28,8	58,1	88,0
Total		Count	2	51	103	156
		Expected Count	2,0	51,0	103,0	156,0

Table 4.20. Observed and Expected frequencies for H2.

	Value	**df**	**Asymptotic Significance (2-sided)**	**Monte Carlo Sig. (2-sided)**		
				Significance	95% Confidence Interval	
					Lower Bound	Upper Bound
Pearson Chi-Square	26,190	2	0,000	0,000	0,000	0,000
Likelihood Ratio	26,698	2	0,000	0,000	0,000	0,000
Fisher-Freeman-Halton Exact Test	26,587			0,000	0,000	0,000
Linear-by-Linear Association	23,032	1	0,000	0,000	0,000	0,000
N of Valid Cases	156					

Table 4.21. Chi-square Exact test for H2.

4.2.4.3 Hypothesis 3

The third Hypothesis relies on the groundwork that has been done throughout Chapter 2 and essentially examines whether CSC is somehow dependent on specific OC types. The consideration behind this lies upon the fact that hypothetically one would expect a Hierarchy type of OC to perform better due to strictness and relevant policies in place.

H3. There is a statistically significant relationship between the OC type with the CSC status.

The relevant Chi-square test was performed, and the following results from tables 4.22 and 4.23 have been provided. Considering the Fisher-Freeman-Halton Exact Test result with a

P-Value of 0,988 for a 2-sided test, the final P-Value to contemplate is 0,494. Since P-Value is larger than the α value (0,05), we fail to accept the Hypothesis. Hence, **there is no statistically significant relationship between the OC type with the CSC status**. This means that regardless of the organization's OC type, CSC status remains an independent factor that needs to be addressed.

			CSC			Total
			Poor	Moderate	Adequate	
OC	Clan	Count	0	12	25	37
		Expected Count	0,5	12,1	24,4	37,0
	Adhocracy	Count	0	2	6	8
		Expected Count	0,1	2,6	5,3	8,0
	Market	Count	0	9	20	29
		Expected Count	0,4	9,5	19,1	29,0
	Hierarchy	Count	2	28	52	82
		Expected Count	1,1	26,8	54,1	82,0
Total		Count	2	51	103	156
		Expected Count	2,0	51,0	103,0	156,0

Table 4.22. Observed and Expected frequencies for H3.

	Value	df	Asymptotic Significance (2-sided)	Monte Carlo Sig. (2-sided)		
				Significance	95% Confidence Interval	
					Lower Bound	Upper Bound
Pearson Chi-Square	2,261	6	0,894	0,909	0,903	0,914
Likelihood Ratio	3,038	6	0,804	0,856	0,849	0,862
Fisher-Freeman-Halton Exact Test	2,179			0,988	0,985	0,990
Linear-by-Linear Association	0,592	1	0,442	0,474	0,464	0,483
N of Valid Cases	156					

Table 4.23. Chi-square Exact test for H3.

4.2.4.4 Hypothesis 4

The fourth Hypothesis examines the relationship between CS resilience, as perceived by the organization's members, and the CSC status. One would expect that members having confidence about their organization's CS status would also imply an adequate CSC status presence.

H4. There is a statistically significant relationship between the status of the CS as perceived by organization members with the CSC status.

The Chi-square test performed provided with results represented in tables 4.24 and 4.25. The Fisher-Freeman-Halton Exact Test result was represented as 0,0, which is lower than the α value (0,05). Therefore, we accept the Hypothesis, and consequently, **there is a statistically significant relationship between the status of the CS as perceived by organization members with the CSC status**. This means that the CS status as perceived by organization's members follows the CSC status.

			CSC			Total
			Poor	Moderate	Adequate	
CS Resilience Perception	Poor	Count	2	1	3	6
		Expected Count	0,1	2,0	4,0	6,0
	Moderate	Count	0	33	13	46
		Expected Count	0,6	15,0	30,4	46,0
	Adequate	Count	0	17	87	104
		Expected Count	1,3	34,0	68,7	104,0
Total		Count	2	51	103	156
		Expected Count	2,0	51,0	103,0	156,0

Table 4.24. Observed and Expected frequencies for H4.

	Value	df	Asymptotic Significance (2-sided)	Monte Carlo Sig. (2-sided)		
				Significance	95% Confidence Interval	
					Lower Bound	Upper Bound
Pearson Chi-Square	95,488	4	0,000	0,000	0,000	0,000
Likelihood Ratio	57,432	4	0,000	0,000	0,000	0,000
Fisher-Freeman-Halton Exact Test	55,994			0,000	0,000	0,000
Linear-by-Linear Association	41,088	1	0,000	0,000	0,000	0,000
N of Valid Cases	156					

Table 4.25. Chi-square Exact test for H4.

4.2.4.5 Hypothesis 5

The fifth and last Hypothesis examines whether a relationship exists between the organization's industry and the CSC. This Hypothesis rationale relies on the assumption that specific activity organizations are supposed to perform in highest standards in CS. For example, Financial services organizations process a significant sum of personal identifiable information, and hence, they should have an adequate CSC instilled.

H5. There is a statistically significant relationship between the organization industry/activity with the CSC status.

The relevant Chi-square test was performed, and the following results from tables 4.26 and 4.27 have been provided. Considering the Fisher-Freeman-Halton Exact Test result with a P-Value of 0,024 for a 2-sided test, the final P-Value to contemplate is 0,012. Since P-Value is lower than the α value (0,05), we accept the Hypothesis, and hence, **there is a statistically significant relationship between the organization industry/activity with the CSC status**. This means that organizations in specific industries perform better or lesser regarding their respective CSC status, which would be adequate or poor, respectively.

			CSC			Total
			Poor	Moderate	Adequate	
Organization Industry	Agriculture, Forestry, Mining	Count	0	1	1	2
		Expected Count	0,0	0,7	1,3	2,0
	Industrial (Manufacturing, Constructions, etc.)	Count	0	5	8	13
		Expected Count	0,2	4,3	8,6	13,0
	Energy, Utilities	Count	0	1	4	5
		Expected Count	0,1	1,6	3,3	5,0
	Transport, Logistics	Count	0	2	4	6
		Expected Count	0,1	2,0	4,0	6,0
	Media, Creative Industries	Count	0	5	0	5
		Expected Count	0,1	1,6	3,3	5,0
	Data Infrastructure, Telecom	Count	1	8	20	29
		Expected Count	0,4	9,5	19,1	29,0
	Healthcare	Count	0	3	4	7
		Expected Count	0,1	2,3	4,6	7,0
	Education	Count	1	6	5	12
		Expected Count	0,2	3,9	7,9	12,0
	Retail/E-commerce	Count	0	2	9	11
		Expected Count	0,1	3,6	7,3	11,0
	Hospitality, Food, Leisure Travel	Count	0	2	7	9
		Expected Count	0,1	2,9	5,9	9,0
	Financial Services	Count	0	2	11	13
		Expected Count	0,2	4,3	8,6	13,0
	Professional Services (Law, Consulting, etc.)	Count	0	0	11	11
		Expected Count	0,1	3,6	7,3	11,0
	Public Sector	Count	0	10	16	26
		Expected Count	0,3	8,5	17,2	26,0
	Non-Government Organization (NGO)	Count	0	4	3	7
		Expected Count	0,1	2,3	4,6	7,0
Total		Count	2	51	103	156
		Expected Count	2,0	51,0	103,0	156,0

Table 4.26. Observed and Expected frequencies for H5.

	Value	df	Asymptotic	Monte Carlo Sig. (2-sided)		
			Significance (2-sided)	Significance	95% Confidence Interval	
					Lower Bound	Upper Bound
Pearson Chi-Square	32,198	26	0,187	0,194	0,186	0,201
Likelihood Ratio	35,103	26	0,109	0,023	0,020	0,026
Fisher-Freeman-Halton Exact Test	38,932			0,024	0,021	0,027
Linear-by-Linear Association	1,417	1	0,234	0,250	0,242	0,258
N of Valid Cases	156					

Table 4.27. Chi-square Exact test for H5.

4.2.4 Factor analysis

Another statistical examination required to be taken into consideration is to explore whether the set of questions introduced for the CSC status are all equally contributing to the status outcome. This section examines this assumption by performing a Factor Analysis.

The preliminary analysis evaluates Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity. A KMO value close to 1 means that factor analysis performed will provide distinct and reliable factors (Field, 2005). A value below 0,5 is unacceptable, between 0,7 and 0,8 are considered good, 0,8 to 0,9 great and above 0,9 excellent (Field, 2005). The result as depicted in Table 4,28 is 0,807, and hence there is confidence in proper and sufficient factor analysis. Next, Bartlett’s test of sphericity proves whether a relationship exists between the variables included in the analysis. As the P-value is represented as 0,0 and α = 0,05, there is confidence that variables are related, and therefore the factor analysis is fitting properly.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,807
Bartlett's Test of Sphericity	Approx. Chi-Square	1166,734
	df	105
	Sig.	0,000

Table 4.28. KMO and Barlett's Test.

Another assumption required to be met to ensure that all factors provided are reliable is by examining the extraction values of Communalities as depicted in Table 4.29. As denoted by MacCallum et al. (1999), for this assumption to be met, all Communalities should have a value above 0,3. Values provided in Table 4.29 indicate that all items are over 0,3, and hence, factors provided should be reliable.

	Initial	Extraction
Q1	1,000	0,486
Q2	1,000	0,688
Q3	1,000	0,692
Q4	1,000	0,601
Q5	1,000	0,595
Q6	1,000	0,693
Q7	1,000	0,612
Q8	1,000	0,571
Q9	1,000	0,390
Q10	1,000	0,760
Q11	1,000	0,712
Q12	1,000	0,772
Q13	1,000	0,666
Q14	1,000	0,658
Q15	1,000	0,544

Table 4.29. Communalities

Table 4.30 provides with results of the total variance explained. As depicted in the Table, three factors can explain approximately 63% of the total variance. Factor 1 represents approximately 34% of the total variance and subsequent 2 and 3, 18% and 10,5% respectively.

Component	Initial Eigenvalues		
	Total	% of Variance	Cumulative %
1	5,130	34,201	34,201
2	2,739	18,260	52,461
3	1,572	10,483	62,944

Table 4.30. Total Variance Explained

Another verification that the present factor analysis provides three factors to consider can be derived from the relevant scree plot, as represented in Figure 4.15. As it is difficult to interpret at which factor the curve's inflection occurs, Kaiser's rule should be incorporated. Kaiser's rule indicates that factors with an Eigenvalue greater than one should be retained (Kaufman & Dunlap, 2000). Hence, the first three principal components, just as discussed in the total variance explained, will be retained.

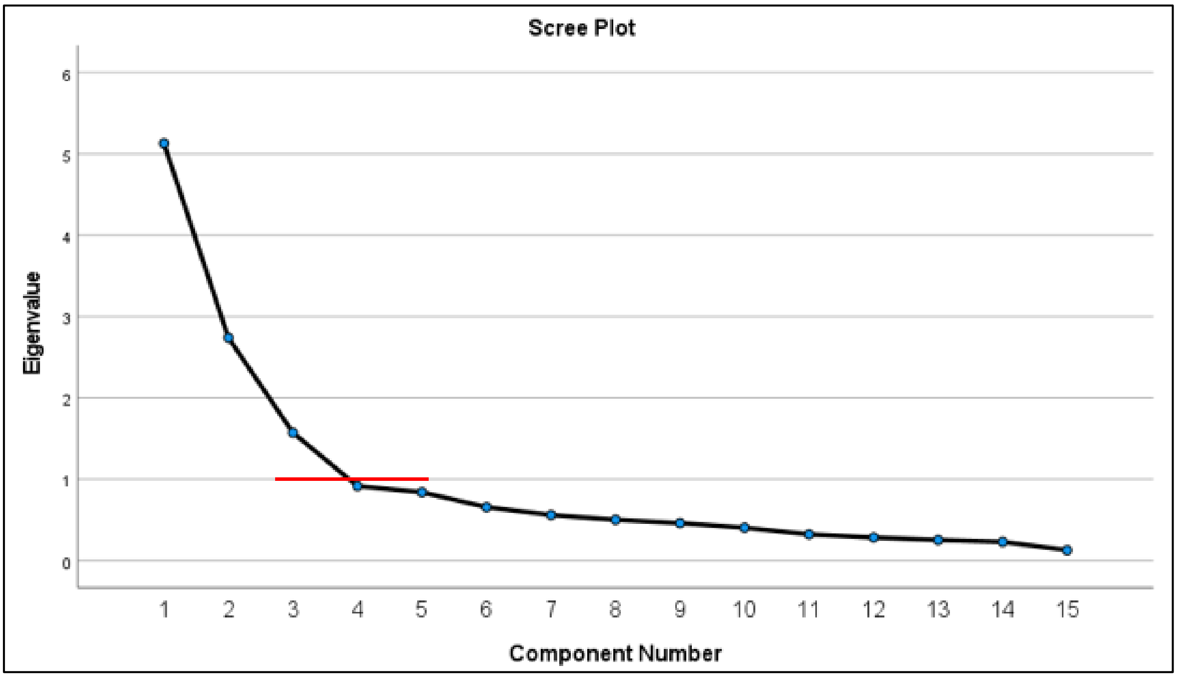


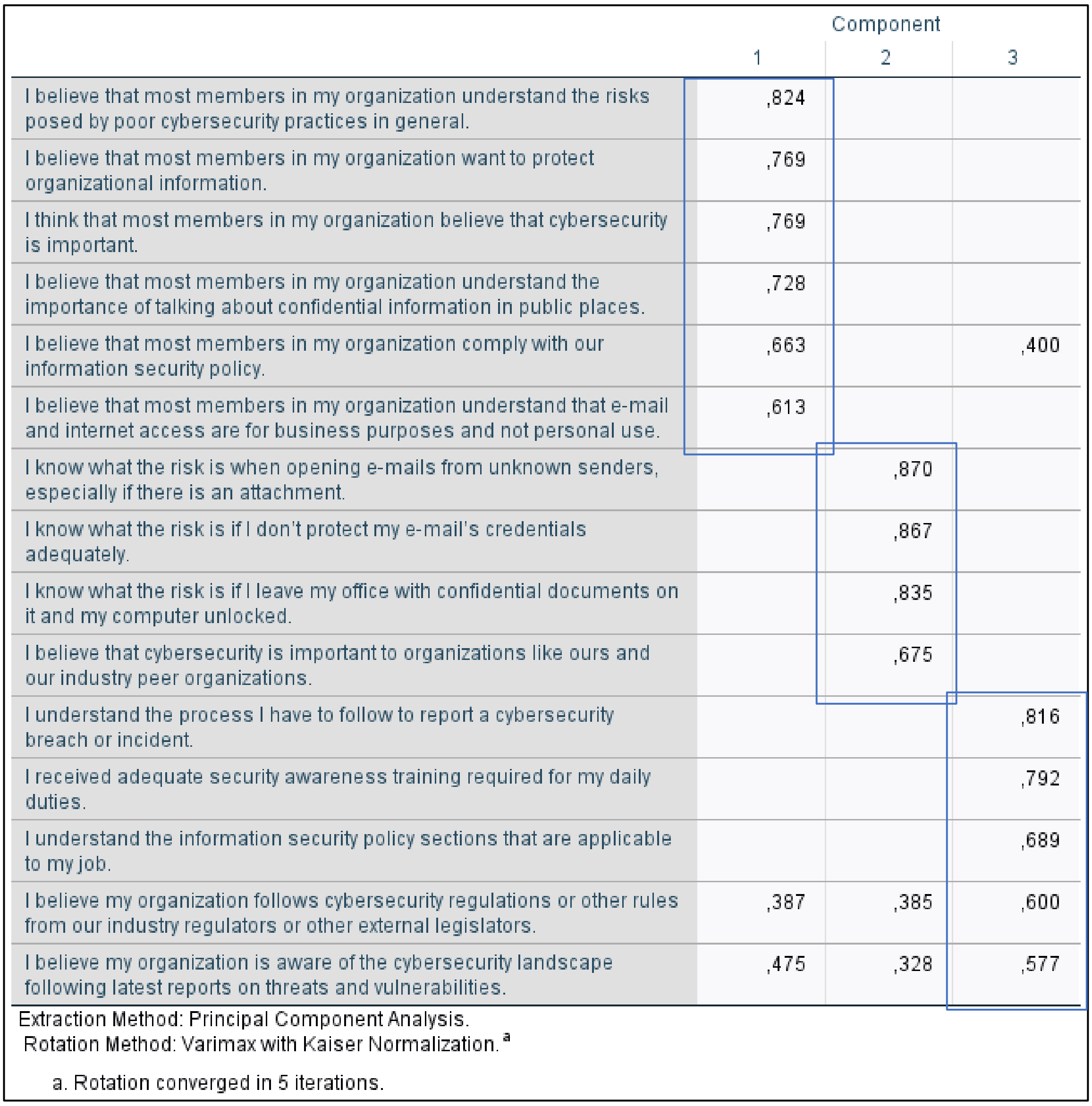
Figure 4.15. Scree Plot.

Finally, the three factors identified should be elaborated based on the variables that comprise them. By examining the rotated component matrix in Figure 4.16 and the relevant items' alignment, one could identify affinities described by Schein's model described in 2.3.3 and depicted respectively in Figure 2.8. Specifically:

Factor 1: Representing the Espoused Values and Shared Tacit Assumptions. Any aspect that is not palpable and consciously (e.g., strategy) or unconsciously (e.g., beliefs and perceptions) incites the CSC status.

Factor 2: Representing the Knowledge and one out of three items from the Superstructural element. Any aspect that practically answers to what, how, and why to provide security operational excellence. Although a Superstructural item fits here, if examined more closely, one could comprehend its conformity since the relevant question exemplifies "Why."

Factor 3: Representing Artifacts and the rest two items from Superstructural element. Artifacts are described as the visible aspects of the culture such as hierarchy, policies, and procedures. It is no surprise that the rest two Superstructural elements fit here as the first embodies any organization's regulation or rules. The second refers to reports that affect the organization's CS.



	Component		
	1	2	3
I believe that most members in my organization understand the risks posed by poor cybersecurity practices in general.	,824		
I believe that most members in my organization want to protect organizational information.	,769		
I think that most members in my organization believe that cybersecurity is important.	,769		
I believe that most members in my organization understand the importance of talking about confidential information in public places.	,728		
I believe that most members in my organization comply with our information security policy.	,663		,400
I believe that most members in my organization understand that e-mail and internet access are for business purposes and not personal use.	,613		
I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment.		,870	
I know what the risk is if I don't protect my e-mail's credentials adequately.		,867	
I know what the risk is if I leave my office with confidential documents on it and my computer unlocked.		,835	
I believe that cybersecurity is important to organizations like ours and our industry peer organizations.		,675	
I understand the process I have to follow to report a cybersecurity breach or incident.			,816
I received adequate security awareness training required for my daily duties.			,792
I understand the information security policy sections that are applicable to my job.			,689
I believe my organization follows cybersecurity regulations or other rules from our industry regulators or other external legislators.	,387	,385	,600
I believe my organization is aware of the cybersecurity landscape following latest reports on threats and vulnerabilities.	,475	,328	,577

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.[a]

a. Rotation converged in 5 iterations.

Figure 4.16. Rotated Component matrix.

The relationship between Schein's CSC enforced model as described in 2.3.3, the relevant questions used in the survey's questionnaire that comprise CSC status, and the underlying factors produced by the factor analysis are depicted in Figure 4.17 below.

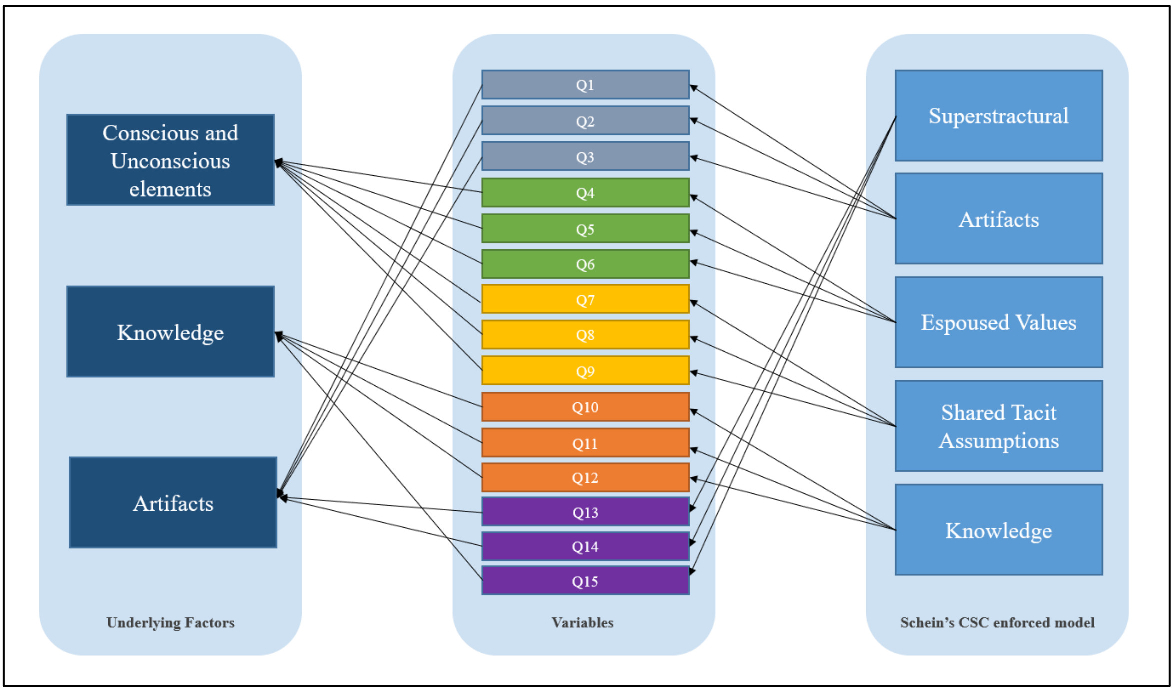


Figure 4.17. Factor analysis and correlation with variables and Schein's CSC enforced model.

4.2.5 Confirmatory Factor Analysis

Following the factor analysis, CFA should take place to measure the overall model that has been derived. CFA is a measurement tool that specifies and tests models comprised of multiple items (Zimmer, 2019). Observed variables (Q1, Q2 etc.) are considered items, while the underlying factors determined in 4.2.6 are the latent variables.

We assume that both variables, latent and observed, are continuous to proceed with the relevant test. Also, it is recommended for the sample to be equal to or greater than 200. However, it is not prohibited to proceed with a sample between 100-200 but definitely to avoid samples lower than 100 as they are considered untenable (*Confirmatory Factor Analysis (CFA) in R with Lavaan.*, n.d.). CFA offers a plethora of fit statistics for relevant assessment. For this survey, Kline's (2010) suggestion of minimum indices of chi-square, root mean square error of approximation (RMSEA), Comparative Fit Index (CFI), and Standardized Root Mean Square Residual (SRMR) will be incorporated to assess the model's goodness of fit.

The first model examined represents the factor analysis as developed through the results depicted in Figure 4.16. The relevant model results are represented in Table 4.31; the visual representation can be found in Figure 4.18.

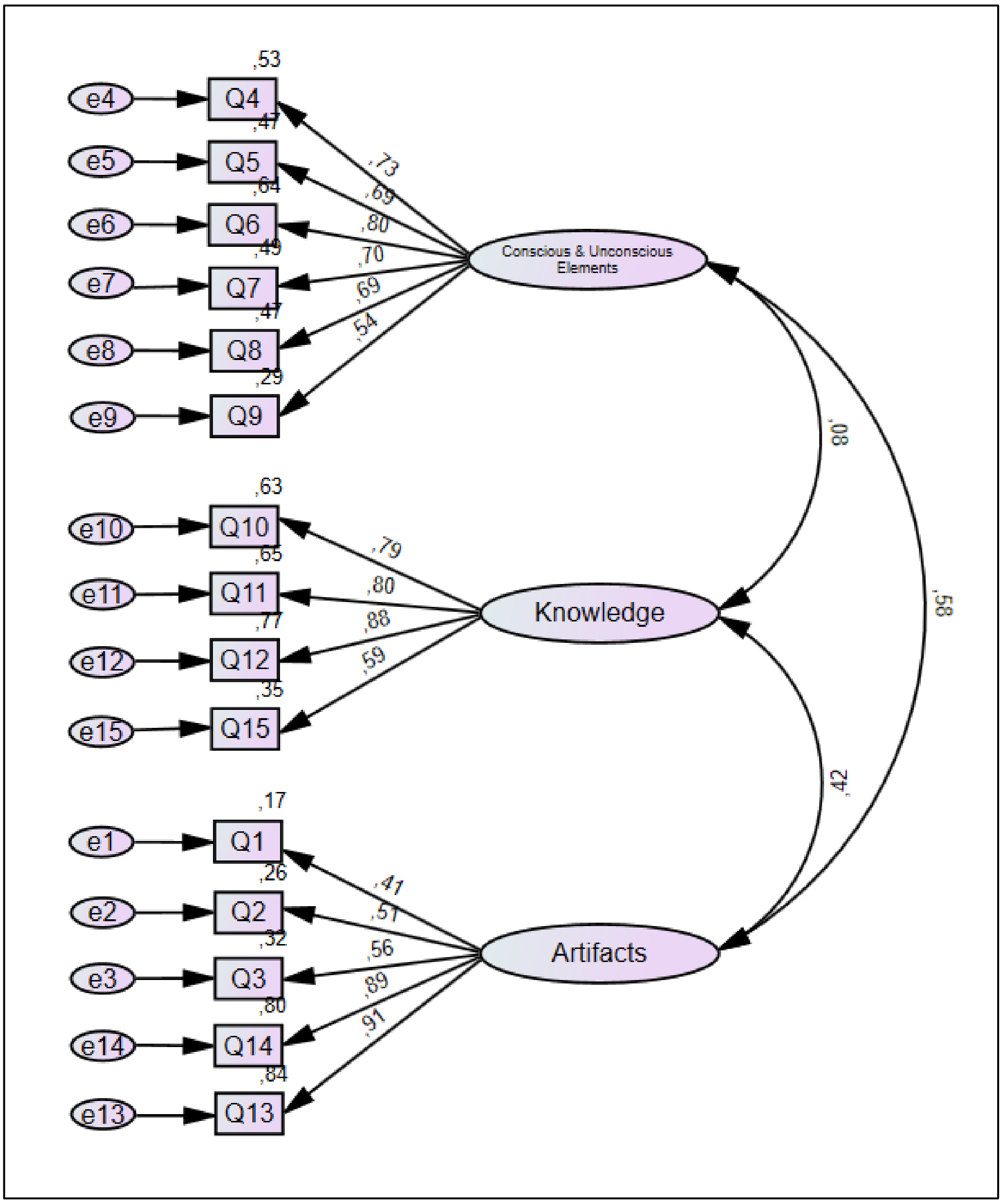


Figure 4.18. CFA model representing initial factor analysis provided.

	Values	Cut-off for good fit
chi-square	241,185	-
df	87	-
p-value	< 0,00001	<0,05
CFI	0,861	>0,90
SRMR	0,081	<0,08
RMSEA	0,107	<0,08

Table 4.31. CFA model goodness of fit values.

Model fit results from the first attempt are prohibitive and hence a further attempt to examine whether another model will fit should take place. Hence, an attempt to incorporate the cross-loadings identified during the factor analysis as represented in Figure 4.16 will occur. The relevant model, including cross-loadings between latent variables, is represented in Figure 4.19, and the respective results are under Table 4.32. While SRMR shows some improvement, CFI and RMSEA values have increased and moved away from the cut-off value for fit.

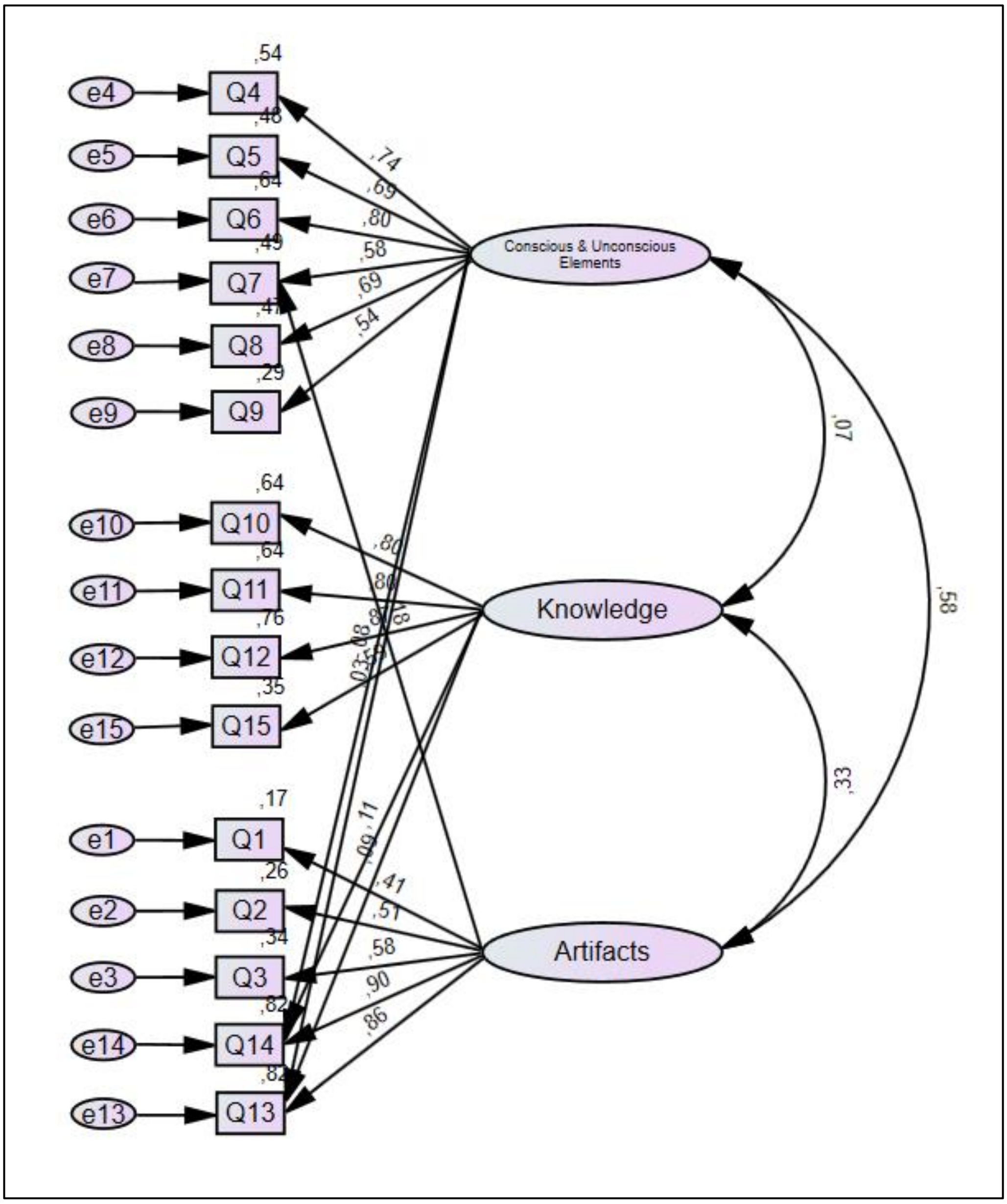


Figure 4.19. CFA model with cross-loading included.

	Values	Cut-off for good fit
chi-square	233,891	-
df	82	-
p-value	< 0,00001	<0,05
CFI	0,863	>0,90
SRMR	0,077	<0,08
RMSEA	0,109	<0,08

Table 4.32. CFA model goodness of fit values including cross-loadings.

Next and last attempt to provide a model fit takes place by scrutinizing the observed variables and taking into account any presence of correlated errors either within or between the latent variables. The results of this model fit are represented in Figure 4.20 and the respective values can be found in Table 4.33.

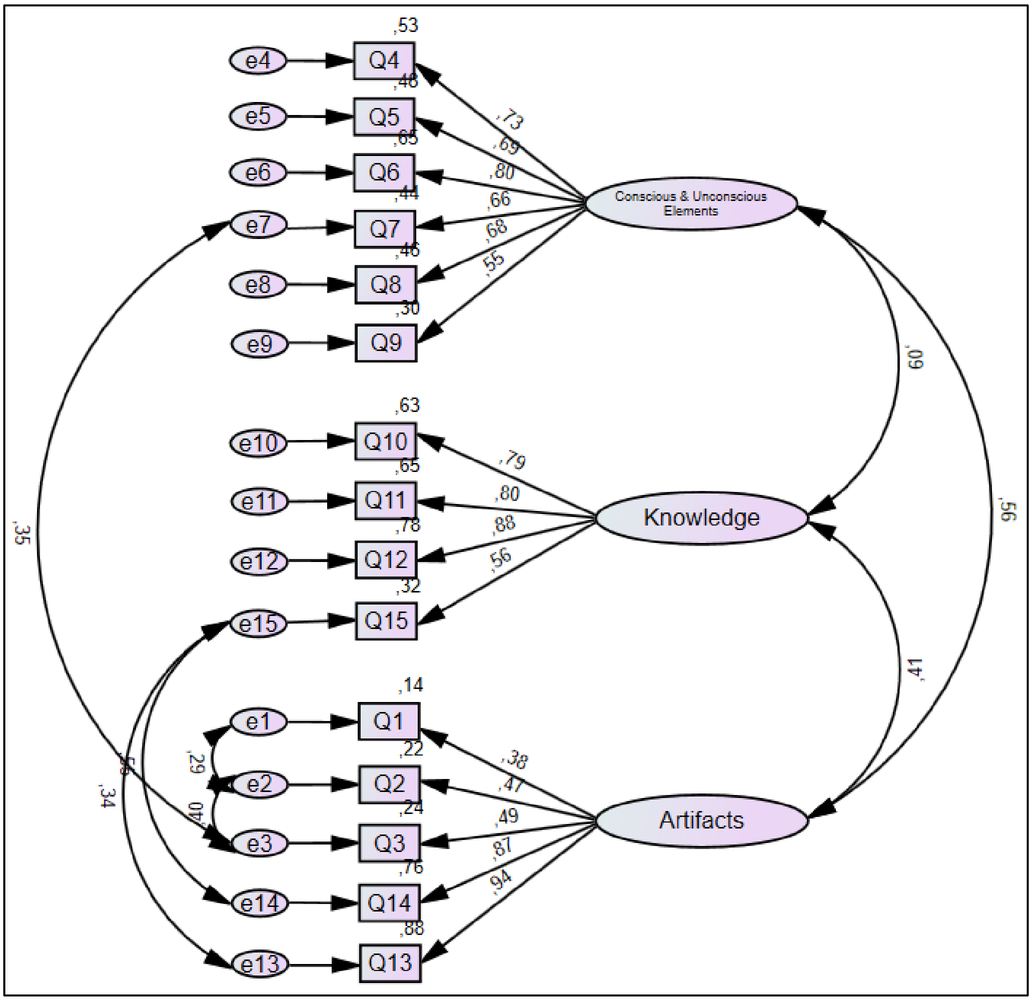


Figure 4.20. CFA model with correlation errors included.

	Values	Cut-off for good fit
chi-square	147,749	-
df	82	-
p-value	< 0,00001	<0,05
CFI	0,941	>0,90
SRMR	0,067	<0,08
RMSEA	0,072	<0,08

Table 4.33. CFA model goodness of fit values including correlation errors.

It is evident that this model's goodness of fit produced values that are acceptable for all indices required. Be that as it may, to accept this model, given that there are correlated errors present, these correlations should be theoretically justified (Meyer, 2019). The correlation errors between Q1 and Q2 and Q2 to Q3 have similar characteristics as part of the survey as they are derived and represent the original Artifacts questions. Correlation errors between Q15 to Q13 and Q15 to Q14 are also highly related as they represent the original Superstructural set of questions in the survey. Finally, Q3 to Q7 do not have that much of similar wording, and Q7 might belong to conscious and unconscious elements; however, they both refer to the information security policy that one would expect, not exclusively to be disseminated through awareness training. A reconsideration of Figure 4.17 and following the above, could provide the visual representation of Figure 4.21. Superstructural element is being reintroduced; however as it is part of Artifacts and all variables represent correlated errors, it remains underemphasized.

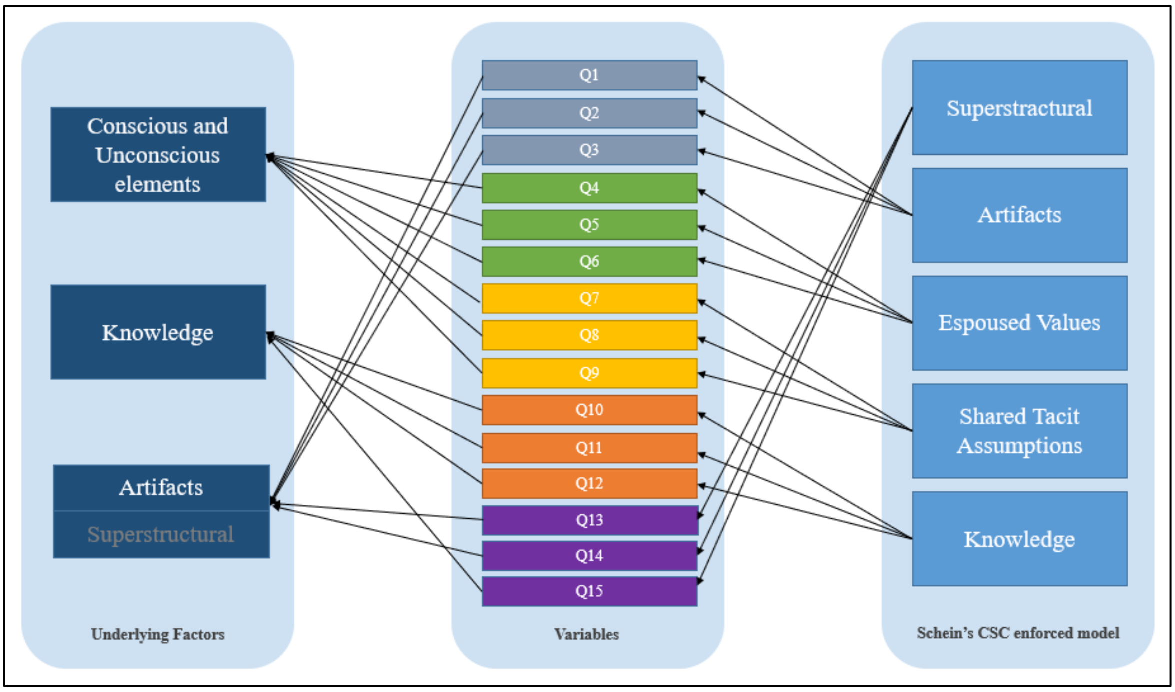


Figure 4.21. Visual representation of Factor Analysis, CFA and variables of Schein's reinforced model.

To conclude, the last model represented in Figure 4.20, given the assumptions and indices discussed, can be accepted. Hence, it represents the respective CFA model that supports the CSC concept sustained by the three factors identified.

4.3 Reflecting on the process to reach the results

Throughout this dissertation, the process can be documented as a clear formation of a path for building a self-sustained assessment tool based on theoretical groundwork and executed and recycled in statistical means. This process could supplement ENISA's CSC instrumentation plan described in 2.3.3.

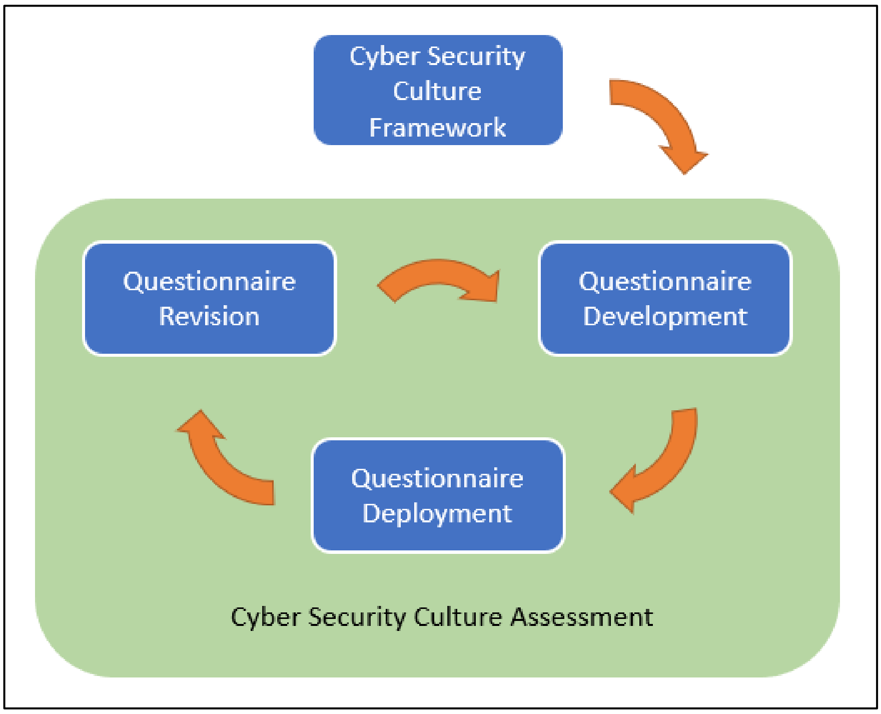

Cyber Security Culture Framework
Questionnaire Revision
Questionnaire Development
Questionnaire Deployment
Cyber Security Culture Assessment

Figure 4.22. CSC assessment process upcycling.

Figure 4.21 represent this process with three plus one steps that should be taken when considering building an assessment tool:

- **CSC Framework**: this is where the theoretical foundations are laid; within this dissertation, a new one has been introduced; however, another can be used either academic or commercial. It is fundamental to choose a framework as assessment elements should be of interest to the organization and fit the relevant requirements. Once this exploratory step is completed and a framework is chosen, the upcycling process begins.
- **Questionnaire development**: based on the framework, specific categories of questions infused with business requirements and utter goals in mind are being developed. This dissertation took place upon Artifacts, Superstructural, and the rest of the elements with a generic approach on questions.

- **Questionnaire deployment**: this step includes building the questionnaire, giving it away, and collecting relevant data. Within this dissertation, Google Forms was used as it was able to produce an Excel file that could, later on, be taken into consideration based on the software as defined in 3.3. Again the options here are limitless for organizations; custom intranet portals could be used or commercial solutions that fit their needs the best way possible.
- **Questionnaire revision**: this is where the steps followed in 4.2.4 and 4.2.5 assist. Factor Analysis and CFA could provide insight on which questions are complementary and require wording changes or even weak enough to remove. Along with relevant factors uncovered and considering organization elements, this is essential feedback to improve the next assessment cycle's questionnaire, going back to the development step.

Most commercial tools present a straightforward questionnaire providing feedback on specific weak areas. The process described above institutes an upcycling tool where the organization builds a custom questionnaire, and while the unmitigated goal is to assess CSC, the tool is being further processed to advance itself the next time it will be used.

5. Conclusions

This study's research objective was to explore the CSC and its contribution to cyber resilience while examining other supporting factors, organization size and industry, the OC type, the presence of a CISO, and the CS perception status. Organizations that interact with the cyber space have a CSC. However, only by assessing the relevant status, building a respective map, and eventually cultivating weaknesses uncovered would improve the organization's cyber resilience.

5.1 Theoretical implications

This study's theoretical approach has unraveled the most prominent frameworks and their relevant elements that contribute both to OC and CSC. OC is considered the forefather of any business culture as it has been a domain in research for over five decades. The groundwork that has been done and the aspects examined have been proved to directly correlate with CSC as elements such as behaviors, values, norms, artifacts, and more are being scrutinized in both cases. Within this study, Schein's OC model has been used as a keystone to examine CSC due to its foundational substance and comprehensive approach. While examining other recent researchers, it has allowed this study to introduce a new framework. Schein's model followed by the readjustment of Redi and van Niekerk's contribution and by adding the most recently published Superstructural element by Granter and Edgell. This new framework has been used for the development of the research questionnaire. Through the factor analysis performed in Chapter 4, it has been proved that no item from any element has been left unused, indicating that the new framework is of significance.

Another aspect to consider is that commercial tools are provided with their theoretical and practical approach, but their assessment tools are not available in public. This study suggests that an assessment tool can be built while relying upon a dependable scientific foundation. This assessment tool can be sculpted based on the organization's needs to uncover weaknesses that require attention. Of course, as in this study, all necessary statistical tools required to verify reliability must be used.

5.2 Practical implications

The questionnaire of this study provided some interesting results regarding the status of CSC in organizations. One of the most unequivocal is affirming the relationship between the CISO presence and the CSC status. ENISA has already upraised the role of CISO within an organization towards all directions, including stakeholders, SMT and members and has also provided with a clear responsibility of the ambassador carrying the message of "*the way we do things*" indicating a direct relationship with CSC (*Cyber Security Culture in Organisations*, 2017).

Another result of the questionnaire indicates that CSC status is statistically related to the relevant organization industry. By considering the development of the CS field where MITRE ATT&CK is currently a standard in evolving countermeasures based on characteristics such as country of operation and industry, this result could be of high importance. For example, results indicated that Financial Services and Data Infrastructure & Telecom organizations stand better in CSC status while Healthcare and Media & Creative Industries are more inadequate. An APT group targeting Healthcare and Media & Creative Industry in the country they operate should reconsider fostering CSC to defend better.

Other characteristics of organizations such as size and OC type have been found not to have a significant relationship with the CSC status. This indicates that no matter what the size and "*how we do things around here"* identity of the organization, CSC should always be a priority. At least for these two organization characteristics, assessment results would not have any suspected expectations.

Following, the CS status as perceived by organization members, seem to have a relationship with the CSC status. Although this is a highly subjective outcome of the results provided, it is important as it brings to light the human aspect of confidence. ENISA contributes to this matter as it amplifies the significance of confidence as a psychological factor that when fostered, can advance the CSC status (*Cyber Security Culture in Organisations*, 2017).

Finally, factor analysis and CFA have also provided significant insight into this research questionnaire tool. Factor analysis has dropped the framework's initial elements from five to three while keeping consistency between the underlying substance of grouped variables. Superstructural element which has been introduced in this study, has proved to be weak by the questions represented and hence, its variables have been agglutinated with other elements. This, however, should not be a disconcerting circumstance about the presence of the Superstructural element. CFA on the other hand, raised concerns on the matter of some points of improvement that could take place regarding the variable's essence and whether specific items could be further revamped to strengthen further the questionnaire.

5.3 Limitations

The concept of examining an organization's CS posture should be done by reaching out to it and assessing its relevant aspects, the CSC in this study's case. While this would be an ideal scenario, performing an assessment of this scale would also unveil and bring to public vulnerabilities that might put the organization at risk. Hence, the survey has been carried out without narrowing down the sample to a single organization's members, but by reaching out to anyone who would like to participate.

Another aspect that should be taken into consideration is the one of resilience. While going through the literature review, it is supported that CSC contributes to strengthening cyber resilience; periodic assessment reviews could only uncover its actual and measurable impact. This would entail that ENISA's instrumentation plan steps should be carried out, including an upcycle of actions that would re-assess CSC status repeatedly until the organization's CS goals are met. This study provides the fundamental theoretical frameworks, practical tools, and a feeling of how one could execute a CSC assessment. Be that as it may, in practice, actual CS resilience evaluation would require a process of months, maybe even years, to develop and complete.

An effort has been made to develop a CFA model following the relevant factor analysis; while the results have provided interesting insights, the model development process has been completed with several constraints. While a dozen fit statistics are available to explore, only four suggested by Kline as a bare minimum have been adopted. As an exploratory aspect of CSC, results derived have been of interest; however, CFA and Structure Equation Modelling require substantial scientific proficiency to carry out this kind of research, which would dissociate from this study's objectives.

5.4 Future research

The CSC framework introduced in section 2.3.3 has been used throughout the course of this study. While its foundation has been supported by studies already available, further exploring of the Superstructural element should occur as it is a recent introduction for the respective OC model and thereinafter for the CSC domain as introduced in this study. Its contribution has been substantial and has been thoroughly elaborated from its inception to discussing the results. Be that as it may, this aspect's additional intensifying research could consolidate it as a standard, justifying this study's work.

While some of Karyda's (2017) suggestions have been elaborated in this study, further organization elements, as proposed by her as well, should be considered. As proved by this study, organizational elements such as CISO presence might be correlated with the CSC status, and hence, further aspects should be explored. For example, organizations with specific certifications such as ISO27001 or HIPAA and organizations with specific CS functions such as Governance, Training, Operations, e.tc. While this is a wide-ranging field to engage with, it could be of interest for organizations considering characteristics such as international operation, size, and industry.

Having established that solid scientific artifacts can elaborate a tool to assess the CSC status, this study provided evidence that the tool itself can statistically be meliorated further. Factor analysis and CFA cultivate in this study can support this inference. This leads to the assumption that a tailor-made tool developed for an organization with periodic implementation can lead to CSC status assessment results and considerable commodities that could improve the tool's effectiveness itself.

References

Akhtar, I. (2016). *Research Design* (p. 17).

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Allaire, Y., & Firsirotu, M. E. (1984). Theories of Organizational Culture. *Organization Studies*, *5*(3), 193–226. https://doi.org/10.1177/017084068400500301

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Blanche, M. T., Blanche, M. J. T., Durrheim, K., & Painter, D. (2006). *Research in Practice: Applied Methods for the Social Sciences*. Juta and Company Ltd.

Blythe, J., & Alashe, O. (2019). *Measuring Cyber Security Culture*. CybSafe.

Brace, I. (2004). *Questionnaire design: How to plan, structure, and write survey material for effective market research*. Kogan Page.

Bremer, M. (2019). *Organizational Culture Assessment Instrument*. https://www.ocai-online.com/sites/default/files/node/files/2019-12/ocai_leaflet.pdf

Brown, A. (1998). *Organizational Culture* (2nd edition). Ft Pr.

Cameron, K., & Quinn, R. (n.d.). *About the Organizational Culture Assessment Instrument (OCAI)*. Retrieved November 26, 2020, from https://www.ocai-online.com/about-the-Organizational-Culture-Assessment-Instrument-OCAI

Confirmatory Factor Analysis (CFA) in R with lavaan. (n.d.). UCLA: Statistical Consulting Group. Retrieved March 1, 2021, from https://stats.idre.ucla.edu/r/seminars/rcfa/

Cooke, R. A., & Rousseau, D. M. (1988). Behavioral Norms and Expectations: A Quantitative Approach To the Assessment of Organizational Culture. *Group & Organization Studies*, *13*(3), 245–273. https://doi.org/10.1177/105960118801300302

CultureAI | The Cyber Security Culture Management System. (n.d.). Retrieved January 3, 2021, from https://www.culture.ai

Cyber Security Culture in organisations. (2017). European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Cybersafety Culture Assessment. (2018). Kaspersky Lab. https://media.kaspersky.com/en/business-security/enterprise/KL_CyberSafety%20Culture%20Assessment_overview.pdf

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *2016 SAI Computing Conference (SAI)*.

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Daft, R. L. (2010). *Management* (9th Edition). Cengage Learning.

Davis, S. M. (1984). *Managing corporate culture*. Ballinger Pub. Co.

Deal, T., & Kennedy, A. (2000). *Corporate Cultures: The Rites and Rituals of Corporate Life* (Revised ed. edition). Basic Books.

Exact Tests. (n.d.). IBM Knowledge Center. Retrieved February 14, 2021, from https://www.ibm.com/support/knowledgecenter/SSLVMB_23.0.0/spss/base/idh_exact.html

Field, A. (2005). *Discovering statistics using SPSS* (2nd ed.). Sage Publications, Inc.

Fruhlinger, J. (2019, January 14). *What is a CISO? Responsibilities and requirements for this vital role*. CSO Online. https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *0*(0), 1–11. https://doi.org/10.1080/08874417.2020.1845583

Harrison, R. (1972). *Understanding your organisation's character*. Harvard Business Review.

Hofstede, G. (n.d.). *Organisational Culture—What you need to know*. Retrieved November 27, 2020, from https://hi.hofstede-insights.com/organisational-culture

Hofstede, G. (2019). *What are the different types of Organisational Culture?* https://news.hofstede-insights.com/news/what-are-the-different-types-of-organisational-culture

Huang, K., & Pearlson, K. (2019, January 8). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2019.769

Hyken, S. (2015). *Drucker Said "Culture Eats Strategy For Breakfast" And Enterprise Rent-A-Car Proves It*. Forbes. https://www.forbes.com/sites/shephyken/2015/12/05/drucker-said-culture-eats-strategy-for-breakfast-and-enterprise-rent-a-car-proves-it/

Jaques, E. (2013). *The Changing Culture of a Factory*. Routledge. https://doi.org/10.4324/9781315013725

Johnson, G., & Scholes, K. (n.d.). *The Cultural Web Model – BusinessBalls.com*.

BusinessBalls. Retrieved November 28, 2020, from https://www.businessballs.com/strategy-innovation/cultural-web-johnson-scholes/

Johnson, G., & Scholes, K. (1998). *Exploring Corporate Strategy* (5th edition). Pearson.

Joint Task Force Interagency Working Group. (2020). *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology. https://www.nist.gov/news-events/news/2020/09/security-and-privacy-controls-information-systems-and-organizations-nist

Kailash, D. (2020). *One year ago we issued a call for solutions to the world's biggest challenges. This is our progress so far*. World Economic Forum. https://www.weforum.org/agenda/2020/09/uplink-one-year-on-progress-sustainable-development-innovation/

Karyda, M. (2017). Fostering Information Security Culture In Organizations: A Research Agenda. *MCIS 2017 Proceedings*. https://aisel.aisnet.org/mcis2017/28

Kaufman, J. D., & Dunlap, W. P. (2000). Determining the number of factors to retain: Q windows-based FORTRAN-IMSL program for parallel analysis. *Behavior Research Methods, Instruments, & Computers*, *32*(3), 389–395. https://doi.org/10.3758/BF03200806

Khatib, T. (1999). *Organizational culture, subcultures, and organizational commitment* [Iowa State University]. https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=12539&context=rtd

Kline, R. (2010). *Principles and Practice of Structural Equation Modeling, Third Edition (Methodology in the Social Sciences)* (Third). The Guilford Press.

KMO and Bartlett's Test. (n.d.). Retrieved February 20, 2021, from https://www.ibm.com/support/knowledgecenter/SSLVMB_23.0.0/spss/tutorials/fac_telco_kmo_01.html

Laycock, A., Petric, G., & Roer, K. (2019). *The seven dimensions of security culture*. CLTRe AS.

Leffingwell, D. (2019). *Core Values—Scaled Agile Framework*. https://www.scaledagileframework.com/safe-core-values/

Lord, N. (2017, August 17). The Cost of a Malware Infection? For Maersk, $300 Million [Text]. *Digital Guardian*. https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million

Lundy, O., & Cowling, A. (1996). *Strategic human resource management*. Routledge.

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. *Psychological Methods*, *4*(1), 84–99. https://doi.org/10.1037/1082-989X.4.1.84

Maher, L. (2014). Building a culture for innovation: A leadership challenge. *World Hospitals and Health Services: The Official Journal of the International Hospital Federation*, *50*(1), 4–6.

Maher, L., Plsek, P., Price, J., & Mugglestone, M. (2010). *Creating the Culture for Innovation*. NHS Institute for Innovation and Improvement. https://www.england.nhs.uk/improvement-hub/wp-content/uploads/sites/44/2017/11/Creating-the-Culture-for-Innovation-Practical-Guide-for-Leaders.pdf

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, *30*(7), 537–542. https://doi.org/10.1177/0267659114559116

McHugh, M. L. (2013). The Chi-square test of independence. *Biochemia Medica*, *23*(2), 143–149. https://doi.org/10.11613/BM.2013.018

Meyer, J. (2019, June 12). Correlated Errors in Confirmatory Factor Analysis. *The*

Analysis Factor. https://www.theanalysisfactor.com/correlated-errors-in-confirmatory-factor-analysis/

Morente, F., Ferràs, X., & Zizlavsky, O. (2018). Innovation Cultural Models: Review and Proposal for Next Steps. *Revista Universidad y Empresa*, *20*(34), 53–81. https://doi.org/10.12804/revistas.urosario.edu.co/empresa/a.5433

Morgan, S. (2018, December 8). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*, *27*(2), 146–164. https://doi.org/10.1108/ICS-12-2016-0095

Non-Probability Sampling: Definition, types, Examples, and advantages. (2018, April 30). *QuestionPro*. https://www.questionpro.com/blog/non-probability-sampling/

O'Reilly, C., & Chatman, J. (1996). Culture and social control: Corporations, cult and commitment. *Research in Organizational Behavior*, *18*, 157–200.

Reegård, K., Blackett, C., & Katta, V. (2019). The Concept of Cybersecurity Culture. *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, 4036–4043. https://doi.org/10.3850/978-981-11-2724-3_0761-cd

Reid, R., & van Niekerk, J. (2014). *From Information Security to Cyber Security Cultures Organizations to Societies*. 1–7. https://doi.org/10.1109/ISSA.2014.6950492

Roer, K. (2015). *Build a Security Culture*. IT Governance Ltd.

Schein, E. H. (2004). *Organizational culture and leadership*. Jossey-Bass. http://www.books24x7.com/marc.asp?bookid=11277

Schneider, W. (1999). *The Reengineering Alternative* (1st edition). McGraw-Hill Education.

Seyran, M., Pizzol, D., Adadi, P., El-Aziz, T. M. A., Hassan, S. S., Soares, A., Kandimalla, R., Lundstrom, K., Tambuwala, M., Aljabali, A. A. A., Lal, A., Azad, G. K., Choudhury, P. P., Uversky, V. N., Sherchan, S. P., Uhal, B. D., Rezaei, N., & Brufsky, A. M. (n.d.). Questions concerning the proximal origin of SARS-CoV-2. *Journal of Medical Virology*, *n/a*(n/a). https://doi.org/10.1002/jmv.26478

Shepherd, M. (2018, April 4). Is Data the New Gold? *CEO Today*. https://www.ceotodaymagazine.com/2018/04/is-data-the-new-gold/

Sinek, S. (2011). *Start with Why: How Great Leaders Inspire Everyone to Take Action* (Illustrated edition). Portfolio.

Tharp, B. (2009). *Defining "Culture" and "Organizational Culture": From Anthropology to the Office*. Haworth. Defining "Culture" and "Organizational Culture": From Anthropology to the Office

The Circumplex. (n.d.). Human Synergistics. Retrieved November 28, 2020, from https://www.human-synergistics.com.au/about-us/the-circumplex

Tolah, A., Furnell, S., & Papadaki, M. (2017). A Comprehensive Framework for Cultivating and Assessing Information Security Culture. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, 52–64.

TreeSolution—Your expert for security awareness. (n.d.). Retrieved January 3, 2021, from https://www.treesolution.com/en/security-awareness-behaviour-culture

Tucker, B., Kolo, B., Rajagopalan, K., & Ware, D. (2018, September 24). *Insider threat: The human element of cyberrisk*. https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

Tziarras, Z. (2014). The Security Culture of a Global and Multileveled Cybersecurity. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-*

Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice (pp. 319–335). Springer. https://doi.org/10.1007/978-1-4939-1028-1_13

Understanding Organizational Culture. (2016). Chartered Management Institute. https://www.managers.org.uk/~/media/Files/PDF/Checklists/CHK-232-Understanding-organisational-culture.pdf

van der Meulen, R. (2017, February 7). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

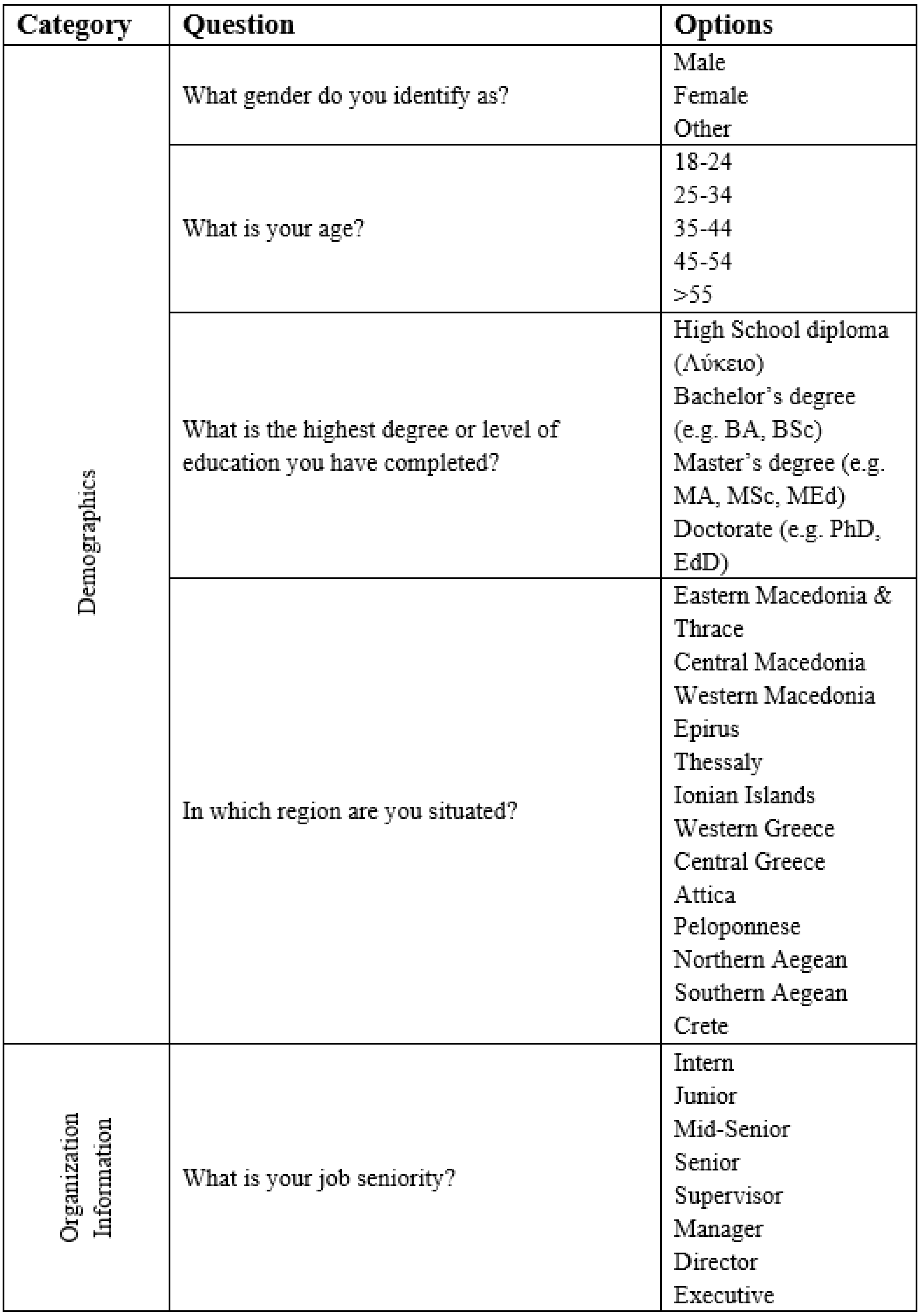
von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, C., Ikemoto, T., Hirasawa, A., Arai, Y.-C., Kikuchi, S., & Deie, M. (2020). Assessment of locomotive syndrome among older individuals: A confirmatory factor analysis of the 25-question Geriatric Locomotive Function Scale. *PeerJ*, *8*, e9026. https://doi.org/10.7717/peerj.9026

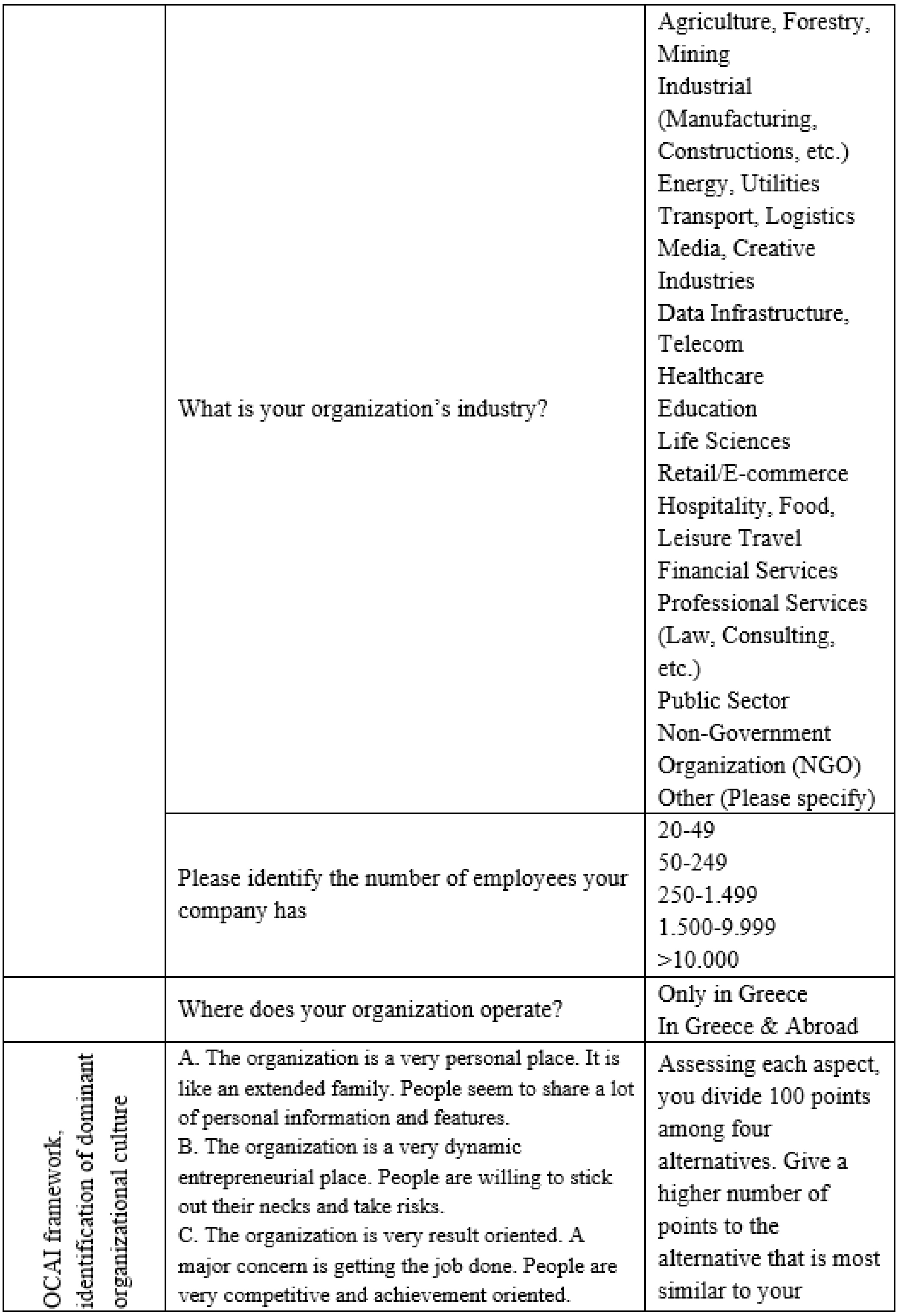
X-Force Threat Intelligence Index 2020. (2020). IBM Corporation. https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf

Zimmer, C. (2019). *Learn to Perform Confirmatory Factor Analysis in Stata With Data From the General Social Survey (2016)*. SAGE Publications, Ltd. https://doi.org/10.4135/9781529700091

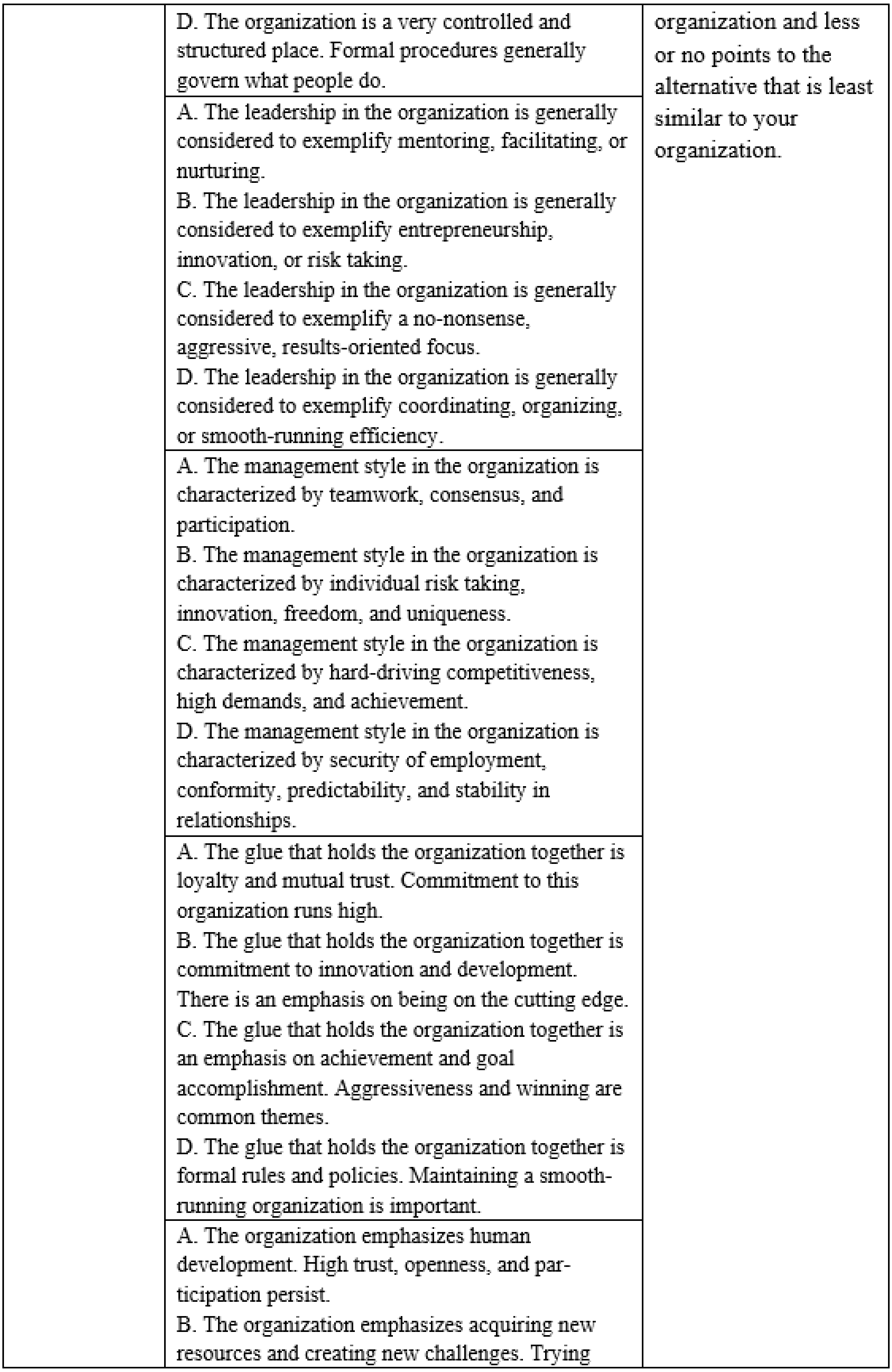
Appendix: Questionnaire



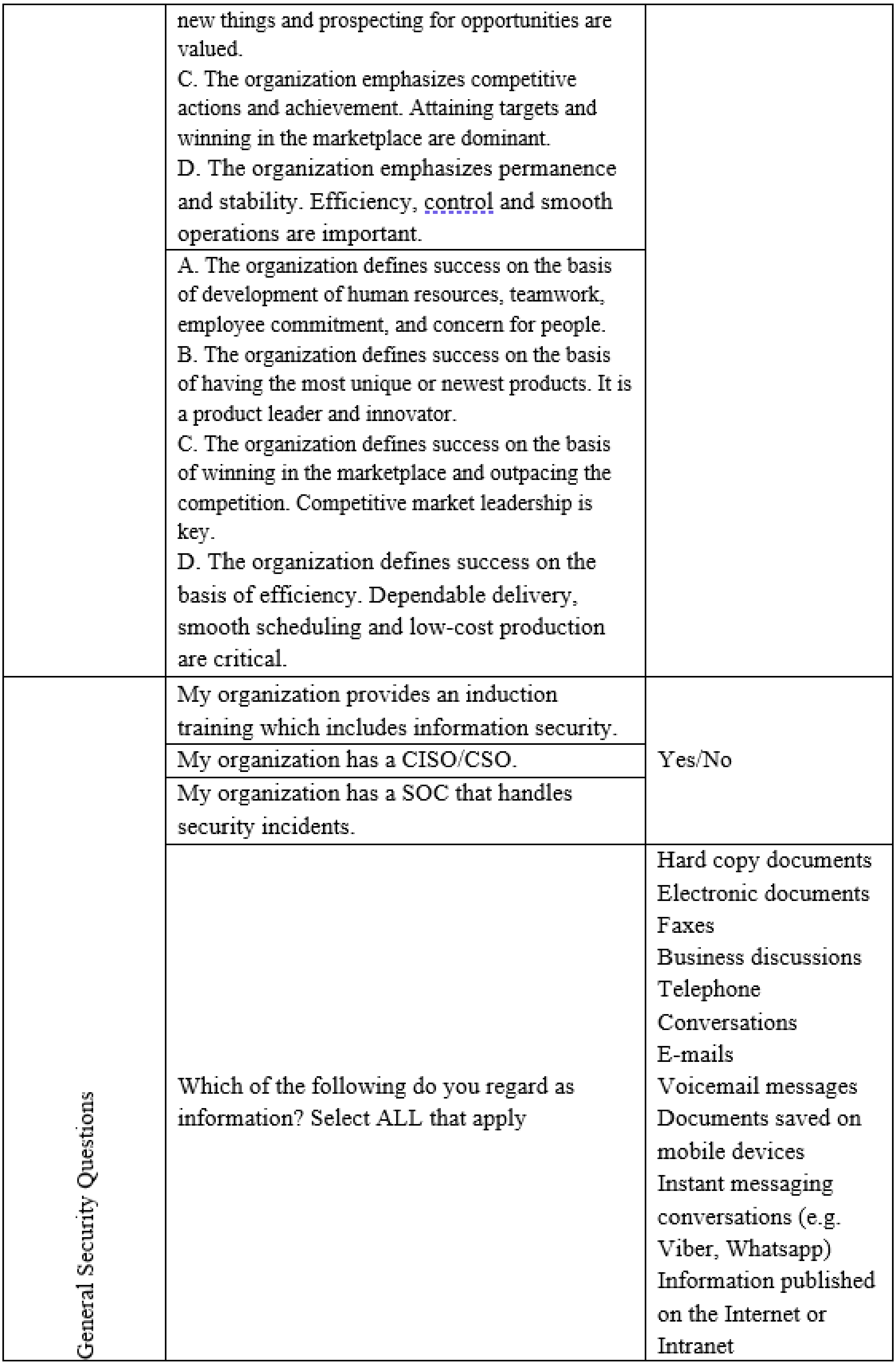
Category	Question	Options
Demographics	What gender do you identify as?	Male Female Other
	What is your age?	18-24 25-34 35-44 45-54 >55
	What is the highest degree or level of education you have completed?	High School diploma (Λύκειο) Bachelor's degree (e.g. BA, BSc) Master's degree (e.g. MA, MSc, MEd) Doctorate (e.g. PhD, EdD)
	In which region are you situated?	Eastern Macedonia & Thrace Central Macedonia Western Macedonia Epirus Thessaly Ionian Islands Western Greece Central Greece Attica Peloponnese Northern Aegean Southern Aegean Crete
Organization Information	What is your job seniority?	Intern Junior Mid-Senior Senior Supervisor Manager Director Executive



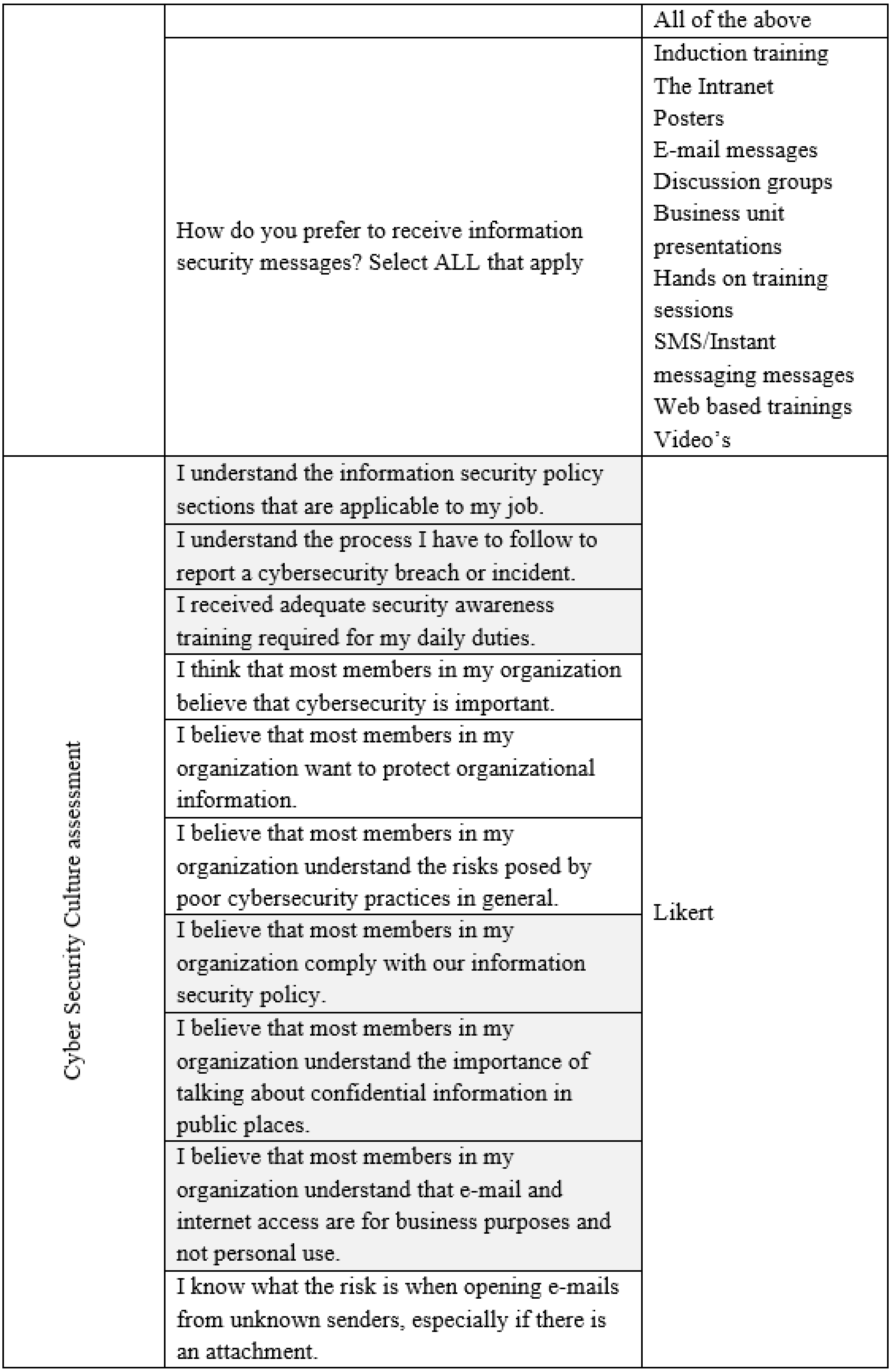
	What is your organization's industry?	Agriculture, Forestry, Mining Industrial (Manufacturing, Constructions, etc.) Energy, Utilities Transport, Logistics Media, Creative Industries Data Infrastructure, Telecom Healthcare Education Life Sciences Retail/E-commerce Hospitality, Food, Leisure Travel Financial Services Professional Services (Law, Consulting, etc.) Public Sector Non-Government Organization (NGO) Other (Please specify)
	Please identify the number of employees your company has	20-49 50-249 250-1.499 1.500-9.999 >10.000
	Where does your organization operate?	Only in Greece In Greece & Abroad
OCAI framework, identification of dominant organizational culture	A. The organization is a very personal place. It is like an extended family. People seem to share a lot of personal information and features. B. The organization is a very dynamic entrepreneurial place. People are willing to stick out their necks and take risks. C. The organization is very result oriented. A major concern is getting the job done. People are very competitive and achievement oriented.	Assessing each aspect, you divide 100 points among four alternatives. Give a higher number of points to the alternative that is most similar to your



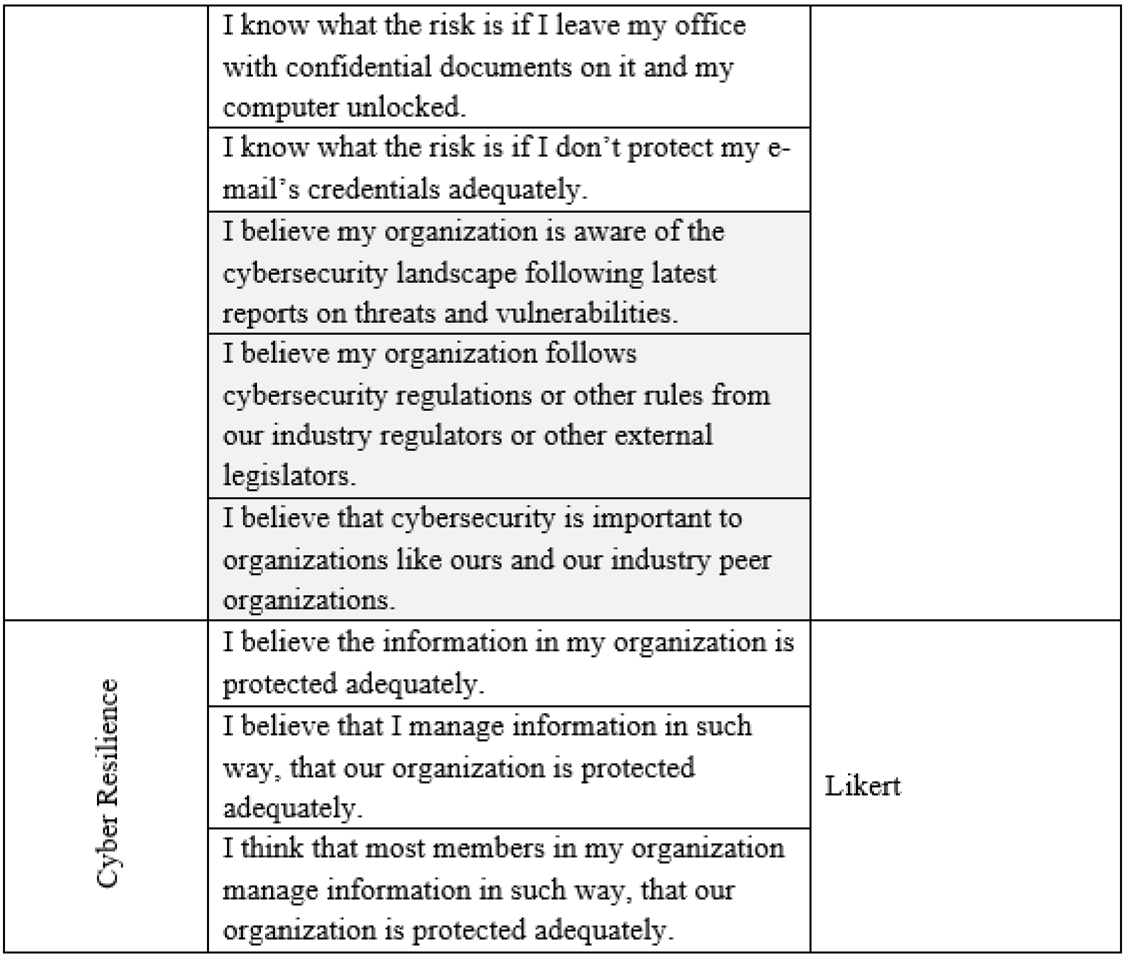
	D. The organization is a very controlled and structured place. Formal procedures generally govern what people do.	organization and less or no points to the alternative that is least similar to your organization.
	A. The leadership in the organization is generally considered to exemplify mentoring, facilitating, or nurturing. B. The leadership in the organization is generally considered to exemplify entrepreneurship, innovation, or risk taking. C. The leadership in the organization is generally considered to exemplify a no-nonsense, aggressive, results-oriented focus. D. The leadership in the organization is generally considered to exemplify coordinating, organizing, or smooth-running efficiency.	
	A. The management style in the organization is characterized by teamwork, consensus, and participation. B. The management style in the organization is characterized by individual risk taking, innovation, freedom, and uniqueness. C. The management style in the organization is characterized by hard-driving competitiveness, high demands, and achievement. D. The management style in the organization is characterized by security of employment, conformity, predictability, and stability in relationships.	
	A. The glue that holds the organization together is loyalty and mutual trust. Commitment to this organization runs high. B. The glue that holds the organization together is commitment to innovation and development. There is an emphasis on being on the cutting edge. C. The glue that holds the organization together is an emphasis on achievement and goal accomplishment. Aggressiveness and winning are common themes. D. The glue that holds the organization together is formal rules and policies. Maintaining a smooth-running organization is important.	
	A. The organization emphasizes human development. High trust, openness, and participation persist. B. The organization emphasizes acquiring new resources and creating new challenges. Trying	



	new things and prospecting for opportunities are valued. C. The organization emphasizes competitive actions and achievement. Attaining targets and winning in the marketplace are dominant. D. The organization emphasizes permanence and stability. Efficiency, control and smooth operations are important.	
	A. The organization defines success on the basis of development of human resources, teamwork, employee commitment, and concern for people. B. The organization defines success on the basis of having the most unique or newest products. It is a product leader and innovator. C. The organization defines success on the basis of winning in the marketplace and outpacing the competition. Competitive market leadership is key. D. The organization defines success on the basis of efficiency. Dependable delivery, smooth scheduling and low-cost production are critical.	
General Security Questions	My organization provides an induction training which includes information security.	Yes/No
	My organization has a CISO/CSO.	
	My organization has a SOC that handles security incidents.	
	Which of the following do you regard as information? Select ALL that apply	Hard copy documents Electronic documents Faxes Business discussions Telephone Conversations E-mails Voicemail messages Documents saved on mobile devices Instant messaging conversations (e.g. Viber, Whatsapp) Information published on the Internet or Intranet



		All of the above
	How do you prefer to receive information security messages? Select ALL that apply	Induction training The Intranet Posters E-mail messages Discussion groups Business unit presentations Hands on training sessions SMS/Instant messaging messages Web based trainings Video's
Cyber Security Culture assessment	I understand the information security policy sections that are applicable to my job.	Likert
	I understand the process I have to follow to report a cybersecurity breach or incident.	
	I received adequate security awareness training required for my daily duties.	
	I think that most members in my organization believe that cybersecurity is important.	
	I believe that most members in my organization want to protect organizational information.	
	I believe that most members in my organization understand the risks posed by poor cybersecurity practices in general.	
	I believe that most members in my organization comply with our information security policy.	
	I believe that most members in my organization understand the importance of talking about confidential information in public places.	
	I believe that most members in my organization understand that e-mail and internet access are for business purposes and not personal use.	
	I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment.	



	I know what the risk is if I leave my office with confidential documents on it and my computer unlocked.	
	I know what the risk is if I don't protect my e-mail's credentials adequately.	
	I believe my organization is aware of the cybersecurity landscape following latest reports on threats and vulnerabilities.	
	I believe my organization follows cybersecurity regulations or other rules from our industry regulators or other external legislators.	
	I believe that cybersecurity is important to organizations like ours and our industry peer organizations.	
Cyber Resilience	I believe the information in my organization is protected adequately.	Likert
	I believe that I manage information in such way, that our organization is protected adequately.	
	I think that most members in my organization manage information in such way, that our organization is protected adequately.	

Author's Statement:

I hereby expressly declare that, according to the article 8 of Law 1559/1986, this dissertation is solely the product of my personal work, does not infringe any intellectual property, personality and personal data rights of third parties, does not contain works/contributions from third parties for which the permission of the authors/beneficiaries is required, is not the product of partial or total plagiarism, and that the sources used are limited to the literature references alone and meet the rules of scientific citations.