CHARACTERIZATIONS OF SECURITY CULTURE

A Systematic Literature Review

Research Project – IT University of Copenhagen
KIREPRO1PE

Frederik Bøye Henriksen
Fhen@itu.dk – ID: 19964

Abstract

This paper characterizes security culture via a systematic literature review. This paper examines 122 primary studies from 214 related articles and finds 15 distinct characteristics and 20 different suggestions for improvements based on the articles' titles, keywords, abstracts, and conclusions. The paper presents a synthesis of the findings through 13 categories. From these results the paper finds that there is currently a trend of academic papers inventing or re-inventing new frameworks, models, and tools, rather than evaluating and using those already existing and used by other researchers.

Acknowledgements

This paper has been written in the spring of 2023, as a 7,5 ECTS individual research project at the IT university of Copenhagen under the supervision of Elda Paja and Oksana Kulyk. I want to thank Elda and Oksana for their valuable guidance, sparring and knowledge that helped me as part of this project.

Contents

1. Introduction

Within the field of software engineering, cybersecurity has always been an important aspect of the software engineering process. Making software secure and safe is obviously a goal for any engineer, but on top of that, there is also the human aspect of cybersecurity that must be considered. [1] What good is an encrypted password service, if the user gives away their password in a plaintext email to a hostile entity? Companies around the world spend a lot of resources and effort into creating a corporate cybersecurity culture, that aims to prevent and combat cybersecurity attacks such as phishing and hacking.

In many ways, due to the nature of how fast-moving cybersecurity can be, and thus how security cultures within companies are ever changing and evolving, both academia and the industry is often lacking behind reality when it comes to understanding and examining security culture. [2]

My goal in this research project is to give a comprehensive answer on how academic literature discusses and examines security culture, based on an analysis of research papers and articles in a systematic literature review. Using the paper's characterizations of security culture, I will identify common categories for an easy overview of how security culture is seen by academic literature, and what these papers propose based on their results. To that effect I will identify how academic literature proposes to improve security culture will give a better understanding of how academic literature treats the subject of security culture and find any emerging trends that needs to be addressed.

For this purpose, I have developed the following research questions that this paper will answer:

RQ1: How has cybersecurity culture been characterized in academic literature?

RQ2: What is the current state of the suggestions for improved research structure put forward by academic literature?

The primary contributions of the paper are:

- A summary of characterizations of security culture within academic literature, synthesizes into categories for easy overview, understanding and comparison with other papers examining a similar subject.
- An overview of the current status of frameworks, models and tools aimed at researchers and practitioners within security culture.

The rest of this paper will present the related works and research method used to perform the literature review in section 2, followed by a presentation of the results in section 3, and finally a discussion of method and results in section 4. These will be the basis on which I will present topics for future research in section 5 and finally sum up the conclusions in section 6.

2. Research Method

2.1 Approach:

This paper follows a method for systematic literature review based on the principles of evidence-based software engineering (EBSE) by Kitchenham et al. [3]. The steps in this process are to be done in the following order:

- Establish the need for a review, and the scope within the resources given to the review team.

- Specifying the research questions for the systematic review.
- Establish the review protocol, such as defining the search strategy, inclusion criteria, limitations, etc.
- Create a library of studies based on the search strategy.
- Select studies from library based on the inclusion criteria.
- Extract data from the selected studies.
- Perform a qualitative synthesis of the data.
- Evaluate the process and results.

Once the above steps have been followed and completed, it will be possible to provide an answer to my research question and sum up a conclusion, as well as reflect and discuss on the findings and set up further questions for future research.

2.2 Scope

This paper aims to answer the research questions put forward in the previous chapter. It will cover a wide range of academic literature found through a systematic approach. While this paper aims to be comprehensive in its research, it is important to highlight that this literature review is performed with a limited number of resources, such as a set deadline and only having a single reviewer perform the search, data extraction and synthesis. As such it will not be possible for this paper to cover all literature touching on security culture. Instead, this paper will take it's jumping off point in a single seminal paper as well as the top 200 papers on security culture (prior to applying exclusion criteria) as ranked by their H-index. By using this method, I can focus my limited resources on only the most relevant papers related to security culture, while still managing to extract valid data within the given deadline.

2.3 Examining related works

To evaluate the need for performing a systematic literature review on cybersecurity culture, it is necessary to investigate related research works. To accomplish this, I performed a literature search to look for what systematic reviews have already been done on this and similar topics previously.

I used the following search string on the Scopus database: ("cybersecurity culture" OR "security culture") AND (“systematic review” OR "systematic mapping" OR "Systematic literature")

The search yielded several previous SLR's on related topics [4-11], that will be evaluated to show their position and findings in relation to the work that this paper will perform.

[4] examines critical success factors within security culture, and how to use these factors to develop security culture. In contrast this paper will identify how literature characterizes and suggest improving security culture. While there are likely overlaps in what is a critical success factor and this paper's found characterization categories, this paper does not distinguish between whether they are critical or not, nor examine how to develop security culture in detail.

[5] also focuses on how to develop cyber security culture within an organization. The paper identifies elements of what makes up security culture, but does so from a much smaller dataset, and only focuses on papers mentioning the string “cyber security culture” explicitly. In contrast this paper also looks at other string references to security culture and thus uses a larger dataset and from a wider perspective.

[6] examines security culture exclusively with focus on DevSecOps, and thus has a much narrower scope than this paper. This paper does not distinguish between what process a company uses.

[7] studies “cyber hygiene” behaviour within software engineers, and as such has limits itself significantly in terms of what elements of security culture emerges from their research. This paper covers a wider range of behaviors that characterize security culture.

[8] is another paper that focuses on a very narrow scope as they only look at security culture within the health informatics sector.

[9] is an SLR on focused only on methods to measure security culture in order to evaluate them. This paper does identify that measurability is a characteristic of security culture, but goes beyond the scope of looking at a single aspect.

The search also yielded two papers, that are much closer in scope to the SLR that this paper aims to do, but still sufficiently different that it warrants the existence of this literature review.

[10] is focused on exclusively looking at definitions and frameworks within security culture in academic literature, and thus features a narrower scope than this literature review. It is also only using literature until 2016, whereas this paper will include papers up until March 2023.

[11] is a very comprehensive review looking at factors that influence security culture. As such these factors could be viewed as elements of how academic literature characterizes security culture, however the paper does not make any wider conclusions on the validity of the factors, nor how they relate to each other. Furthermore, despite being a very recent paper, it was not possible to recreate their search results when using the same research method for database searches that they applied. It is not the role of this paper to validate their method, but it is worth noting, since this paper identifies some of the same elements of security culture, and as such there is an overlap in the findings of both papers.

By looking at what related work has taken place already, it shows that no other paper has been written with the same scope of this paper, to the current knowledge of this author based on the search findings. In order to answer the research questions put forward in this paper, there is a clear opening for a systematic literature review on this topic.

2.4 Creating the library from data sources

To build a library of relevant articles for my literature review, I made use of a search building software Publish or Perish (PoP) [12] to retrieve and analyze academic sources from Scopus and Google Scholar. PoP allows for easy access to multiple academic search databases using the same search string and returns the results in a .csv file sorted by their H-index.

I started with a basic search string of key words *“cybersecurity culture”.* Note that the data source API I am searching with does not distinguish between case sensitivity, and thus implicitly this search string also catches different cases of the same wording.

On Scopus this string resulted in 52 hits. When also accounting for different spelling and including “cyber security culture” in the search, the result increases to 75 papers.

From these 75 results I inspected which academic publications were prominent in featuring articles about the subject, and by going through other papers published by these journals and conference articles, found by using Google Scholar, I identified that it was necessary to modify the search string yet again. Looking over the keywords included in these papers, I discovered the frequent use of other phrases such as information security or simply security when referring to cybersecurity.

Therefore, I deem it would be more beneficial to reduce the part of the search string to simply "security culture", since this string also encompasses the results from "cyber security culture" and "information security culture".

Thus, the result was a search string that returns 200 pieces of literature.

"cybersecurity culture" OR "security culture"

2.5 Performing a complementing verification of keyword choice – Forward Snowballing

To confirm that my final search string indeed does find the results needed for a relevant systematic literature review, I chose to do a complementary forward snowballing of a highly cited seminal paper *'Users are not the Enemy'* [13] on the topic of Cybersecurity Culture. By looking at what papers cite Adams and Sasse cite in [13], I will be able to verify that these papers are within the subject area of security culture and use keywords that relate to my search string, and cross reference this with the ones found by my search string in PoP. Indeed when looking at some of these papers, I found that early papers tended to use the keyword 'information security culture' [14] or just some variety of 'security' [15, 16, 17]. By snowballing further into the citations of the citations, the term 'cybersecurity culture' starts to appear as well [18] as the papers become more recent.

With the scope of this paper, the search string "security culture" would indeed find the intended papers, and the snowballing also proceeded to result some of the same papers that already had been found by PoP. Duplicates were not included in the dataset of this literature review.

Another positive outcome from the snowballing is that it found several papers that had not been caught by the initial keyword search, due to for example the paper not having a searchable abstract or keywords available, and thus avoided being discovered. Thus, to provide a better foundation for data extraction, I will include papers found via the snowballing method in the library of papers. However, since this is a manual task and due to the limited resources available in this project and the seminal paper has over 2200 citations, it will not be possible to include and filter every citation. Instead, only the few top relevant citations and the citations of those papers will be included in the final library for this systematic review.

2.6 Screen and select articles

Following Kitchenham's method [19], to ensure the review is focused, comprehensive and of high quality, I applied a set of exclusion criteria to reduce the data set into only the most relevant and useable papers.

The following exclusion criteria (EC) were used:

EC 1: All 'grey' literature, such as books, book chapters, Notes, Editorials, etc. Additionally, I also exclude other literary reviews.

EC 2: All papers not covering topics related to cyber/information security culture in their title or abstract.

EC3: All papers not in English.

EC4: Duplicate papers

EC5: All papers not available via ITU access.

2.7 Extracting data from library

Kitchenham describes the need for a data collection form, to ensure each paper is handled in a systematic way during the data extraction [19]. In order to create the data collection form, once the library of papers has been reduced to only the most relevant articles, I will proceed to go through their content to extract data about how each source characterizes and contextualizes security culture.

Firstly, standard information such as title, author, year, and publication is extracted from each article to excel. Additionally for each paper, I read through the title, abstract and keywords and write down keywords for two main focus areas: What characterizes security culture in this specific paper, and what does the paper propose or conclude must be done to improve security culture? For those papers where it was not possible to extract any keywords from the abstract or title, I also incorporate the paper's conclusion and results in data extraction process. Lastly each paper is assigned a unique ID consisting of 'P' + an integer, to distinguish them from other sources and references used in this paper.

Table 1 Example of Data Collection Form

ID	Author	Title	Year	Publication	Characterizations	Improvement

P1	A. Uthor	Title	2000	Journal	Keyword1;
					Keyword2;
						Keyword 3;
						Keyword 4;

It is worth taking into account that some papers may have multiple characterizations of security cultures or improvements, and it may be necessary to write down multiple keywords separated by a semi colon.

Before proceeding, I find it highly relevant to explain in detail what I mean by characterization and Improvement when I look through the papers contents.

How a paper characterizes security culture, is based on what aspect of security culture they are examining as the status quo. i.e. what makes up security culture in the context of the specific paper. In short, the question one should ask themselves when reading the paper is "What does this paper think security culture is?"

Furthermore, the papers all present their conclusions on how security culture can improve in the future. All papers come up with a final suggestion or recommendation based on their results, which characterizes the work that will improve security culture going forward. A good question to ask while reading is "what improvement does this paper propose?"

As such I aim to uncover not just what the paper characterizes as status quo regarding security culture, but also how the paper aims to advance the status quo according to their proposed recommendations for improvements.

An example extraction of characterization and improvements could be a paper that discusses security culture in terms of how employees act in the workplace and proposes and develops a new framework for better understanding this employee behaviour. In this example the article characterizes security culture as "employee behaviour" and the suggested improvement would be "framework".

Kitchenham states that while systematic literature reviews and systematic mappings are different disciplines with different goals, albeit often with overlaps in said goals, it is sometimes needed for literature reviews to organize the review by categories accompanied by a detailed description to make better sense of ones findings [20]. As such, I will synthesize my results by organizing the papers into categories according to their characterization and suggest improvements of security culture.

3. Results & Synthesis

As a result of applying the exclusion criteria on the total dataset, the number of articles in the library was severely reduced from 214 to 122. It is also worth noting that, I did not find any papers that would have been caught by exclusion criteria 3, and thus it is not reflected in the results presented in Figure 1.

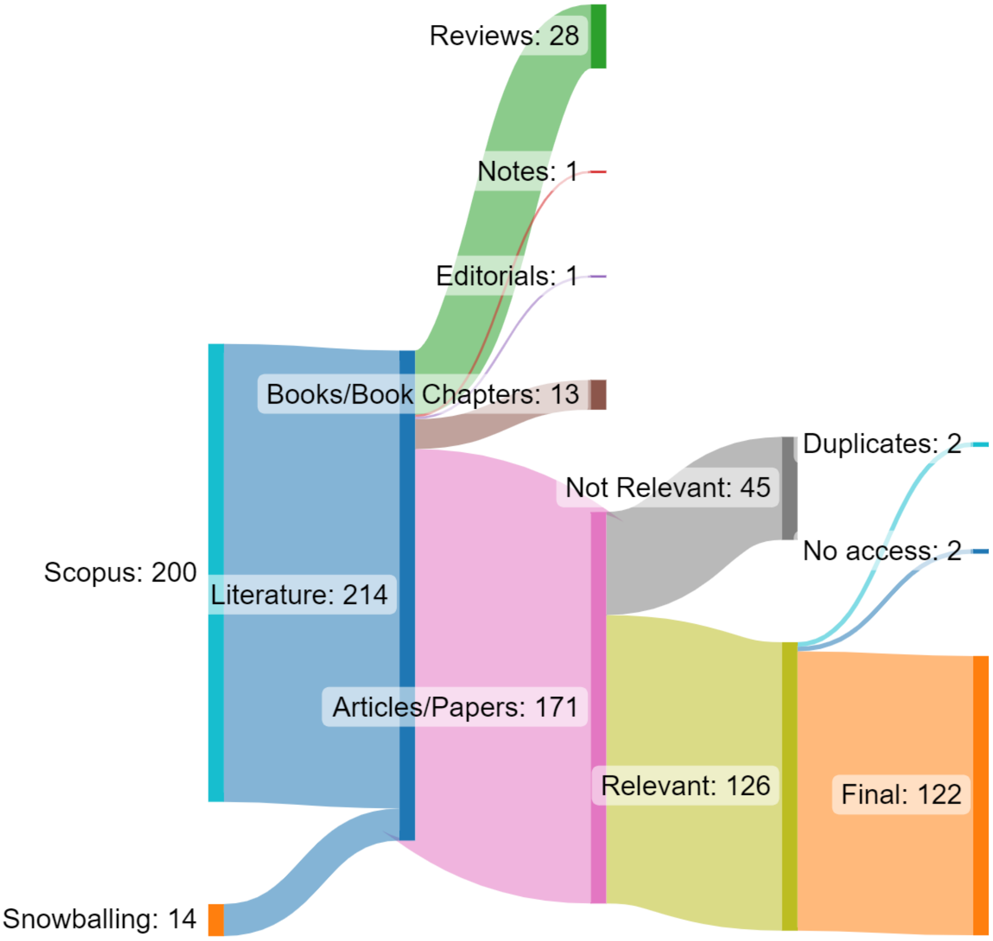

Figure 1 Systematic Review Library

For each of the 122 articles, identifying keywords for the characterization and context of security culture was noted in a data collection sheet. For characterizations 15 different keywords were found 151 times across all articles, as indeed some papers had more than one keyword as part of their characterization. For keywords on the context of security culture in the papers, 20 keywords were found 154 times across all articles.

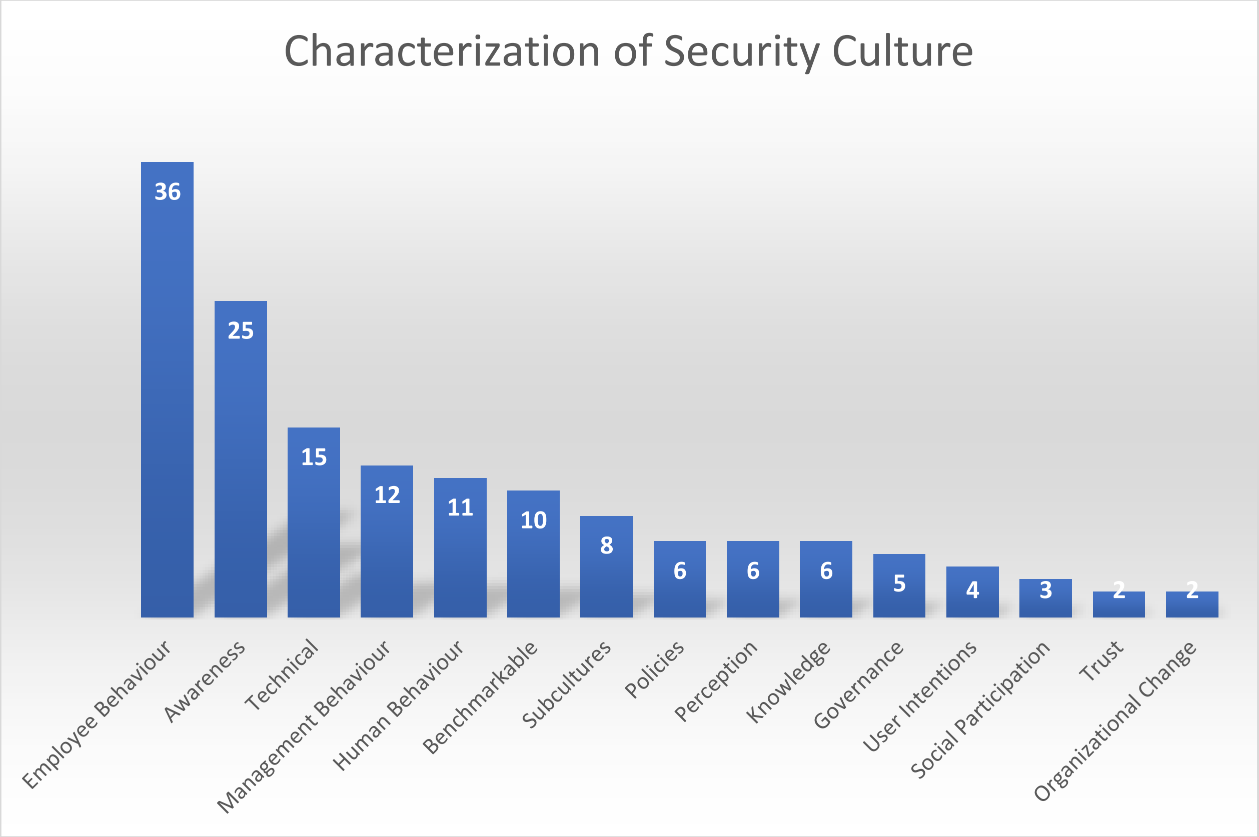

Figure 2 Characterization keywords found in papers.

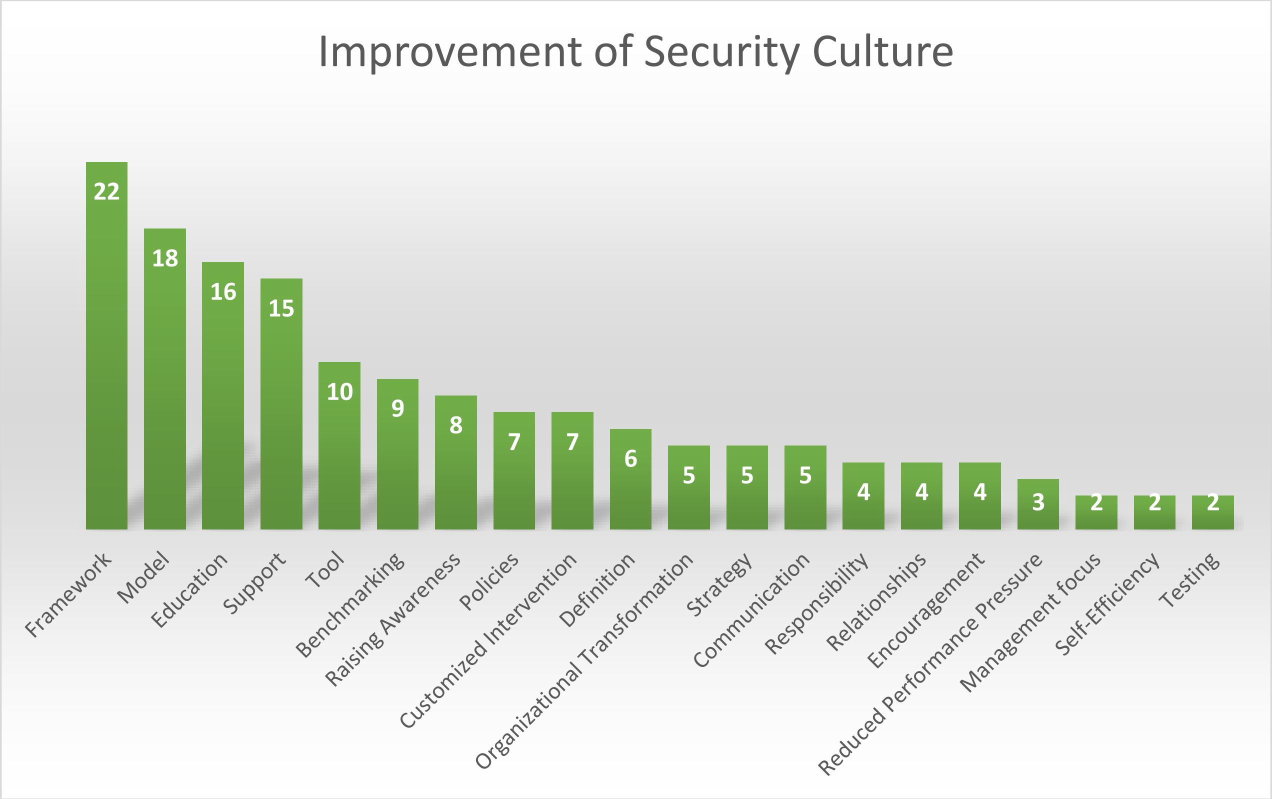

Figure 3 Improvement keywords found in papers.

3.1 Security culture categorizations

From the collected data, I was then able to condense the findings into a set of 6 distinct categories that characterizes security culture, based on the findings in the 122 articles in the dataset.

Each category makes up a defining characterization of security culture, constructed from the assigned keywords for each paper. This mapping allows for further condensation of the findings by relating each keyword to an overall category that may later be used to map the characterization in relation to the context of the paper.

#	Security Culture Characterization Categories [1]
1	**Behaviour** A large part of the dataset was identified to have behaviour as a key part of the characterization of security culture. Furthermore, it was noted that these paper can be further subcategorized into 4 different viewpoints of what constitutes behaviour in security culture. In total 58 papers focused on behaviour in security culture. **1.1. Employee Behaviour.** This characterization comes from the idea that employees are notoriously unsafe, and that in order to better understand, improve or examine security culture, one must look at how employees behave in the workplace. This was the most significant characterization with 36 out of 122 papers highlighting this aspect. **1.2. Management Behaviour.** In opposition to the above characterization, 12 papers identified the management's behaviour as the key to security culture. The argument in these papers are that employees cannot be to blame for an organization's security culture (or lack thereof), as it is the responsibility of the company management to lead by example when it comes to security culture. An example of detrimental management behaviour is when management is seen to be in violation of the security policies they set up themselves. **1.3. Human Behaviour** During the data analysis, a pattern emerged that was hard to distinguish when it came to papers dealing with behaviour in regard to security culture. While 1.1 and 1.2 clearly characterized security culture within the scope of ordinary enterprises or organizations, several papers dealt with behaviour both inside and outside of people's work relations or hierarchical position. Example of 'human behaviour' is how people act in their home sphere, how they act as users of a product or simply as a generalization of every person in an organization without regards to their role, status or expertise within the subject of cybersecurity. To sum up all these different viewpoints, I chose to combine them into the subcategory of human behaviour. 11 out of 122 papers identified this type of behaviour as a key characterization of security culture. 1.4 **User Intentions** Finally, 4 papers touched on the subject of how while a user's behaviour may be a negative influence on security culture, it is important to look at what the user's intention were when they behaved in a certain way. Thus, it becomes more important to identify why they acted in the way they did, as opposed to studying what they did.

[1] See Appendix A for a full table of the literature sources that make up the characterization categories. Some papers contain multiple characterizations of security culture, and thus appear multiple times in the list.

2	**Cybersecurity Awareness** While somewhat related to the first category, this overall category is derived from papers that deal with being aware of everything related to security. With proper knowledge of possible dangers, pitfalls, or influences, it is possible for people to create a stronger security culture. As part of this category, I identified 3 characterizations that fit under the umbrella term of cybersecurity awareness. **2.1. Awareness** The second most significant characterization of security culture within the dataset with 25 of 122 papers, and the namesake for the overall category. Noticeably this keyword was often identified in combination with employee or management behaviour, as the key motivator behind why a person behaves the way they do. However, it was also used in papers that dealt with how awareness is achieved or what constitutes awareness within security culture. **2.2. Knowledge** Knowledge in this context refers to multiple layers of important understanding that a person may have or need in regard to security culture. For example, it could be the knowledge of dangers, that could lead to gaining awareness, but in some papers it also refers to technical skills in which the user needs to have expert know-how to utilize a tool, technology or analysis in the right way. 6 papers identified knowledge as part of their characterization. **2.3. Perception** The term perception covers 6 papers that deal with how users perceive cybersecurity. While related to awareness and knowledge, the key difference is that awareness and knowledge deals with understanding aspects of security, whereas perception is how user's interpret aspects of security.
3	**Social Relations** The dataset revealed that an important aspect of security culture is the social relations between people, usually within an organization. The way that employees interact with each other is a large contributing factor that makes up the culture within the company. Furthermore, bad relations can be a major hinderance to creating a unified security culture, due to misaligned subcultures or a lack of trust between people. The category is made up of 3 subcategories identified from the dataset. **3.1. Social Participation** While not a significant portion of the dataset, 3 papers uniquely explored how social participation contributes to security culture. Employees relations with each other, as part of security improvement initiatives or policy governance, is the driving factor behind creating a strong security culture. **3.2. Subcultures** 8 papers focused on security culture as a superset made up of multiple subcultures. While each paper focuses on different aspect of what makes up a subculture, the general aspects were focused on geography, work roles, cultural background or similar. As such these papers suggest that security culture must be seen through the lens of each subculture, and not as a whole singular aspect. **3.3. Trust** Finally, 2 papers identified trust as a key factor, as mutual trust between employee's, trust between management and staff, or between users and developers, helps create a security culture where everyone takes responsibility.

4	**Organizational Management** From the perspective of 12 papers the organizational processes or the organizational management surrounding security culture was the key characterization. Companies and organizations have a multitude of ways to govern, police or otherwise influence their security culture, as identified by the three subcategories that make up the organizational management category. **4.1. Governance** Effective governance is essential for ensuring a well-defined security culture within an organization. 5 papers in the dataset focused on how good governance may lead to increased compliance and thus how important governance is in the characterization of security culture. **4.2. Policies** Closely related to governance and often in combination with management behaviour, the policies that a company sets up, naturally has a massive effect on its security culture. Good policies can be a critical success factor in creating a strong security culture, whereas bad policies or broken policies is a very negative influence on the company's security culture. In total 6 papers discussed policies regarding security culture. **4.3. Organizational Change** 2 papers identified how organizational change is a key factor in the transition process when creating, fostering, or improving security culture. As culture is not a static state, companies must be aware of how the organization handles change, in order to understand how it affects the organizations security culture.
5	**Benchmarkable** 10 papers in the dataset characterized security culture as something concretely measurable that can be benchmarked and quantified. These papers usually focus on discussing ways for academics to produce some concrete data that can be compared and analyzed over time, so that it is possible to measure the effect of various endeavors the organization more easily may take that influences its security culture.
6	**Expertise and technical disciplines** Lastly a noticeable set of papers in the dataset discussed security culture through the lens of an expert's knowledge. Generally, for these papers, they identified security culture as something that an expert should influence, rather than the average employee. This could be a classic software engineer using development method such as working with secure technologies to prevent cyberthreats, or working in framework methodologies that encourage security to be built into the software the developer produces. Similarly, it could be a CISO making up good governance policies or establishing compliance across the organization. These papers also discuss how in security culture it is irrelevant to look at the average employee's or users' behaviour, as it is up the experts to produce safe and secure software that forces the user to act in secure ways. The view of these papers often sees security culture as something carefully crafted by experts, and where users do not have the same influence the previous 5 categories would suggest. They do not mention the average employee as being completely non-influential, but simply put their focus on the expert.

69 papers were placed in only one category, 32 papers were placed in two categories, and four papers were placed in three categories. Finally, 18 papers did not contain any identifiable characterization of security culture, but did feature a relevant suggested improvements, and has been left in the dataset, keyworded as N/A.

3.2 Security culture improvements

Using the same method, I went through the collected data for the entire dataset and condensed the papers into categories that cover the suggest improvements that the papers discuss in regards to security culture and research surrounding the topic.

#	Security Culture Improvement Categories [2]
1	**Improving Research Structure** By far the largest portion of articles in the dataset was in the context of attempting to put security culture in some sort of framework, model or tool that allows for a better understanding of the subjects as well as standardize and analyze the data in a better and easier way. This category is created from 3 different keywords identified across all papers. **1.1. Framework** 22 papers dealt with security culture in the context of some sort of framework. This was either trying to come up with a new and better framework to allow other researchers in the future to better understand security culture, or the papers looked at security culture in the context of an already existing framework. **1.2 Model** Similar to the frameworks, 18 papers were published in the context of attempting to view security culture through the lens of some existing model, or trying to come up with a new model that could be used in further research. **1.3 Tool** Lastly 10 papers focused mostly on the usage or development of some tool that is meant to help organizations or researchers understand their security culture.
2	**Organizational Support** Many papers dealt with some small aspect of an organization's possibilities for helping their employees to build a better security culture within the company. In the dataset 5 different sub-contexts were identified, that each make up an aspect in which the overarching goal of the paper was to examine or explain how each context affects or can improve the security culture. **2.1. Support** While support is a very generic term that encompasses a lot of different disciplines, it was still found to be a keyword that provided a lot of value during the data collection. Papers published in the context of support mostly deals with examining how management can better provide supportive structures for their employees, or how employees can provide mutual support for each other to improve security culture. **2.2. Customized Intervention** 7 papers identified that while general support was nice, there are some cases where it is impossible to come up with general support structures that will always work within security culture. For these cases it was necessary to instead focus on customizing the intervention for each business' needs, subcultures, policies, and governance structures. **2.3. Encouragement** Closely related to 2.1, but these papers were written in the context of how management can provide encouragement in order to reinforce behaviour that is beneficial to the companies security culture. For example through verbal encouragement, monetary compensation, or some other reward structure.

[2] See Appendix B for a full table of the literature sources that make up the improvement categories. Some papers contain multiple contexts of security culture, and thus appear multiple times in the list.

	2.4. Reduced Performance pressure 3 papers dealt explicitly with how management must reduce the performance pressure they apply on their employees. If performance pressure is high, employees are more likely to take risks that could result in insecure behaviour and thus negatively impact the security culture of the company. **2.5. Self-Efficiency** Whereas the above context focuses on what management can do from a top-down perspective, self-efficiency focuses on what employees themselves can do to improve their efficiency, which can lead to reduced pressure, that in turn leads to avoiding insecure behaviour.
3	**Employee Training** It comes as no surprise that a significant number (21) of papers were written in the context of exploring and examining how employees may be better trained and educated, and how this affects the security culture within an organization. This context is made up of two distinct keywords, that offers two different viewpoints, and yet is closely related. **3.1. Awareness Raising** Given the number of papers that characterize awareness as a key aspect of security culture, it is also no surprise that multiple papers are written in the specific context of how companies may work on raising awareness of rules, threats or policies in their employees. This is usually also in the additional context of education or management support. **3.2. Education** Some papers dealt with a more overall definition of training, that I have identified under the keyword education. Most awareness raising falls under education in some form, but in this context, education is meant to cover those papers that dealt with how employees may learn or be taught some new skill, gain some knowledge or otherwise improve themselves in a way that is beneficial to the security culture of their organization.
4	**Strategic Management** All companies strive to achieve a better security culture, and indeed most papers in the dataset views security culture as something that must be handled on a strategic level by management to be improved sufficiently. 5 different keywords were identified that relates to strategic management of cybersecurity. **4.1. Policies** 7 papers touched on improving or examining how companies may create better policies regarding cybersecurity. **4.2. Organizational Transformation** As organizations change their structure, governance, policies or otherwise change, it affects security culture within the company. Some papers thus examine security culture in the context of organizational transformation and examine how it is possible to aid the transition process in terms of cybersecurity. **4.3. Strategy** On a more overall level, 5 papers elaborate on how it is necessary to have or create an overall cybersecurity culture strategy, either on a national level or organizational level, to act as a guide for how companies should evolve their security culture. **4.4. Responsibility** Taking and placing responsibility within a company when it comes to security culture is an important aspect of changing or improving said culture. Thus 4 papers examine how taking better responsibility is beneficial in terms of creating a better security culture.

	4.5. Management Focus Finally viewing security culture in the context of increasing management focus on cybersecurity as a whole. By having more focus from the top of an organization, it affects all other employees in the organization.
5	**Benchmarking and Testing** 9 papers were in the context of benchmarking some aspect of security culture. As previously explained in the characterization, these benchmarks aim to make security culture more measurable in certain metrics, and thus easier to study. Additionally 2 papers aimed to explore measurability of security culture through concrete testing as a way of providing comparable metrics.
6	**Communication and Social Relationships** The dataset contained 9 papers that dealt with the social context of security culture within an organization. Looking at security within the context of communication allows for better sharing of information, knowledge, threats, or raising awareness. With good communication you can build social relationships that act as a common understanding of the company's security culture.
7	**Definition** Finally, 6 papers were written on the context of trying to come up with a definition of security culture or more precisely a subsection of security culture. These papers find that there is a need for better definition of security culture for example within journalism or in the perspective [P110] or on a national level [P101].

102 papers fit into a single context category, 17 fit into two categories, and three papers were placed into three context categories.

3.3 Zooming in on improved research structure

Since the largest number of papers suggested improving security culture through the context of either using a framework, model, or tool (FMT), I find it highly relevant to zoom in further on this category specifically. The papers from improvement category #1 were examined by doing a keyword search for terms relating to how they applied, developed, proposed, conceptualized, integrated, evaluated, or extended their framework, model, or tool. 4 different subcategories of improvement category #1 were found.[3]

[3] See Appendix C for a full table of the literature sources that make up the subcategories for improved research structure.

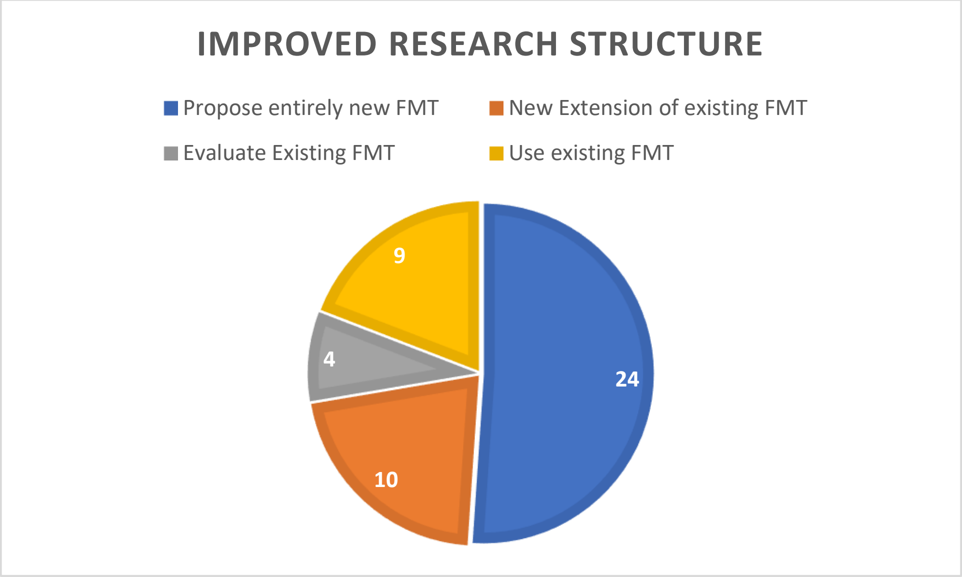

Figure 4 Chart over how papers suggest frameworks, models or tools can improve research structure.

Propose entirely new FMT. 24 papers propose the development or conceptualization an entirely new framework, model, or tool to improve future research and work on security culture. Through keyword search it was found in these papers, that 8 of them provided a foundation of validity to their proposal by applying the developed FMT either through case studies (5) or through interviews or surveys (3). In contrast 16 papers did not provide any validation of their proposal.

New Extension of existing FMT. 10 papers took their offset in some already established framework but found it to be lacking elements in the context of security culture, and thus proposed an extension of these already existing models to incorporate the missing elements. Only one of these papers put their new extended framework into use through a case study, while the remaining 9 papers were left on a theoretical level.

Evaluate Existing FMT. Only 8 papers had an explicit evaluation of what frameworks and tools already exist. Of these 3 papers came up with an entirely new framework as a result, and 1 paper proposed an extension of an already existing framework as the best course of action. Moving those papers to the above categories, it leaves 4 papers remaining did not make any conclusions regarding the need for new FMTs.

Use existing FMT. Lastly 9 papers concluded that it was possible to examine cybersecurity culture through an already existing FMT, for example by directly applying the framework on case studies.

4. Discussion

4.1 Method

Following Kitchenham's EBSE method for literature reviews, it is necessary to evaluate the performance of the review and reflect on the process. [21] I want to highlight three aspects of this review that could have been better and thus improved the validity of the results.

First, the review's initial search for papers to create the library of articles, should under the best circumstances have used additional databases. By only using one database as the basis for finding literature, there may be highly relevant papers that were not uncovered by the search, as they are only available on other databases. I try to mitigate this by also incorporating a forward snowballing method, but given more time and resources, I would have liked to verify my results by including additional databases.

Additionally, the snowballing process also had to be reduced in scope, and it was not possible to include multiple seminal papers to perform snowballing on. Given the thousands of papers that cited Adams and Sasse's paper [13], it would likely be possible to extract several tens or hundreds of relevant papers on security culture with the snowballing method, provided that enough time was given. Likely most of those papers would have been duplicates of those found via the database search, which would also have strengthened the overall confidence in the search results and final data validity.

It is also worth noting that my method in data extraction differs from the recommendation of Kitchenham [19], in that this research project only has one researcher assessing each paper, but should have used two researchers, either both doing independent data extraction and then comparing, or one researcher doing data extraction and another acting as a checker and validator [22]. To combat this weakness, I instead used my supervisors as a way of checking and validating my data extraction through discussions.

Overall there were also very successful aspects of this paper's methodology. The use of the Publish or Perish program made it very simple to test multiple strings and compare search results, as well as provide a very easy transition from search result to data extraction. Additionally the data extraction itself was done in a systematic way, and albeit slow and manual with the caveat mentioned above, it was highly rewarding and gathered a lot of insights in a structured manner.

4.2 Results and contributions

Although previous research has been done on identifying characterizing elements of security culture [11] [5], this research presented in this paper has done so on a bigger dataset, and using a different methodological approach, revealing new information that was not previously identified.

With the 6 different characterizations and 7 different improvements, it is relevant to see if there is any overlap between the categories. An overlap could indicate a high relation, but too big of an overlap could also indicate that the two different categories should be combined.

Indeed there appears to be a link between security culture as related to behaviour and awareness, indicated by 18 papers that identify both as central elements in security culture in one form or another. A majority, 75 papers, identified either behaviour, cybersecurity awareness or both as a key characterization of security culture, and only 28 papers did not mention behaviour or awareness as part of their characterization. While the remaining 4 categories are still relevant, the data points to academic literature being heavily focused on these two aspects of cybersecurity. This is in line with the previous research that identified factors of security culture, stating that awareness and behaviour are dominant factors [11].However this paper also identifies social relations as being of much bigger importance than what [11] identified.

Regarding improvements, the majority (102) only feature one focus area, and of all the papers the most significant category (47) are the papers that discuss security culture in the context of improving research structure for the future. As I went through these 47 papers in greater detail, it quickly appeared that the majority is focused on coming up with new ways of understanding and structuring the approach to security culture, rather than using existing methods from much more mature fields of science. While [5] did identify that some frameworks presented in literature are purely theoretical, this paper highlights how significant this problem is within academic literature. With only 6 out of 36 newly developed frameworks and tools having been applied through a case study, it leaves practitioners, companies, and future researchers with a big challenge of having to choose between many different options for which framework will work best for them. And with a minority of the papers applying or evaluating already existing frameworks, it begs the question if enough research has been done to establish the need for all these newly developed frameworks. These findings lead to a range of further research that will be suggested later in this paper.

In the same way that I zoomed into the frameworks, the same exercise can be done for the remaining categories to reveal underlying patterns and define further works. For example, when examining the papers that come up with a new definition, it is clear that these papers work on specific subsections of security culture. With my current method, it is not possible to determine if there exists a problem with the current overall definitions of security culture, or if these industries are just so special that they require a more refined definition. Once again, this could be a question for further research.

Lastly there appears to be no significant link between how a paper characterizes security culture, and in what improvements the paper suggested. My initial expectations were that it would be possible to see commonalities between papers, such as papers dealing with behaviour would be suggesting somewhat similar improvements going forward. However, this turned out not to be the case. This could point towards there being multiple solutions to the same problems, that there is a missing alignment amongst researchers for the most efficient solutions, or that my current research method does not correctly contain the to conclude if these links exist or not.

Based on the results, this paper contributes to the body of knowledge firstly by identifying what characterizes security culture within current academic literature through the categories presented. The results are supported by the conclusions of similar research done previously [4] [5] [9] [11], but also identifies new common categories that make for easier relation between characteristics.

Secondly this paper identifies that current academic literature has a lack of focus on evaluation and is highly focused on developing or inventing new theoretical frameworks, models, and tools. There is lacking research into applying these new tools on real cases.

While the data does not support a direct recommendation based on my results, this paper can serve as an invitation to reflection on whether it is strictly necessary to further invent new frameworks, without having first carefully evaluated the many options already out there.

4.3 Validity of data

Despite the restraints to the scope of this project, the data was collected in a systematic matter according to the literary review process. Even with the identified weak points in the data gathering process as previously discussed, steps were taken to mitigate the risks and improve the data validity. Overall, the data validity is strong enough to support a conclusion and suggest further research.

5. Future Work

Given the findings of this paper, I have defined a new range of questions that can make up further research into this area.

Why are researchers so focused on developing new frameworks, models and tools for security culture? One might wonder if the current lack of using existing frameworks is due to lack of knowledge of their existence, or because they simply do not apply to aspects of security culture. Similarly it is prudent to ask if too many newly developed frameworks pose a problem to researchers and practitioners within the security culture field? To answer these questions, I propose a qualitative study aimed at experts and researchers would be the first step to gauge the current knowledge of frameworks, models and tools available, and to evaluate how this affects their work. If it is established that a problem exists, this could also lead onto research on what steps can be taken to align users' knowledge on what frameworks are best used in their case, or when it is necessary to develop something new.

In a wider perspective, it would be prudent to answer if this is a unique problem within the field of cybersecurity culture, or is it also present in other fields of research? A systematic literature review on usage and development of frameworks, tools, and models within other fields of research could provide an answer.

Finally, this paper's improvement categories could be the jumping off point for research into other aspects of proposed improvements. For example, zooming in on how academic literature proposes to improve cybersecurity education could reveal interesting patterns similar to those revealed within frameworks by this paper.

6. Conclusion

This study developed a comprehensive list of categories for both characterization and context of security culture within academic literature, by performing a systematic literature review.

The literary review has found that across 122 relevant academic articles, it was possible to identify 6 different characterizations of security culture and 7 different categories for improvement of security culture.

The most significant characterizations of security culture were behaviour and cybersecurity awareness with half of the academic literature featuring either one or both of the characterizations in their writing. The most significant improvement regarding security culture were papers aiming to improve research structure through models, frameworks or tools, and papers examining how a organizational support may affect security culture.

This paper identified that currently academic literature has a significant focus on developing or extending new frameworks, models, and tools to better understand security culture, while there is very little work done into evaluating and using already existing frameworks, models and tools. The status of current suggestions of improvements in research structure presents a trend leaning towards inventing new frameworks, models and tools that may prove problematic.

Based on these findings, this paper serves as an invitation to reflection on the need to develop new frameworks, tools or models, as opposed to evaluating and using the ones already available and tested in practice previously.

Finally, this paper proposes new research is done into finding out why academic literature seems to prefer developing new frameworks rather than using the current ones already existing, and examining whether the current status poses a problem across other topics.

7. References

[1] S. &. C. N. Furnell, "Power to the people? The evolving recognition of human aspects of security.," *computers & security,* vol. 31, no. 8, pp. 983-988, 2012.

[2] A. A. L. V. B. A. &. H. M. Da Veiga, "Defining organisational information security culture—Perspectives from academia and industry," *Computers & Security,* vol. 92, 2020.

[3] B. A. Kitchenham, D. Budgeon and P. Brereton, Evidence-Based Software Engineering and Systematic Reviews, Boca Raton: CRC Press, 2016.

[4] S. AlGhamdi and E. V.-G. Win Khin Than, "Information security governance challenges and critical success factors: Systematic review," *Computers & Security,* December 2020.

[5] B. Uchendu, J. R. Nurse, M. Bada and S. Furnell, "Developing a cyber security culture: Current practices and future needs," *Computers & Security,* October 2021.

[6] M. Sanchez-Gordon and R. Colomo-Palacios, "Security as Culture: A Systematic Literature Review of DevSecOps," *Proceedings - 2020 IEEE/ACM 42nd International Conference on Software Engineering Workshops, ICSEW 2020,* pp. 266-269, 2020.

[7] S. Kalhoro, M. Rehman, V. Ponnusamy and F. Shaikh, "Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review," *IEEE Access,* January 2021.

[8] N. H. Hassan, N. Maarop, Z. Ismail and W. Z. Abidin, "Information security culture in health informatics environment: A qualitative approach," *2017 5th International Conference on Research and Innovation in Information Systems (ICRIIS),* July 2017.

[9] S. Orehek and G. Petric, "A systematic review of scales for measuring information security culture," *Information and Computer Security,* pp. 133-158, May 2021.

[10] A. Mahfuth, S. Yussof, A. A. Baker and N. Ali, "A Systematic Literature Review: Information Security," *2017 International Conference on Research and Innovation in Information Systems (ICRIIS),* pp. 46-52, 2017.

[11] E. N. Mwim and J. Mtsweni, "Systematic Review of Factors that Influencethe Cybersecurity Culture," *IFIP International Federation for Information Processing 2022,* pp. 147-172, July 2022.

[12] A. Harzing, "Publish or Perish," [Online]. Available: https://harzing.com/resources/publish-or-perish.

[13] A. Adams and A. Sasse, "Users Are Not the Enemy," *Communications of the ACM,* pp. 40-46, December 1999.

[14] T. &. T. S. Schlienger, "INFORMATION SECURITY CULTURE," *Security in the Information Society,* pp. 191-201, 2002.

[15] D. Ashenden and A. Sasse, "CISOs and organisational culture: Their own worst enemy?," *Computers & Security,* pp. 396-405, November 2013.

[16] A. Sasse, "Scaring and Bullying People into Security Won't Work," *IEEE Security & Privacy,* pp. 80-83, 2015.

[17] A. Adams and a. Blandford, "Bridging the gap between organizational and user perspectives of security in the clinical domain," *International Journal of Human-Computer Studies,* pp. 175-202, July 2005.

[18] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Computers & Security,* November 2020.

[19] B. Kitchenham, Procedures for Performing Systematic Reviews, Keele: Keele University, 2004, pp. 1-26.

[20] B. Kitchenham, D. Budgen and O. Brereton, "The value of mapping studies – A participant observer case study," *Proceedings of the 14th International Conference on Evaluation and Assessment in Software Engineering,* pp. 25-33, 2010.

[21] B. A. Kitchenham, T. Dybå and M. Jørgensen, "Evidence-Based Software Engineering for Practitioners," *IEEE Software,* no. 05, pp. 58-65, 2005.

[22] B. A. B. P. B. D. T. M. &. K. M. Kitchenham, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of systems and software,* pp. 571-583, 2007.

8. Dataset References

[P1] A. Da Veiga, "A framework and assessment instrument for information security culture," Computers and Security, 2010.

[P2] J.F. Van Niekerk, "Information security culture: A management perspective," Computers and Security, 2010.

[P3] K. Knapp, "Information security: Management's effect on culture and policy," Information Management and Computer Security, 2006.

[P4] A. Da Veiga, "An information security governance framework," Information Systems Management, 2007.

[P5] A.B. Ruighaver, "Organisational security culture: Extending the end-user perspective," Computers and Security, 2007.

[P6] R. Von Solms, "From policies to culture," Computers and Security, 2004.

[P7] K.L. Thomson, "Cultivating an organizational information security culture," Computer Fraud and Security, 2006.

[P8] A. Martins, "Information security culture," IFIP Advances in Information and Communication Technology, 2002.

[P9] J. D'Arcy, "Security culture and the employment relationship as drivers of employees' security compliance," Information Management and Computer Security, 2014.

[P10] S. Kraemer, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists," Applied Ergonomics, 2007.

[P11] A. Alhogail, "Design and validation of information security culture framework," Computers in Human Behavior, 2015.

[P12] T. Schlienger, "Analyzing information security culture: Increased trust by an appropriate information security culture," Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2003.

[P13] A. Da Veiga, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," Computers and Security, 2015.

[P14] Y. Chen, "Impacts of comprehensive information security programs on information security culture," Journal of Computer Information Systems, 2015.

[P15] T. Schlienger, "Information security culture the socio-cultural dimension in information security management," IFIP Advances in Information and Communication Technology, 2002.

[P16] A. Wiley, "More than the individual: Examining the relationship between culture and Information Security Awareness," Computers and Security, 2020.

[P17] W. Rocha Flores, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," Computers and Security, 2016.

[P18] S. Talib, "An analysis of information security awareness within home and work environments," ARES 2010 - 5th International Conference on Availability, Reliability, and Security, 2010.

[P19] S. Alfawaz, "Information security culture: A behaviour compliance conceptual framework," Conferences in Research and Practice in Information Technology Series, 2010.

[P20] D. Lacey, "Understanding and transforming organizational security culture," Information Management &amp; Computer Security, 2010.

[P21] A. Da Veiga, "Information security culture and information protection culture: A validated assessment instrument," Computer Law and Security Review, 2015.

[P22] G. Dhillon, "Interpreting information security culture: An organizational transformation case study," Computers and Security, 2016.

[P23] M. Tang, "The impacts of organizational culture on information security culture: a case study," Information Technology and Management, 2016.

[P24] K.M. Parsons, "The influence of organizational information security culture on information security decision making," Journal of Cognitive Engineering and Decision Making, 2015.

[P25] A. da Veiga, "Defining organisational information security culture - Perspectives from academia and industry," Computers and Security, 2020.

[P26] L. Drevin, "Value-focused assessment of ICT security awareness in an academic environment," Computers and Security, 2007.

[P27] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Computers and Security, 2020.

[P28] A. da Veiga, "Defining and identifying dominant information security cultures and subcultures," Computers and Security, 2017.

[P29] S. Dojkovski, "Fostering information security culture in small and medium size enterprises: An interpretive study in australia," Proceedings of the 15th European Conference on Information Systems, ECIS 2007, 2007.

[P30] J.S. Lim, "Embedding information security culture emerging concerns and challenges," PACIS 2010 - 14th Pacific Asia Conference on Information Systems, 2010.

[P31] P.A.H. Williams, "In a 'trusting' environment, everyone is responsible for information security," Information Security Technical Report, 2008.

[P32] K.J. Knapp, "Information Security Effectiveness: Conceptualization and Validation of a Theory," International Journal of Information Security and Privacy (IJISP), 2007.

[P33] J.S. Lim, "Exploring the relationship between organizational culture and information security culture," Proceedings of the 7th Australian Information Security Management Conference, 2009.

[P34] N. Gaunt, "Practical approaches to creating a security culture," International Journal of Medical Informatics, 2000.

[P35] T. Helokunnas, "Information Security Culture in a Value Net," IEEE International Engineering Management Conference, 2003.

[P36] A. Da Veiga, "Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study," Information and Computer Security, 2016.

[P37] S. Ramachandran, "Information security cultures of four professions: A comparative study," Proceedings of the Annual Hawaii International Conference on System Sciences, 2008.

[P38] A. Da Veiga, "A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument," Proceedings of 2016 SAI Computing Conference, SAI 2016, 2016.

[P39] N. Alharbi, "The impact of security and its antecedents in behaviour intention of using e-government services," Behaviour and Information Technology, 2017.

[P40] D. Gritzalis, "A baseline security policy for distributed healthcare information systems," Computers and Security, 1997.

[P41] H.U. Khan, "Violators versus non-violators of information security measures in organizations - A study of distinguishing factors," Journal of Organizational Computing and Electronic Commerce, 2019.

[P42] A. AlKalbani, "Organisational security culture and information security compliance for e-government development: The moderating effect of social pressure," Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings, 2015.

[P43] M. A. Alnatheer, "Information security culture critical success factors," Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015, 2015.

[P44] O. Zakaria, "Internalisation of information security culture amongst employees through basic security knowledge," IFIP International Federation for Information Processing, 2006.

[P45] N. Tomas, "An empirical study on culture, automation, measurement, and sharing of DevSecOps," 2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019, 2019.

[P46] R. Sabillon, "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)," Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017, 2018.

[P47] L. Ngo, "Understanding transition towards information security culture change," Proceedings of 3rd Australian Information Security Management Conference, 2005.

[P48] N. Gaunt, "Installing an appropriate information security policy," International Journal of Medical Informatics, 1998.

[P49] R. Reid, "From information security to cyber security cultures," 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference, 2014.

[P50] T. Schlienger, "Tool supported management of information security culture: Application in a private bank," IFIP Advances in Information and Communication Technology, 2005.

[P51] I. Okere, "Assessing information security culture: A critical analysis of current approaches," 2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference, 2012.

[P52] K. Koh, "Security governance: Its impact on security culture," Proceedings of 3rd Australian Information Security Management Conference, 2005.

[P53] K.A. Alshare, "Information security policy compliance: a higher education case study," Information and Computer Security, 2018.

[P54] S. Ramachandran, "Variations in information security cultures across professions: A qualitative study," Communications of the Association for Information Systems, 2013.

[P55] J.M. Haney, ""We make it a big deal in the company": Security mindsets in organizations that develop cryptographic products," Proceedings of the 14th Symposium on Usable Privacy and Security, SOUPS 2018, 2019.

[P56] R.M. Clark, "Protecting drinking water utilities from cyberthreats," Journal - American Water Works Association, 2017.

[P57] K. Dong, "The effect of organizational information security climate on information security policy compliance: the mediating effect of social bonding towards healthcare nurses," Sustainability (Switzerland), 2021.

[P58] A. McCormac, "The effect of resilience and job stress on information security awareness," Information and Computer Security, 2018.

[P59] J. Malcolmson, "What is security culture? Does it differ in content from general organisational culture?," Proceedings - International Carnahan Conference on Security Technology, 2009.

[P60] A. Georgiadou, "Assessing mitre att&ck risk using a cyber-security culture framework," Sensors, 2021.

[P61] A. Georgiadou, "Working from home during COVID-19 crisis: a cyber security culture assessment survey," Security Journal, 2022.

[P62] A. Da Veiga, "An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture," Information and Computer Security, 2018.

[P63] A. Gagné, "Identifying differences between security and other IT professionals: A qualitative analysis," Proceedings of the 2nd International Symposium on Human Aspects of Information Security and Assurance, HAISA 2008, 2008.

[P64] A. Morton, "Privacy is a process, not a PET a theory for effective privacy practice," Proceedings New Security Paradigms Workshop, 2012.

[P65] S. Dojkovski, "Enabling information security culture: Influences and challenges for Australian SMEs," ACIS 2010 Proceedings - 21st Australasian Conference on Information Systems, 2010.

[P66] K. Renaud, "Health service employees and information security policies: An uneasy partnership?," Information Management and Computer Security, 2012.

[P67] S. Kraemer, "Computer and information security culture: Findings from two studies," Proceedings of the Human Factors and Ergonomics Society, 2005.

[P68] F. Nel, "Key elements of an information security culture in organisations," Information and Computer Security, 2019.

[P69] B. Green, "On the significance of process comprehension for conducting targeted ICS attacks," CPS-SPC 2017 - Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, co-located with CCS 2017, 2017.

[P70] T.C.C. Tan, "Information security governance: When compliance becomes more important than security," IFIP Advances in Information and Communication Technology, 2010.

[P71] N. Martins, "An Information security culture model validated with structural equation modelling," Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.

[P72] I. Lopes, "Understanding information security culture: A survey in small and medium sized enterprises," Advances in Intelligent Systems and Computing, 2014.

[P73] M. Silic, "Factors impacting information governance in the mobile device dual?use context," Records Management Journal, 2013.

[P74] S. Dojkovski, "Challenges in fostering an information security culture in australian small and medium sized enterprises," 5th European Conference on Information Warfare and Security 2006, ECIW 2006, 2006.

[P75] C. Willems, "A distributed virtual laboratory architecture for cybersecurity training," 2011 International Conference for Internet Technology and Secured Transactions, ICITST 2011, 2011.

[P76] S. Ghernouti-Hélie, "A national strategy for an effective cybersecurity approach and culture," ARES 2010 - 5th International Conference on Availability, Reliability, and Security, 2010.

[P77] A. Nasir, "Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework," ACM International Conference Proceeding Series, 2017.

[P78] N. Gcaza, "A strategy for a cybersecurity culture: A South African perspective," Electronic Journal of Information Systems in Developing Countries, 2017.

[P79] A. Da Veiga, "The influence of information security policies on information security culture: Illustrated through a case study," Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.

[P80] E. Kolkowska, "Security subcultures in an organization-exploring value conflicts," 19th European Conference on Information Systems, ECIS 2011, 2011.

[P81] N. Gcaza, "A general morphological analysis: Delineating a cyber-security culture," Information and Computer Security, 2017.

[P82] A. Alkalbani, "Conceptual framework for information security in public organizations for e-government development," Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014, 2014.

[P83] A.A. Hogail, "Cultivating and assessing an organizational information security culture; an empirical study," International Journal of Security and its Applications, 2015.

[P84] C. Oehri, "Social media security culture," 2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference, 2012.

[P85] A.B. Ruighaver, "Ethical decision making: Improving the quality of acceptable use policies," Computers and Security, 2010.

[P86] T. Damenu, "Analysing information security in a bank using soft systems methodology," Information and Computer Security, 2017.

[P87] O. Beris, "Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors," ACM International Conference Proceeding Series, 2015.

[P88] K. Huang, "For what technology can't fix: Building a model of organizational cybersecurity culture," Proceedings of the Annual Hawaii International Conference on System Sciences, 2019.

[P89] A. Nasir, "A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions," Information Security Journal, 2019.

[P90] S. Talib, "Establishing a personalized information security culture," International Journal of Mobile Computing and Multimedia Communications, 2011.

[P91] T. Steyn, "Identity theft - Empirical evidence from a phishing exercise," IFIP International Federation for Information Processing, 2007.

[P92] O. Drozd, "Development of ICT Models in Area of Safety Education," 2020 IEEE East-West Design and Test Symposium, EWDTS 2020 - Proceedings, 2020.

[P93] C. Weir, "Interventions for long-term software security: Creating a lightweight program of assurance techniques for developers," Software - Practice and Experience, 2020.

[P94] T. Fagade, "Security by compliance? A study of insider threat implications for Nigerian banks," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016.

[P95] E. Sherif, "Awareness, behaviour and culture: The ABC in cultivating security compliance," 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015, 2016.

[P96] G. Božić, "The role of a stress model in the development of information security culture," MIPRO 2012 - 35th International Convention on Information and Communication Technology, Electronics and Microelectronics - Proceedings, 2012.

[P97] B. James W, "Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers," Proceedings of the Annual Hawaii International Conference on System Sciences, 2011.

[P98] L.Y. Connolly, "Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees," Information Systems Management, 2019.

[P99] Y. Ahmed, "Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems," International Symposium on Medical Information and Communication Technology, ISMICT, 2019.

[P100] T. Sommestad, "Work-related groups and information security policy compliance," Information and Computer Security, 2018.

[P101] N. Gcaza, "An ontology for a national cyber-security culture environment," Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.

[P102] A. Santos-Olmo, "The importance of the security culture in SMEs as regards the correct management of the security of their assets," Future Internet, 2016.

[P103] S. Govender, "The influence of national culture on information security culture," 2016 IST-Africa Conference, IST-Africa 2016, 2016.

[P104] A. Da Veiga, "Information security culture: A comparative analysis of four assessments," Proceedings of the 8th European Conference on Information Management and Evaluation, ECIME 2014, 2014.

[P105] K. Renaud, "The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014.

[P106] L. Astakhova, "The concept of the information-security culture," Scientific and Technical Information Processing, 2014.

[P107] S. Fenz, "A community knowledge base for IT security," IT Professional, 2011.

[P108] A. Georgiadou, "A Cyber-Security Culture Framework for Assessing Organization Readiness," Journal of Computer Information Systems, 2022.

[P109] G. Solomon, "The influence of organisational culture and information security culture on employee compliance behaviour," Journal of Enterprise Information Management, 2020.

[P110] M. Crete-Nishihata, "The Information Security Cultures of Journalism," Digital Journalism, 2020.

[P111] D. Ashenden, A. Sasse, "CISOs and organisational culture: Their own worst enemy," Computers & Security, 2013.

[P112] A. Sasse, "Scaring and Bullying People into Security Won't Work," IEEE Security & Privacy, 2015.

[P113] A. Adams, a. Blandford, "Bridging the gap between organizational and user perspectives of security in the clinical domain," International Journal of Human-Computer Studies, 2005.

[P114] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Computers & Security, 2020.

[P115] Da Veiga, A., & Martins, N., "Improving the information security culture through monitoring and implementation actions illustrated through a case study," Computers & Security, 2015.

[P116] Da Veiga, Adele, et a, "Defining organisational information security culture - Perspectives from academia and industry," Computers & Security, 2020.

[P117] Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S., " Developing a cyber security culture: Current practices and future needs," Computers & Security, 2021.

[P118] A. Da Veiga, "An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture," Information and Computer Security, 2018.

[P119] Wiley, A., McCormac, A., & Calic, D., "More than the individual: Examining the relationship between culture and Information Security Awareness," Computers & Security, 2020.

[P120] Ion, I., Reeder, R., & Consolvo, S., "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices.," Symposium on Usable Privacy and Security, 2015.

[P121] Alshaikh, M., & Adamson, B, "From awareness to influence: toward a model for improving employees' security behaviour," Personal and Ubiquitous Computing, 2021.

[P122] Adams, A., & Sasse, M. A, "Users are not the enemy," Communications of the ACM, 1999.

Appendix A

Categorization references for security culture characterizations

Category #	Literature reference
1.1	[P1], [P2], [P6], [P7], [P8], [P9], [P11], [P13], [P17], [P18], [P23], [P24], [P27], [P30], [P33], [P34], [P51], [P53], [P58], [P59], [P76], [P79], [P87], [P89], [P90], [P91], [P94], [P95], [P98], [P105], [P109], [P114], [P115], [P116], [P121]
1.2	[P3], [P5], [P25], [P32], [P42], [P43], [P67], [P71], [P73], [P94], [P97], [P117]
1.3	[P15], [P21], [P61], [P62], [P65], [P84], [P88], [P96], [P112], [P120], [P122]
1.4	[P10], [P15], [P59], [P105]
2.1	[P20], [P25], [P26], [P28], [P31], [P34], [P36], [P42], [P43], [P46], [P48], [P49], [P71], [P74], [P79], [P86], [P90], [P91], [P95], [P97], [P113], [P116], [P117], [P119], [P121]
2.2	[P20], [P44], [P49], [P65], [P75], [P116]
2.3	[P39], [P41], [P45], [P87], [P100], [P118]
3.1	[P52], [P67], [P114]
3.2	[P28], [P37], [P54], [P72], [P80], [P98], [P103], [P110]
3.3	[P31], [P39]
4.1	[P52], [P70], [P73], [P76], [P86]

4.2	[P22], [P40], [P43], [P66], [P71], [P117]
4.3	[P47], [P76]
5	[P4], [P12], [P14], [P16], [P35], [P38], [P81], [P99], [P108], [P119]
6	[P22], [P45], [P54], [P55], [P56], [P61], [P63], [P69], [P75], [P76], [P88], [P92], [P93], [P120], [P122]
N/A	[P19], [P29], [P50], [P57], [P60], [P64], [P68], [P77], [P78], [P82], [P83], [P85], [P101], [P102], [P104], [P106], [P107], [P111]

Appendix B

Categorization references for security culture improvements

Category #	Literature reference.
1.1	[P1], [P2], [P4], [P5], [P8], [P10], [P11], [P19], [P29], [P33], [P60], [P64], [P65], [P68], [P77], [P82], [P83], [P87], [P92], [P95], [P103], [P108]
1.2	[P14], [P38], [P46], [P47], [P63], [P71], [P84], [P86], [P88], [P89], [P92], [P102], [P105], [P108], [P109], [P115], [P119], [P121]
1.3	[P12], [P21], [P50], [P59], [P75], [P80], [P84], [P107], [P112], [P120]
2.1	[P3], [P15], [P23], [P25], [P27], [P29], [P34], [P42], [P43], [P55], [P66], [P67], [P73], [P74], [P97], [P117]
2.2	[P28], [P37], [P40], [P70], [P98], [P100], [P118]
2.3	[P23], [P24], [P25], [P53]
2.4	[P54], [P58], [P66]
2.5	[P96], [P97]
3.1	[P1], [P18], [P20], [P27], [P39], [P42], [P43], [P56], [P61], [P122]
3.2	[P6], [P7], [P20], [P29], [P32], [P43], [P45], [P53], [P56], [P58], [P67], [P73], [P90], [P91], [P93], [P104]
4.1	[P32], [P39], [P40], [P43], [P48], [P79], [P85]
4.2	[P17], [P30], [P62], [P76], [P118]
4.3	[P22], [P76], [P78], [P81]
4.4	[P26], [P31], [P52], [P72]
4.5	[P16], [P34]
5	[P12], [P13], [P14], [P36], [P41], [P51], [P69], [P91], [P99], [P115], [P119]
6	[P9], [P25], [P27], [P35], [P57], [P94], [P111], [P113], [P114]
7	[P44], [P49], [P101], [P106], [P110], [P116]

Appendix C

References for improved research structure

Propose entirely new FMT.	[P1], [P4], [P8], [P12], [P19], [P38], [P46], [P47], [P50], [P59], [P63], [P64], [P65], [P71], [P75], [P82], [P84], [P88], [P89], [P95], [P105], [P107], [P108], [P109]
New Extension of existing FMT.	[P2], [P5], [P10], [P11], [P14], [P21], [P33], [P68], [P77], [P87]
Evaluate Existing FMT.	[P60], [P92], [P103], [P112]
Use existing FMT.	[P80], [P83], [P86], [P102], [P115], [P119], [P120], [P121]