UNIVERSITY OF THE AEGEAN

School of Engineering
Department of Information & Communication Systems Engineering
Karlovassi, Samos
Greece

Master Thesis

Identifying the role of biases in the Internalization of Information Security Policies

by

Olga Thanou

February 2021

Η Διπλωματική Εργασία
παρουσιάστηκε ενώπιον
του Διδακτικού Προσωπικού του
Πανεπιστημίου Αιγαίου

Σε Μερική Εκπλήρωση
των Απαιτήσεων για το Δίπλωμα του
Μηχανικού Πληροφοριακών και Επικοινωνιακών Συστημάτων

της
ΘΑΝΟΥ ΟΛΓΑΣ
ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2021

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΠΙΚΥΡΩΝΕΙ
ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΤΗΣ ΘΑΝΟΥ ΟΛΓΑΣ:

ΚΟΚΟΛΑΚΗΣ ΣΠΥΡΟΣ, Καθηγητής, Επιβλέπων Ημερομηνία
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΚΑΡΥΔΑ ΜΑΡΙΑ, Αναπληρώτρια Καθηγήτρια, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΤΣΩΧΟΥ ΑΓΓΕΛΙΚΗ, Επίκουρη Καθηγήτρια, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2021

Περίληψη

Ο στόχος της παρούσας εργασίας είναι η δημιουργία μιας μεθόδου για τον εντοπισμό των πολιτισμικών προκαταλήψεων των υπαλλήλων ενός τυπικού οργανισμού ώστε να τους ταξινομήσουμε σε τέσσερις πολιτισμικές ομάδες και συγκεκριμένα σε ιεραρχιστές (hierarchists), ισονομιστές (egalitarians), ατομικιστές (individualists), και μοιρολάτρες (fatalists).

Οι πολιτισμικές προκαταλήψεις των ατόμων μπορούν να εξηγήσουν τη διακύμανση των αντιλήψεων κινδύνου μεταξύ τους και οι διαφορετικές πολιτισμικές ομάδες μπορεί να σχετίζονται με ανησυχία ή έλλειψη ανησυχίας. Τα άτομα αντιλαμβάνονται τους κινδύνους διαφορετικά και οι ομοιότητες των ατομικών αξιών προέρχονται από παρόμοια κοινωνικά υπόβαθρα. Ως εκ τούτου, πιστεύουμε ότι ο προσδιορισμός των πολιτισμικών προκαταλήψεων των ατόμων είναι εφικτός και θα μπορούσε να μας προσφέρει μερικές χρήσιμες πληροφορίες σχετικά με τη συμπεριφορά τους όσον αφορά την ασφάλεια των πληροφοριών εντός ενός οργανισμού.

Οι πολιτισμικοί παράγοντες των ατόμων έχουν μεγάλη σημασία και πρέπει να λαμβάνονται υπόψη κατά το σχεδιασμό προγραμμάτων ενημερότητας σχετικά με την ασφάλεια των πληροφοριών. Για το λόγο αυτό, δημιουργήσαμε μια μέθοδο, την ICBU-Q για τον εντοπισμό των πολιτισμικών προκαταλήψεων των υπαλλήλων ενός οργανισμού που σχετίζονται με την ασφάλεια των Πληροφοριακών Συστημάτων. Δεδομένου ότι τα άτομα θεωρούνται ο πιο αδύναμος κρίκος στην ασφάλεια των πληροφοριών, ο εντοπισμός των πολιτισμικών τους προκαταλήψεων θα μπορούσε να παρέχει χρήσιμες πληροφορίες για τη συμπεριφορά τους σχετικά με την ασφάλεια των πληροφοριών που μπορούν να χρησιμοποιηθούν για να δημιουργηθούν στοχευμένες παρεμβάσεις.

Λεξεις Κλειδιά – Προγράμματα Ενημερότητας Ασφάλειας, Αντιλήψεις Κινδύνου στην Ασφάλεια Πληροφοριών, Συμπεριφορά στην Ασφάλεια Πληροφοριών, Πολιτισμικές Προκαταλήψεις των Χρηστών, Ερωτηματολόγιο.

Abstract

The present Thesis aims to create a method for identifying the cultural biases of a typical organization's employees in order to classify them into four cultural groups, namely hierarchists, egalitarians, individualists, and fatalists.

The cultural biases of individuals can explain the variation in perceptions of risk between them, and different cultural groups can be associated with concern or lack of concern. Individuals perceive risks differently and the similarities of individual values stem from similar social backgrounds. Therefore, we believe that identifying individuals' cultural biases is feasible and could provide us with some useful information about their information security behavior within an organization.

Individuals' cultural biases are very important and should be taken into account when designing information security awareness programs. For this reason, we have created a method, namely the ICBU-Q, to detect the cultural biases of an organization's employees related to Information Systems security. As individuals are considered the weakest link in information security, identifying their cultural biases could provide useful information about their information security behavior that can be used to create targeted interventions.

Keywords – Information Security Awareness Programs, Information Security Risk Perceptions, Information Security Behavior, Cultural biases, Questionnaire.

[OLGA THANOU]
Department of Information and Communication Systems Engineering
UNIVERSITY OF THE AEGEAN

Ευχαριστίες - Αφιερώσεις

Θα ήθελα να ευχαριστήσω την αναπληρώτρια καθηγήτρια, κα Μαρία Καρύδα για τις πάντα εύστοχες και πολύτιμες συμβουλές και παρατηρήσεις της, καθώς και για την βοήθειά της σε όλη την διάρκεια της παρούσας εργασίας. Ευχαριστώ πολύ τον κ. Ιωάννη Στύλιο για τη βοήθειά του και τις πολύτιμες συμβουλές και παρατηρήσεις του. Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για την πλήρη στήριξή τους στην ολοκλήρωση της διαδικασίας συγγραφής της παρούσας εργασίας καθώς και σε όλη την πορεία του μεταπτυχιακού προγράμματος.

Στην Alice.

Πίνακας Περιεχομένων

1 Introduction

Awareness programs include activities that aim to keep users "informed" about security issues and policies. The widely used security awareness standards and guidelines (1998 NIST 800-16 [1], 2009 ENISA [2], 2003 NIST 800-50 [3], 2013 NIST 800-53 [4]), provide guidance on developing material that informs employees about the importance of information security and the content of security policies. The standards and guidelines focus mainly on the procedures and content of the awareness program, addressing the question "What behavior do we want to reinforce?" (NIST, 2003 [3]). Awareness programs are designed by following the assumption that users fail to adopt secure practices either because they are unaware of the risks or because they do not understand the consequences of security breaches or because they do not understand how to act. However, security standards and guidelines do not take into account whether knowledge of the information material will lead to improved security behavior.

Transforming security behavior goes beyond gaining knowledge about security policies and recognizing the importance of security. Research on security policy compliance (e.g., [5, 6, 7]) shows that, in order to influence user security behavior, we need to influence the way users perceive security-related risks. Awareness programs should go beyond simply communicating security-related information and align with the individual decision-making process. In the work of [8], it was shown that programs based on one-way transmission of predefined content are not suitable for security awareness.

The Information Systems' security managers should, during their practice on security awareness, enhance security behavior in addition to informing the personnel only about the security behavior policy. To do this, we need to understand how individuals incorporate security awareness information to shape security-related decision-making. Therefore, we aim to create a method for the identification of a typical organization's employees' cultural biases and to classify them into four groups, namely, fatalists, hierarchists, individualists and egalitarians. We will concentrate on the behavior and attitudes of the employees which can be measured through their perceptions [81].

1.1 Subject of the Thesis

The present thesis aims to create a method for the identification of cultural biases of a typical organization' s employees. For this reason, we have carried out a literature review on topics including the following: Information Security Awareness Programs, Information Security Risk Perceptions, Information Security Behavior and Cultural biases to identify the issues related to the aim of our work. In the literature review, we present a collection of selected published sources relevant to the topic of the thesis, which is accompanied by annotation, the main conclusions of each study, and critical analysis of contents. Our findings show that in a large corpus of research the cultural biases of individuals regarding information security behavior are overlooked and not considered when designing information security awareness programs. In addition, while there are a few methods for the investigation of information security behavior, up to our knowledge, none of them identifies the cultural biases in organizations' personnel. Therefore, we have developed a method, namely the ICBU-Q (Identification of Cultural Biases of Users - Questionnaire), to identify the cultural biases of an organization' s employees regarding information security awareness and to classify them into four groups, namely, fatalists, hierarchists, individualists and egalitarians. Finally, there is a lack of targeted information security awareness programs that consider the cultural biases of organizations' employees. Therefore, our method can help towards the identification of an organization's employees' cultural biases and assist in creating targeted interventions.

Afterward, a grouping of the gathered literature sources took place, based on some of their common characteristics, such as the research problem, the goals/ objectives, the research approach, the findings, etc.

1.2 Contribution

The purpose of the literature review is the critical analysis of the contents and the detection of possible gaps in the literature on the particular subject/ topic. Our aim is to see the most common research methods in the field in order to develop a method for the classification of Information Systems' users according to their cultural biases. Following we develop our model and our method.

1.3 Organization of the Thesis

In Chapter 2 we present the Literature review as well as the Method and Scope of the literature review. Also, we refer to Information Security Policies in Organizations, the concept of Information Security Policies, the human factor in Information Security Policies, Information Security Behavior, and Cultural Biases.

In Chapter 3 we present the Model development and Methodology.

In Chapter 4 we present a Discussion and the Conclusions.

2 Literature Review

In this chapter we present a collection of selected publications which are relevant to the subject of our thesis /research. Furthermore, they are accompanied by an analysis of context and apposition of the basic conclusions of every study/ research. The scope of our literature review is to identify the issues related to the identification of cultural biases of an organization' s employees. Therefore, we have carried out a literature review on topics including Information Security Awareness Programs, Information Security Risk Perceptions, Information Security Behavior and Cultural biases.

Information security research focuses on the "human factor", as people are considered to be the weakest link in information security. Organizations use security policies to address this issue. However, it is a common phenomenon, that users do not comply with security policies, mainly out of ignorance or because they mistakenly believe that the security of the Information System is not their responsibility or because they do not understand the consequences of security breaches. To address this problem, but also to address regulatory compliance requirements (e.g., HIPAA, FISMA), information security awareness programs have become key elements of security management. Information security awareness programs aim at risk management by influencing individual behavior.

Most of the protection methods and security approaches in organizations are mainly concentrated on external attacks and fail to minimize the number of security incidents [17], as they do not address the security awareness weaknesses of individuals. Usually, most of the effort for providing security in IS focuses on technology, and only recently, studies have proved that human factors do have a significant role [24]. Individuals perceive risks differently and similarities of individual values stem from similar social backgrounds. As suggested in the work of Rippl [31], it is possible to infer cultural aspects from individual-level data. Our aim is to develop a method for the identification of cultural biases of a typical organization' s employees regarding information security awareness and to classify them into four groups, namely, fatalists, hierarchists, individualists and egalitarians. Following, the organization can proceed with creating targeted interventions, if necessary.

2.1 Method and Scope of literature review

Proper information security behavior of individuals plays a critical role in organizations and a large corpus of research has been conducted in its investigation. The human aspect remains the weakest link in information security chain and the behavior of IS users and their IS security awareness requires assessment and evaluation. While there are a few methods for the investigation of information security behavior, up to our knowledge, none of them identifies the cultural biases in organizations' personnel which are overlooked and not considered when designing information security awareness programs.

Our method is based on the collection of selected published sources that are relevant to the subject of the present Thesis. Moreover, they are accompanied by the main conclusions of each study, the critical analysis of the contents and the detection of possible gaps in the literature on the topic. There was no limitation in books and journal articles only, but the subject of the literature review may also be other information material, such as websites. A prerequisite of a systematic search for suitable publications is the definition of indexing terms. To increase the efficiency of the search, we used combined indexing words like «and» / «or» / «not». Some of the indexing terms that we used are the following: Information Security Awareness Programs, Information Security Risk Perceptions, Information Security Behavior, Cultural biases, Questionnaire.

Afterward, a grouping of the gathered literature sources took place, based on some of their common characteristics, such as the research problem, the goals/ objectives, the research approach, the findings, etc.

In addition, our method uses an extremely useful tool, the literature distribution table that shows the timeline of the publications presented below. The purpose of the literature review is the critical analysis of the contents and the detection of possible gaps in the literature of the subject/ topic.

Study	Content	Method	Participants
[9] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, Tara Zwaans. 2017	The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies	HAIS-Q	Students/ Employees
[10] Stefan Bauer, Edward W.N. Bernroider, Katharina Chudzikowski. 2017	Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks	Semi-structured interviews	Employees
[11] Dirk Snyman, Hennie A. Kruger. 2017	The Application of Behavioural Thresholds to Analyse Collective Behaviour in Information Security	Behavioral threshold analysis method	Students
[12] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol and M. Angela Sasse. 2016	Productive Security: A scalable methodology for analysing employee security behaviours	Productive Security (ProdSec) methodology	Employees
[13] W.D. Kearney, H.A. Kruger. 2016	Can perceptual differences account for enigmatic information security behaviour in an organisation?	First fishing experiment/ security training/ second fishing experiment	Employees
[14] Wayne D. Kearney, Hennie A. Kruger. 2016	Theorising on risk homeostasis in the	Examination of risk homeostasis	

	context of information security behaviour		
[15] Marek, Jennifer. 2015	Presence of optimistic bias and illusion of control in information security risk perceptions	Questionnaire	Employees

Table 1. The literature distribution table.

Parsons et al., [9] tried to holistically measure Information Security Awareness by using a research tool of their own design named HAIS-Q (Human Aspects of Information Security Questionnaire). Their questionnaire measured 63 aspects which were grouped into one of the seven areas of information security focusing specifically on Password management, Email use, Internet use, Social media use, Mobile devices, Information handling and Incident reporting. Each area of focus was additionally divided into three specific sub-areas, resulting in 21 areas of interest. Each of those areas was measured through an independent element of knowledge, attitude and behaviour.

They conducted two studies as follows: In the first study, 112 students completed HAIS-Q and also participated in an empirical lab-based phishing experiment. As shown by the results, participants who had higher scores in HAIS-Q also had better performances in the phishing experiment. This indicated that HAIS-Q can predict an aspect of information security behavior and provided evidence of consistent validity. In the second study, HAIS-Q was given to a larger and more representative population of 505 Australian workers to confirm the strength of the instrument. The results of factor analysis and other statistical techniques provided evidence for the validity of HAIS-Q as a powerful ISA measurement tool. Their study provided further evidence of the validity of HAIS-Q which can indeed predict behavior in an electronic fishing experiment.

Meanwhile, Bauer et al., [10] conducted a study in which they analyzed the endeavors of Information Security administrators to plan successful Information Security Awareness programs by making a comparison between the current design recommendations proposed in the literature and the actual ISA programs design practices in three banks. Additionally, they investigated how users perceive the ISA programs and the related implications of

consistent IS behavior. They used a multiple case design to investigate three banks from Central and Eastern Europe.

Each research case consisted of interviews inside the bank branch as well as headquarters' users, IS administrators and ISA program materials. The interest in this study was not focused on a specific user but on how user narratives reflect ISP compliance and ISA project design recommendations.

Their data collection followed three phases. First, it was updated by a literature review, they started a workshop in 2013 including focus groups to achieve a deeper understanding of IS and ISP compliance inside the banks. Secondly, they conducted 33 semi-structured interviews with IT professionals and users and analyzed ISA program materials such as intranet messages or leaflets. This helped them achieve a deeper insight into the design and implementation of the ISA program. Finally, they conducted semi-structured interviews with users of the three banks.

They concluded by making a series of mutually depended suggestions to improve the levels of behavioral compliance in the ISP. They proposed the incorporation of an integrated combination of ISA interventions into ISA, the implementation of a long-term strategy that allows for a controlled adaptation of an ISA program based on careful assessment, the non-technocratic two-way communication in an ISA program and the diversification of target audiences. Finally, they suggested that ISA programs that investigate particular interventions for user groups are more likely to reduce specific neutralization techniques that are common to the respective user group.

At the same time, Snyman and Kruger [11] examined security behavior by employing the behavioral threshold analysis method. Even though this tool was at an early stage it was shown that it is promising for measuring, analyzing and predicting security behavior and awareness. They showed that behavioral threshold analysis is possible in the context of information security and can provide useful guidance on how to build information security awareness programs. A general behavioral threshold analysis was presented and then applied in the field of information security by collecting data on the behavioral thresholds of individuals in a group and how individuals affected each other regarding security behavior.

To collect data the authors used a questionnaire based on passwords. The participants were students and were asked whether they would share their passwords if enough of their colleagues were opted to do so and if yes, how many students need to share their passwords before they would also share their own passwords. Individuals in a group were asked to sincerely respond to a series of questions about two separate results of a situation in which individuals as part of a group can find themselves. Individuals were asked to fill in a value for x. The reported value represented the inherent threshold for that person. Once responses were received, they were recorded and represented in graph format. Threshold analysis was then performed at the observed values to predict the outcome of the behavior of the observed group. Thresholds represented the limit of an individual to participate in an action (Action A) that will lead to the result A. In other words, the number of people that have to perform Action A before the person whose threshold is marked participates and executes the same Action.

Behavioral threshold analysis method can contribute to security awareness by helping to identify which security issues are pressure-sensitive by colleagues or are easily influenced by colleagues' behavior. If these issues can be identified, this means that these are the issues that security awareness campaigns should focus on. Moreover, it can serve as an anti-fatigue countermeasure by defining the key issues on which safety awareness programs should focus on. Additionally, it can help save time and money thus providing a positive contribution to the costs of security awareness. Behavioral threshold analysis method can be used later, after interventions through security awareness campaigns, in a follow-up process to record the progress of security awareness levels. Finally, it proposes a new way of measuring the importance of security awareness issues in an organization.

In a previous study, conducted by Beautement et al., [12] a methodology for collecting large scale data sets on the behavior and attitudes of employees via scenario-based surveys was presented, named Productive Security (ProdSec). According to this methodology, they firstly conducted semi-structured interviews with a vertical cross-section of the organization to capture attitudes and behaviors in as many roles, physical locations and demographic groups as possible. Based on interview findings, they carefully designed a scenario-based survey that reflected dominant security-related issues. They adapted their survey to each operational environment, to ensure that survey questions were relevant and identifiable by the participants, aiming at generating more realistic and authentic responses.

Once this cycle has been completed, security professionals have the option of following the situation in the long run by repeating the measurement cycle at some point in the future (e.g., 6 months later), or actively participating in any problems.

Their methodology allows organizations to take steps for the empirical assessment of security culture as well as understanding the dominant behaviors and attitudes identified within the organization. The authors showed that their approach allows the detection of statistically significant differences between groups of employees which can contribute to targeted interventions. The employment of targeted interventions focused on specific groups of employees can save these employees from participating in non-targeted interventions and from having to determine whether they apply to them or not. Except for that, targeted interventions are a positive step in reducing employees' compliance costs.

Simultaneously, Kearney et al. [13] conducted two practical phishing experiments in a large utility company as part of a larger study aiming to understand users' behavior regarding information security and risk management in security. The results of these phishing experiments inspired a follow-up study on trust, in addition to another study on possible perceptual differences between management and users.

According to the results from the first fishing exercise, 280 users responded to the email, with 231 (83%) correctly giving their usernames and passwords. As it was shown by further analysis, 159 (69%) out of 231 who gave their personal data, had already attended the company's security training program that taught them how to identify and react to possible phishing scams.

The second and follow-up fishing exercise was conducted after a while. They aimed to make a comparative analysis in an attempt to determine whether the behavior of the user had changed positively from the first test. Unfortunately, the results of the second trial were unexpected and quite disappointing. Even though a lower percentage of users gave valid user names and passwords, the actual number rose from 231 users to 312 users (the total number of users who responded to the message increased from 280 in the first test to 490 in the second test). Moreover, the number of users who had completed the security training and who had given the correct usernames and passwords also increased from 159 to 288.

The authors proposed an information security model that is reliable and safe. This model consists of three organizational groups (management, technology and users) that need to be combined to achieve a state of compatibility in information security. The alignment of perception between the three groups proved to be a prerequisite for a successful combination. Without this alignment, the goal of a secure information environment would be difficult to obtain and would probably remain a theoretical objective. Based on the result of this study it was shown that there is a certain degree of difference in perceptions between the three organizational groups of the company where the study was conducted. These differences in perception (within the proposed security model) help illustrate and understand the disappointing results of phishing tests in an environment with sufficient security awareness and training programs as well as a high level of user confidence in their own but also in the potential of the organization.

Meanwhile, Kearney and Kruger [14] investigated the risk homeostasis as an information security risk management model and showed that it could aid in explaining the contradictory human behavior, for example, the privacy paradox. On a more practical level, it could provide decision-makers with useful information and comprehension that would be beneficial in a strategic planning process.

Risk homeostasis is considered a behavioral framework that attempts to explain behavior in terms of risk, and there are many distinct similarities between Risk homeostasis and other behavioral models. By considering the popularity of other models and approaches to information security behavior, it must be mentioned that there is a significant lack of studies on Risk homeostasis as a possible explanatory theory for behavior in information security.

Previously, Marek [15] conducted a study aiming to depict the human element in the risk assessment of sensitive information threats in organizations. By using a survey developed by Rhee et al., [85], her research explored levels of optimistic bias and illusion of control existing in IT professionals and end users. The human element of risk assessment was examined by investigating the differences in perceived risks based on the organizational role. The different roles in the examined organizations were information technology professionals and end-users.

In her study risk perception was defined as the level of optimistic bias and the illusion of control measured in the respondents' answers to the questionnaire. By using an indirect measurement of these two structures, participants were told to evaluate the risks and threats for their organization first and following for an average organization in the same field. The analysis showed that both IT professionals and end-users showed similar levels of optimistic bias but IT professionals displayed higher levels of control illusion.

We saw that Parsons et al., [9] predicted behavior by employing the Human Aspects of Information Security Questionnaire (HAIS-Q) while Bauer et al., [10] conducted semi-structured interviews to investigate how bank employees perceive the ISA programs and related implications of consistent IS behavior. Snyman and Kruger [11] investigated how individuals affected each other regarding security behavior via a questionnaire. Beautement et al., [12] used a scenario-based survey for the empirical assessment of security culture and to understand the dominant behaviors and attitudes identified within an organization. In the work of Kearney and Kruger [13], two fishing experiments were conducted, and the second fishing experiment took place after the employees of an organization completed a security training program. The authors showed that there is a certain degree of difference in perceptions between the three organizational groups (management, technology, and users) of the company where their study was conducted. Moreover, they suggested that the alignment of perception between the three organizational groups is necessary to achieve a secure information environment. In another work by the same authors [14], they investigated the risk homeostasis as an information security risk management model and showed that it could help explain the contradictory human behavior, for example, the privacy paradox. Marek [15] used a survey to explore the levels of optimistic bias and illusion of control existent in IT professionals and end-users. The previously mentioned studies investigated human behavior regarding information security but none of them identified the cultural biases in organizations' personnel. Since individuals are considered to be the weakest link in information security the identification of their cultural biases could provide more information on their behavior regarding information security.

2.2 Information Security Policies in Organizations

Although organizations and their customers experience many advantages due to web-based technologies, information security breaches remain a concern [36, 37]. All technological aspects that address information security, such as anti-virus, anti-malware, anti-spam, anti-phishing, anti-spyware, firewall, authentication, and intrusion detection systems cannot guarantee a secure environment for information [37, 38]. Hackers target individuals, rather than computers, to create a security breach. The most common examples of user mistakes include inappropriate information security behavior, such as using their social security number as username and password, keeping their passwords on paper, sharing their username and password with their colleagues, opening emails from unknown senders, and downloading their attachments, as well as downloading dubious software from the Internet. Appropriate information security behavior should preferably be combined with technological aspects [40]. Therefore, it is necessary to apply multiple security approaches to mitigate the risk of information security breaches.

In the work of Von Solms and Van Niekerk [42] they investigated different aspects of cybersecurity, and they reported that even though information security and cybersecurity overlap, they are not completely analogous. The general definition of information security comprises availability, integrity, and confidentiality. Cybersecurity includes additional aspects that extend beyond the boundaries of information security, including humans in their personal capacity and society at large. To establish a secure environment for both information security and cybersecurity the collaboration inside the organization is necessary [43].

Information security breaches not only result in extra costs for organizations, but they also affect their reputation [44]. The appropriate information security behavior, apart from the technological aspects of information security, also mitigates the risk of information security breaches in organizations. Several studies have shown that the information security awareness of employees constitutes a significant aspect in mitigating the risk associated with their behavior in organizations [45, 46]. Kritzinger and von Solms [47] split users into two groups, namely home and organizational users, and they reported that information

security awareness plays a vital role in both groups. Their study also revealed that delivery methods and enforcement components play important roles in this domain. Information security awareness originates from employees' experience in this domain. Information security experience leads to comprehension, familiarity, and the ability and skill to manage incidents [37].

As shown in several studies, organizations that have not focused on individuals have experienced unsuccessful efforts [48, 49, 50]. Experts in the domain, suggest multi-perspective approaches for protecting organizations' information assets [51]. Even though organizations invest in the technological aspects of information security and tools, the number of security incidents and breaches remains a great issue due to the lack of attention in organizations' employees [52]. The amendment and improvement of employees' information security behavior, in line with information security organizational policies and procedures (ISOP), constitute an effective and efficient approach [53, 54].

2.3 The concept of Information Security Policies

Information security is an important activity within organizations given today' s security threats such as continued data breaches, systems outages, and malicious software [55, 56, 57]. Although external factors, as, external hackers and natural disasters constitute a major threat to the security of an organization's information and technology resources, the behavior of employees are often viewed as being an even greater security risk [58]. To address the risks associated with these insiders the organization should adopt information security policies that specify the standards, boundaries, and responsibilities of users regarding information and technology resources to facilitate the prevention, detection, and response to security incidents [5, 59]. However, security issues that stem from employees' behavior remain a constant issue for organizations [60, 61, 62].

Therefore, organizations depend on information security policies that are partly developed to guide employee compliance with external regulations such as the Sarbanes–Oxley (SOX) Act, The Health Insurance Portability and Accountability Act (HIPAA), The Payment Card

Industry Data Security Standard (PCI DSS), and the European Union Data Protection Directive (EU DPD) [63, 64, 65, 66]. Also, the financial, reputational, and legal implications of information security incidents have motivated organizations to implement detailed policies related to topics including access controls and authorization, data classification, data storage, and virus protection [67, 68, 69].

Most organizations have adopted some type of information security policy [70]. However, security policies are quite different among organizations depending on the value and sensitivity of the information and technology resources aimed to protect, as well as the potential implications of damage, modification, or disclosure of the information to the organization [71, 72]. As the term "information security policy" has a different meaning depending on the context of its usage, we can find numerous definitions and related concepts in the literature. A common classification is the following three-level division of security policies [73, 74]. At the highest level is the enterprise information security policy, or what is known as the security program policy. This executive-level document is not a policy per se, but a top management's articulation of the organization's strategic direction, scope, and tone for all security efforts [74, 75]. Enterprise information security policies are philosophical in nature and lead the development, implementation, and management of the security program, as well as assign responsibilities for the various areas of security. A key motivation for an enterprise information security policy is to guarantee compliance with regulatory requirements by exhibiting evidence of a comprehensive security program [75].

In the lower level we can find the issue-specific information security policies that address specific areas of technology, such as the use of e-mail, the Internet, or social media, the configuration of employee workstations, the use of personal equipment on organizational networks and the prohibitions against hacking or testing organizational security controls, are some examples. Issue-specific security policies include the guidelines and procedures, i.e., the acceptable use policies that employees must follow in their daily interactions with information and technology resources and describe penalties for non-compliance and other undesirable computing behaviors. These policies describe employees' roles and responsibilities in operational terms; therefore, they are usually associated with the term security policy and have received the bulk of attention. For example, studies of the drivers of employees' security compliance have described security policies as "established rules

that address specific security issues by providing instructions to the employees as to what they should do when they interact with the information and technology resources of their organization" [5] and as "a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations" [59].

At the lowest level we can find the technical security policies that relate to the security architecture of technological systems. Unlike enterprise and issue-specific security policies, technical security policies, also known as automated security policies [73], are not formalized as written documents, distributed to users, and agreed upon. Instead, technical security policies combine standards and procedures with the configuration or maintenance of a system. Some common examples include access control lists that define whether users may or may not access a particular system, as well as firewall rulesets which designate the flow of network traffic into and out of an organization [70, 74].

2.4 The human factor in Information Security Policies

Many organizations have valuable information and services in the control of individuals who are not aware of its value, the importance of maintaining its protection, or the implications in case that information is exposed [76, 77]. According to Kearney [78], individuals can help prevent security breaches only if they are aware of the dangers and are taught secure behaviors as part of their normal work training. However, the apathy of employees is an obstacle in creating an environment where management and employees are working towards the same information security goals [79]. Organizations must promote a culture in which employees share the responsibility of defending the company against attacks [78]. To guarantee that a policy is implemented and effective, the policy must initially be understandable. When employees do not understand what is expected of them, they find it difficult to comply. A policy that does not consider the objectives of the business, and fails to recognize the business mission, is sure to be overlooked every time it interferes with productivity or generating revenue [77]. We also must consider that when employees feel committed to their job, they are more likely to feel satisfied with it and be motivated to perform at their best. In the work of Thomson and Niekerk [79], it was shown

that instructions or orders influence behavior only if they are consciously accepted by each employee and then translated into specific goals. When an individual perceives that it is impossible to achieve a goal, his/ her commitment reduces greatly [80]. Therefore, those information security goals must be perceived as feasible to ensure the commitment of employees. Policies must be easily accessible or available to employees to ensure that they will not be overlooked. The exact role and responsibilities of each employee in terms of security must be clear.

2.5 Information Security Behavior

New technologies have led to the increase of Cyber threats [16]. This has led to the development of a great number of software and hardware protection tools to achieve higher information security since they make it quite difficult to exploit information systems (IS) due to software and hardware gaps. Nevertheless, in spite of these investments, the number of security incidents does not drop [17]. In the work of Abawajy [18], it was pointed out that regardless of the number and power of the layers of technological defenses in an organization, the information security is only as strong as its weakest link, and different methods, as for example social engineering, can be employed to target individuals, who can be considered to be the weakest link of the security chain [19, 20, 21, 22, 23]. Even the best technological solutions that can be utilized to reduce the various IS security issues cannot work successfully unless the individuals in organizations act rightly. Typically, most of the effort for providing security in IS was concentrated on technology, and only lately, studies have proved that human factors do have an important role [24]. Nevertheless, most of the protection methods and security approaches in organizations are still concentrated mostly on external attacks and fail to minimize the number of security incidents [17], as they do not address the security awareness weaknesses of individuals.

As reported in the work of Zhang et al., [22] previous studies investigate end-user security omitting however the use or misuse of IS security mechanisms. Surprisingly, this occurs even in organizations that handle sensitive, personal information such as healthcare. A recent study showed that 70% of health care employees do not have data privacy and security alertness [25]. More than 90% of successful hacks are due to the inducement of

individuals to click on a link, open a document, or forward something [26]. In addition, in the work of Aurigemma and Panko [27], it was shown that the total success of both software and hardware security mechanisms employed to address the risks in IS depends on users' effective behavior of the specific IS. Similarly, the significance of employees in preventing and detecting security incidents is emphasized in a plethora of works [23, 24, 28]. These studies show that the effective behavior of users leads to the success of IS security and that appropriate and constructive behavior can enhance IS security, while inappropriate and destructive behavior can block it. In a study of Schultz et al., [21] where they attempted to address the human factors in information security, they highlighted the resistance of users to information security measures and emphasized that users' use of information security mechanisms and tools is definitely not optimal.

Based on all these findings, it is concluded that security issues are not due to technology but a problem of human nature, and the behavior of IS users and their IS security awareness requires assessment and evaluation. The cultural biases of individuals remain an overlooked aspect of human behavior in all the previously mentioned works. The identification of cultural biases could provide some useful insight regarding the behavior of individuals in terms of information security.

2.6 Cultural Biases

The Cultural Theory of Risk [29] stemmed from the acceptance that the psychometric paradigm [30] concentrates on cognitive factors that affect the individual perception of risk, thus ignoring the cultural and social influences. The Cultural Theory of Risk clarifies how social structures relate to individual perceptions of societal dangers. Individuals perceive risks differently, depending on the social structures to which they are exposed, and the values embedded in them. This means that the values of certain social or cultural contexts form the individual's perception and evaluation of risks [31]. As a result, values function as a filter in interpreting risk-related information, for example, individuals with environmental values will assess a given piece of information about the possibility of accidents in nuclear power plants completely differently than supporters of nuclear power [32].

A vital component of the Cultural Theory of Risk is the classification of cultural ways of life, also referred to as the grid/group typology, which serves as a heuristic divide to classify individuals into four cultural groups that share the same cultural biases. The group dimension of the typology refers to the degree to which an individual is incorporated into social units and absorbs group activities. The grid dimension refers to the degree to which the boundaries of social units constrain the free movement of individuals. In other words, "high group" indicates that the individual's choices are subject to a high degree of collective control. "High grid" indicates a way of life that emphasizes roles and authority that bind life choices. Four categories of cultural groups stem from this classification: fatalists, hierarchists, individualists, and egalitarians. Figure 1 illustrates a description of the different behavior expected by the four cultural groups with respect to risk [33, 34, 35].

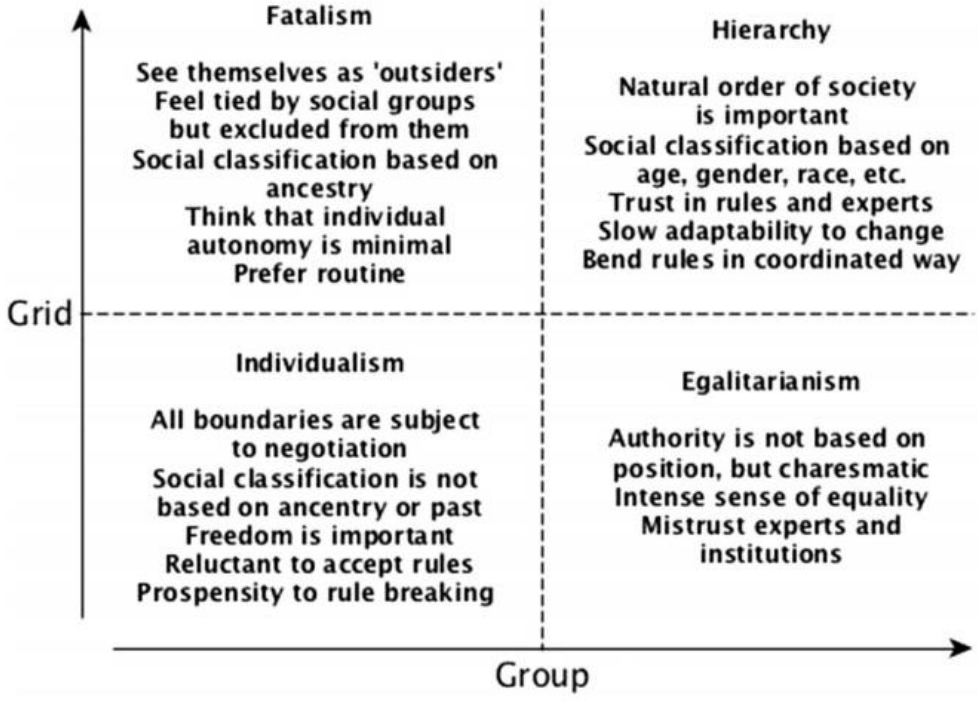

Figure 1. The Grid/Group typology: Cultural groups and their behavior [32].

Individuals who fit in the same group perceive risks in a similar way and distinctly from individuals fitting in the other groups. For example, individuals with hierarchic orientations are assumed to fear risks that threaten the social order (e.g., demonstrations or crime), and are assumed to accept risks if decisions about those risks are justified by governmental

authorities or experts. Individuals with egalitarian orientation are assumed to distrust risks that are forced on them by the decisions of a small elite of experts or governmental authorities and are assumed to overestimate risks that will inflict irreversible dangers on many people or on future generations. Individuals with the orientation of individualism perceive risk as an opportunity and fear risks that would limit their freedom. People with an orientation to fatalism prefer to remain unaware of risks and believe that they cannot do anything about them. In the work of Brenot et al., [36], it was illustrated that cultural individual biases can explain variance in risk perceptions. Though correlations found are weak, they are statistically important and show that different cultural groups were associated with concern, or lack of concern, for the particular types of risks expected for each of the worldviews.

Rippl [31], presented the different views expressed in the literature about the level of analysis when applying the Cultural Theory of Risk. Although one view is that we cannot measure culture as an aggregation of individual values, another view is that it is possible to infer cultural aspects from individual-level data. In that view, similarities of individual values are a result of similar social backgrounds (e.g., preferred social relations). Adopting this viewpoint, the author recommends measuring cultural biases at the individual level, which is not a direct measure of the cultural types but a measure of the processes that are connected to the cultural types.

As suggested in the work of Rippl [31], it is possible to infer cultural aspects from individual-level data. Individuals perceive risks differently and similarities of individual values stem from similar social backgrounds. The identification of cultural biases of individuals could provide useful information regarding their behavior in terms of information security within an organization. Our aim is to develop a method for the identification of cultural biases of a typical organization' s employees regarding information security awareness and to classify them into four groups, namely, fatalists, hierarchists, individualists and egalitarians.

2.7 Results

In the literature review, we examined several studies that suggest a number of methods for the investigation of human behavior regarding information security. More specifically HAIS-Q was proven as a powerful ISA measurement tool in the work of Parsons et al., [9], while Bauer et al., [10] incorporated semi-structured interviews with IT professionals and users, to analyze ISA program materials such as intranet messages or leaflets. This helped them make a series of proposals to improve the levels of behavioral compliance in the ISP. Snyman and Kruger [11] investigated security behavior using the behavioral threshold analysis method for measuring, analyzing, and predicting security behavior and awareness. In the work of Beautement et al., [12] it was shown that the Productive Security (ProdSec) methodology allowed the detection of statistically significant differences between groups of employees which can contribute to targeted interventions. In addition, the (ProdSec) methodology allows organizations to take steps for the empirical assessment of security culture as well as understanding the dominant behaviors and attitudes identified within the organization. In the two phishing experiments of Kearney et al., [13] the results in the second experiment were unexpected and rather disappointing. As they showed, the number of users who had completed the security training and who had given the correct usernames and passwords increased from 159 in the first experiment to 288 in the second. Keamey and Kruger [14] showed that the examination of risk homeostasis as an information security risk management model would help explain the contradictory human behavior, for example, the privacy paradox. Marek [15] defined risk perception as the level of optimistic bias and the illusion of control was measured in IT professionals' and end-users answers via a questionnaire. Her analysis showed that both IT professionals and end-users showed similar levels of optimistic bias but IT professionals displayed higher levels of control illusion.

In addition, most of the security approaches and protection methods in organizations still concentrate on external attacks and do not decrease the number of security incidents [17], as they fail to address the security awareness weaknesses of individuals. Also, the importance of employees in the prevention and detection of security incidents is emphasized in a plethora of works [23, 24, 28]. These studies clearly indicate that the success of IS security depends on the effective behavior of its users and that appropriate

and constructive behavior can improve, while inappropriate and destructive behavior can block IS security. Based on these findings, it is concluded that security is a problem of human nature and that the behavior of IS users and their IS security awareness needs assessment and evaluation.

Moreover, cultural biases of individuals remain an overlooked aspect of human behavior in all the previously mentioned works. According to the work of Rippl [31], it is possible to infer cultural aspects from individual-level data. Since individuals are considered to be the weakest link in information security the identification of their cultural biases could provide useful information on their behavior regarding information security.

3 Model development and Methodology

In this section, we will describe the model development and our methodology. Our goal is to classify the users of a typical organization's Information System into the four cultural groups that share the same cultural biases, namely fatalists, hierarchists, individualists, and egalitarians. Our focus will be on the behavior and attitudes of the employees which can be measured through their perceptions [81]. Since questionnaires and surveys are an acceptable research method used in the context of social sciences [81, 82, 83] to measure attitudes and opinions of employees [84], we have decided to develop a questionnaire to achieve our goal.

As reported in the literature review section, previous research has employed questionnaires to holistically measure Information Security Awareness [9], to examine how users perceive the ISA programs [10], to examine how individuals affect each other, and to obtain useful guidance on how to build information security awareness programs [11]. A survey was also used in the work of Beautement et al., [12] to help organizations take steps for the empirical assessment of security culture as well as understanding the dominant behaviors and attitudes identified within the organization. Marek [15] employed a questionnaire to define risk perception of users.

The perspective of our approach stemmed from the Cultural Theory of Risk aiming to identify the cultural biases of individuals which result from cultural and social values. According to the Cultural Theory, we have four cultural biases, namely the cultural bias of hierarchy or hierarchical cultural bias, the cultural bias of egalitarianism or egalitarian cultural bias, the cultural bias of individualism or individualistic cultural bias, and finally, the cultural bias of fatalism or fatalistic cultural bias [87].

The characteristics of the four cultural biases are the following:

• In a hierarchy, superiors and inferiors share ethical values, such as respect for other members, and identify themselves with the collective. Nature, and generally the world, are

perceived as controllable, and stable within limits that can be determined by certified experts. Perception of time is long-term, supporting thorough planning. Human nature is seen as sinful and thus calling for adequate regulation [87].

• In egalitarianism, human nature is thought of as fundamentally altruistic, but subject to corruption by status and power [87]. Amongst individuals that share the cultural bias of egalitarianism, there is an intense sense of equality and mistrust of experts and institutions. Also, authority is not based on position but charisma [32].

• In individualism, others are perceived as mostly self-interested, without this being a bad thing [87]. Also, all boundaries are subject to negotiation and freedom is important [32]. Individuals that share the cultural bias of individualism pursue liberty, they are reluctant to accept rules and they tend to break the rules [32, 41].

• In fatalism, there is no meaningful, reliable pattern to be found in anything. Solidarity is inexistent and manipulative while unpredictable, deceitful despots are free to exploit a society of isolated individuals [87]. Individuals that share the cultural bias of fatalism see themselves as "outsiders" and feel tied by social groups but excluded from them [32].

According to the characteristics of each cultural bias, the hierarchical cultural bias is expected to be expressed in individuals as fear of risks that threaten the social order and acceptance of risks if decisions about those risks are justified by governmental authorities or experts. The egalitarian cultural bias is expected to be expressed as a distrust of risks that are forced on individuals by the decisions of a small elite of experts or governmental authorities. The individualistic cultural bias is expected to be present in individuals who perceive risk as an opportunity and fear risks that would limit their freedom, while the fatalistic cultural bias is expected to be present in individuals who prefer to remain unaware of risks and believe that they cannot do anything about them.

As suggested in the work of Rippl [31], it is possible to infer cultural aspects from individual-level data. In that view, similarities of individual values are a result of similar social backgrounds (e.g., preferred social relations). Adopting this viewpoint, the author recommends measuring cultural biases at the individual level, which is not a direct measure of the cultural types but a measure of the processes that are connected to the cultural types. In our case, we used the behavior and attitudes of individuals in the context of information security awareness. We formulated the constructs of our model aiming to cover nine areas of interest, namely, E-mail security, Internet security, Passwords management, Viruses/ malware, Physical security/ access to buildings, Information management, Information security incidents, Security updates and corrections, and Contractor security. The aforementioned areas of interest represent aspects of information security policies, they cover all employees' groups, they can be found in all typical organizations and they are most likely to be breached. Each area of interest is further divided into sub-areas.

The areas of e-mail security, internet security, passwords management, information management, and information security incidents were included in the work of Parsons et al., [9]. In the work of Beautement et al., [12] they included the areas of information management and information security incidents. Our work adds four areas of interest to the aforementioned areas, namely the areas of viruses/ malware, physical security/ access to buildings, security updates, and contractor security.

We draw on the Cultural Theory of Risk aiming to identify the cultural biases of individuals which result from cultural and social values. The identification of cultural biases can facilitate the assessment of needs and provides an alternative criterion for separating awareness participants into groups. This is because individuals' cultural biases intervene with the processing of the risk information that users receive and shape their attitudes and perceptions. Therefore, awareness programs can be more efficient since they will be customized to the needs of their participants [32].

Our purpose is to identify the cultural biases of a typical organization's employees regarding information security awareness and to classify them into four groups, namely,

fatalists, hierarchists, individualists, and egalitarians. For this purpose, we have developed a method, namely the ICBU-Q (Identification of Cultural Biases of Users Questionnaire). The ICBU-Q classifies users according to their answers on nine areas of interest, namely, E-mail security, Internet security, Passwords management, Viruses/ malware, Physical security/ access to buildings, Information management, Information security incidents, Security updates and corrections, and Contractor security. The aforementioned areas of interest resulted since they represent aspects of information security policies, they cover all employees' groups, they can be found in all typical organizations and they are most likely to be breached. Each area of interest is further divided into sub-areas. Following, we provide a detailed description of our method.

Although we have pointed out the feasibility of identifying the cultural biases of individuals, our method remains a theoretical framework. However, we plan to use the ICBU-Q soon and test its validity.

3.1 Construct of Model

Our model covers nine areas of interest, namely, E-mail security, Internet security, Passwords management, Viruses/ malware, Physical security/ access to buildings, Information management, Information security incidents, Security updates and corrections and Contractor security. The aforementioned areas of interest resulted since they represent aspects of information security policies, they cover all employees' groups, they can be found in all typical organizations and they are most likely to be breached. Each area of interest is further divided into sub-areas. Following, we provide a detailed description of our method. Each area of interest is further divided into sub-areas. Our aim is to classify a typical organization' s employees into four groups, namely, fatalists, hierarchists, individualists and egalitarians according to their responses.

The areas of e-mail security, internet security, passwords management, information management and information security incidents were included in the work of Parsons et al., [9]. In the work of Beautement et al., [12] they included the areas of information management and information security incidents. Our work adds four areas of interest to the

aforementioned areas, namely the areas of viruses/ malware, physical security/ access to buildings, security updates and contractor security.

Following we will describe the constructs and the questions of each construct that are covered by our model to make clear how our model works:

- E-mail security (C01): In this area we ask users if they click on links or open attachments when they receive e-mails from known or unknown senders and who they believe is responsible for e-mail-security.

- Internet security (C02): Here, we ask users if they download files on their work computer such as films, texts, music, when they are at work and if they access dubious websites. Also, we ask them if they enter any information online (passwords, personal data), and who they believe is responsible for Internet security on the organization's resources (computers on which they work on), when they are at work.

- Passwords management (C03): We ask users if they use the same password on more than one accounts, if they share their passwords and who they believe is responsible for Passwords.

- Viruses/ malware (C04): Here, we ask users if they update the antivirus program and the antispyware program of the computer on which they work on, when automatically recommended, when they are at work. Also, we ask who they believe is responsible for dealing with Viruses/malware.

- Physical security/ access to buildings (C05): In this area we ask users if they are familiar with the Organization' s facilities and if they know the process of entering the Organization' s facilities as a visitor. Also, we ask them if they check all people entering or exiting the Organization' s facilities, if they can estimate the importance

of an incident when reported to them and if they know the handling procedure of an incident.

- Information management (C06): We ask users if they lock their computer when they move away from their office and if they dispose printouts which contain sensitive information in the same way as non-sensitive ones. Also, we ask them if they would plug a USB stick found in a public place into their work computer and if they would leave printouts that contain sensitive information on their desk overnight. Moreover, we ask users if they have a secure draw or storage area that they can use and who they believe is responsible for Information management.

- Information security incidents (C07): Here, we ask users who to would they report a security concern and a security incident. Also, we ask them if they would you ignore poor security behavior by their colleagues, and if they would report a suspicious acting by someone in their workplace.

- Security Updates and Corrections (C08): We ask users if they have a plan to identify systems where automatic operating system updates are not available. Also, we ask them if they have a plan that states which resource(s) will be used to determine if an operating system update is available. Moreover, we ask them if they have a plan that directs how and by whom the update will be installed.

- Contractor security (C09): Here, we ask users if they think that a courier company employee entering the building could be a threat.

Our model is presented in figure 2 that follows:

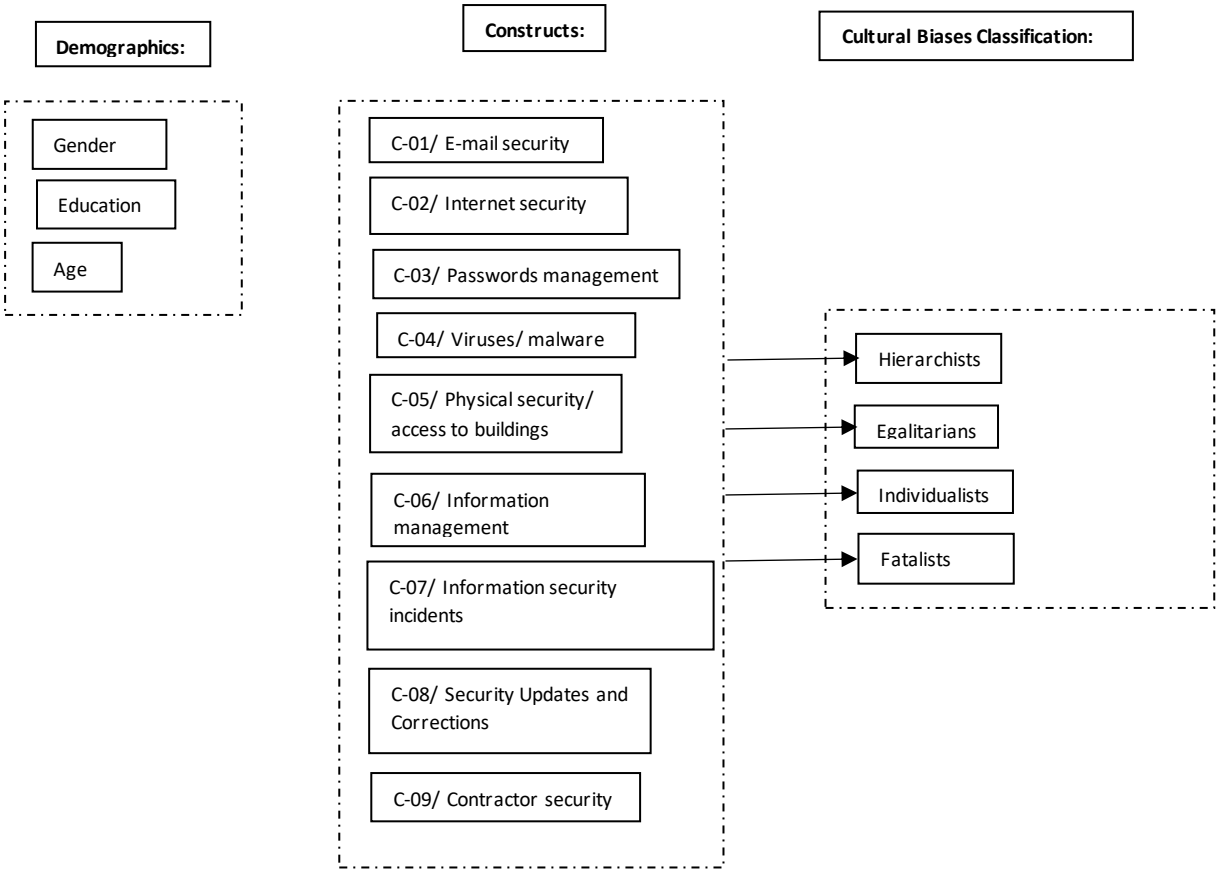

Figure 2. Our model

According to the Cultural Theory of Risk we have four cultural biases, namely the cultural bias of fatalism, the cultural bias of hierarchy, the cultural bias of individualism, and finally, the cultural bias of egalitarianism [86]. Our aim is to classify a typical organization' s employees into four groups, namely, fatalists, hierarchists, individualists and egalitarians according to their responses.

As suggested in the work of Rippl [31], it is possible to infer cultural aspects from individual-level data. In that view, similarities of individual values are a result of similar social backgrounds (e.g., preferred social relations). Adopting this viewpoint, the author recommends measuring cultural biases at the individual level, which is not a direct measure of the cultural types but a measure of the processes that are connected to the cultural types. In our case, we used the behavior and attitudes of individuals in the context of information security awareness.

We have divided the organizations employees into groups according to the tasks they perform and their responsibilities within the organization. Our grouping has resulted in the following groups of employees:

- Personnel of the organization with the capabilities of importing, searching, and changing data in the organization' s Information System (G01).
- Personnel of the organization which accesses and manages documents / forms with personal data content (G02).
- Information System managers mainly oriented on technical issues (G03).
- Personnel of the organization that develops applications for Information Systems (G04).
- Mid-level executives of the organization responsible for supervising lower-level executives (G05).
- Top executives of the organization who take strategic decisions on the majority of the organization's issues, including security issues (G06).
- Personnel of the organization responsible for the physical safety of the organization's facilities (G07).
- Non-members of the organization belonging to a) a company for guarding the organization's building facilities and b) cleaning services of the building facilities (G08).

Each group of employees is asked to answer the questions of different constructs according to its responsibilities and tasks performed. More specifically:

- The group of the organization's personnel with the capabilities of importing, searching, and changing data in the organization' s Information System (G01), is asked to answer the questions of the constructs E-mail security (C-01), Internet security (C-02), Passwords management (C-03), Viruses/ malware (C-04), Information management (C-06) and Information security incidents (C-07).

- The group of the organization's personnel which accesses and manages documents / forms with personal data content (G02), is asked to answer the questions of the constructs E-mail security (C-01), Internet security (C-02), Passwords management (C-03), Viruses/ malware (C-04), Information management (C-06) and Information security incidents (C-07).

- The group of Information System managers mainly oriented on technical issues (G03), is asked to answer the questions of the constructs E-mail security (C-01), Internet security (C-02), Passwords management (C-03), Viruses/ malware (C-04), Information management (C-06), Information security incidents (C-07) and Security Updates and Corrections (C08).

- The group of Information System managers mainly oriented on technical issues (G03), is asked to answer the questions of the constructs E-mail security (C-01), Internet security (C-02), Passwords management (C-03), Viruses/ malware (C-04), Information management (C-06), Information security incidents (C-07) and Security Updates and Corrections (C08).

- The group of the organization's personnel that develops applications for Information Systems (G04) is asked to answer the questions of the constructs E-mail security (C-01), Internet security (C-02), Passwords management (C-03), Viruses/ malware (C-04), Information management (C-06), Information security incidents (C-07) and Contractor security (C09).

- The group of the organization's mid-level executives that are responsible for supervising lower-level executives (G05), is asked to answer the questions of the constructs E-mail security (C-01), Internet security (C-02), Passwords management (C-03), Viruses/ malware (C-04), Information management (C-06) and Information security incidents (C-07).

- The group of the organization's top executives who take strategic decisions on the majority of the organization's issues, including security issues (G06), is asked to answer the questions of the constructs Information security incidents (C-07) and Contractor security (C09).

- The group of the organization's personnel that is responsible for the physical safety of the organization's facilities (G07), is asked to answer the questions of the constructs E-mail security (C-01), Internet security (C-02), Passwords management (C-03), Viruses/ malware (C-04), Information management (C-06) and Information security incidents (C-07).

- The group of the organization's non-members belonging to a) a company for the guarding of the organization's building facilities and b) cleaning services of the building facilities(G08), is asked to answer the questions of the constructs Physical security/ access to buildings (C05) and Information security incidents (C-07).

In Table 2 that follows we can see a summary of the groups of recipients and the constructs that are addressed to them:

Groups of recipients	**Constructs**
G01- Personnel of the organization with the capabilities of importing, searching, and changing data in the organization' s Information System.	C-01, C-02, C-03, C-04, C-06, C-07
G02- Personnel of the organization which accesses and manages documents / forms with personal data content.	C-01, C-02, C-03, C-04, C-06, C-07
G03- Information System managers mainly oriented on technical issues	C-01, C-02, C-03, C-04, C-06, C-07, C-08
G04- Personnel of the organization that develops applications for Information Systems.	C-01, C-02, C-03, C-04, C-06, C-07, C-09
G05- Mid-level executives of the organization responsible for supervising lower-level executives.	C-01, C-02, C-03, C-04, C-06, C-07

G06- Top executives of the organization who take strategic decisions on the majority of the organization's issues, including security issues.	C-07, C-09
G07- Personnel of the organization responsible for the physical safety of the organization's facilities.	C-01, C-02, C-03, C-04, C-06, C-07
G08- Non-members of the organization belonging to a) a company for the guarding of the organization 's building facilities and b) cleaning services of the building facilities.	C-05, C-07

Table 2. Summary of the groups of recipients and the constructs that are addressed to them.

3.2 Questionnaire Development

We have named our method ICBU-Q (Identification of Cultural Biases of Users - Questionnaire) which is a closed ended multiple-choice questionnaire with a single response. The ICBU-Q helps us classify users according to their answers on nine areas of interest, namely, E-mail security, Internet security, Passwords management, Viruses/ malware, Physical security/ access to buildings, Information management, Information security incidents, Security updates and corrections and Contractor security. The ICBU-Q is generally administered with a set of demographics questions, while the areas of interest resulted because they represent aspects of information security policies, they cover all employees' groups, they can be found in all typical organizations and they are most likely to be breached. The areas of e-mail security, internet security, passwords management, information management, and information security incidents were included in the work of Parsons et al., [9]. In the work of Beautement et al., [12] they included the areas of information management and information security incidents. Our work adds four areas of interest to the aforementioned areas, namely the areas of viruses/ malware, physical security/ access to buildings, security updates, and contractor security.

Each area of interest contains a set of questions some of which are adopted from previous works from other authors while others are self-developed. More specifically:

- E-mail security consists of four questions, three of them are adopted from the work of Parsons et al., [9] and one question is self-developed.
- Internet security has four questions, three of which are adopted from the work of Parsons et al., [9] and one question is self-developed.
- Passwords management contains three questions, two of which are adopted from the work of Parsons et al., [9] and one question is self-developed.
- Viruses/ malware has three self-developed questions.
- Physical security/ access to buildings consists of five self-developed questions.

- Information management has six questions, three of which are adopted from the work of Beautement et al., [12], two are adopted from the work of Parsons et al., [9] and one question is self-developed.
- Information security incidents contains four questions, one of them is adopted from the work of Beautement et al., [12] and three from the work of Parsons et al., [9].
- Security updated and corrections has three self-developed questions.
- Contractor security has one self-developed question.

According to the answers of a typical organization' s employees to these questions we identify their cultural biases regarding information security awareness, and we classify them into four groups, namely, fatalists, hierarchists, individualists and egalitarians. We have put a great effort to make each possible answer clearly distinct and analogous to the four types of cultural biases we expect to identify. To form our answers, we have assumed that individuals with hierarchic orientations fear risks that threaten the social order, and they are expected to accept risks if governmental authorities or experts justify decisions about those risks. Regarding individuals with egalitarian orientation, we have assumed that they distrust risks that are forced on them by the decisions of a small elite of experts or governmental authorities and we expect that they will overestimate risks that will inflict irreversible dangers on many people. As for individuals with the orientation of individualism we have assumed that they perceive risk as an opportunity and that they fear risks that would limit their freedom. Finally, individuals with an orientation to fatalism are assumed to prefer to remain unaware of risks and we expect them to believe that they cannot do anything about them.

In Table 3 that follows, we can see the ICBU-Q (Identification of Cultural Biases of Users - Questionnaire):

			Self-developed			
Author	**Construct**	**Questions**	**Individualist**	**Egalitarian**	**Hierarchist**	**Fatalist**
Parsons et al., [9].	E-mail security	Do you click on links in emails from known senders?	Yes, I can be trusted to keep my computer safe.	I ask a colleague whom I trust what to do.	Yes, Information managers told us that it is safe.	I click on the link because I was asked to.
Parsons et al., [9].		Do you click on links in emails from unknown senders?	No, I know how to keep my computer safe.	I ask a colleague whom I trust what to do.	No, Information managers told us that it is risky.	I click on the link because I was asked to.
Parsons et al., [9].		Do you open attachments in emails from unknown senders?	No, I know how to keep my computer safe.	I ask a colleague whom I trust what to do.	No, Information managers told us that it is risky.	I open the attachments because I was asked to.
Self-developed.		Who do you believe is responsible for e-mail-security?	Me	Everyone, we are all equally responsible.	Information managers.	Not me.
Parsons et al., [9].	Internet security	When at work, do you download files on your work computer such as films, texts, music?	No, I know how to keep my computer safe.	I ask a colleague whom I trust what to do.	No, Information managers told us that it is risky.	If I need them, yes.
Parsons et al., [9].		Do you access dubious websites?	No, I know how to keep my	Only if colleagues I trust	No, Information managers	If necessary, yes.

			computer safe.	do the same.	told us that it is risky.	
Parsons et al., [9].		Do you enter any information online (passwords, personal data)?	No, I know how to keep my computer safe.	Only if colleagues I trust do the same.	No, Information managers told us that it is risky.	If necessary, yes.
Self-developed.		When at work, who do you believe is responsible for Internet security on the organization's resources (computers on which you work on)?	Me, each one is responsible separately.	Everyone, we are all equally responsible.	We all share our piece of responsibility.	Information managers.
Parsons et al., [9].	Passwords management	Do you use the same password on more than one accounts?	No, I know how to keep my accounts safe.	Only if colleagues I trust do the same.	No, Information managers told us that it is risky.	Yes, what could go wrong?
Parsons et al., [9].		Do you share your passwords?	No, I know how to keep my accounts safe.	Only with colleagues I trust.	No Information managers told us that it is risky	Yes, what could go wrong?
Self-developed.		Who do you believe is responsible for Passwords?	Me, each one is responsible separately.	Everyone, we are all equally responsible.	We all share our piece of responsibility.	Information managers.

Self-developed.	Viruses/ malware	When at work, do you update the antivirus program of the computer on which you work on, when automatically recommended?	Yes, I can be trusted to keep my computer safe.	Only if colleagues I trust do the same.	Yes, Information managers told us that it is necessary.	If I have time, yes.
Self-developed.		When at work, do you update the antispyware program of the computer on which you work on, when automatically recommended?	Yes, I can be trusted to keep my computer safe.	Only if colleagues I trust do the same.	Yes, Information managers told us that it is necessary.	If I have time, yes.
Self-developed.		Who do you believe is responsible for dealing with Viruses/malware	Me, each one is responsible separately.	Everyone, we are all equally responsible.	We all share our piece of responsibility.	Information managers.
Self-developed.	Natural security/ access to buildings	Are you familiar with the Organization's facilities?	Yes		No	

Self-developed.		Do you know the process of entering the Organization's facilities as a visitor?	Yes		No	
Self-developed.		Do you check all people entering or exiting the Organization's facilities?	Yes		No	
Self-developed.		Can you estimate the importance of an incident when reported to you?	Yes		No	
Self-developed.		Do you know the handling procedure of an incident?	Yes		No	
Beautement et al., [12].	Information management	Do you lock your computer when you move away from your office?	Yes, I know how to keep my computer safe.	Only if colleagues I trust do the same.	Yes, Information managers told us that it is necessary.	No, what could go wrong?
Parsons et al., [9].		Do you dispose print-outs which contain sensitive information in the same way	No, I know how to keep documents I handle safe.	Only if colleagues I trust do the same.	No, Information managers told us that it is risky.	Yes, what could go wrong?

		as non-sensitive ones?				
Parsons et al., [9].		Would you plug a USB stick found in a public place into your work computer?	No, I know how to keep my computer safe.	Only if colleagues I trust do the same.	No, Information managers told us that it is risky.	Yes, what could go wrong?
Parsons et al., [9].		Would you leave print-outs that contain sensitive information on your desk overnight?	No, I know how to keep documents I handle safe.	Only if colleagues I trust do the same.	No Information managers told us that it is risky.	Yes, what could go wrong?
Beautement et al., [12].		Do you have a secure draw or storage area you can use?	Yes, I made one myself.	Yes, I share one with one of my colleagues.	Yes, I asked for one from my supervisor.	No, I was not given one.
Self-developed.		Who do you believe is responsible for Information management?	Me, each one is responsible separately.	Everyone, we are all equally responsible.	Information managers.	Not me.
Beautement et al., [12].	Security risk incidents	Who would you report a security concern to?	To the information managers, they are	To a colleague whom I trust.	To the information managers, as we were advised.	To the information managers.

			responsible.			
Parsons et al., [9].		Who would you report a security incident to?	To the information managers, they are responsible.	To a colleague whom I trust.	To the information managers, as we were advised.	To the information managers, they know what to do.
Parsons et al., [9].		Would you ignore poor security behavior by your colleagues?	No, each one should conform.	Only if colleagues I trust do the same.	No, Information managers told us that we should report immediately any poor security behavior.	Yes, it is not my job to supervise them.
Parsons et al., [9].		If you see someone acting suspiciously in your workplace, would you report it?	Yes, I know how to keep my workplace safe.	I ask a colleague whom I trust what to do.	Yes, Information managers told us that we should report immediately any suspicious behavior.	No, why should I?
Self-developed.	Security Updates and Corrections	Do you have a plan to identify systems where automatic	Yes, I have a plan of my own design.	Yes, I have created one with colleagues I trust.	Yes, I have created one according to standards.	No, I was not asked to create one.

		operating system updates are not available?				
Self-developed.		Do you have a plan that states which resource(s) will be used to determine if an operating system update is available?	Yes, I have a plan of my own design.	Yes, I have created one with colleagues I trust.	Yes, I have created one according to standards.	No, I was not asked to create one.
Self-developed.		Do you have a plan that directs how and by whom the update will be installed?	Yes, I have a plan of my own design.	Yes, I have created one with colleagues I trust.	Yes, I have created one according to standards.	No, I was not asked to create one.
Self-developed.	Contractor security	Do you think that a courier company employee entering the building could be a threat?	Yes		No	

Table 3. The ICBU-Q (Identification of Cultural Biases of Users - Questionnaire).

According to the work of Brenot et al., [36], cultural biases of individuals can explain the variance in risk perceptions amongst them and different cultural groups can be associated with concern or lack of concern. In addition, Rippl [31], suggests that it is possible to infer cultural aspects from individual-level data. Individuals perceive risks differently and similarities of individual values stem from similar social backgrounds. Therefore, we believe that the identification of cultural biases of individuals is feasible and could provide

us some useful information regarding their behavior in terms of information security within an organization. Finally, in the work of Tsohou et al. [32] it was emphasized that the cultural factors of individuals are of great importance and should be considered when designing information security awareness programs. Our method, namely the ICBU-Q, can help towards the identification of an organization's employees' cultural biases and assist in creating targeted interventions.

4 Discussion and Conclusions

In Chapter 3 we have presented our model which aims to identify the cultural biases of a typical organization' s employees regarding information security awareness and to classify them into four groups, namely, fatalists, hierarchists, individualists and egalitarians. As suggested in the work of Rippl [31], individuals perceive risks differently and similarities of individual values stem from similar social backgrounds. The author also suggest that it is possible to derive cultural aspects from individual-level data. In addition, according to the work of Brenot et al., [36], cultural biases of individuals can explain the variance in risk perceptions amongst them and different cultural groups can be associated with concern or lack of concern. These suggestions were considered in our work since we support that it is feasible to identify the cultural biases of individuals which will help us understand in more detail their behavior in terms of information security. Moreover, the importance of individuals' cultural factors is stressed out in the work of Tsohou et al., [32] and the author suggests that they should be considered when designing information security awareness programs.

The human aspect is still the weakest link in the information security chain and the behavior of IS users and their IS security awareness requires assessment and evaluation. While there is a number of methods that investigate the information security behavior, up to our knowledge, none of them identifies the cultural biases in organizations 'personnel which are neglected and not taken into account when designing information security awareness programs. Since there is a lack of targeted information security awareness programs that consider the cultural biases of organizations' employees, we hopefully believe that our method can be used toward this direction. Our method, namely the ICBU-Q, can help organizations to identify their employees' cultural biases and assist in creating targeted interventions, if necessary.

Our work is not of course without limitations. We were not able to employ and test our method in an organization to see if we are indeed able to classify the employees based on their cultural biases by using it. Even though we have pointed out the feasibility of identifying the cultural biases of individuals, our method remains a theoretical framework. However, we plan to use the ICBU-Q soon and test its validity.

Bibliography

[2] Information Technology Security Training Requirements: a Role- and Performance-Based Model. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-16/final. [Accessed 20 December 2020].

[1] ENISA's ten security awareness good practices. [Online]. Available: https://www.enisa.europa.eu/publications/archive/ar-security-practices-en. [Accessed 21 December 2020].

[3] Building an Information Technology Security Awareness and Training Program. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-50/final. [Accessed 22 December 2020].

[4] Building an Information Technology Security Awareness and Training Program. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-50/final. [Accessed 23 December 2020].

[5] Bulgurcu, Burcu & Cavusoglu, Hasan & Benbasat, Izak. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. 34. 523-548. 10.2307/25750690.

[6] D'Arcy, John & Hovav, Anat & Galletta, Dennis. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research. 20. 79-98. 10.1287/isre.1070.0160.

[7] Tejaswini Herath & H Raghav Rao (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations, European Journal of Information Systems, 18:2, 106-125, DOI: 10.1057/ejis.2009.6

[8] Karjalainen, Mari and Siponen, Mikko (2011) "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches," Journal of the Association for Information Systems: Vol. 12 : Iss. 8 , Article 3. DOI: 10.17705/1jais.00274

[9] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, Tara Zwaans, The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, Computers & Security, Volume 66, 2017, Pages 40-51, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.01.004.

[10] Bauer, Stefan & Bernroider, Edward & Chudzikowski, Katharina. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & Security. 68. 145–159. 10.1016/j.cose.2017.04.009.

[11] Snyman, D. and H. Kruger. “The application of behavioural thresholds to analyse collective behaviour in information security.” Inf. Comput. Secur. 25 (2017): 152-164.

[12] Beautement, Adam & Becker, Ingolf & Parkin, Simon & Krol, Kat & Sasse, Angela. (2016). Productive Security: A scalable methodology for analysing employee security behaviours.

[13] Kearney, WD & Kruger, Hennie. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation?. Computers & Security. 61. 10.1016/j.cose.2016.05.006.

[14] Kearney, Wayne D. and Hennie A. Kruger. “Theorising on risk homeostasis in the context of information security behaviour.” Inf. Comput. Secur. 24 (2016): 496-513.

[15] Marek, Jennifer M.. Presence of optimistic bias and illusion of control in information security risk perceptions. Capella University, 2015.

[16] Gizem Öğütçü, Özlem Müge Testik, Oumout Chouseinoglou, Analysis of personal information security behavior and awareness, Computers & Security, Volume 56, 2016, Pages 83-93, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2015.10.002.

[17] S. Pahnila, M. Siponen and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance," 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, HI, 2007, pp. 156b-156b, doi: 10.1109/HICSS.2007.206.

[18] Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol 2014;33(3):237–48.

[19] Arce I. The weakest link revisited. IEEE Secur Priv 2003;1(2):72–6.

[20] Jansson K, von Solms R. Phishing for phishing awareness. Behav Inf Technol 2013;32(6):584–93.

[21] Schultz EE, Proctor RW, Lien M-C, Salvendy G. Usability and security an appraisal of usability issues in information security methods. Comput Secur 2001;20(7):620–34.

[22] Zhang J, Reithel BJ, Li H. Impact of perceived technical protection on security behaviors. Inf Manag Comput Secur 2009;17(4):330–40.

[23] Stanton JM, Mastrangelo PR, Stam KR, Jolton J. Behavioral information security: two end user survey studies of motivation and security practices. In: Proceedings of the Tenth American Conference on Information Systems. New York: 2004.

[24] Trcˇek D, Trobec R, Pavešic´ N, Tasicˇ JF. Information systems security and human behaviour. Behav Inf Technol 2007;26(2):113–18.

[25] Snell, E., 2018. 78% of Healthcare Workers Lack Data Privacy, Security Preparedness. HealthIT Security (On-line). Retrieved from https://healthitsecurity.com/news/ 78-of-healthcare-workers-lack-data-privacy-security-preparedness.

[26] Morgan, S. (2017). Please don't send me to cybersecurity training. CSO (On-line). Retrieved from https://www.csoonline.com/article/3225471/security/ please-dont-send-me-to-cybersecurity-training.html.

[27] Aurigemma S, Panko R. A composite framework for behavioral compliance with information security policies. In: System Science (HICSS) 45th Hawaii International Conference on System Sciences. Maui, HI: 2012. p. 3248–57.

[28] Ng B-Y, Kankanhalli A, Xu Y. Studying users' computer security behavior: a health belief perspective. Decis Support Syst 2009;46(4):815–25.

[29] Douglas M, Wildavsky A. Risk and culture: an assay on the selection of technological and environmental dangers. Berkeley: California University Press; 1982.

[30] Slovic P, Fischhoff B, Lichtenstein S. Behavioral decision theory perspectives on risk and safety. Acta Psychol 1984;56(1e3):183e203.

[31] Rippl S. Cultural theory and risk perception: a proposal for a better measurement. J Risk Res 2002;5(2):147e65.

[32] Tsohou, Aggeliki & Karyda, Maria & Kokolakis, Spyros. (2015). Analyzing the role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs. Computers & Security. 52.10.1016/j.cose.2015.04.006.

[33] Langford I, Georgiou S, Bateman I, Day R, Turner R. Public perceptions of health risks from polluted coastal bathing waters: a mixed methodological analysis using cultural theory. Risk Anal: An Int J 2000;20(5):691e705.

[34] Marris C, Langford IH, O'Riordan T. A quantitative test of the cultural theory of risk perceptions: comparison with the psychometric paradigm. Risk Anal 1998;18(5):635e47.

[35] Tsohou A, Karyda M, Kokolakis S, Kiountouzis E. Formulating information systems risk management strategies through cultural theory. Inform Manag Comput Secur 2006;14(3):198e217.

[36] Brenot J, Bonnefous S, Marris C. Testing the cultural theory of risk in France. Risk Anal 1998;18(6):729e39.

[37] Safa, Nader & Furnell, Steven. (2015). Information security policy compliance model in organizations. Computers & Security. 10.1016/j.cose.2015.10.006.

[38] Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. Comput Secur 2015;53(0):65–78. http://dx.doi.org/10.1016/j.cose.2015.05.012.

[39] Furnell S, Clarke N. Power to the people? The evolving recognition of human aspects of security. Comput Secur 2012;31(8):983–8. http://dx.doi.org/10.1016/j.cose.2012.08.004.

[40] Safa NS, Ghani NA, Ismail MA. An artificial neural network classification approach for improving accuracy of customer identification in e-commerce. Malays J Comput Sci 2014;27(3):171–85.

[41] Coyle, D. J., 1994: The theory that would be king. Politics, Policy and Culture, D. J. Coyle and R. J. Ellis, Eds., Political Cultures Series: Westview Press.

[42] Von Solms R, Van Niekerk J. From information security to cyber security. Comput Secur 2013;38(0):97–102. http://dx.doi.org/10.1016/j.cose.2013.04.004.

[43] Werlinger R, Hawkey K, Botta D, Beznosov K. Security practitioners in context: their activities and interactions with other stakeholders within organizations. Int J Hum Comput Stud 2009;67(7):584–606. http://dx.doi.org/10.1016/j.ijhcs.2009.03.002.

[44] Safa NS, Ismail MA. A customer loyalty formation model in electronic commerce. Econ Model 2013;35(0):559–64. http://dx.doi.org/10.1016/j.econmod.2013.08.011.

[45] Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol 2014;33(3):236–47. doi:10.1080/0144929X.2012.708787.

[46] Arachchilage NAG, Love S. Security awareness of computer users: a phishing threat avoidance perspective. Comput Human Behav 2014;38(0):304–12. http://dx.doi.org/10.1016/j.chb.2014.05.046.

[47] Kritzinger E, von Solms SH. Cyber security for home users: a new way of protection through awareness enforcement. Comput Secur 2010;29(8):840–7. http://dx.doi.org/10.1016/j.cose.2010.08.001.

[48] Li H, Zhang J, Sarathy R. Understanding compliance with internet use policy from the perspective of rational choice theory. Decis Support Syst 2010;48(4):635–45. http://dx.doi.org/10.1016/j.dss.2009.12.005.

[49] Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Comput Secur 2005;24(2):124–33. http://dx.doi.org/10.1016/j.cose.2004.07.001.

[50] Webb J, Ahmad A, Maynard SB, Shanks G. A situation awareness model for information security risk management. Comput 12 computers & security 56 (2016) 1–13 Secur 2014;44(0):1–15. http://dx.doi.org/10.1016/j.cose.2014 .04.005.

[51] Herath T, Rao HR. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst 2009;47(2):154–65. http://dx.doi.org/10.1016/j.dss.2009.02.005.computers & security 56 (2016) 1–13 11

[52] Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83–95. http://dx.doi.org/10.1016/j.cose.2011.10.007.

[53] Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur 2013;32(0):90–101.http://dx.doi.org/10.1016/j.cose.2012.09.010.

[54] Son J-Y. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf Manage 2011;48(7):296–302. http://dx.doi.org/10.1016/j.im.2011.07.002.

[55] W. Alec Cram, Jeffrey G. Proudfoot & John D'Arcy (2017) Organizational information security policies: a review and research framework, European Journal of Information Systems, 26:6, 605-641, DOI: 10.1057/s41303-017-0059-9

[56] Pwc (2016) The global state of information security survey 2016. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

[57] Verizon (2016) 2016 data breach investigations report. http://www.verizonenterprise.com/DBIR/2015/

[58] Willison R Warkentin M. Beyond deterrence: An expanded view of employee computer abuse MIS Quarterly20133711-20

[59] Lowry P B Moody G D Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies Information Systems Journal2015255465-488

[60] Johnston A C Warkentin M Mc Bride M Carter L Dispositional and situational factors: Influences on information security policy violations European Journal of Information Systems2016253231-251

[61] Schmerken I (2015) Morgan Stanley data theft exposes insider threat & need for more restrictions. http://www.wallstreetandtech.com/security/morgan-stanley-data-theft-exposes-insider-threat-and-need-for-more-restrictions

[62] Weldon D (2015) Are your biggest security threats on the inside? http://www.cio.com/article/2985790/security/are-your-biggest-security-threats-on-the-inside.html

[63] Kiel, Joan & Ciamacco, Frances & Steines, Bradley. (2015). Privacy and data security: HIPAA and HITECH. 10.1007/978-3-319-20765-0_25.

[64] King N J Raja V T Protecting the privacy and security of sensitive customer data in the cloud Computer Law & Security Review2012283308-319

[65] KOOPS B- J The trouble with European data protection law International Data Privacy Law201444250-261

[66] Wall J D Lowry P B Barlow J B Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess Journal of the Association for Information Systems201617139-76

[67] Siponen M Information security standards focus on the existence of process, not its content Communications of the ACM200649897-100

[68] Spears J L Barki H User participation in information systems security risk management MIS Quarterly2010343503-522

[69] Wiant T L Information security policy's impact on reporting security incidents Computers & Security2005246448-459C

[70] Goel S Chengalur-Smith I N Metrics for characterizing the form of security policies Journal of Strategic Information Systems2010194281-295

[71] Landoll D J Information Security Policies, Procedures, and Standards2016Boca Raton CRC Press

[72] Whitman M E Town send A M Aalberts R J DHILLON G Information systems security and the need for policy Information security management: Global challenges in the new millennium2001IGI Global Hershey PA10-20

[73] Baskerville R Siponen M An information security meta-policy for emergent organizations Logistics Information Management2002155/6337-346

[74] Whitman, Michael. (2008). Security policy: From design to maintenance. Advances in Management Information Systems. 11. 123-151.

[75] Dhillon G Managing Information Security 1997 London Macmillan

[76] Efthymia Metalidou, Catherine Marinagi, Panagiotis Trivellas, Niclas Eberhagen, Christos Skourlas, Georgios Giannakopoulos, The Human Factor of Information Security: Unintentional Damage Perspective, Procedia - Social and Behavioral Sciences, Volume 147, 2014, Pages 424-428, ISSN 1877-0428, https://doi.org/10.1016/j.sbspro.2014.07.133.

[77] Orshesky, C. (2003). Beyond technology - The human factor in business systems. Journal of Business Strategy, 24, 4, 43-47.

[78] Kearney, P. (2010). Security: The Human Factor. Cambridgeshire: IT Governance Publishing.

[79] Thomson, K., & Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behavior. Information Management & Computer Security, 20, 1, 39-46.

[80] Layton, T.P. (2005). Information Security Awareness – The Psychology behind the Technology. Bloomington IN: AuthorHouse.

[81] Ashkanasy, N. & Broadfood, L. & Falkus, S.. (2000). Questionnaire Measures or Organizational Culture. Handbook of Organizational Culture and Climate.

[82] Adéle da Veiga, Nico Martins, Defining and identifying dominant information security cultures and subcultures, Computers & Security, Volume 70, 2017, Pages 72-94, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.05.002.

[83] P. Brewerton, L. Millward Organizational research methods Sage, London (2001).

[84] Berry, M.L., Houston, J.P. 1993. Psychology at work Brown and Benchmark, Madison, WI (1993).

[85] Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. Computers & Security, 31(2), 221-232. doi: 10.1016/j.cose.2011.12.001

[86] Wildavsky, A., & Dake, K. (1990). Theories of Risk Perception: Who Fears What and Why? Daedalus, 119(4), 41-60. Retrieved February 24, 2021, from http://www.jstor.org/stable/20025337

[87] Favre, M. and Sornette, D. Forms of Social Relationships in Distinct Cultural Settings (April 29, 2016). Available at SSRN: https://ssrn.com/abstract=2772520 or http://dx.doi.org/10.2139/ssrn.2772520