**Cybersecurity Readiness Model Based on Human Factors**

Human error is one of the leading cause of data and security breaches as attackers prey on psychological manipulations to push users into performing unwanted actions or providing information. The human factor is a weak link in both prevention and mitigation of cyberattacks and as a result, organizations are prone to phishing, business email compromise and malware types of cybersecurity attacks. The objectives of this thesis are: (1) to understand the human factors that influence cybersecurity and (2) to develop a readiness model to help organizations assess and implement security practices for cybersecurity from human factor perspective. We performed a multivocal literature review to identify human factors and respective best practices that influence cybersecurity. Next, the identified factors and best practices were employed to develop a readiness model. The readiness model was validated by applying to real world scenario using the case study approach. We also aim to develop an online tool to support the implementation of the readiness model. This thesis will provide other researchers with a firm basis and knowledge on developing effective threat prevention strategy for human factors in cybersecurity.

General Terms:

Multivocal literature review; Readiness model; Cybersecurity; Human factor

# Introduction

Cybersecurity has developed over the years and is centered around keeping up the secrecy, trustworthiness, and accessibility of Information Technology (IT) frameworks and systems [1]. Cybersecurity ensures an interlinking process of securing computing assets and information through resources identification and risk assessment; recognition of malware and malevolent conduct; reacting to observed vicious activities; and recuperating systems to a normal state. The cybersecurity implementation that are employed for such operations include role-based authentication, intrusion detection system, encryption, etc. [1].

One technique of enabling effective cybersecurity is to play it as a game by shifting the defense to the attackers, which is a concept known as moving target defense. It is a stratagem through which the defenders will preempt and predict the likely modes and methods the attackers could use to launch their havoc and thereby work in advance to make such attacking endeavors futile. The cybersecurity techniques that can be employed for this purpose include address space layout randomization, instruction set randomization, in-place code randomization, IP randomization, port randomization, etc. In this paper, we adopt cybersecurity definition as *“the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets* [2]*.”*

Research [3],[4],[5],[6],[7] indicates that workers’ negligence in following cybersecurity procedures is often due to extraversion, agreeableness, ignorance, conscientiousness, and openness to experience. For example, in one of the industrial report [8], it was mentioned that 95% of all security incidences can be traced to human factors; attackers utilize several social engineering techniques to take advantage of the vulnerabilities that arise from human behaviors. Some of the practices that lead to such susceptibilities are malicious software installations, fixing bugs by means of irregular software patching, divulging of sensitive information, connectivity to insecure and untrusted networks such as Wi-Fi, unprofessional web applications, and database management that gives way to exploitation by cross-site scripting and SQL Injection [3],[4],[9],[10].

As pointed out by Mancuso (2014), *“The Human Factors community has begun to address human-centered issues in cyber operations, but in comparison to technological communities, we have yet to scratch the surface”* [11]. And according to the definition by Human Factors and Ergonomics Society (HFES) [12], *“Human factors (or ergonomics) is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data, and other methods to design in order to optimize human well-being and overall system performance.”* Indisputably, virtually all networks comprise humans as essential parts.

The different perspectives in which humans are viewed in the cyber environment can be either defenders or attackers. Not only just attacking role, all types of roles played by humans in the network are liable to put it into serious hazards [13]. This is however different from the general believe. A higher percentage of people conceives the notion that cyberattacks use to be initiated by an attacker or adversary. Conversely, this is not always the case. Often at times, the sources originate from inside, either as a result of incompetency or carelessness of the defenders, or through a security breach emanating from the organization itself, which is often as a result of failure in conforming to any of the cybersecurity best practices.

In recent times, cyber attackers have exploited human vulnerabilities by deceiving people into breaching standard security practices. Cyber attackers prefer to exploit human factors related vulnerabilities because it requires little efforts compared to devoting lot of resources and time to break through fortified security devices and systems [4]. Human factor is situated within the insider attacking perimeter; It is often triggered by annoying and sadist employees or appeals to personnel’s intuition via social engineering [9]. The human factor is a weak link [14] in both prevention and mitigation of cyberattacks and as a result, organizations are prone to phishing, business email compromise and malware types of cybersecurity attacks.

Despite importance of understanding role of human factors in cybersecurity, only few empirical studies have been done to oversee the effectiveness of handling the human factors; and human factors assessment is very vital for organizations to figure out the technical and non-technical employees weaknesses [15],[16]. Even though researchers and industrial practitioners have investigated cybersecurity human factors in both white (published journal papers and conference proceedings) and grey (technical reports, online forums and blog posts) literature, yet we found only about 3 published secondary studies ([17],[18],[19]) somewhat focusing on the topic area. However, none of these found reviews considered the inclusion of both the academic literature and practitioners’ documentations. It is also worthy of note to state that our study is closely based on the human factors’ aspect of the cybersecurity. We believe cybersecurity is a very wide subject, thereby limiting our research scope will ensure an in-depth exploration and realistic endeavor.

The aim of this thesis is to propose a readiness model that will be built from the identified success and barrier human factors to be considered in the cybersecurity tradition within the organization. The identified human factors will be the product of a meticulous review of the available literature and empirical investigation in industries. The proposed model will assist organizations and practitioners to better handle human factors in the security cyberspace. This thesis contributes… our work will assist organizations and researchers alike in better understanding the different affecting roles played by the human factors in the cybersecurity environment.

The remainder of the paper is arranged as follows. In section 2, we discuss the background and review related work. In section 3, we state the research objective and questions.

In section 4, we describe the methodology. In section 5 and 6, we broadly detail and discuss the findings’ reports. In section 7, we treat the threats to validity. In section 8, we conclude the study and highlight future direction.

# BACKGROUND AND Related Work

In this section we review literature related to human factors in cybersecurity, present the background of readiness model. We round off the section by examining the related studies to our work that cover the human factors of cybersecurity; we also analyzed their research gaps and what distinguish our work from theirs.

## Review of Existing Literature

Gyunka and Christiana [4] posited human factors as the major cybersecurity threats. Authors analysed the attackers and defenders’ roles in cyber threats’ ubiquity and the future effects their activities will have on security infrastructures. They performed a case study research approach using the attack against a security firm in the USA, HBGary Federal. Their analysis exposed that individuals and organizational security are damaged and impacted by human attitudes and errors such as ignorance, carelessness, negligence, sabotage by insiders - often disgruntled employees, and also illiteracy to some security practices.

Hadlington [15] undertook an exploratory research regarding attitudes on cybersecurity in companies and organizations, and relationship among some risky cybersecurity behaviors, including impulsivity and addiction to the internet. Author collected data via questionnaire in an online survey involving participants working as part-time and full-time in the UK. Out of 538 sent questionnaire, 515 were answered and used for data analysis. The results of the survey showed that internet addiction was significantly responsible for risky cybersecurity behaviours. It was additionally mentioned that aspects of personality and employee attitudes are also problematic to effective cybersecurity practices. Authors finally suggested focusing on awareness mechanisms and adequate training to strengthen organizational cybersecurity culture.

Vieane et al. [20] set up a panel composed of specialists from the human factors domain to discuss how to collectively take maximum advantage of the past and present research works in human factors in cyber operations. Panelists argued that the available works only do focus mainly on the cyber technological aspects. They furthermore opined that there is still a major existing gap as regards understanding the human factors and the current research meant to deal with relevant issues. The areas addressed by the panelists include Training Challenges in Cyber Security, Cyber-Cognitive Situation Awareness, Cognitive Coordination of Multi-Sensor Cyber Data, Vigilance in Cyber Security, Attention Switching in Cyber Security.

Lathrop et al. [1] documented the core human factors of cyberspace activities viewing from a practitioner’s perspective. Authors claimed that innovation and their associated resources give primary focus on technology, and do not really emphasize on human factors relating to recruitment, training, and keeping up with capabilities. They stated that failure to comprehend the nature of the cognitive work and the goals in cyberspace operations has led researchers and vendors to erroneously apply information technology solutions to cyberspace operations problems. Authors concluded by proffering recommendations on how to effectively incorporate cognitive engineering and experimental psychology practices into research and development projects.

Henshel et al [21] proposed integrating individuals’ national culture into the human factors component of the cybersecurity risk assessment framework. Authors maintained that such inclusion will enable measuring and more understanding of how cybersecurity risk is affected by human factors. They pointed that culture is an important human element factor but has been understudied in cybersecurity literature. They identified key cultural metrics and then integrated them into a Human Factors Framework and Ontology which was modelled for figuring out cybersecurity risk assessment metrics. It was researched that the types of culture that affect human behavioral characteristics and interactions with the internet are ethnic, geographic, national, religious, organizational, and social. They finally recommended assessment of attacks and cultural indications intent which will enable incorporation of cultural metrics and biases in predictive modeling.

Widdowson and Goodliff [22] developed a tool for cyber human error assessment that addresses human factors in cybersecurity assessment. Authors believe that existing works on human factors do not fully take into account the Psychological motivations that result to human error in cyber-security situations. They therefore designed a tool employing Applied knowledge of human limitations and cognitive biases to structurally capture human errors. The tool proactively assesses organization’s cybersecurity vulnerability and identifies human-related root causes during formal incident investigations. The authors held that recognizing the Psychological root causes behind human errors in cyber-security scenarios will be useful in recognizing appropriate risk management and mitigating techniques.

Whitty et al. [23] researched that people still indulge in risky password practices despite having been advised regarding such through many campaigns. Authors also stated that there is not enough available researches on the individual differences that exist in cybersecurity behaviors. They then undertook an online questionnaire-based survey hosted on Qualtrics survey platform for collecting data regarding how people behave in their daily activities. They got responses from 497 participants. It was found that individuals who scored high on a lack of perseverance would likely have their passwords shared. Also, younger people and those who score high on self-monitoring would likely share passwords as well.

Marble et al. [24] conducted a review to find out how cyber threats spread and the roles of the attackers and defenders (users). Authors also explored the users’ unawareness of cyber threats and the modern cyber environment complexity which include cyber risks, engineering approaches and the tools used in mitigating the threats. They further reviewed required researches at individual and group levels relating to users’ psychology which will thus assist organizations to implement actions against cyber threats. Authors summed up future research needs and conclusions which are (1) cyber threats continually make cyber environments more uncomfortable for users; (2) The use of “red” teams to search vulnerabilities in cyber defenses enables users and organizations to better protect themselves (3) Timely actions are essential to oppose attacks threats that mostly occur at internet speeds.

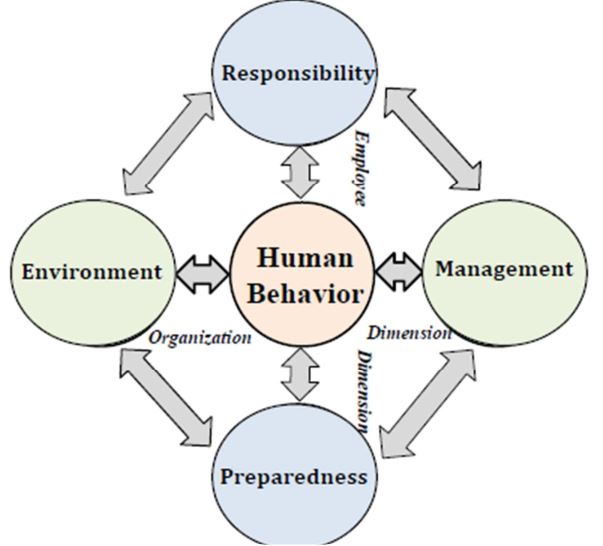


Figure 1: The human factor diamond (HFD) framework [25]

## Readiness Model

Readiness model is employed in software development for the purpose of measuring organizations' readiness in addressing and handling a collection of tasks or concerns.

Ali and Khan [26] built a software outsourcing partnership model to discover factors that are critical for vendors to convert their existing outsourcing relationship to partnership. In order to identify these critical success factors, authors conducted systematic literature review and subsequently categorized the identified factors into partnership levels according to the CMMI and based on the readiness model of a previous work on Software Outsourcing Vendors. They then validated and evaluated the SLR findings using a questionnaire survey and case studies of outsourcing industries.

Mufti et al. [27] designed a readiness model for security requirements engineering for allowing organizations to identify and analyze their readiness levels. Authors performed a systematic mapping study to identify and analyze relevant studies, and thereafter built the readiness model based on the categorization of the best practices extracted from the mapping study.

Wu [28] developed a readiness model to measure if IT organizations can fulfil criteria for web service adoption. Authors analyzed characteristics of web service adoption using readiness constructs. The characteristics that were analyzed are high compatibility, high customizability, and high divisibility

## Related Work (Secondary Studies, Framework, and Model)

Glaspie and Karwowski [18] performed a review on human factors as regards information security culture. The authors mentioned the factors that are important for the security culture of an organization. They maintain that their review findings will help further research in the area of security culture.

Ani et al. [17] reviewed cybersecurity issues and solutions. Authors highlighted several solutions which are initial comprehension of IT security trends that are related to cyber threats, vulnerabilities, risks, attacks, and how they affect the industries as well as the individuals that work in them.

Young et al. [29] proposed a framework by depicting cybersecurity as a system state. Authors modeled that entity's behavior causes system change. Furthermore, they opined that interventions are capable of changing entities’ behavior in order to augment desirable behavior and prevent undesirable behavior. They held that their framework recognizes three modes of actor behavior in the system that impacts cybersecurity, and they promote coming up with successful interventions.

Ani et al. [30] presented a workforce cybersecurity capability evaluation model to assist enterprises identify specific cybersecurity vulnerabilities. Authors categorized industrial control systems workforce into three parties which are IT security experts, engineers/field operators/technicians, and corporate managers. They claimed their model will help organizations determine the employees' cybersecurity awareness levels and responsiveness.

### Motivation and Research Gaps

The closest found references to our work are [29] and [30]. The former introduced a system state cybersecurity framework by modeling entity's behavior that causes system change, while the latter proposed a workforce cybersecurity capability evaluation model to aid enterprises identify specific cybersecurity vulnerabilities. However, the studies have observable limitations. Authors did not systematically collect the data that were used for their models, and also, the models were not empirical validated using the industrial practitioners who are the ones that are well-versed in the researched-topic domain.

According to the best of our knowledge, no research to date has built a readiness model by considering human factors that impact cybersecurity as well as the factors that hamper its management in the industrial environment. The existing literature were mostly dedicated to general survey of classifying cyber threats operations and corresponding issues. This thesis will provide other researchers with a firm basis and knowledge on developing effective threat prevention strategy for human factors in cybersecurity.

# RESEARCH OBJECTIVE AND QUESTIONS

In this section, we state the objective of the research as well as the research questions.

## Research Objective

The objective of this research is to propose a Cybersecurity readiness model based on human factors. In order to achieve the objective, we have the following sub-objectives:

• To identify barrier human factors that hinder and impede cybersecurity processes based on findings from the literature

• To identify success human factors that facilitate and help cybersecurity operations based on findings from the literature

• To develop a readiness model to assess an organization’s readiness for cybersecurity from human factor perspective

• To evaluate the readiness model in the real-world environment

## Research Questions

The research questions of the study are as follows:

**• RQ1**: What are the human factors that have a negative impact on cybersecurity?

We aim to use this question to discover the inherent aspects of a human that are disadvantageous to the cybersecurity framework. The term human here is referring to the end users and employees in the cybersecurity environment. So, we are basically interested in their behaviors that often lead to the failure or unsuccessful of the cybersecurity fortress. Either during their private operations or company’s public connection with the computing devices and information technology facilities.

**• RQ2**: What are the human factors that have a positive impact on cybersecurity?

We intend to use this question to figure out the innate characteristics of a human that are advantageous to the cybersecurity stronghold. What we are concerned about is their behaviors that help in the improvement and progress of the cybersecurity fortress. Either during their private or public connection with computing devices and information technology facilities.

**• RQ3**: How can a practical and robust readiness model to manage human factors for cybersecurity be developed?

The rationale behind this research question is to utilize the findings of RQ1 and RQ2 to come up with a structural model that will be capable of assessing and checking organizational readiness towards maintaining effective cybersecurity.

# Research METHODOLOGY

The research methodology for this thesis work consists of six chronological phases which are as follow:

* First Phase: Setting up criteria for the readiness model
* Second Phase: Data collection through Multivocal Literature Review (MLR)
* Third Phase: Analysis, rationalization, and structuring of the findings from phase 2.
* Fourth Phase: Development of the readiness model based on the outcome of Phase 3
* Fifth Phase: Evaluation of the readiness model through case studies.
* Sixth Phase: Building of the online tool/framework

An overview of the research methodology is shown in Figure 2.

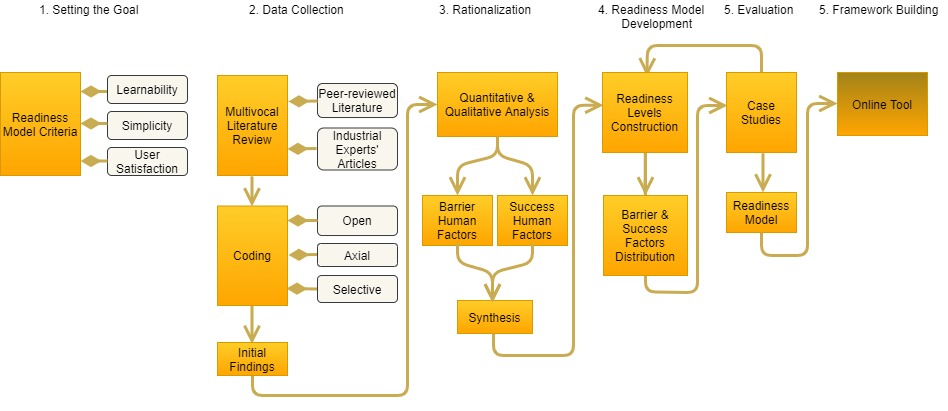


Figure 2: Overview of Readiness Model Methodology

## Readiness Model Criteria

This is the first phase of the readiness model. The rationale behind coming up with criteria is to serve as our foresight and target during the development of the readiness model. Our objective is to eventually build a model that will be potentially utilized by end users. We adopted one criterion directly from [31], and developed some other two. The criteria are as follows.

### Learnability

The readiness model should be a design in which all steps for its overall derivation are carefully explained such that end-users and organizations can comprehend it without requiring any complementary or supplementary assistance either in person or material.

### Simplicity

The model should not be structured in a big, complex, and highly technical way which will make it difficult and time consuming for the end users and organizations to follow.

### User Satisfaction [31]

The end users should be satisfied with the results of the model and be able to utilize it to meet their objectives regarding their needs and expectations.

## Data Collection

This is the second stage of the readiness model. In this phase, we employed an MLR to collect needed data from varying sources. To capture and extract data that are sparsely distributed in the literature, it is required to systematize the task. Therefore, we are employing an MLR in order to classify, link, and synthesize the state-of-the-art and practice in human factors area of cybersecurity. Details of the collection processes are explained in sequel.

### Multivocal Literature Reviews

Multivocal literature review is now also gaining ground in Software Engineering (SE). Before in SE, the two most popular review methodologies being used are the systematic literature review (SLR) and systematic mapping (SM). However, in the present age, the MLR is now also getting rapidly embraced. The limitation of SLR and SM studies to only formally published papers has prompted researchers to require its necessity. From Ogawa and Malen [32], *“Multi-vocal literature is comprised of all accessible writings on a common, often contemporary topic. The writings embody the views or voices of diverse sets of authors (academics, practitioners, journalists, independent research and development firms, and others).”* In MLR, all kinds of online artifacts are useful, including presentation materials, documentations, and short articles.

Many software practitioners do not normally publish in academic settings [33], and for the fact that SE is a practical-oriented area, there is need to have a review which provides more insight into the “state of the practice” and thereby leads to a synergy between the state-of-the art and practice [34].

Quite a few MLRs have been published in SE, even though some of the available works did not explicitly follow adopt the multivocal technique. Its advent into SE can be traced to the year 2013 in [10]. Also, there are some SLRs too that contain very few grey literature. Typically, the main difference between the SLR and the MLR is that, in MLR, a considerable amount of grey literature must be involved in the review. The grey literature refers to print or electronic literature that is produced by government, academia, business and industry and is not controlled by commercial publishers [35].

For this work, our MLR procedure can be found in Figure 3.

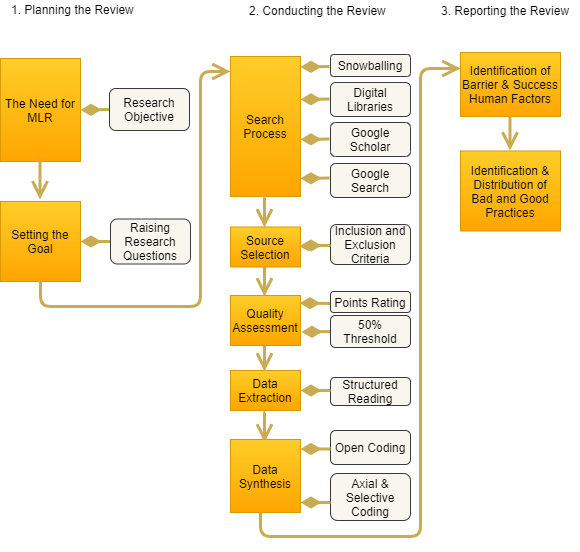


Figure 3: Multivocal Literature Review Methodology

We adopt the guidelines by Garousi et al. [36]. The guidelines are broadly divided into three phases which were also in turn obtained from Kitchenham and Charters SLR protocol [37]. These phases are:

• planning

• conducting and

• reporting the review for conducting MLRs

#### Planning the Review

According to the authors of the guideline, the planning phase should entail raising the need for an MLR, setting the goal, and raising the research questions. All these have been aptly taken care of in the previous section of the paper where we stated the motivation and objective of the study.

#### Conducting the Review

This phase consists of other five chronological steps which shall be followed in sequel. The steps are:

• search process

• source selection

• quality assessment

• data extraction and

• data synthesis

#### Search Process

We collected data by first applying snowballing on the three secondary studies [17],[18],[19] found which are closely related to the topic. Snowballing [38] is a technique of identifying additional papers through the papers contained in the reference list or through the citations to the paper. When reference list is used, it is called backward snowballing but when citations to the paper is used, it is known as forward snowballing.

In addition to the snowballing, digital libraries, Google Scholar, Google searches were performed to obtain more papers on cybersecurity human factors. The search string was constructed using (1) keywords in relevant papers, (2) keywords’ synonyms and alternative spellings, and (3) applying the Boolean operators AND and OR for the combination of alternative spellings, major terms and synonyms. Below is the search string with the different used permutations of the search terms to acquire the publications from search engines: (“human factor” OR “human factors”) AND (“behaviour” OR “behaviours” OR “behavior” OR “behaviors”) AND (“cyber security” OR “cybersecurity” OR “cyber-security” OR “computer security” OR “information security” OR “security”). The retrieved publications make a set of initial articles. The sum total of preliminary publications fetched from this process were 287 articles. Their titles and authors were entered into

the spreadsheet.

* + - * 1. **Source Selection**

All the scientific and grey literature from the snowballing and the repositories search were taken and subjected to further selection process to determine the relevant and discard the irrelevant studies.

In the case of the snowballing, in the backward snowballing, we took all references from the 3 papers which gave a total of 306 references; in the forward snowballing, 64 papers were gotten from Google Scholar from all the citations of the 3 papers. Then at this stage, some selection criteria [37] were applied to filter both set of papers in the references and citations categories. This thereby reduced the 306 references’ papers to 13 and 11 for the barrier and success factors respectively, whereas the 64 citations’ papers were reduced to 8 and 7 for the barrier and success factors respectively. The snowballing procedure for the barrier and success factors are pictured in Figures 4 and 5 respectively.

And in the case of the studies from the repositories search, the title column was then sorted in alphabetical order to reveal duplicates. Thereafter, after reviewing the titles and analyzing some of the papers’ abstracts, few papers were discarded. Furthermore, the full texts of the remaining papers were scrutinized and carefully reviewed to determine the studies which will eventually meet the inclusion criteria. The flow of the search process as described is displayed in Figure 6.

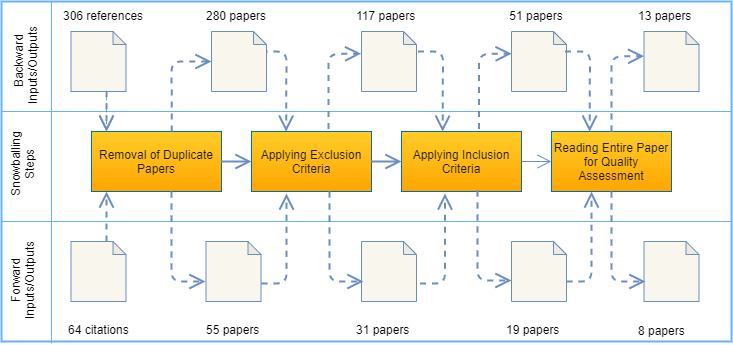


Figure 4: Snowballing procedure for barrier human factors

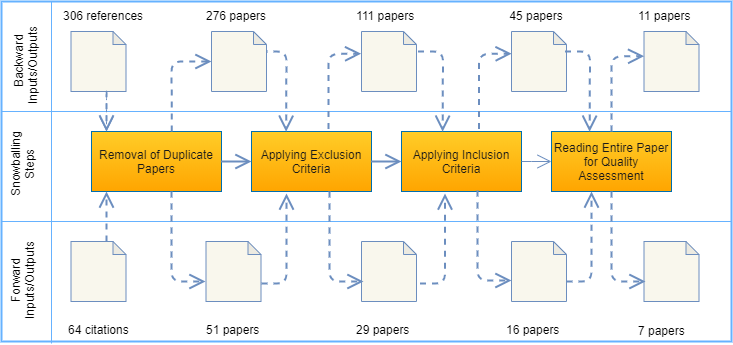


Figure 5: Snowballing procedure for success human factors

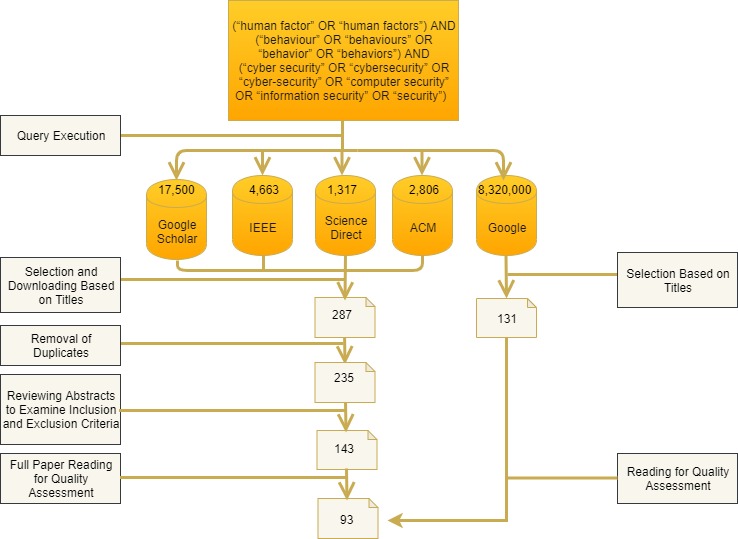


Figure 6: Search and source selection flow

At this stage, we then carried out inclusion and exclusion criteria to be able to filter the set of significant primary papers that will be most essential for extracting the barrier and success human factors. In the criteria designed to consider the inclusion eligibility of any primary study; the study must discuss human factors in relation to cybersecurity and contain at least either one barrier or success human factor. On the other hand, studies which are not written in English, or the full-text is not available online, or studies originating from the same authors with same themes are all excluded. Table 1 and Table 2 contain the inclusion and exclusion criteria for formal and grey literature respectively.

Table 1: INCLUSION AND EXCLUSION CRITERIA FOR FORMAL LITERATURE

|  |  |
| --- | --- |
|  | **Inclusion Criterion** |
| 1 | Discusses human factors in relation to cybersecurity |
| 2 | Must contain at least one barrier or success human factor |
| 3 | Journal and conference papers |
|  | **Exclusion Criterion** |
| 1 | Non-English written |
| 2 | Full-text not accessible online |
| 3 | Publications from same authorship with very similar themes |
| 4 | Books and book chapters |

Table 2: INCLUSION AND EXCLUSION CRITERIA FOR GREY LITERATURE

|  |  |
| --- | --- |
|  | **Inclusion Criterion** |
| 1 | Discusses human factors in relation to cybersecurity |
| 2 | Must contain at least one barrier or success human factor |
| 3 | Reports, short articles, blog posts, and presentations |
|  | **Exclusion Criterion** |
| 1 | Non-English written |
| 2 | Full-text not accessible online |

* + - * 1. **Quality Assessment**

We formulated the quality assessment criteria as follow-up to the inclusion and exclusion criteria to further determine the validity of each source and the extent to which it is bias free. This is particularly important because of the involvement of the grey literature which obviously would not have undergone any prior controlled review. The quality assessment checklist can be found in Table 3 and Table 4 for both formal and grey literature respectively. We designed the checklist according to the laid down guidelines in [36] so as to take care of the grey literature validity and reliability requirements. A criterion was also developed to check for a research question of this study.

Any study that contains answer to a criterion in the checklist is awarded 1 point. But if the study does not satisfy the criterion, then it receives 0 point. Afterwards, when the summations of the points are calculated, and the percentages are computes, whichever study attains the 50% threshold and above qualified as the primary study of the review while others were discarded. Eventually, a total of 114 articles made the final list.

* + - * 1. **Data Extraction**

Now we aim to obtain direct evidence about the research questions. As recommended by Cruzes and Dyba [38], prior to starting the extraction we had first read all the set of the papers in order to be familiar and immersed with the depth of evidence in the data. The reading helped us to grab initial ideas and to establish the likely direction through which we would shape the data.

We undertook a structured reading for extracting data from the studies. Structured reading is a technique proposed by Cruzes et al. [39]. The technique assists in exploring evidences in a procedural way. It makes identifying context information and paper findings relatively easy,

Table 3: QUALITY ASSESSMENT (QA) CRITERIA CHECKLIST FOR FORMAL LITERATURE

|  |  |
| --- | --- |
| **Criterion Number** | **Quality Assessment Criterion** |
| C1 | Is there a stated methodology for the source? |
| C2 | Does it have a clearly stated aim? |
| C3 | Does it contain objective statement? |
| C4 | Does it cover a specific question? |
| C5 | Does it enrich the research? |
| C6 | Is there a barrier or success cybersecurity human factor mentioned? |
| C7 | Are there authoritative references? |

Table 4: QUALITY ASSESSMENT (QA) CRITERIA CHECKLIST FOR GREY LITERATURE

|  |  |
| --- | --- |
| **Criterion Number** | **Quality Assessment Criterion** |
| C1 | Is the online article organization reputable? |
| C2 | Does it have a clearly stated aim? |
| C3 | Are the statements in it as objective as possible? |
| C4 | Does it enrich the research? |
| C5 | Does it enrich the research? |
| C6 | Is there a barrier or success cybersecurity human factor mentioned? |
| C7 | Is there a clearly stated date? |

effective, and efficient.

We prepared a data extraction form as depicted in Table 5 to facilitate the recording of full details of the papers under review and to be specific about how each of them addressed the research questions.

Table 5: DATA EXTRACTION FORM

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Study data** | **Description** | **Research Question** |
| 1 | Study ID |  |  |
| 2 | Authors, Title, Year |  |  |
| 3 | Publication Source | Journal, conference, organization, blog |  |
| 4 | Type of article | Paper, report, short article, presentation |  |
| 5 | Application context | Academic or industrial |  |
| 6 | Barrier human factor | What are the human factors that have a negative impact on cybersecurity? | RQ1 |
| 7 | Success human factor | What are the human factors that have a positive impact on cybersecurity? | RQ2 |

The data extraction shows general information about each study, and contains information such as authors, title, year of publication, paper source, article type, and the data regarding each research question was carefully recorded. The motive behind all these is to have a documentation that will enable easy collection and gathering of data from the final primary studies that are included in the review.

* + - * 1. **Data Synthesis**

we utilized qualitative coding to synthesize the data. The coding step entails two main procedures. They are (1) open, and (2) axial and selective coding.

* **Open Coding**: In open coding, the researcher’s mission is to inspect the data to comprehend the bottom line of what is being expressed [40]. In this work, we investigated the multivocal review extracted data, which provided answers to the extraction form. We devised conceptual names called codes to denote our understanding of the statements in the data extraction form. Codes are represented by a single of word, or combination of two or more words. The open coding resulted in collecting the human factors relating to the research questions.
* **Axial and Selective Coding:** The axial coding deals with grouping or relating concepts in order to give rise to new categories [40]. We used the concept to precisely link connections and relationships among several success human factors and barriers as they spread across the pool of the studies.

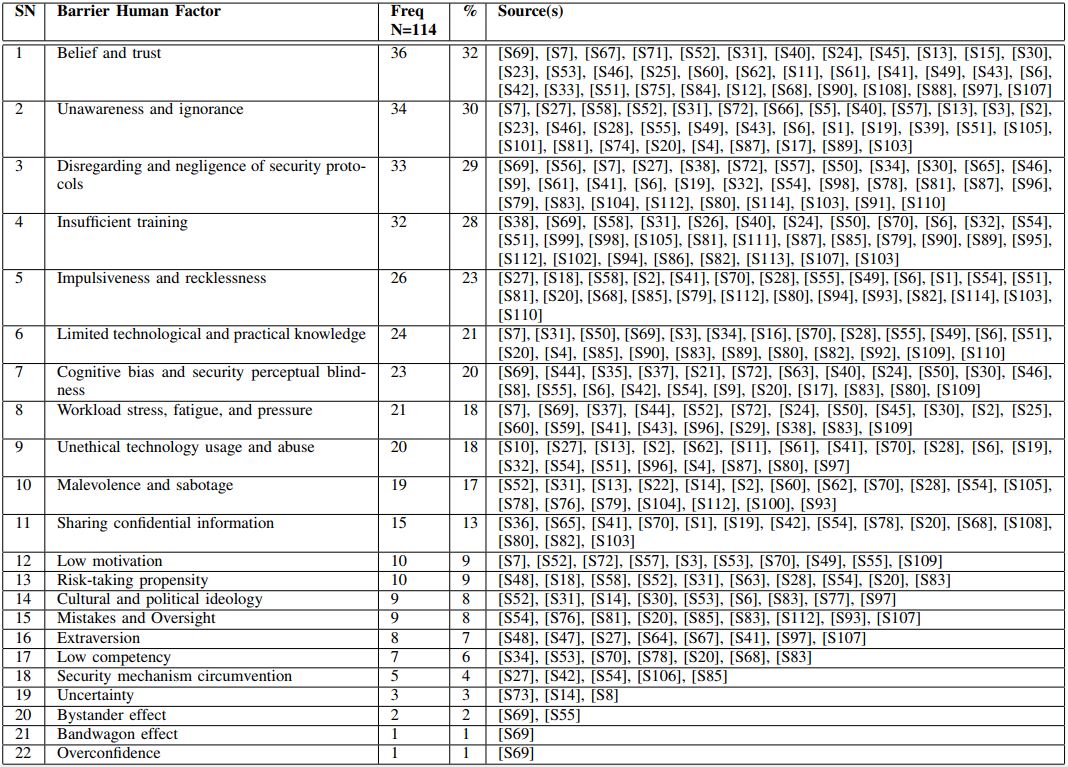
## Analysis and Rationalization

This is the third phase of the readiness model. In this section, we will present the results of RQ1 and RQ2.

### Barrier Human Factors of Cybersecurity, as Identified in the Literature (RQ1)

In this result, we identified the human factors that are impediments to a successful cybersecurity endeavor and culture according to the evidences from the literature. We accomplished our identification, classification, and categorization by utilizing the coding approach which is based on the techniques of grounded theory. We have described these coding procedures in an earlier section. The identified barrier human factors are presented in Table 6. The higher the frequency or percentage of a factor indicates its popularity across the literature. We elucidate each barrier in the following subsections appended with their citations for mapping correspondence.

Table 6: BARRIER HUMAN FACTORS OF CYBERSECURITY



#### Belief and trust

This is the most evidenced barrier found in our study among the primary studies. It occurs in 36  
studies. This barrier is related to how humans can be exploited as a result of the feelings they have on the system or on other people that they would not be harmed and there will not be a consequence for their actions. They would be tempted to do things that are damaging and that will have repercussions to the cybersecurity. Luo et al [S42] explained beliefs as “referring to the differences between the victim’s beliefs about the SE attacker and SE attacker’s beliefs about his anticipated or definite victims.” Often in several situations people tend to have beliefs in their closed ones, be it relatives or colleagues  
in work places, without knowing what is in the intention of the other person that is being trusted. As it is, cyberattacks can originate and come from anywhere, even from the closest of friends and loved ones. Widdowson and Goodliff [S69] supported this that there is “increased likelihood of believing information passed from friend or colleague,...”

Huang et al [S33] as well examined the belief. Authors state that “there are two critical determinants of users’ belief: one is perceived usefulness (PU), defined as the extent to which a person believes that using a particular technology or system will be useful or will enhance his/her task performance; the other is perceived ease of use (PEOU), defined as the extent to which a person believes that using a technology or a system will be effortless.” We understand from the authors that users are interested in what will enhance and ease their systems’ usage. This implies that they will not mind in performing the abominable acts in order to fulfill their aim with the system. Some of these acts lead them to fall into cybersecurity bad practices by so doing. It was also mentioned that attackers do gather necessary details about victims by manipulating trust. According to Luo et al. [S42] the attacker will then “try to build rapport with the intended victim to gain his/her trust. Exploiting the established trust, the SE attacker can then persuade the victim to perform desired actions (i.e., revealing confidential information) which would not normally occur otherwise”. Another additional view on trust was explored by Posey et al. [S60],[S59]. In a case whereby “employees experiencing increased scrutiny from internal security measures will attribute more of a lack of trust from their supervisors and will engage in more deviance.” Such situations will tend to make the victimized employees lose their respect and thereby will also engage in bad practice as a result.

And in relation to technology “trust may also contribute to cyber-security incidents. Some people may place too much trust in technology and its ability to protect them from a cyber attack [S69]”

#### Unawareness and ignorance

This is the second most cited barrier according to our study. It appears in 34 studies. This is the human factor associated with the lack of awareness and reason for an effective and efficient cybersecurity. From the explanation by Dutt et al. [S17] and Barford et al. [S8] Awareness from cybersecurity perspective “includes situation recognition: the perception of the type of cyber attack, source (who, what) of the attack, and target of the attack; situation comprehension: understanding why and how the current situation is caused and what is its impact; and situation projection: determining the expectations of a future attack, its location, and its impact.” Linkov et al. [S41] also emphasized how problematic the unawareness of cybersecurity is and mentioned the necessity of knowing and working towards it. Metalidou et al. [S49] stated that “lack of awareness is related with a lack of general knowledge about attacks.”

Based on a fact report from mti [S101], there is indication that “over 75% of large organizations suffered staff-related security breaches in 2016, and half of the worst of these were caused by human error based on a lack of user awareness or knowledge.” There is obviously no gainsaying to this. It is typical of employees whenever they are new to an organization or a system to be unaware of the activities and operations already going on, so this will of course affect the security aspects in that sense.

#### Disregarding and negligence of security protocols

This barrier is found among 33 studies in our review. The employees’ attitudes of taking work practices for granted is a commonplace. But if it is done as regards security, the price is always high. Parsons et al. [S56] conducted a questionnaire-based survey. Authors mentioned about “cases where employees know an information security policy and may believe that it is unnecessary or excessive.” There is a predisposition by employees and users to underplay cyberattack risks, particularly when it means such risks would cause a change in their personal or work lifestyle [S69].

Another reason for the barrier of neglecting and not caring about security protocols as highlighted by Parkin et al. [S54] is if employees find it difficult and complex to adapt with a mandated security practice. They would rather surrender rather than struggle with the custom. Beautement et al. [S9] also upheld the notion that “there is a limit to the amount of effort individuals are prepared to expend on compliance unless there is a perceived benefit to balance it.”

#### Insufficient training

This is the fifth barrier human factor in our study. The barrier’s frequency is 19 in the review.  
Kraemer et al. [S38] conducted a qualitative study involving computer and information security experts that were divided into 2 focus-group sessions of 5 members each. Focus Group 1 mentioned “no user training” as a human factor while Focus Group 2 also reported “lack of training and education” as a factor

Additionally, Daniel [S78] also related that “historically, IT teams are not given sufficient training in the ‘people’ part of their roles, as more time is spent focusing on technology and process than communication and collaboration.”

#### Impulsiveness and recklessness

This barrier is a human factor that involves acting or behaving carelessly and not pondering enough about what the consequences might be. Egelman and Peer [S18] proposed a Security Behaviour Intentions Scale which they employed to study the link between information security and impulsivity. The scale was utilized to explore awareness and engagement in good cybersecurity practices. From their findings, they reported that impulsivity negatively correlated to security behaviours.

In addition, findings from a comparative analysis performed by Wisniewska et al. [S70] have it that “malpractice statistics show that external attacks are a relatively rare phenomenon, while the majority of security breaches involve an organization’s employees.” Authors mentioned recklessness as one of the underlying causes of security breaches. Supporting this further, when Adam [S87] was analyzing examples of human errors, it was stated that “42 percent cited ‘general carelessness’ in the report.”

#### Limited technological and practical knowledge

This barrier is pertaining to the human factor deficiency in relevant cybersecurity skills and expertise. Badie and Lashkari [S7] expatiated on this that even though appropriate technical solutions are implemented, there would still be failure if the human is not handled. Authors maintained that “knowledge and culture are among the few effective tools to manage risks related to people. Not providing proper awareness and training to the people who may need them can expose the company to a variety of security risks.”

In addendum, Henshel et al. [S15] buttressed that “the detection accuracy of a defender can be measured by the percent of false positive and false negative incident reports filed by an individual defender. It would be expected that a skilled defender with expertise would have lower false positive and false negative rates than those of a less skilled defender.” Oltramari et al. [S52] also supported further in their study that “a defender with insufficient knowledge can present a higher risk”

Often, it is difficult to comprehend a risk and the threat that it poses without an accurate understanding of the specifics of the risk in question. [s55]

#### Cognitive bias and security perceptual blindness

This barrier is found among 19 studies in the review. According to [S17], cognitive is explained as “the processes and mechanisms involved in performing a task.” Cognitive bias exists when managing the human element in cybersecurity whereby there would be necessity for the consideration of the cybersecurity mechanisms impacts on the workforce as well as how the workforce will also react to the various mechanisms. Beautemant et al. [S9] and Parkin et al. [S54] pointed out that “an individual will be less willing to comply with security policies if they perceive them as having a detrimental effect upon their primary work tasks.”

#### Workload stress, fatigue, and pressure

This barrier also occurs among 19 primary studies in the review. Hamornik and Krasznay [S29] discussed the implication of workload and stress in relation to employees. Authors noted, “regarding human factors, it is important to note that monotony is a strong source of stress for analysts: the monitoring task is repetitive, this is, among others, a cause that contributes to large fluctuation, and shift working in 24/7 is the other factor that contributes to heavy workload and stress.”

Another corroboration was also obtained from Infosec Institute [S96] in their article on Human Factors in Information Security Management Systems (ISMS), “obstacles in this study are the restraining forces, which prevent changes and consequently creating risks and unable the system to fulfill the goals. For example, human stress preventing people to adopt changes that ensure ISMS performs effectively.”

#### Unethical technology usage and abuse

This barrier is related to the wrong behavior that accompanies internet and technology usage. Chen et al. [S10] pointed out that “internet addiction can lead to internet abuse, which not only can devastate an individual’s life but also destroy an organization’s goodwill.” In addition, Og˘utcu et al. [S51] put it that “cyber¨ threats increase continuously with the introduction of new technologies and the legal boundaries related to the privacy of personal information and its use by the corporations are not clear and are often subject to legal interpretation.”

#### Malevolence and sabotage abuse

This barrier originates right in the inside perimeter of the cybersecurity by a typical sadistic employee within the organization. According to Colwill [S13], “a malicious insider has the potential to cause more damage to the organization and has many advantages over an outside attacker: they have legitimate and often privileged access to facilities and information, have knowledge of the organization and its processes and know the location of critical or valuable assets.”

Shropshire [S62] laid more emphasis that such “criminal activities may be committed as a retribution for firing or dismissal, to please a spouse or a friend, because one’s judgment has been impaired by controlled substances such as drugs or alcohol”

#### Sharing confidential information

This barrier is related to the carefree human attitude that make them share information that is very personal to them. khidzir et al. [S36] highlighted that people get carried away when sharing information about their activities till “they are not realizing that the information that they share in Online Media Social could contribute to the cybersecurity risks that might be difficult to manage and mitigate.”

And Daniel [S78] also posited that “the social media boom has created a sharing culture. Without really knowing who’s on the other side of the screen, people share the most personal and private details about their lives at home and at work.”

#### Low motivation

This barrier is related to the perception of the humans having the thought of what personal benefits will be derived from adopting or not adopting a particular security behavior. Parsons et al. [S55] held that “Employees need to be motivated to adopt secure behaviours and practices, and management need to be able to identify what motivates their staff.” Oltramari et al. [S52] futhermore supported further “that a defender with poor motivation will pose a very high risk.

#### Risk-taking propensity

This is the barrier that has to do with the liability of humans to engage in a risky behavior that could later negatively affect the cybersecurity. Parkin et al. [S54] advised that “the propensity for risk, must be adequately represented in the information security policies of the organization. Individual employees can be capable of behaving in a ‘risky’ manner to further the goals of the organization.” it was mentioned that the right risks are free to be taken at the right time, and that risks that senior management do not want being taken should be prevented at all times. In relation to risk, Mccormac et al. [S48] also revealed “that older adults were more risk averse, with regard to their Information Security behaviours, than younger adults.

#### Cultural and political ideology

This is the barrier connected with the individual societal belief and settlement upbringing. Alhogail et al. [S6] explored and found that “national culture determines organization’s members’ values and beliefs as it influences how people view their duties and interact with others, and define the acceptable and the unacceptable behavior”

Crossler et al. [S14] made an awaken contribution expressing why the cultural aspect of human factor should be monitored. Authors lamented that “little has been done to examine cross-cultural considerations involved with insider behavior, IT security compliance, hacking, security violations, and so forth.”

Culture and climate can certainly have a significant impact on values, attitudes and behaviours. [S55]

#### Mistakes and Oversight

Parkin et al. [S54] identified vulnerabilities exposed in security processes that may be influenced directly or indirectly by human behaviour. Some of the behavior mentioned is an unintentional mistake or oversight.

#### Extraversion

This barrier deals with the liveliness and socializing attitudes of humans which could make them be susceptible to cyber attacks. McBride [S47] noted that “people scoring high on the extraversion scale tend to be sociable and assertive, and they prefer to work with other people.” making them likely to fall prey of cybersecurity errors. Welk et al. [S67] also held the same view that “individuals who are generally extraverted might be more likely to trust non-authentic emails.”

#### Low competency

Regarding this barrier factor Islam and Dong [S34] highlighted “Personal competency of employing the development methods, language and tools” as risk factor of individuals and teams.

#### Security mechanism circumvention:

Hoonakker et al. [S32] discussed how users can choose to circumvent security mechanism which would be a barrier factor. Authors reported “users can use several workarounds to overcome their limitations” That is, limitation that occurs when they are not able to fulfill their desired mission of using the system.

Henry [S106] also mentioned that if workers notice “that security slows them down, they are more likely to find smart ways to work around the solution, from unauthorised devices or using unsanctioned applications.”

#### Uncertainty

According to Zhang and Lowry [S73], uncertainty occurs when “the members of a culture feel threatened by uncertain or unknown situations.” Authors further illustrated with the examples of Denmark and Singapore. Authors reported that “Singapore has low uncertainty-avoidance national cultures; whereas, Japan is an example of high-uncertainty avoidance. Given their propensity to shun uncertainty, it is likely that a Japanese end-user is less likely to fall prey to phishing emails whereas people who are more open to uncertainty might be more likely to be victimized by a phishing attack”

Uncertainty in perceived data could lead to distorted situation awareness. For

example, attack graph analysis toolkits are designed to do deterministic attack

consequence estimation. In real time cyber situation-awareness, such

consequence estimates could be very misleading due to various uncertainties.

Alert correlation techniques cannot handle the inherent uncertainties associated

with inaccurate interpretations of intrusion detection sensor reports

(such inaccurate interpretations lead to false positives/negatives in determining

whether an IDS alert corresponds to an attack).

Lack of data or complete knowledge may raise additional uncertainty management

issues. For example, lack of data leads to incomplete knowledge of “us”.

Such incompleteness may be caused by imperfect information about system

configurations, incomplete sensor deployment, [S8]

#### Bystander effect

Parsons et al [S55] explained bystander effect “as a social effect which could influence the manner in which people respond to, or perceive, risks. This effect is based on the idea that as the number of people present increases, people will shift their responsibility, so that the likelihood of any one person responding decreases. Hence, in large groups, individuals may feel less personal responsibility for security.

Also, a contribution from Widdowson and Goodliff [S69] elaborated that “the bystander effect addresses the dissolution of responsibility and expectation that someone else, in this case technology system, will take responsibility for cyber-security”

#### Bandwagon effect

This barrier occurs in one study in our review. Widdowson and Goodliff [S69] explained The bandwagon effect as “the human tendency to follow the crowd.” This can be a human factor in a situation whereby an activity is performed by a user simply because others are performing it, and whereby the user would not imagine performing such act could later backfire.

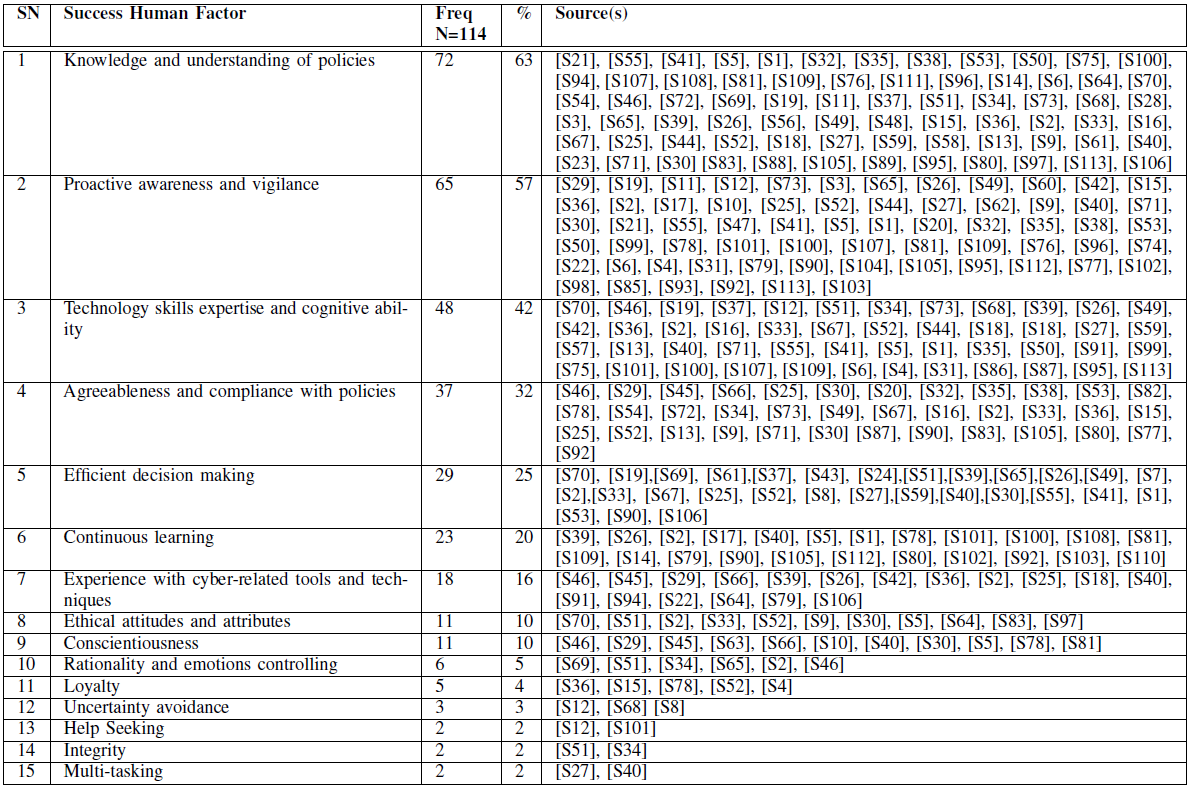
#### Overconfidence

This barrier was found in only one study. In an assessment methodology by Widdowson and Goodliff [S69], overconfidence was listed as one of the indicators of human vulnerability.

### Success Human Factors of Cybersecurity, as Identified in the Literature (RQ2)

In this result, we identified the human factors that are progressive to a successful cybersecurity endeavor and culture according to the evidences from the literature. We accomplished our identification, classification, and categorization by utilizing the coding approach which is based on the techniques of grounded theory. We have described these coding procedures in an earlier section. The identified success human factors are presented in Table 7. The higher the frequency or percentage of a factor indicates its popularity across the literature. We elucidate each success in the following subsections appended with their citations for mapping correspondence.

Table 7: SUCCESS HUMAN FACTORS OF CYBERSECURITY



#### Knowledge and Understanding of Policies

This is the human factor that has the highest frequency in the reviewed sources. It was found in 72 studies. This study has made it evident that ‘Knowledge and Understanding of Policies’ (63%) is a crucial human element for a successful cybersecurity. Huang et al. [S35] stressed that knowledge is a key factor that influences the gap between the security as perceived by people and the real security of the information system. Ani et al. [S6] further emphasizes that identification of prior attacks can be assisted by the understanding of cybersecurity knowledge measure and the industrial workforce skill capacities.

Parsons et al. [S55] pointed out that technical knowledge is required by people for understanding the magnitude or implications of potential security breaches. This means people will want to continue following essential safety security precautions if they understand the reason for such. Cyber Security should be seen as everyone’s responsibility. Data breach and all potential of information technology (IT) systems should be inculcated to people in easy to comprehend layman’s terms. Additionally, the provision of IT security onboarding for all employees will narrow the security knowledge gap between entry and older employees [S100].

#### Proactive Awareness and Vigilance

This success human factor is the second most cited in our study. It appears in 65 studies and covers 57% of the collection. As stated by Alhogail et al. [S5], continuous awareness and training programs help employees to keep abreast of security requirements as well as various securities polices documentations; such movement also gets them up to date regarding security issues and risks. Eustace et al. [S21] held that cybersecurity measures should begin with prevention measures which will be made up of developing a self-awareness and intervention model and maintaining the awareness. They came up with the notion that awareness building strategies and training needs of personal ICT security can be realized by implementing cyberattack phases model for behavioral response. Cybersecurity awareness is a critical issue which it will be necessary to increase knowledge about it, such as training employees to be aware of the likely social engineering techniques, and they should be equipped with appropriate responses [S40], [S55].

The creating of awareness across all organizational levels is very instrumental to a successful cybersecurity. The awareness must cut across everyone with no exception; even the top echelons should be involved [S79]. It should be noted that awareness is not the same as training. As in Newcombe [S102], “There’s a difference between awareness and training, and most people are providing training, not awareness. Training is putting a fixed body of knowledge on employees and testing them. Awareness is about changing behavior.”

#### Technology Skills Expertise and Cognitive Ability

This is the third success human factor in our study. The factor’s frequency is 49 (43%) in the review. According to the Widdowson and Goodliff [S70], evidence suggests that aspects of individuals’ personality or cognitive style will possibly have effects on the manner by which they react to information hazards. They then mentioned the significance of the people-factored individual knowledge and skills which are often derived from training. In terms of cognitive ability, Kelley et al [S37] elaborated that it is really necessary to recognize the influence of individual differences, personality traits and cognitive abilities. Individuals interaction with computers and decisions made regarding information security are dynamic and complex. And often there are biases and heuristics that affect individuals’ perception.

Furthermore, Parkin et al. [S53] explained that when the human element of information security is being managed, it is crucial to take into consideration that security mechanisms impact which will be upon the workforce and how those mechanisms would be reacted to. This will be vital to relate why individuals make certain decisions and why specific behaviours may be observed [37].

Ani et al. gathered that skill capacities of the industrial workforce and being current with the latest trends of cyber threat can assist in prior identification of attacks [S6].

#### Agreeableness and Compliance with Policies

This success factor is found among 36 studies in the review. As defined by Padayachee [S52] “compliant information security behavior refers to the set of core information security activities that have to be adhered to by end-users to maintain information security as defined by information security policies.” A basic requirement for any given information security endeavor is to develop the end-user’s compliance intention and let him/her know the benefits of obeying and upholding such information security measures. A survey conducted by Eminağaoğlu et al. [S20] on some employees revealed that 50% of the employees that are in compliance with the information security policies and procedures are not exposed to vulnerabilities.

In addition, Huang et al. [S35] strengthens the fact that IT users’ compliance to security practice is important to guard the information systems security. Changing users’ perception of information security can enhance their compliance to security practices.

#### Efficient Decision Making

Regarding this success human factor, Parkin et al. [S53] disclosed that individual employees can have the capability to behave in a ‘risky’ manner in order to further the goals of the organisation. However, the Chief information security officers (CISOs) should be in the position to make sure that the right risks should be taken at the right time, and not allow the harmful and unwanted risks to be taken. Employees must be educated about the several biases associated with risk perception such as the availability heuristic and the optimism bias. Comprehension of these biases will be influential to individual’s ability in making judicious and reasonable decisions pertaining to possible risk [S55].

Widdowson and Goodliff [S70] advised that employees need to be consulted regarding decisions that affect them. Such consultation will reduce the risk of loss of sensitive data and breach of data protection legislation. Welk et al. [S69] added that personality characteristics that support reserved behavior and low impulsivity reduce susceptibility in a decision-making task. It was further recommended that training programs should be structured to promote behaviors and characteristics that will support decreased susceptibility through informed decision making.

#### Continuous Learning

This factor was found in 23 studies in the review. Lathrop et al [S39] maintained that learning should be continuous in order to catch up with clever adversaries and their numerous techniques. Cyberspace operations demand a thorough comprehension of several functionalities and protocols. Efforts channeled towards the learning must be linked with the evolving and latest cyber security strategies and policies [S21]. Positive change in behavior can be realized by educating employees about the phenomena that would bring about it. Continuous learning will enable employees to be conversant of thes possible social engineering techniques, and to be equipped and prepared ahead.

Öğütçü et al. [S50] made known that the level of education in terms of information security and training receiving helps reduce risk level in users’ behaviors. It is a must to arrange regular training and best practice cyber security workshops; the training needs to be tailored to fit the organization and its particular systems and processes [S100].

#### Experience with Cyber-Related Tools and Techniques

This factor has a total frequency of 18 in the study. As documented in the review of McBride et al. [S45], openness to experience gives higher information security awareness scores and linked to lower risk taking. Individuals who are opened to experience will be less likely to oppose cyber-security policies [S45], [S66].

In the model designed by Dutt et al. [S18], whereby a defender’s model was defined by experience of threats. Based on the predictions from the model, authors stated that “a defender’s prior threat experiences and his or her tolerance to threats are likely to predict detection accuracy” [S18]. Naturally, humans can be able to compare their past computer interactions to their present experience.

#### Ethical attitudes and attributes

This success human factor has to do with the individual behavioral conduct towards self-conservative and constraint to the advantage of his/her company or organization. According to Beautement et al. [S9], Individuals generally have the choice either to comply with security policies or not. And often, the individuals own goals, attitudes, and norms have influences on the choice. An addition from Ahlan et al. [S2], beliefs, habits and behaviors in form of attitude all combine to influence how policies and regulations are being reacted [S2]

Eustace et al. [S21] recommended that cybersecurity researchers require a special ‘dark ethics’ policy which should be employed to defend against making logical error in surrendering any form of rights that are forfeited by the behavior of adversaries.

#### Conscientiousness

This success human factor was identified as a success human factor in 11 studies in the review. As defined by Hadlington [S30], conscientiousness is a “socially prescribed impulse control that facilitates task and goal-oriented behavior, such as thinking before acting, delaying gratification, following norms and rules, and planning, organizing, and prioritizing tasks.” Several exploratory studies on information security behaviors indicated that conscientiousness contributes positively to information security [S46]. Conscientious individuals will possibly adhere to cybersecurity guidelines. Such persons are distinguished for their sense of purposefulness and responsibility which them strong willed and achievement oriented.

In the review of Shropshire et al. [S63] conscientiousness was found as one of the influencing personality types in workplace environment. It was further supported that previous studies have revealed conscientiousness to be one of the better predictors of organizational citizenship behaviors which include the complying with rules and procedures when behavior is not monitored.

#### Rationality and emotions controlling

In evidences gathered with respect to this success factor, Henshel et al [S34] explained that people that are more rational behaves and respond more predictably which helps build up trust. Rationality has to do with inherent ability in reasoning and is also influenced by emotions and experiences. Perceived rationality, benevolence and characteristics of expertise lead to gaining additional trust [S34]. Several results have shown that perceived ability to keep emotions under control positively correlated with general accuracy; and state of emotions affects decisions [S65], [S69].

#### Loyalty

This success factor is pertaining to the employee’s commitment, sense of belonging, and trust to its workplace. As opined by Colwill et al. [15], arguably, organizations having a large percentage of long-term employees would have seen more buy-in to security by establishing reliance on the organization and the longing for it to survive in order to protect the employees’ own futures. Loyalty can be temporary and ought not to be just assumed, but must rather be supported by suitable behavioral evidence and understanding.

Engagement of employees and the feeling of personal responsibility to protect the organization and fellow colleagues will make them willing to be involved in security programs. They will also be more sensitive and cautious in the way they handle delicate information [S78]

#### Help Seeking

This factor was found cited in two studies in the review. There are positive results in the internet interactions made by users with each other in getting assistance and social support in the ways they deal with security threats [S13]. Ensuring people collaborate with one another will enable organizations to easily discover misalignments and thereby implement policies that will take into consideration the real ways people work [S101].

#### Integrity

This success factor was cited in two studies in the review. As noted by Oltramari et al. [S51], users having integrity qualities will not behave maliciously within the network and they will be trusted to stick to good security conduct and policies. Integrity as a behavioral characteristic which is associated with individual’s intention influences predictability [S34].

#### Uncertainty avoidance

This human factor was cited twice in the review. Barford et al. [S8] revealed that uncertainty of information that are utilized for cyber situational awareness create some forms of difficulty. Authors then mentioned that finding ways to reduce such uncertainty is really critical to the cybersecurity success. One of such ways can be leveraging the recent advances in trusted computing. Another way suggested for managing uncertainty is the incorporation into distributed framework constructed using Bayesian networks. It was also highlighted by Chen and Zahedi [S12], that uncertainty can be handled in workplace using unambiguous rules and regulations clearly letting the employees know what are expected from them.

## Readiness Model Development (RQ3)

This is the fourth phase, and which provides result to RQ3. Readiness model is built to assist organizations in assessing their strength and weaknesses regarding designing, applying, and judging appropriate strategies to support software development [31].

### Readiness Model Development Process

We came up with our readiness model by adopting the approaches as done in [41], [42], [27] and [43]. The models are meant to determine organization's capability by measuring the rate at which processes are decided and controlled [26]. The flow of the readiness development model is depicted in Figure 2.

After reviewing the literature through the MLR. We identified the barrier and success human factors by applying the open, axial, and selective coding techniques of the Grounded Theory. We developed the model composing of four readiness levels. The levels were constructed by two researchers to avoid any potential bias that could result from human judgement if it is to be done by a single researcher. The success human factors and their corresponding best practices were distributed across the four readiness levels. We presented these levels and the success human factors with their corresponding practices to Software Engineering research panel, and we made necessary changes that were proffered. Furthermore, an external reviewer scrutinized the work and we effected subsequent modifications accordingly. Lastly, we evaluated the model in two case companies involving cybersecurity industrial experts. The participants of the case studies …

### Readiness Model Development Structure

In our readiness model structure, we adopted concepts of the People Capability Maturity Model (P-CMM) [44] to develop a readiness model for cybersecurity based on human factors. Our model is depicted in XXX showing the relationship among levels, factors and practices. The figure illustrates how the readiness levels signify organization’s capability and how the MLR’s findings feed into the levels. The overall model will guide industrial practitioners to control and improve their cybersecurity culture. The structure of the readiness model is implemented upon the following dimensions:

* Readiness stages;
* Success human factors in each stage;
* Practices under each human factor
* Assessment

This thesis started with the formulation of readiness model criteria and the collection of data via multivocal literature review. In the review, we answered research questions regarding barrier human factors that have negative impacts on cybersecurity as well as the success human factors that have positive impact on cybersecurity. We identified a total of 22 barrier human factors and 14 success human factors. Even though however both the barrier and success human factors were used for the synthesis to come up with the readiness levels, we only distributed the success human factors across the levels because they make up a step-by-step guide regarding what practitioners and organization should inculcate for a successful cybersecurity endeavor. For proper implementation, we have also classified and mapped several best practices gotten from the review to each readiness level and their respective human factors. The readiness model (XXX) demonstrates that practitioners and organizations must address and deal with each factor to reach a progressive readiness level. The model structure evolves from an unready stage to a ready state.

#### Readiness Stages

Our readiness model is comprised of four levels (XXX) based on the People Capability Maturity Model (P-CMM) [44]. We designed our levels to accommodate the characteristics of the cybersecurity human factors readiness implementation. We present the four stages of the readiness model for cybersecurity human factors:

* **Initial:** This is the first level of the readiness model. It is the stage where people are not talented as regards cybersecurity practice. At this stage, companies and organizations are in unprepared state. People performed cybersecurity practices in an ad hoc and inconsistent manner with little or no analysis of their impact.
* **Receptive:** This is the readiness model level 2. Receptive is defined by the Oxford Advanced Learner's Dictionary as ‘’willing to listen to or to accept new ideas or suggestions’’. We termed the second level **Receptive** because ‘Knowledge and understanding’ and ‘Proactive awareness and vigilance’ appeared as the two most critical success human factors in the empirical study. They were cited 72 times (63% of the total studies) and 65 times (57% of the total studies) respectively. Cybersecurity human factor readiness model entails adopting new security practices. Therefore, it is very crucial to promote awareness of cybersecurity human factors and circulate it among practitioners and organizations. Proactive awareness is extremely important at the beginning of the cybersecurity implementation plan. Awareness initiatives can be organized in companies whereby security personnel will be invited to give lecture to employees for understanding the goals, significance and advantages of maintaining healthy cybersecurity habits, and the stratagems that should be deployed by employees and organizations to develop those healthy habits.
* **Informed:** At level 3 of the readiness model, individual capability on cybersecurity gets developed through relevant training and knowledge. This readiness level emphasizes on guaranteeing that individuals have been equipped with the right set of awareness and training. The derived knowledge from the awareness sessions plus the individuals’ innate-cognitive intelligence and domain-experience competencies are necessary to succeed in the cyberspace and the computing environment. An effective means through which companies can strengthen their employees’ security knowledge base is by sponsoring them to cybersecurity conferences and workshops. The success of cybersecurity regarding human factors is largely dependent on individuals’ compliant information security behavior. Of what benefit is the knowledge gathered if it is not being applied. So, not only that the cybersecurity policies must be learnt, the employees and end users should also be ready to adhere to the companies’ and manufacturers’ security regulations respectively. The prior education of the people on the several biases associated with security risk perceptions will also play important roles in the ability to make judicious decisions in tight security decision-making situations.
* **Optimizing:** This is level 4 level of the readiness model.At this final level, the individual focuses on continuously improving his/her capability. The dynamism and evolution in social engineering techniques demand that people must also regularly upgrade their cybersecurity defense knowledge and approaches with respect to the latest trends in cyber threats. People can personally engage in individual program to enhance their cybersecurity culture which will lead them to carry out competency-based processes. Empowerment programme needs to be provided by organizations to update employees in making positive changes in their security routine in a way that will improve their performance; in turn, employees should recommend lessons learned from experiences to the company. It is the duty of the existing employees, especially those in the security unit that have attained the highest level of cybersecurity competencies to transfer the capability knowledge to others that are less experience in the organizational workforce. This type of knowledge transfer will create rapport among the matured and onboard employees; and enable easy discovery of any security misalignments and vulnerabilities. The improvement in this level also necessitates analyzing and assessing to check whether there are propagated activities from earlier transitional levels that should be fine-tuned and modified.

We are optimistic that these four levels are adequate for cybersecurity human factors readiness implementation because the four levels align with all the success human factors. The readiness levels are inspired by the People Capability Maturity Model and the success human factors are products of a meticulous multivocal literature review involving studies from both academic researchers and industrial experts who are really working in the cybersecurity domain.

#### Barrier and Success Human Factors in each Stage

Table 8: Success and Barrier Human Factors Distribution

|  |  |  |
| --- | --- | --- |
|  | Success Human Factors | Barrier Human Factors |
| Optimizing | SHF14: Conscientiousness  SHF13: Rationality and emotion controlling  SHF12: Ethical attitudes & attributes  SHF11: Loyalty  SHF10: Integrity | BHF22: Security mechanism circumvention  BHF21: Malevolence and sabotage  BHF20: Unethical technology usage and abuse  BHF19: Belief and trust  BHF18: Overconfidence  BHF17: Extraversion  BHF16: Mistakes and Oversight  BHF15: Impulsiveness and recklessness |
| Mentoring | SHF9: Continuous learning  SHF8: Help Seeking | BHF14: Bandwagon effect  BHF13: Bystander Effect |
| Informed | SHF7: Uncertainty avoidance  SHF6: Efficient decision making  SHF5: Agreeableness and compliance with policies  SHF4: Experience with cyber-related tools and techniques  SHF3: Technology skills expertise and cognitive ability | BHF12: Risk-taking propensity  BHF11: Uncertainty  BHF10: Sharing confidential information  BHF9: Disregarding and negligence of security protocols  BHF8: Cognitive bias and security perceptual blindness  BHF7: Workload stress, fatigue, and pressure |
| Receptive | SHF2: Knowledge and understanding of policies  SHF1: Proactive awareness and vigilance | BHF6: Low motivation  BHF5: Low competency  BHF4: Limited technological and practical knowledge |
| Initial |  | BHF3: Insufficient training  BHF2: Unawareness and ignorance  BHF1: Cultural and political ideology |

**REFERENCES**

[1] S. D. Lathrop, S. Trent, and R. Hoffman, “Applying human factors research towards cyberspace operations: a practitioner’s perspective,” in *Advances in Human Factors in Cybersecurity*, Springer, 2016, pp. 281–293.

[2] “ITU.” [Online]. Available: http://www.itu.int/en/itu-t/studygroups/com17/pages/cybersecurity.aspx.

[3] A. Aziz, “The evolution of cyber attacks and next generation threat protection,” in *RSA conference*, 2013.

[4] B. A. Gyunka and A. O. Christiana, “Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary.,” *Comput. Inf. Syst.*, vol. 21, no. 2, 2017.

[5] M. McBride, L. Carter, and M. Warkentin, “Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies,” *RTI Int.-Inst. Homel. Secur. Solut.*, vol. 5, no. 1, p. 1, 2012.

[6] J. Shropshire, M. Warkentin, and S. Sharma, “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior,” *Comput. Secur.*, vol. 49, pp. 177–191, 2015.

[7] S. Uebelacker and S. Quiel, “The social engineering personality framework,” in *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 2014, pp. 24–30.

[8] IBM, “Ibm security services,” 2015. [Online]. Available: IBM Global Technology Services., Cyber Security Intelligence Index.

[9] M. S. James, *10 things security experts wish end users knew. Global Knowledge*, 2015. .

[10] S. Dafydd and P. Marcus, *The web application hacker’s handbook: Finding and exploiting security flaws*. John Wiley & Sons, 2011.

[11] V. F. Mancuso, J. C. Christensen, J. Cowley, V. Finomore, C. Gonzalez, and B. Knott, “Human factors in cyber warfare II: Emerging perspectives,” in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2014, vol. 58, pp. 415–418.

[12] “HFES.” [Online]. Available: https://www.hfes.org/about-hfes/what-is-human-factorsergonomics.

[13] A. Oltramari, D. S. Henshel, M. Cains, and B. Hoffman, “Towards a Human Factors Ontology for Cyber Security.,” in *STIDS*, 2015, pp. 26–33.

[14] D. C. Acuña, “Effects of a comprehensive computer security policy on computer security culture,” *MWAIS 2016 Proc.*, vol. 10, 2016.

[15] L. Hadlington, “Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours,” *Heliyon*, vol. 3, no. 7, p. e00346, 2017.

[16] T. Aoyama, H. Naruoka, I. Koshijima, and K. Watanabe, “How management goes wrong?–The human factor lessons learned from a cyber incident handling exercise,” *Procedia Manuf.*, vol. 3, pp. 1082–1087, 2015.

[17] U. P. D. Ani, H. He, and A. Tiwari, “Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective,” *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, 2017.

[18] H. W. Glaspie and W. Karwowski, “Human factors in information security culture: A literature review,” in *International Conference on Applied Human Factors and Ergonomics*, 2017, pp. 269–280.

[19] K. Jenab and S. Moslehpour, “Cyber security management: A review,” *Bus. Manag. Dyn.*, vol. 5, no. 11, p. 16, 2016.

[20] A. Vieane, G. Funke, R. Gutzwiller, V. Mancuso, B. Sawyer, and C. Wickens, “Addressing human factors gaps in cyber defense,” in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2016, vol. 60, pp. 770–773.

[21] D. Henshel, C. Sample, M. Cains, and B. Hoffman, “Integrating cultural factors into human factors framework and ontology for cyber attackers,” in *Advances in Human Factors in Cybersecurity*, Springer, 2016, pp. 123–137.

[22] A. J. Widdowson and P. B. Goodliff, “CHEAT, an approach to incorporating human factors in cyber security assessments,” 2015.

[23] M. Whitty, J. Doodson, S. Creese, and D. Hodges, “Individual differences in cyber security behaviors: an examination of who is sharing passwords,” *Cyberpsychology Behav. Soc. Netw.*, vol. 18, no. 1, pp. 3–7, 2015.

[24] J. L. Marble, W. F. Lawless, R. Mittu, J. Coyne, M. Abramson, and C. Sibley, “The human factor in cybersecurity: Robust & intelligent defense,” in *Cyber Warfare*, Springer, 2015, pp. 173–206.

[25] A. Alhogail, A. Mirza, and S. H. Bakry, “A COMPREHENSIVE HUMAN FACTOR FRAMEWORK FOR INFORMATION SECURITY IN ORGANIZATIONS.,” *J. Theor. Appl. Inf. Technol.*, vol. 78, no. 2, 2015.

[26] S. Ali and S. U. Khan, “Software outsourcing partnership model: An evaluation framework for vendor organizations,” *J. Syst. Softw.*, vol. 117, pp. 402–425, 2016.

[27] Y. Mufti, M. Niazi, M. Alshayeb, and S. Mahmood, “A readiness model for security requirements engineering,” *IEEE Access*, vol. 6, pp. 28611–28631, 2018.

[28] C. Wu, “A readiness model for adopting Web services,” *J. Enterp. Inf. Manag.*, 2004.

[29] H. Young, T. van Vliet, J. van de Ven, S. Jol, and C. Broekman, “Understanding human factors in cyber security as a dynamic system,” in *International Conference on Applied Human Factors and Ergonomics*, 2017, pp. 244–254.

[30] U. P. D. Ani, H. M. He, and A. Tiwari, “Human capability evaluation approach for cyber security in critical industrial infrastructure,” in *Advances in Human Factors in Cybersecurity*, Springer, 2016, pp. 169–182.

[31] S. Khan, M. Niazi, and R. Ahmad, “A readiness model for software development outsourcing vendors,” in *2008 IEEE International Conference on Global Software Engineering*, 2008, pp. 273–277.

[32] R. T. Ogawa and B. Malen, “Towards rigor in reviews of multivocal literatures: Applying the exploratory case study method,” *Rev. Educ. Res.*, vol. 61, no. 3, pp. 265–286, 1991.

[33] R. L. Glass, *Software Creativity 2.0*. developer.\* Books, 2006.

[34] V. Garousi, M. Felderer, and T. Hacaloğlu, “Software test maturity assessment and test process improvement: A multivocal literature review,” *Inf. Softw. Technol.*, vol. 85, pp. 16–42, 2017.

[35] P. Auger, *Information sources in grey literature*. Walter de Gruyter GmbH & co KG, 2017.

[36] V. Garousi, M. Felderer, and M. V. Mäntylä, “Guidelines for including grey literature and conducting multivocal literature reviews in software engineering,” *Inf. Softw. Technol.*, vol. 106, pp. 101–121, 2019.

[37] B. Kitchenham and S. Charters, “Guidelines for performing systematic literature reviews in software engineering,” 2007.

[38] D. S. Cruzes and T. Dyba, “Recommended steps for thematic synthesis in software engineering,” in *2011 international symposium on empirical software engineering and measurement*, 2011, pp. 275–284.

[39] D. Cruzes, M. Mendonca, V. Basili, F. Shull, and M. Jino, “Extracting information from experimental software engineering papers,” in *XXVI International Conference of the Chilean Society of Computer Science (SCCC’07)*, 2007, pp. 105–114.

[40] J. Corbin and A. Strauss, *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[41] M. Niazi, D. Wilson, and D. Zowghi, “A framework for assisting the design of effective software process improvement implementation strategies,” *J. Syst. Softw.*, vol. 78, no. 2, pp. 204–222, 2005.

[42] M. Niazi, D. Wilson, and D. Zowghi, “A maturity model for the implementation of software process improvement: an empirical study,” *J. Syst. Softw.*, vol. 74, no. 2, pp. 155–172, 2005.

[43] M. Alshayeb, A. K. Abdellatif, S. Zahran, and M. Niazi, “Towards a framework for software product maturity measurement,” in *The Tenth International Conference on Software Engineering Advances*, 2015.

[44] B. Curtis, B. Hefley, and S. Miller, “People capability maturity model (P-CMM) version 2.0,” CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2009.