Identifying Strategies to Address Human Cybersecurity Behavior: A Review Study

Mazen Hakami and Moneer Alshaikh
mahakami@uj.edu.sa malshaikh@uj.edu.sa
University of Jeddah, College of Computer Science and Engineering, Saudi Arabia

Abstract
Human factor represents a very challenging issue to organizations. Human factor is responsible for many cybersecurity incidents by noncompliance with the organization security policies. In this paper we conduct a comprehensive review of the literature to identify strategies to address human factor. Security awareness, training and education program is the main strategy to address human factor. Scholars have consistently argued that importance of security awareness to prevent incidents from human behavior.

Keywords:
Human Factor, cybersecurity, security behavior, security awareness.

1. Introduction

In today's computer-mediated world, organizations rely primarily on information to run their businesses. Information has become an indispensable asset for organizations and should be secured from unauthorized leaks, modification, or damage [2]. Despite the progress of cybersecurity technologies dedicated to protecting information, the rise of data breaches is considered by both frequency and costs [3]. Verizon Data Breach investigation report for 2019 indicated that 43% of breaches involved small business victims and 33% involved social engineering tactics, and 32% of breaches involved phishing [4].
In the study by Ponemon Institute and IBM, the results revealed that 24% of data breaches are caused by human error and the average cost to remediate a breach caused by human error is $3.5 million. In the United Kingdom, the information commissioner office reported that, in 2019, 90% of UK data breaches were occurred due to human error [5]. Therefore, various data and information breaches often occur due to human error. These statistics are brought to highlight human behavioral factors and technical aspects to pay attention to these elements. Accordingly, humans may be considered one of the weakest links in the information security chain. Developing cybersecurity cultures inside organizations can decrease human factor risk, positively affecting efficiencies and security by mitigating business risks [6].

1.1 Human factors in cybersecurity

Human factors can be defined as environmental, organizational, career, and individual features that influence human behavioral outcomes. However, it is well-defined as referred to in the science of ergonomic architecture design [7, 8]. Human factors have a different effect on managing cybersecurity. It is also one of the most severe barriers to creating adequate cybersecurity. Several forms of cyber-attacks are resulted due to the involvement of human factors and human errors. Human factors and their impacts make substantial difficulties for data security frameworks. In light of human nature, individuals often make conflicting, speculative, and inconsistent choices and evaluations that represent a considerable hazard to information [9]. Although human behaviors need to be identified and measured, their subjectivity makes this endeavor very difficult. A detailed analysis of the leading human factors that affect cybersecurity is a critical concern. The present review adopts a comprehensive literature review to determine human factors that may endanger data security from an organizational perspective.
Human factors can be differentiated based on the different roles humans can take regarding cybersecurity, attackers, defenders, or users—this research emphasizes the human factors as users and employees in business organizations. Many studies divided human factors into three primary categories; personality, demographic attributes, and cultural context. Hence, the research is delimited to elaborate on the cultural context in business organizations [10-13].

1.2 Cybersecurity culture in organizations

The concept of cybersecurity culture is known as the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and standards of people regarding cybersecurity, and they manifest themselves in human behavior with information systems [14-16]. Cybersecurity culture deals with ordinary subjects, including cybersecurity awareness and data security structures; however, it is more extensive in scope and application [16]. It also makes data security contemplations a basic piece of workers' activity, habits, and conduct, implanting them in their routine activities. There are multiple reasons behind the importance of cybersecurity culture within organizations [17]. Shared beliefs within an organization will lead to acceptance of the values and norms of the organization, including their attitudes towards cybersecurity [16, 18]. Researchers

Manuscript received April 5, 2022
Manuscript revised April 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.4.37

argued that cyber security culture within organizations and business environments stimulates and arouses appropriate worker's security behaviors and conduct towards adherence and commitment. Therefore, building up a culture of security can contribute to minimizing or avoiding cyber security breaches [19].

1.3. Statement of the problem

The research problem is how to promote both the understanding and up-gradation of cybersecurity programmers and training within the organization and how to develop good practice methodological tools and step—by—step procedures to promote employees' understanding of cybersecurity to protect the assets of their assets organizations internally. According to this, the research questions can be stated as:

1-What are the most significant human factors in cybersecurity, and how could they affect organizations' information security?

2- How would implementing a cybersecurity culture help organizations mitigate and avoid cyber-attacks providing a friendly business environment to employees?

3-What are the best methods and procedures for providing cybersecurity culture in organizations and business environments?

1.4. Aims of the Study

Accepting that the human factor is the weakest link in cyber security, this research aims to identify critical human factors in cybersecurity [16]. Developing and fostering a cybersecurity culture within organizations and business environments would protect the organization's information assets, promote security awareness, and transform organizations [16]. Hence, employees also become intelligent human firewalls against cyber-attacks.

1.5. Objectives of the Study

The main research objectives are;

1- To identify the main human factors such as attitudes and behaviors related to cybersecurity in organizations and business environments.

2- To propose methods and procedures that could help information security personnel in organizations promote employees' understanding of cybersecurity and mitigate cyber-attacks.

3- To highlight the importance of a cybersecurity culture for organizations and business environments.

4- To identify cybersecurity attacks that exploit human factors.

2. Literature Review

2.1. Backround and Overview of Related Work

Technological solutions alone cannot address cybersecurity issues. "While organizations have applied many security technologies, e.g., anti-virus software, firewalls, access control, intrusion detection techniques, encrypted login, or biometrics techniques to protect their critical information, humans remain the weakest link in the information security environment and associated security processes" [20]. It becomes evident that cybersecurity is not only a technical issue that needs to consider understanding human behavior countering cybersecurity risks and attacks effectively [21, 22]. It has been acknowledged that organizations and business environments and the weakest links in the information security chain are employees [14]. Usually, humans within the organization could be divided into four categories: individual, team, management, and customer/consumers. These human interlocutors interact with technological elements in an interconnected world called 'information security.' People have their own unique culture, attitudes, skills, knowledge, understandings, behavior, and interests depending on their organizational roles. Despite advanced technical solutions to protect information security, malicious actors can access targeted systems by taking advantage of human error using social engineering, malware, poor security policies, and noncompliance [23]. Researchers and practitioners believe that a research gap exists in human performance and behavior in cybersecurity and call for urgent attention from human factors practitioners and psychology-based experts [24, 25]. This section will identify human behavior that affects cybersecurity in organizations.

They argued that Cyber Security is essentially a behavioral factor that remains unknown—overlooking the human factor impacts upon an organization's information security, which is a factor [20, 26]. Most researchers have categorized human factors in cybersecurity in organizations into direct and indirect factors. Direct human factors depend on individual perception, behavior, and knowledge of information security. Indirect human factors are influenced by forces beyond human power and how humans understand and interpret it, such as organizational culture and information security policies.

2.2 Direct Human Factors

Human factors are categorized into different areas, for instance, external influences, human error, management, organization, performance, resource management, policy issues, technology, and training [27, 28]. Following these classifications, human factors are categorized into two main groups: human factors and organizational factors. Meanwhile, human factors encompass lack of awareness, risky belief, risky behavior, inadequate use of technology,

lack of motivation. Human errors are defined as *Any action leading to undesired result* that emphasizes human errors or human factors as one of the highest areas of organizational vulnerability. For instance, an employee who cannot memorize his password consisting of letters, digits, or special characters may write it unsafely; consequently, others would see and misuse it. Hence, it is an example of a human error that can lead to a data breach. An organization's business strategy should encompass creating adequate information security-oriented organization. However, human error leads to data breaches, cyber-attacks, and ransomware. Indication of that type of lack of motivation is also one of the human factors that can affect cybersecurity; according to previous research, employees need to adopt the motivation for secure behaviors and practices. Management needs to identify what motivates their tasks, primarily that motivation occurs when security problems are shared, and users are involved in decision-making to follow security procedures. For instance, apathy[1] is one of the essential human factors in cybersecurity. In an organizational context, apathy is seen as the unwillingness of employees to contribute and participate in achieving the organizational goals and objectives. Moreover, apathy reflects itself in the unwillingness of employees while implementing organizational information security procedures. Human factors initiatives can be solidified through organizational culture by implementing practices and processes to increase awareness of human performance and decision-making.

Although the technical perspective of human factors and information security appears dominant in many types of researches that view it from various perspectives such as behavioral, psychological, and management sciences, for instance, Pattinson et al [29] claim that individuals with a positive personality trait are considered susceptible to information security-related risk, they investigated the five-factor personality model through a survey including 500 employees and found that employees who were more agreeable, less impulsive, more conscientious, and more open were more likely to be involved in information security-related threats. These studies highlight that inherent personality traits influence how an individual may demonstrate safe or risky cybersecurity attitudes and behaviors, which directly links personality traits and susceptibility to social engineering attacks. In conclusion, they suggested that individuals exhibiting conscientiousness, extraversion, openness to experience, and agreeableness were highly susceptible to social engineering attacks. They argued that aspects of personality, problematic internet usage, and employee attitudes could impact the potential to engage in effective information security behaviors.

2.2 Indirect Human Factors

Incentive and disincentive are considered one of the indirect human factors as reported by employees in previous researches regarding information security policy, which could be considered severe, which is one of the critical indirect human factors. Moreover, previous researches reveal that setting and promoting information security policy can be considered the cornerstone element of any information security management program/system. It is argued that an organization's cybersecurity policies bear a significant influence on security awareness behavior. Similarly, various researchers showed how security policies awareness by employees contributed to their initiative skills, action skills, and computer skills related to cybersecurity studying the interaction between employees and security policies in organizations. They stated that while managing the human task in information security, it is necessary to consider both; the impact of security mechanisms on the workforce and the reaction of the mechanisms. Placement of the burden on employees, like the restriction of work capabilities, tight deadlines, and other processes and information to remember and recognize, can lead to negative attitudes of employees towards cybersecurity policies. Top management support is a critical factor to implement information security policies and information security culture, and they should actively participate from the design phase to evaluation [30-32]. Top management must support and deliver a clear view of its information security policies and goals to the rest of the organization. The role of management in enforcing security policies has not been extensively researched. According to research [30], top management support has the most decisive influence on cybersecurity knowledge sharing. There are associations between management support and cybersecurity awareness which are supported by the information security culture. The personnel who share security knowledge raise awareness, and those who work together on common security goals show a positive attitude towards compliance [33]. Communication is also a critical unintended human behavior in organizations. The actual communication is that it must cover all employees in organizations at any level of hierarchy. Such communication forms can be security awareness workshops, E-mail, phone, or on-prem meetings. Hence, prompt communication in case of an incident results in a quick response from the cybersecurity team.

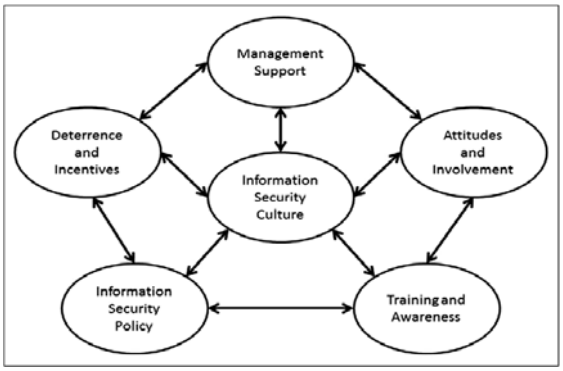
2.3 Information Security Awareness (ISA)

Information security awareness provides understanding which enhances human behavior, beliefs, and perceptions about information and its security to understand and enhance organizational culture as a countermeasure against rapidly evolving threats [16].

1 lack of interest, enthusiasm, or concern.

According to ISA, it is most frequently referred to as a cognitive state of mind, characterized by recognizing the importance of information security and being aware and conscious about its objectives, risks, and threats. It is often focused while acquiring the required knowledge to use information systems responsibly [34].
Employees' information security awareness (ISA) and behavior have attracted and increased academic levels over the past decade. According to ISA, it has been found to affect employee adherence to policy and security behavior positively. Information security culture (ISC) can be defined as the "collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in an organization to influence employees' security behavior to preserve information security" [35].

The visibility of information security policy has an appositive impact on employees' behavior towards policy compliance. Awareness training and education have a positive impact on employees' attitudes and behavior towards information security policy. The importance of information security awareness in mitigating cybersecurity and information security threats is almost an agreed-upon issue; however, various approaches and conceptual frameworks have been developed to implement ISA effectively. Usually, the differences are in what human factors to consider when designing a model for ISA. An example proposed a model that considers the attitudes, involvement, training, awareness, ISA, deterrence and incentives, and management support as the human factors to consider while implementing an ISA program in organizations.



A model to implement ISA in organizations from adapted from [1]

3.4 Critical Analysis

Literature review and analysis of the human factors within cybersecurity has revealed that almost all of the studies reviewed have highlighted and emphasized the importance of human factors concerning cybersecurity topics and activities. It is a fact that there are studies fewer studies available/published that investigate human factors thoroughly in business organizations. Therefore, reviewing the various studies, this research focuses on human factors that affect cybersecurity in organizations. For instance, most of the previous studies examine one or two of the human factors of business organizations. Thus, it seems that there may be a literature gap available in this area to conduct a new study. Most studies examined focused on specific attributes, and only two studies examined a combination of factors. Most studies are built on different backgrounds and theories, such as behavioral-based theory, information systems theories, and organizational theories, so it will be difficult to compare them since they are based on fragmented discipline. Such a situation calls for an interdisciplinary approach to cybersecurity which will have the potential to provide a holistic view integrating computer science, behavioral sciences, and management science.

3. Research Approach

3.1 Comprehensive literature Review

We did a thorough and rigorous study of the literature on human cybersecurity behavior. We searched ScienceDirect, SpringerLink, IEEE Xplore, the ACM digital library, Google Scholar, and ProQuest for professional and academic literature using the following keywords: ' cybersecurity security policy, ' human cybersecurity behavior management, and so on. There were many scholarly publications, industrial standards, and technical reports included in the preliminary results. After eliminating 20 publications not relevant to security policy, 100 security policy-related papers searching from Google scholar (25), Science Direct (15), IEEE explore (25), ACM (15), Jstor (5) and Emerald (15) dated between 2007 and 2020 remained. Twenty publications discussed the process of developing security policies, 16 articles proposed security policy lifecycles, and 84 publications discussed specific aspects of security policy, such as policy quality, compliance, and employee attitudes toward security policies. The identified papers were synthesized using a coding technique to generate a comprehensive understanding of security policy management.

Digital library	Total publication found
Google Scholar	25
Science Direct	15
IEEE explore	25
ACM	15
Jstor	5
Emerald	15
Total	100

Additionally, a model for managing security policies [27] was presented based on the information gained during the

reviewing and synthesizing process. The review and analysis of the literature were conducted following the guidelines established by Okoli and Schabram [36]. The evaluation process began with the fourteen papers presenting security lifecycle proposals. Each article was reviewed; paragraphs were distilled into themes, and sentences pertaining to policy formulation were highlighted. Then, on the margins, ideas and notions were jotted down. After going over the entire document, the key themes were summarized on the back of the final page. By the end of the overall review, the summaries assist the researcher in recalling the major ideas presented in work. The articles were synthesized using the coding technique after reviewing the fourteen papers on the policy formation lifecycle. Neuman [37] detailed coding process involves open, axial, and selective coding. The second evaluation began with a greater emphasis on the highlighted excerpts and summaries from the first review. The management of policies began to emerge as a theme. The researchers examined the identified topics, paying special attention to those covered often across the publications. Themes were subdivided into sub-themes, and numerous closely related concepts were consolidated into a single, more comprehensive notion. A comparison was made between the recurring themes in various locations. A similar review procedure was used to evaluate the 92 publications that did not directly touch on security policy development. However, the review process was influenced by the findings of the security policy lifecycle review. Although no new themes were identified, the examination revealed additional information regarding previously identified themes from lifecycles and located evidence to corroborate previously reported themes. For instance, several security policy lifecycles emphasize the significance of involving stakeholders in the policy formulation process. However, they did not identify stakeholders or discuss their roles and duties during the policy creation process. These details may be found in several of the extra 92 publications. Our definition of security policy management procedures led the evaluation process. We describe policy management techniques as the high-level activities that organizations do to manage their security policies. Security policy management entails the creation, implementation, and evaluation of security policies. The coding procedure resulted in the identification of seven techniques for managing security policies. Each practice includes a variety of tasks. These behaviors are classified into three stages.

3.2 Comprehensive Literature Review (CLR) Protocol

Comprehensive Literature Review (CLR) protocol is a set of tasks that have to be carried out to answer research questions. The review protocol consists of six components, i.e., research questions, designing the search terms, searching strategy, publication selection criteria, publication-quality assessment, data extraction, and data synthesis. Guidelines stated in (Kitchenham and Charters, 2007), the procedures used to implement the CLR protocol are detailed below.

3.3 Research Question

Population, Intervention, Comparison, Outcomes, and Context (PICOC) structure of questions are shown in Table 1. The primary focus of this study is to understand and identify the human factors in cybersecurity and solutions, tools and techniques that can be implemented to mitigate the risk of human factors in cybersecurity in organizations. In order to identify to what extent the human factors in cybersecurity and solutions to mitigate it has been studied; this work investigates to answer the following primary research questions:

Population	Any Organization
Intervention	Human factors(behaviors) in cyber security/Solutions to mitigate human factors(behaviors) in cyber security
Comparison	None
Outcomes	Human factors(behaviors) in cyber security/Solutions to mitigate human factors(behaviors) in cyber security
Context	Review of any studies of human factors in cybersecurity within the domain of any study in any organization. No restriction on the type of study applied

Table 1: PICOC Structure

RQ1: What are the human factors in cybersecurity that are related to the user in organizations?
RQ2: What solutions, tools, and techniques can be implemented to mitigate the risk of human factors in cybersecurity in organizations?

The results of the search term are shown below

Digital library	Total publication found
Google Scholar	25
Science Direct	15
IEEE explore	25
ACM	15
Jstor	5
Emerald	15
Total	100

Table 2: Digital Libraries Searched

Publications Selection

Publication selection based on selecting papers that were related and relevant to research questions. Therefore, inclusion and exclusions criteria are shown in table 3 below.

Inclusion criteria	Publications that were written in the English language
	Publication in the time frame from 2007 to 2020
	Research papers that were available in full text
	Research that was related to the study
	Research and studies which explicitly defined cybersecurity or information security were considered
	Researches that described and listed the human factor explicitly in cybersecurity and how to mitigate it In organizations based on the role of the human as users
	Papers that are free of charge(open access)
Exclusion criteria	Studies and research that did not fulfill inclusion criteria as mentioned above were excluded.

Table 3: Inclusion and Exclusion Criteria

4. Statistical Analysis

Papers that are selected for CLR will be analyzed qualitatively and quantitatively, Shown in the appendix

4.1. Overview of the Studies

Publication Year

Following the CLR protocol, we restricted the search is to be between 2007 and 2020. As mentioned earlier, 33 studies have been selected to identify human factors in cybersecurity. Although our list is not exhaustive, it represents a high-quality publication at the forefront of Human factors research. Below is a breakdown of studies published between 2007 and March 2020.

Year	Study number	Total	Percentage (%)
2007	S22	1	3.1
2009	S15,S27,S29	3	9.3
2010	S13,S28	2	6.25
2012	S7,S14,S16	3	9.3
2013	S10,S25	2	6.25
2014	S6,S24	2	6.25
2015	S1,S4,S19,S20	4	12.5
2016	S11,S26	2	6.25
2017	S8,S9,S12,S18	4	12.25
2018	S3	1	3.1
2019	S2,S5,S30,S31,S32,S33	6	18.75
2020	S17,S23	2	6.25
Total		**32**	

Table 1-4: Studies publication year

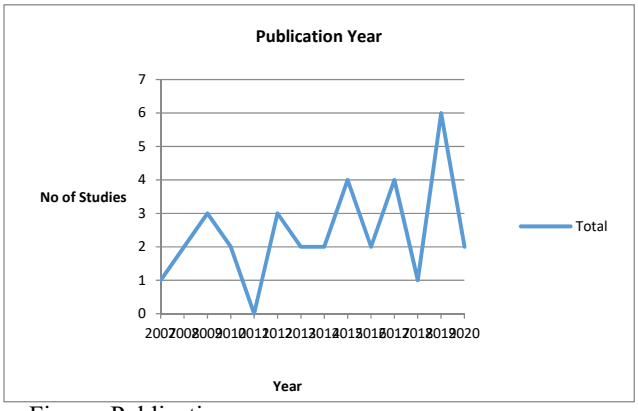


Figure: Publication year

An increase in the publication is noted between 2015 and 2020; we think this is due to increases in cyber-attacks involving human factors. We did not find publication in 2011, but we noted that the publication process from receiving a research paper until publishing takes not less than six months, and this makes some researches done in 2011 to be published in 2012 and so for the rest of the years. Our finding also might support claims by many researchers that the field of human factors in cybersecurity is still under researched, even though the human is acknowledged as the weakest link in the cybersecurity chain. On the other hand, human factors in cybersecurity are a sensitive topic as the studies involving humans need special arrangements and take a long time.

4.2 Research methodologies used in the selected Studies

As part of the overview from selected studies, methodologies used in studies are also extracted and presented in detail in the table below. From the table, we note that 40.6% (13 out of 33) of papers used survey methodology, 12.5% (4 out of 33) used Cybersecurity Expert report and literature review respectively, 9% (3 out of 33) used case study methodology,6.25% (2 out of 33) used conceptual framework, 6.25%(2 out of 33) used interview methodology. In contrast, cybersecurity assurance, experiment, intervention, and observation methodologies are used in 3% (1 of 33) in each of the rest four studies, respectively.

Methodology	Study ID	Total	Percentage (%)
Survey	S1,S2,S4,S7,S8, S9,S14,S15, S16,S17,S30,S3 1,S33	13	40.6
Expert Report	S26,S27,S28,S2 9	4	12.5

Literature review	S3,S23,S24,S25	4	12.5
Case Study	S10,S12,S18	3	9.4
Conceptual	S6,S19	2	6.25
Interview	S22,s32	2	6.25
Cybersecurity Assurance	S11	1	3.13
Experiment	S5	1	3.13
Intervention	S13	1	3.13
Observation	S20	1	3.13

Table 2-4: Methodologies used in the selected studies

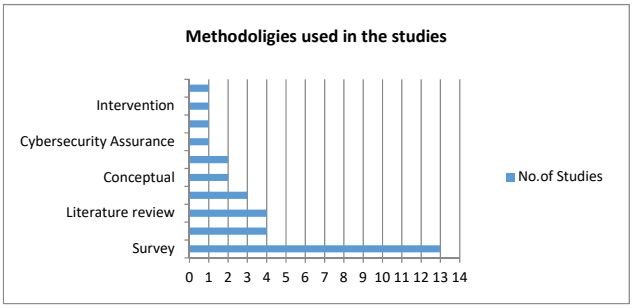


Fig 4-2: methodologies used

Active Research Communities

Data extracted was used to identify countries in which human factors in cybersecurity researches are active. Studies selected for CLR review have been distributed into continent and country levels, as shown in the table below.

Continent/Country	Study Number	Number of Studies	%
Australia		**2**	**6**
Australia	S28,S32	2	6
Africa		**1**	**3**
Nigeria	S18	1	3
Asia		**8**	**24.2**
Japan	S20	1	3
Korea	S14	1	3
Malaysia	S7,S25	2	6
Saudi Arabia	S19	1	3
Singapore	S15	1	3
Vietnam	S32,S33	2	
Europe		**10**	**30.3**
UK	S9,S10,S11,S12,S27,S30	6	18
Finland	S4	1	3
Greece	S6	1	3
Norway	S13	1	3
Turkey	S1	1	3
North America		**12**	**36.4**
USA	S2,S3,S5,S8,S16,S17,S21, S22,S23 S24,S26,S29	12	36.4

Table 3-4: Active Research Communities

36.4% of the work (12 out of 33 studies) has been carried out in the United States. 30.3% (10 out of 33 studies) have been carried out in Europe. 24.2%(8 out of 33 studies) has been carried out in Asia, and 6% (2 out of 33 studies) has been done in Australia, while only 1%(1 out of 33 studies) has been done in Africa. This might reflect the fact that the more a country is dependent on IT to carry out business and services, the more likely it will be cyber attacked.

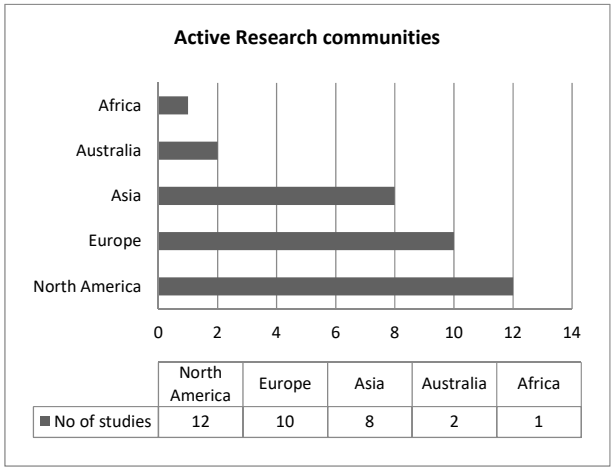


Fig 3-4: Active Research communities

5. Synthesis of identified Human Factors in Cybersecurity

In this section human factor in cybersecurity is identified from data synthesis. Eleven factors have been identified and coded from CHF1 TO CHF11. The findings show that

CHF1 (Human Cybersecurity behavior) has been mentioned and researched in 18 out of 33 studies and has the highest frequency with a percentage of 54.5%. Risky cybersecurity behavior could expose data and information to breaches: personality influence an individual's perception, attitude, and behaviors towards cybersecurity. Internet addiction could be a predicator for risky cybersecurity behavior in organizations. At the same time, a positive attitude towards cybersecurity is negatively related to risky cybersecurity behaviors [38]; also, personality traits such as impulsivity are found to be a predicator for negatively cybersecurity behavior [38], and individuals who have impulsivity are more susceptible to cyber-attacks [8]. Human behavior becomes more protective when they become aware of threats [39]. The best approach towards improving behaviors and culture among organizations employees is applying ongoing awareness activities [40]. However, despite all that, The problem of human behavior and its vulnerabilities in cybersecurity is manifested because it cannot be quantified, and there are no agreed-upon measured values regarding them [41]. This fact makes dealing with human behavior regarding cybersecurity a tedious task, especially for cybersecurity practitioners. More researches are needed to address the problem of human behavior in cybersecurity. One of the practical solutions is to make security policies clear and visible. The employee also should be rewarded when follows good behavior and punisher otherwise. Also, proper

training and awareness programs could be used to change negative behavior among employees in organizations.

Code	Human Factor	Studies	Factor Frequency	%
CHF1	Human Cybersecurity Behavior	S1,S2,S6,S7,S8,S9,S10,S11,S12,S13,S14,S15,S16,S17,S18,S19,S20,S24	18	54.5
CHF2	Training	S1,S5,S6,S7,S8,S9,S10,S12,S13, S14,S19, S20,S26,S29,S31	15	45.4
CHF3	Cybersecurity Awareness	S2,S4,S6,S7,S10,S12,S13,S19,S26,S31	10	30.3
CHF4	Human error	S3,S10,S11,S21,S22,S23,S25,S29	8	24.2
CHF5	Lack of motivation	S6,S7,S10,S24	4	12
CHF6	Education	S9,S14,S27,S28	4	12
CHF7	Security self-efficacy	S4,S8,S17	3	9
CHF8	Experience	S10,S32	2	6
CHF9	Skills	S10,S32	2	6
CHF10	Stress	S10,S33	2	6
CHF11	Gender	S4,S8	2	6

Table: 4-4 Human factors in cybersecurity identified

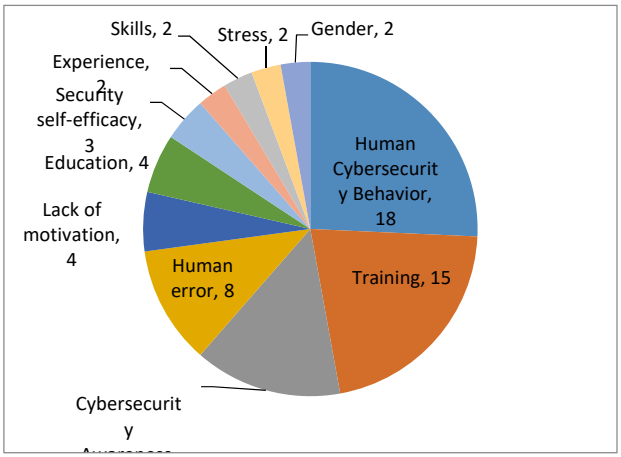


Figure 4-4: Human Factors in Cybersecurity

Training (CHF2) is the second most identified human factor in cybersecurity. The findings show that CHF2(Training) has been mentioned and researched in 15 out of 33 of the selected studies and has a frequency with a percentage of 45.4%. Our finding reveals that training is a significant factor to consider for mitigating cybersecurity attacks and changing employees' risky behaviors, and it results in a positive security behavior [24, 42]. When employees receive proper cybersecurity training, they adhere to security policies [39], and they also become satisfied [43]. Non-trained employees expose companies to varieties of information security risks [44]. Providing proper training for employees, factors such as user role, user security need, and expected security risks should be counted for [38, 44], which means training should be tailored according to individual's needs. Also, taking feedbacks from trainees is essential to assess them [38]. Some researchers argued that training must be gender-specific as women have less self-efficacy than men [43], but we think that one research can't be generalized and more research is needed to prove such claims. Providing training in cybersecurity using only classes is not appropriate for some cybersecurity risks such as phishing [8]; in phishing training, it is better to execute training practically, that is to phish users and, when caught responding to phishing e-mails, present them with short, easy-to-read training documents showing how to recognize an attack.

Cybersecurity Awareness (CHF3) is the third most cited human factor. The findings show that CHF3 (cybersecurity awareness) has been mentioned and researched in 10 out of 33 studies with 30.3%. Awareness and lack of awareness among an organization's employees as a human factor have been investigated in many studies reviewed. Lack of awareness contributes to many information security risks, such as employee's risky behavior and belief [44]. Raising security awareness among employees can mitigate cybersecurity risks caused by human weakness and errors [43, 45]. Cybersecurity awareness among employees results in positive cybersecurity behavior improvement [40, 42]. Awareness programs fail to

fulfill their purposes when dealt with as a tick-box exercise and must be an ongoing process, and they are likely to be successful when supported by top management [40]. Some factors might impact information security awareness, such as gender and education, and demographic factors. Gender, living place, and information security-related training have a statistically significant correlation with attained ISA level [40, 46], but such conclusions need more research as it is impossible to generalize such findings [43]. In our point of view, human cybersecurity awareness plays a vital role in mitigating cybersecurity risks and attacks. However, the concept is generally and theoretically described, and more studies and researches are required to give the best ways to achieve cybersecurity awareness in organizations. we agree with [40] that awareness programs should be delivered in an attractive way to encourage employees to engage in it actively and be on -ongoing basis and supported by top management.

Human error (CHF4) is the fourth most cited human factor. The findings show that CHF4 (Human error) has been mentioned and researched in 8 out of 33 studies with 24.2%. Human error leads to data breaches, cyber-attacks, and ransomware [42, 47]. More studies need to be carried out [47] (Nobels 2018) because human error is complex (Kramer, 2007). Human error in cybersecurity is multi-disciplinary research that needs collaboration between scholars in different fields such as Human-computer interface (HCI), Psychologists, human factors specialists, and IT specialists [47]. One of the research selected [41] proposed measuring human errors using qualitative and quantitative methods such as the Human Reliability Measure (HRA). According to Evans et al, [41] a human reliability measure describes a human's ability to carry out a given task without any errors in a given condition over a given time.

Lack of motivation (CHF5) is the fifth most cited human factor. The findings show that CHF5 (lack of motivation) has been mentioned and researched in 4 out of 33 studies with a percentage of 12%. Lack of motivation leads employees not to follow information policies. One of the ways to motivate employees is to share security issues with them [45].

Education (CHF6) is the fifth most cited as the same as lack of motivation. The findings show that CHF6 (Education) has been mentioned and researched in 4 out of 33 studies with a percentage of 12%. As errors are committed by the individual, which leads to cyber-attacks, most of the time comes from ignorance, so education is essential. Visible security policy and staff education drive security topics integrated into the business behavior (Colwell, 2009).

Security self-efficacy (CHF7) The finding shows that CHF7 (Security self-efficacy) has been mentioned and researched in 3 out of 33 selected studies and has the frequency with a percentage of 9%. Security self-efficiency enables an individual to deal with security issues and make a decision towards them. It is a personality trait that can be improved through training and education.

Experience (CHF8) The finding shows that it has been mentioned and researched in 2 out of 33 selected studies and has a frequency with a percentage of 6%. Prior experience can predict an individual cybersecurity behavior [43].

Skills (CHF9) The finding shows that it has been mentioned and researched in 2out of 33 selected studies and has a frequency with a percentage of 6%. Individuals with cybersecurity skills perform better than those without it, enhancing employee attitude towards cybersecurity behavior. The absence of skilled personnel can increase the probability of cyber-attacks [42]. Training and education programs play a significant role in improving staff and employees' skills.

Stress (CHF10) The finding shows that it has been mentioned and researched in 2 out of 33 selected studies and has the frequency with a percentage of 6% Stress affects employees' adherence to security policy [11]. Stress occurs due to high job work and the complexity of information policies [11].

Gender (CHF11) This finding shows that CHF11 (Gender) has been mentioned and researched in 2 out of 33 selected studies and has the frequency with a percentage of 6%. The gender human factor has been studied from the perspective of cybersecurity behavior. Gender has an effect on prior experience and computer skills [43]. Gender also has been found to be related to information security awareness [48]. Males have a higher score in information security awareness, and Women's self-efficacy is lower than men's in terms of computer skills and prior experience [43], and training on awareness and cybersecurity for employees should be gender-specific [43]. It is difficult to generalize these findings, and more research is required to highlight gender issues as a human factor in cybersecurity.

5.1 Summary of Finding

RQ1: What are the human factors in cybersecurity that are related to the user in organizations?

From the CLR studies, 33 types of research and studies related to human factors in cybersecurity in different organizations implemented by scholars in human factors have been identified. This research aims to identify the main human factors in cybersecurity and how to mitigate risks associated with them. The human factors mentioned below are identified from literature synthesis that will answer the first research question.

Human Factor	Factor Frequency	%
Human Cybersecurity Behavior	18	54.5
Training	15	45.4
Cybersecurity Awareness	10	30.3
Human error	8	24.2
Lack of motivation	4	12
Education	4	12
Security self-efficacy	3	9
Experience	2	6
Skills	2	6
Stress	2	6
Gender	2	6

We noted that there is an appositive correlation between cybersecurity human behavior and cybersecurity awareness from one side and a positive correlation between awareness and training from another side. That is to say that the more individuals have an awareness of cybersecurity risks, they will tend to have positive behavior towards it and behave in a proper way that mitigates the cybersecurity attacks and risks. Training also improves individual's cybersecurity awareness and provides them with necessary knowledge and skills that will prevent them from committing risky behavior and all that will lead to a reduction in human error, which will lead to mitigation of cybersecurity attacks and transfer individuals to human firewall instead of being the weakest link in the cybersecurity chain. My results also agree with the previous research, but previous research focuses on two or 3 human factors, but here we give eleven human factors in cybersecurity that build on the evidence of those research.

RQ2: What solutions, tools, and techniques can be implemented to mitigate the risk of human factors in cybersecurity in organizations?

Information security awareness (ISA) and cybersecurity awareness are necessary and play a significant role in protecting an organization from cyber threats. Metalidou et al., [45] indicated that Information security awareness is the key to mitigating security threats caused by human weaknesses. For employees to apply and follow security policies, security functions have to be meaningful and as little intrusive as possible, and security policies need to be easy to understand and easy to reach. Alavi et al. [42] also indicated the importance of information security awareness and training for positive security behavior. Most of the researchers studied have highlighted the role of ISA in mitigating the risk of human factors in cybersecurity, but most of them did not outline the best ways to implement it. According to [40], implementing cybersecurity awareness and changing

behavior is a challenging mission for reasons such as that awareness program is often treated as tick-box exercises and fails to achieve their objectives. Also, some of these programs rely on scaring the participants of the consequences of cybersecurity attacks to change participants' behavior. They also argued that one of the best approaches to change behavior is applying ongoing awareness activities. They suggested applying a persona-centered methodology to approach awareness and behavior programs. The personas, grounded in empirical data, offer a valuable method for identifying audience needs and security risks, enabling a tailored approach to business-specific awareness activities.

6. Conclusion and limitations

Despite technical countermeasure, cybersecurity attacks and threats are increasing daily and ever-growing, causing damage and financial losses to organizations. Cyber attackers are targeting human weakness to get access to systems and data. The study of human factors that impact cybersecurity has become more vital to mitigate the risks and damages caused by security breaches.

This research investigated the main human factors that impact users and employees in organizations and solutions and tools to mitigate it. It started by outlining the damages and risks caused by cybersecurity attacks and the financial damage that it can cause to the organization. It overviewed the most types of attacks used by cybercriminals that exploit the human weakness, such as social engineering attacks. To answer research questions, this research implemented the Comprehensive Literature Review (CLR) methodology. It started by formulating an CLR protocol to select the publication used to answer research questions. Data from these publications have been extracted, synthesized, and analyzed. Thirty-three studies have been selected for the CLR process. This study identified human factors in cybersecurity are behavior, training and education, gender, information and cybersecurity awareness, human error, education, stress, experience, skills, and lack of motivation. The answer to the second research question is to implement ongoing cybersecurity awareness programs to mitigate risks and cybersecurity attacks caused by human factors. One of the limitations of this research is that it only reviewed a limited size of literature, but the focus was on high-quality research that paved the way for conducting other research. It is also limited to the role of users and employees in organizations, and the focus was on human factors that depend on individual perception, behavior, and knowledge of information security. It has not identified other human factors related to an organization, such as budget and management support. Although the results of this research cannot be generalized, they can be used to explore further the human factors that impact cybersecurity in organizations. This research might be beneficial to cybersecurity practitioners as it highlighted the main human factors in organizations, the weak points that could be addressed, and the best methodologies to address them.

References

[1] A. AlHogail and A. Mirza, "Information security culture: A definition and a literature review," in *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 2014, pp. 1-7.

[2] M. Alshaikh and B. Adamson, "From awareness to influence: toward a model for improving employees' security behaviour," *Personal and Ubiquitous Computing,* 2021/03/15 2021.

[3] M. Alshaikh, S. B. Maynard, and A. Ahmad, "Applying social marketing to evaluate current security education training and awareness programs in organisations," *Computers & Security,* vol. 100, p. 102090, 2021/01/01/ 2021.

[4] Verizon, "Data Breach Investigations Report," Verizon Enterprises, 2019," ed, 2019.

[5] P. Carey, *Data protection: a practical guide to UK and EU law*. Oxford University Press, Inc., 2018.

[6] S. Stolfo, S. M. Bellovin, and D. Evans, "Measuring Security," *IEEE Security & Privacy,* vol. 9, no. 3, pp. 60-65, 2011.

[7] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors Related to Cyber Security Behavior," (in English), *Ieee Access,* Article vol. 8, pp. 125140-125148, 2020.

[8] T. Cuchta *et al.*, "Human risk factors in cybersecurity," in *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 2019, pp. 87-92.

[9] T. Y. Wang and F. H. Wen, "Research on Employee Attribute Correlation of Information Security Awareness in Organization," in *International Conference on Artificial Life and Robotics (ICAROB)*, Japan, 2019, pp. 63-65, OITA: Alife Robotics Co, Ltd, 2019.

[10] N. H. Abd Rahim, S. Hamid, M. L. M. Kiah, S. Shamshirband, and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," *Kybernetes,* 2015.

[11] I. Chong, A. Xiong, and R. W. Proctor, "Human factors in the privacy and security of the internet of things," *Ergonomics in design,* vol. 27, no. 3, pp. 5-10, 2019.

[12] M. Sas, G. Reniers, K. Ponnet, and W. Hardyns, "The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour," (in English), *Safety Science,* Article vol. 144, p. 8, Dec 2021, Art. no. 105447.

[13] J. Abawajy, "User preference of cyber security awareness delivery methods," (in English), *Behaviour & Information Technology,* vol. 33, no. 3, pp. 237-248, Mar 4 2014.

[14] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Computers & Security,* vol. 98, p. 102003, 2020/11/01/ 2020.

[15] A. Tolah, S. M. Furnell, and M. Papadaki, "A Comprehensive Framework for Understanding Security Culture in Organizations," in *IFIP World Conference on Information Security Education*, 2019, pp. 143-156: Springer.

[16] A. Da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, "Defining organisational information security culture—Perspectives from academia and industry," *Computers & Security,* vol. 92, p. 101713, 2020.

[17] A. AlHogail, "Design and validation of information security culture framework," *Computers in Human Behavior,* vol. 49, pp. 567-575, 2015.

[18] F. Nel and L. Drevin, "Key elements of an information security culture in organisations," *Information & Computer Security,* vol. 27, no. 2, pp. 146-164, 2019.

[19] ENISA, "Cyber security culture in organisations. European Union Agency for Network and Information Systems.," 2018, Available: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

[20] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences,* vol. 80, no. 5, pp. 973-993, 2014.

[21] A. N. Singh, A. Picot, J. Kranz, M. Gupta, and A. Ojha, "Information security management (ISM) practices: Lessons from select cases from India and Germany," *Global Journal of Flexible Systems Management,* vol. 14, no. 4, pp. 225-239, 2013.

[22] M. Alshaikh, "Information security management practices in organisations," 2018.

[23] P. Carpenter, *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us about Driving Secure Behaviors*. John Wiley & Sons, 2019.

[24] R. Alavi, S. Islam, and H. Mouratidis, "An information security risk-driven investment model for analysing human factors," *Information & Computer Security,* 2016.

[25] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Computers & Security,* vol. 88, p. 101640, 2020.

[26] M. Warkentin and R. Willison, "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems,* vol. 18, no. 2, pp. 101-105, 2009/04/01 2009.

[27] M. Alshaikh, A. Ahmad, S. Maynard, and S. Chang, "Towards a Taxonomy of Information Security Management Practices in Organisations," in *25th Australasian Conference on Information Systems*, Auckland, New Zealand, 2014.

[28] H. Altukruni, S. B. Maynard, M. Alshaikh, and A. Ahmad, "Exploring Knowledge Leakage Risk in Knowledge-Intensive Organisations: behavioural aspects and key controls," presented at the ACIS, Perth, Australia, 2019.

[29] M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, and D. Calic, "Factors that influence information security behavior: An Australian web-based study," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2015, pp. 231-241: Springer.

[30] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computers & Security,* vol. 57, pp. 14-30, 2016/03/01/ 2016.

[31] S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," *Computers & Security,* vol. 61, pp. 169-183, 8// 2016.

[32] A. Tsohou, M. Karyda, S. Kokolakis, and E. Kiountouzis, "Managing the introduction of information security awareness programmes in organisations," *European Journal of Information Systems,* vol. 24, no. 1, pp. 38-58, 2015.

[33] P. Balozian, D. Leidner, and M. Warkentin, "Managers' and Employees' Differing Responses to Security Approaches," *Journal of Computer Information Systems,* vol. 59, no. 3, pp. 197-210, 2019/05/04 2019.

[34] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations," presented at the Proceedingsofthe51st Hawaii International Conference on System Sciences, Hawaii, US, 2018.

[35] 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: Springer.

[36] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," *Sprouts: Working Papers on Information Systems,* 2010.

[37] W. L. Neuman, "Social research methods: Qualitative and quantitative approaches," 2006.

[38] 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.

[39] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Computers & Security,* vol. 56, pp. 83-93, 2// 2016.

[40] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Computers & Security,* vol. 70, pp. 663-674, 2017/09/01/ 2017.

[41] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Security and Communication Networks,* vol. 9, no. 17, pp. 4667-4679, 2016.

[42] R. Alavi, S. Islam, H. Jahankhani, and A. Al-Nemrat, "Analyzing human factors for an effective information security management system," *International Journal of Secure Software Engineering (IJSSE),* vol. 4, no. 1, pp. 50-74, 2013.

[43] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior,* vol. 69, pp. 437-443, 2017.

[44] N. Badie and A. H. Lashkari, "A new evaluation criteria for effective security awareness in computer risk management based on AHP," *Journal of Basic and Applied Scientific Research,* vol. 2, no. 9, pp. 9331-9347, 2012.

[45] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The human factor of information security: Unintentional damage perspective," *Procedia-Social and Behavioral Sciences,* vol. 147, pp. 424-428, 2014.

[46] V. Ismatullina and I. Voronin, "Gender differences in the relationships between Big Five personality traits and intelligence," *Procedia-Social and Behavioral Sciences,* vol. 237, pp. 638-642, 2017.

[47] C. Nobles, "Botching human factors in cybersecurity in business organizations," *HOLISTICA–Journal of Business and Public Administration,* vol. 9, no. 3, pp. 71-88, 2018.

[48] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information security awareness in educational institution: An analysis of students' individual factors," in *2015 IEEE Trustcom/BigDataSE/ISPA*, 2015, vol. 1, pp. 352-359: IEEE.