A Systematic Review on Human Factors in Cybersecurity

Ahmed Alghamdi,

Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah,
Jeddah, Saudi Arabia

Abstract
A huge budget is spent on technological solutions to protect Information Systems from cyberattacks by organizations. However, it is not enough to invest alone in technology-based protection and to keep humans out of the cyber loop. Humans are considered the weakest link in cybersecurity chain and most of the time unaware that their actions and behaviors have consequences in cyber space. Therefore, humans' aspects cannot be neglected in cyber security field. In this work we carry out a systematic literature review to identify human factors in cybersecurity. A total of 27 papers were selected to be included in the review, which focuses on the human factors in cyber security. The results show that in total of 14 identified human factors, risk perception, lack of awareness, IT skills and gender are considered critical for organization as for as cyber security is concern. Our results presented a further step in understanding human factors that may cause issues for organizations in cyber space and focusing on the need of a customized and inclusive training and awareness programs.

Key words:
Cybersecurity, human factors, systematic literature review.

1. Introduction

Organizations collect, transmit and store data to perform various activities related to their routine business operations[1] . This data proliferation makes them target for cyber criminals (hackers). Enterprises are investing huge amount of money on technology to safeguard their systems from cyber threats. However, with the availability of latest technology, hackers can still get access to organization critical systems and data [2]. Most organizations think that cyber security is only a technical issue [3], in fact it is not. A little attention is given, and small budget is reserved for human factors and security culture within enterprises. Cyber security practitioners and academia are agreed on the fact that human who interact with the systems are the weakest link in cyber security [4] as a result several human factors cause serious issues for organizations in cyber space. The undesirable human actions (factors) are the direct reflection of enterprise cyber culture which define the motivation for most of the threat actors [5].

Human factors is a scientific discipline where researchers study how people (users) use technology [6]. When human interact with systems, they can make errors because of various reasons like carelessness, negligence, accidental or deliberate action [7]. Therefore, it is important for enterprises to apply a people-centric approach toward cybersecurity and invest resources in building an inclusive cybersecurity culture.

Hackers, now a days are attacking people rather than technology with the aim to exploit human factors. According to [8], 99% successful cyberattacks and major cause of data breaches are because of human factors. Enterprises are adopting latest computing technologies to achieve their business objectives, however, the human involvement in routine technological operations make them more susceptible to cyber threats. Wrong decision taken by the users either because of lack of awareness or following wrong operational plans, hacker take advantages and penetrate int to the enterprise information systems. Human error is a complicated security issue and main cause of majority of reported cyber incidents and breaches [9]. Human involvement cannot be eliminated so does human errors. Therefore, it is important to investigate human factors in cyber security to protect the systems up to acceptable level.

The goal of this research study is to identify human factors in cyber security using systematic literature review (SLR) methodology. The research also investigates how identified human factors cause problem for organizations in cyber space. Along with the human factors, this research study also identifies counter measures/ solutions to exist in existing literature to finish or minimize human error up to acceptable level. To date, there have been few SLR conducted to identify human factors in cybersecurity. Moreover, considering the growing demand of human factors, we need to investigate a research agenda for cyber security. This SLR identifies, classifies and synthesis a comparative overview of peer literature and enable knowledge transfer in the research community.

Rest of the paper is structures as follows: Section 2 describes literature review, section 3 explains our research methodology, research questions and scope. Section 4 provides results and discussion, and section 5 concludes the paper.

2. Literature Review

Cyber security is an important filed of research. Industry and academia are exploring cyber security from various perspectives. 'Human factors' is an important

Manuscript received October 5, 2022
Manuscript revised October 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.10.36

focus area in the field of cyber security. In this section we present studies that are relevant to our work.

In their study [10] analyzed the concepts of human factors in cyber security from end user perspectives. They statistically proved that gender wise difference in the knowledge of cyber security where male employees within organization have more knowledge of cyber security as compared to female employees. They also claimed that only cyber security knowledge is not enough for protection from cyber-attacks, end user behaviors play a significant difference. They emphasis on well-planned and effective cyber security training programs for end users to eliminate or reduce human errors up to acceptable level.

In their study [11] argued that it is difficult to address cyber security only through technology, in fact it required socio-technical approach to deal with cyber-attacks. They consider human factors as one of the weakest and obscure links while creating a safe and secure digital environment. Human factors like gender, age, education, and experience have impact on cyber security.

A survey was conducted [12] in which students were presented various definitions of cyber threats and rated them according to their familiarity. Students were then categorized into three groups according to their knowledge, time they spent on the Internet and experience. The authors argued that level of students' familiarity with cyber threats is considered as a predicator of Internet attitudes and security behavior.

The authors [13] surveyed 515 employees working part time and full time with the aim to explore relationship between risk behaviors, employees' attitude in business environment, Internet addition and impulsivity. They concluded that Internet addiction and impulsivity (attentional and motor) play a major role in risky cyber security behaviors.

In [10] correlate human factors i.e., decision making capability, demographics, personality traits and risk-taking preferences with cyber security behaviors among students and employees of a public sector university using a survey questionnaire. They found that all these human factors are good predicators of security behaviors. According to their study gender has correlation with the strength of password because weak passwords are adopted more by females as compared to males.

From the above discussion human factors in cyber security is an important issue, which needed to be investigated in detail. It is also worth noting that most of the available literature studied human factors from a specialized users (i.e., programmers, security experts and application testers, etc.) perspective. The role of end users while interacting with Information Systems and challenges they face needs investigation. These issues motivated us to investigate and apply a holistic approach to explore human factors in cybersecurity.

The objective of this SLR differs from the previous studies in two aspects. First, the focus of this review is on identifying all those human factors which have impact on cybersecurity. Second, this systematic review is a mean of evaluating and interpreting all available research that is relevant to research question, topic area of interest. This reach can also discover the structure and pattern of existing research, and hence identify gaps that can be filled by future research. The results of this study will help organizations in better understanding issues related cybersecurity because of human factors.

3. Literature Review

SLR is a methodological technique to collect and analyze data from published studies for investigating underlying research question [14]. SLR is different than non-structure/ traditional review because it reduces research biasness and follows precise sequence of steps. In this study, we followed the guidelines proposed by [15] with three steps review process i.e. planning, conducting and documenting. The details for these steps are given in the following subsections.

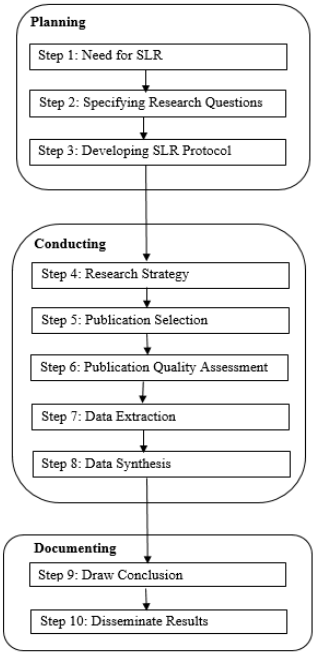

Fig. 1: SLR Steps

3.1 Planning and Review

The planning phase of SLR starts with the identification of need for SLR and results into review protocol.

Step 1 – Need for SLR

In planning SLR, the first step is to identify why we need to conduct an SLR. The need of SLR in this study is identified in section 2. The general goal and scope of this study is also formulated using population, intervention, comparison, outcome, and context (PICOC) criteria given in Table 1.

Table 1: PICOC criteria

Criteria	***RQ***
Population	Cyber security
Intervention	Identification; Data extraction and synthesis
Comparison	Comparing various factors affecting cyber security
Outcome	Human factors in cyber security; Hypothesis for future research
Context	A systematic investigation to consolidate the peer reviewed research

Step 2 – Specifying Research Questions

The research question used in this study is based on our motivation i.e., answer provide us an evidence-based overview of cyber threats because of human factors. Two research questions are defined that represent the foundation for deriving the search strategy for identifying relevant literature for data extraction, see **Table 2**

Table 1: Research questions

Research Question	***Motivation***
RQ: What human factors, as identified in literature, are posing cyber security threats for organizations?	The aim is to get insight that what are the main factors related to human errors or negligence that are considered problematic in cyber space.

Step 3 – Developing SLR Protocol

A pre-defined SLR protocol is necessary which specifies methods that will be used to conduct a specific literature review and will reduce researcher bias [15]. A review protocol was developed by a teamwork of authors and externally evaluated by an expert having experience in SLRs before its execution. Changes were made to the protocol based on the feedback of reviewer.

3.2 Conducting the Review

Conducting is the second phase of SLR which starts with search strategy and results in data extraction and synthesis.

Step 4 – Search Strategy

SLR search strategy is used to plan the following:

- Constructing search terms
- Finding alternate spellings and synonyms
- Using Boolean operators

Human Factors < OR > Human Error < OR >

Human Issues

AND

Cyber Security < OR > Cyber Safety < OR >
Internet Security < OR > Cyber Space Security

Fig. 2. Search strings

The goal of search strategy is to find published papers in journals using available search engines and databases like Google Scholar, ScienceDirect, ACM, SpringerLink and IEEE Xplore.

Step 5 – Publication Selection

Inclusion Criteria: It is used to decide which study/ paper identified through search terms will be used for data extraction. We considered papers related to human factors in cyber security only, and paper related to technological factors were ignored. Initially we did not limit the search to human factors in cyber security because we intended to have broader picture of the cyber security literature. However, in the final selection of papers only human factors papers were considered. We used the following inclusion criteria.

- Papers that are peer reviewed.
- Papers that are published only in journals.
- Papers that describe human factors in cyber security.

Exclusion Criteria: Papers retrieved through search strings might not be all relevant. Therefore, we developed the following exclusion criteria to determine which paper need to be excluded.

- Non peer reviewed literature, white papers, thesis, and book chapter.
- Papers that do not describe human factors in cyber security.
- Papers that describe technological factors in cyber security.

Study Selection Process: It is a two-step process i.e., initial section and final selection. Initial selection of studies is done by screening of titles and abstracts of potential primary studies against inclusion/ exclusion criteria. The studies included in initial selection are read thoroughly with the aim to include it in final selection or not. After this step, 23 studies were selected. References and citation of these 23 studies were also reviewed as a snowballing technique to identify any relevant paper. As a result, we came across with 5 more studies relevant to our research question. Finally, we have 27 papers for review (see Appendix). The inter-rater reliability test was

performed to reduce research bias, where secondary reviewer chose five random studies and performed initial and final selection processes. The result was then compared with the results of primary reviewer and no disagreement was found.

Step 6 – Publication Quality Assessment

The quality of 27 finally selected studies were measured in parallel at the time of data extraction. The publication quality checklist contained the following questions:

- Is the study under consideration focus on the human factors in cyber security?
- In the study under consideration focus on the counter measure/ solutions related cyber threats because of human error?

These questions were marked with YES or NO and result was used in the selection of studies. After applying quality assessment criteria, we are left with same number of papers i.e. 27.

Step 7 - Data Extraction

In this step, 27 finally selected papers were used to extracted data by using a predefined data extraction form. The following data is extracted from each study.

- Name of authors
- Title of paper
- Publication year
- Journal
- Study setting
- Human factors in cyber security
- Types of cyber attacks
- Recommended solution

Data extraction process was performed by primary reviewer (first author). A secondary reviewer was consulted in case of any confusion related to data extraction. It is also important to mention that secondary reviewer was responsible to randomly select studies and extracted data and then compared his results with the results of primary reviewer.

Step 8 - Data Synthesis

Data synthesis is performed by primary reviewer with the help of secondary reviewer. After data extraction process explained in step 7, a list of human factors in cybersecurity from 27 studies were created. The primary researcher reviewed the identified human factors to make category list.

4. Result

A total of twenty-seven papers discusses the human factors in cyber security. Before presenting the results and analysis of the identified human factors, we present a short overview of the general characteristics of the studies.

4.1 Publication over time

The papers that we reviewed were published between 2009 and 2020. The increased interest in human factors in cyber security appears in 2015 to 2017 (62.5%), which indicate an increased interest in human factors, pointing to the relevance of the research area. A complete breakdown of the studies is given in **Table 3.**

Table 3. Publication over time

Year	*Study #*	*Total*	*%*
2009	S17	1	3.7%
2012	S13	1	3.7%
2014	S20	1	3.7%
2015	S2, S5, S6, S15, S19, 27	6	22.2%
2016	S7, S11, S16, S25, S26	5	18.5%
2017	S1, S3, S4, S14	4	14.8%
2018	S18, S24	2	7.4%
2019	S10, S12, S21, S22, S23	5	18.5%
2020	S8, S9	2	7.4%

4.2 Research methodology used

The seventy-seven reviewed papers were classified according to the research methods used. Questionnaire survey (62.5%) constitute a clear majority of the studies, followed by literature review (20.83%) and experiments (16.6%). It is interesting to note that SLR research methodology is used in one paper only. The details of used methodologies in these papers are given in Table 4.

Table 4. Research methodologies

Methodology	*Study ID*	*Total*	*%*
Survey	S3, S4, S5, S6, S9, S10, S14, S19, S20, S21, S22, S23, S25, S26, S27	15	62.5%
Literature Review	S7, S11, S13, S17, S18	5	20.83%
Experiments	S6, S15, S16, S24	4	16..6%
SLR	S12,	1	3.70%
Case Study	S1, S2	2	7.40%

4.3 Active Research Community

Table 5 shows active research community in the area of human factors in cyber security. Country wise distribution of these twenty-seven papers indicate that the USA is clearly leading with total 10 papers (41.66%), followed by the UK with 4 papers (14.81%).

Table 5. Active research community

Country	*Study #*	*No. of studies*
USA	S2, S3, S5, S6, S7, S18, S19,	10

	S21, S25, S26	
UK	S11, S15, S16, S17	4
Australia	S10, S12, S27	3
China	S8	1
Poland	S14	1
Serbia	S9	1
Greece	S20	1
Italy	S22	1
Netherlands	S24	1
India	S23	1
Cameron	S4	1

4.4 Human Factors in Cybersecurity

In order to answer research question, Table 6 presents a list of human factors identified through the SLR. The main objective of this research study is to find all those human factors which have impact of cyber security for organizations. We have identified fourteen human factors from prior literature and categorize them into three sections i.e., demographic factors, cognitive factors and knowledge and skills factors. Two human factors i.e., risk perception and awareness are marked critical because its frequency is higher than 40%.

Table 6. Human factors in cyber security

Demographic Factors	***Study #***	***%***
Age	S4, S12, S16, S18, S23, S27	22.2%
Gender	S4, S7, S9, S11, S12, S16, S18, S26	29.6%
Qualification	S19, S23, S26, S27	14.8%
Experience	S7, S12, S14, S21, S23	18.5%
Work Environment	S11, S12, S14, S15, S23, S24	22.2%
Cognitive Factors		
Distraction	S2, S13, S18, S27	14.8%
Fatigue	S2, S3, S10, S14	14.8%
Decision Making	S3, S6, S16	11.1%
Risk Perception	S2, S3, S5, S6, S8, S9, S11, S16, S21, S22, S26	40.7%
Mental Stress	S14, S17, S19, S20, S24, S25, S27	25.9%
Emotional Stability	S4, S5, S8, S10, S15, S18, S27	25.9%
Human Skills and Knowledge Factors		
Awareness	S1, S2, S3, S6, S10, S12, S17, S18, S19, S20, S21	40.7%
IT Skills	S5, S7, S9, S15, S22, S25, S26, S27	29.6%
Poor Passwords	S1, S9, S18	11.1%

Demographics Factors

No matter how strong technical security solution is implemented, it can be compromised and one of its main causes are human factors. Therefore, it can be argued that cyber threats cannot be prevented by relaying only on technical solutions. Organizations allocated huge budget for the technological solutions to eradicate cyber threats but still cyber incidents happen due to employee's lack of awareness or attention [16].

When it comes to humans (employees), demographics characteristics play an important role in successful or unsuccessful cyber-attack. This fact is clear from our data extraction process as well. Demographic factors that we extracted from prior studies are age, gender, qualification, work experience and work environment.

Gender is the most common demographic factor in our study, i.e., 29.6%. Women are normally more concerned about privacy than men and more likely to comply with organization's security policies and procedures [17] and do not share information on social networking site, which protect them from social engineering attacks [18]. On the other side, men like to share their personal information and are not concern that much about privacy issues, as a result become the victim of social engineering attack. In most of the cyber breaches' men are involved, the reason might be that men are more willing to take risk as compared to women. Women are slightly at lower levels in computer skills, prior experience in cyber security and low cues-to-action scores as a result become the target of cyber intervention [17]. The general opinion found in prior studies is that men are more likely to be non-compliant with cyber security policies and procedures than women and become target of cyber-attacks. Therefore, it can be argued that both genders pose an equal threat to organization in cyber space.

Our results also indicate that age (22.2%) and work environment (22.2%) are the second important demographic factors in cyber security. Young employees are significantly more prone to cyber-attacks because they are open to experimentation and engage in poor practices like password sharing [19]. Young employees have more knowledge about computers and security which make them overconfident as a result become victim of cyber-attack. On the other hand, old age employees have less security knowledge and experience who do not understand the importance of cyber security and breaches. It can be argued that any employee whether young or old can be compromised and therefore it is important for organization to provide cyber security training and arrange awareness programs.

Work environment and organization's culture have impact on employees' performance. Those organization which has well written documented security policies and procedures are less prone to cyber security. Many employees within organization are unaware of security policies and relevant organizational requirements. A questionnaire survey was conducted by [20] in which they found that 50% employees are not aware of organizational security policies. Employees' unawareness result into non-compliance of security policies, which is a primary human problem/ factor. It can be argued that work environment/

culture play an important role in eradicating cyber-attacks because it leads to increased compliant cyber security behavior.

Experience (18.5%) and qualification (14.8%) are other two factors in demographic category. Prior experience in security is consider a positive factor in overall awareness and ability of employee to deal with cyber risks. Similarly, employee's qualification has positive impact on cyber security posture of an organization. Employees have experience and IT qualification can better understand cyber risks and mitigating strategies [21].

Cognitive factors

Risk perception (40.7%) and decision making (33.3%) are two most common cognitive factors found in our study. Risk perception play an important role in eradicating cyber threats. Several researchers linked risk perception with cyber security knowledge and argued that well trained employees have good perception of security risk and impact of security vulnerabilities [22] [23]. Risk perception is done in two ways i.e. (1) risk as feeling (instinctive reactions to cyber danger), (2) risk as analysis (scientific reaction to cyber danger) [24]. End users generally perceived risk and acted upon in first way. However, there could be a mismatch between risk perception and actual risk which results into a wrong decision by users. In [25] the researchers defined five possible factors where users risk perception can diverge from actual risk: (a) risk severity (b) risk probability (c) cost magnitude (d) risk countermeasures (e) the tradeoff itself. The security requirements of organizations are changing with the passage of time, which has effect on user risk perception as well. In such circumstances it is necessary for organizations to provide training and arrange cybersecurity awareness workshops to help employees to understand changing security requirement which will make the employees ready to deal with cyber threats.

Mental stress (25.9%) and emotional stability (25.9%) are two other cognitive factors found in our study. Mental stress has been associated with human errors in several ways. Users having mental stress and emotional instability are not motivated to adopt secure behavior and practices. Stress and emotional instability have negative impact on effective decision making [26] which could lead to the problems discussed in previous paragraph. Both factors are responsible for narrowing attention as a result users cannot pay proper attention to risky security situations.

Fatigue (14.8%) and distraction (14.8%) are the other two cognitive factors found in our study. Fatigue has negative impact on human performance and is considered a causal factor in cyber security incidents [27].

Human Skills and Knowledge Factors

Awareness (40.7%) is the most important human factor in our findings. Lack of awareness is related with lack of general knowledge about cyber security vulnerabilities and attacks [28]. Awareness is an important part of organization's cyber security while employees are important assets of organizations because of their capability to make important decision in case of any suspicious cyber activity. Therefore, it is important for any organization that their employees are completely aware of cyber security vulnerabilities. Cyber-attacks like social engineering and phishing can only be dealt with users who have knowledge of cyber threats an organization is facing. Lack of awareness is a negative factor which could have adverse impact on organization security in cyber space. Several researcher [28] [29] [30] argued the importance of cybersecurity awareness and training programs to educate every single user and to establish cyber security culture in the workplace because users can be a potential point of entry for attackers. Therefore, cybersecurity training and awareness programs are essential in reducing human vulnerabilities.

IT skills (29.7%) is also an important human factor in our findings. Employees with good IT and cybersecurity skills have better understanding of cyber incidents and risk perception [31]. Therefore, it can be argued that employees with cyber security knowledge and skills have less chances to become victims of cyber-attacks.

Password (11.1%) is mentioned in three studies in our SLR. The role of password is important in cyber security because it is a cheapest and most common used method of computer authentication [32]. However, password guessing and password cracking using brute force attack causing issues as well for organizations.

To conclude the discussion, two human factors i.e., risk perception and lack of awareness are considered critical among identified 14 factors. Cyber security training and awareness programs can help organization to eliminate or reduce cyber threats because of these factors up to acceptable level. Therefore, organizations should arrange sophisticated cybersecurity training and awareness programs in which focus should be on up-to-date cyber threats and changing security requirements of an organization.

5. Conclusion

Using systematic literature review, we have identified human factors which needed to be addressed by organizations to keep themselves secure in cyber space. We suggest that focusing on the identified human factors can help organizations in improving their readiness and cyber posture. The results presented in this paper are of core importance to organizations who are concern about cyber security. Our findings indicate that 'risk perception'

and 'awareness' are two critical human factors in cyber security because of their significant influence on organizational cyber security initiatives and could cause serious cyber threats to them. Our results also indicate that well organized cyber security awareness and training programs can minimize cyber threats to organizations. Cyber-attacks such as social engineering and phishing can be dealt with awareness and properly trained employees because aware employees have good risk perception and can take good decision in case any cyber situation.

Acknowledgement

This project was funded by the Deanship of Scientific Research (DSR), University of Jeddah, Jeddah, Saudi Arabia (Project number: UJ-02-18-DR).

Appendix – List of Papers

Paper ID	Title	Reference
S1	Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary	[33]
S2	The Human Factors of Cyber Network Defense	[27]
S3	Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS)	[34]
S4	Human factor in cyber security: link between attitude towards security and intention to perform security related behavior	[35]
S5	Towards a Human Factors Ontology for Cyber Security	[26]
S6	The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace	[36]
S7	Gender Difference and Employees' Cybersecurity Behaviors	[17]
S8	Defining Social Engineering in Cyber security	[37]
S9	Factors Related to Cyber Security Behavior	[38]
S10	Challenges of implementing training and awareness programs targeting cyber security social engineering	[28]
S11	Information Security Policies: A Review of Challenges and Influencing Factors	[22]
S12	Towards an Improved Understanding of Human Factors in Cyber security	[39]
S13	Securing the human to protect the system: Human factors in cyber security	[40]
S14	Information systems and ways of communication with regard to human factor in the face of the challenges posed by modern battlefield	[41]
S15	CHEAT, an approach to incorporating human factors in cyber security assessments	[42]
S16	Neural Markers of cybersecurity: An fMRI Study of Phishing, and Malware Warnings	[43]
S17	Human factors in information security: The insider threat e Who can you trust these days?	[44]
S18	Correlating human traits and cyber security behavior intentions	[45]
S19	Trust as a human factor in holistic cyber security risk assessment	[46]
S20	The Human Factor of Information Security: Unintentional Damage Perspective	[6]
S21	Investigating the impact of cybersecurity policy awareness on employee's cybersecurity behavior	[47]
S22	Building organizational risk culture in cyber security: The role of human factors	[48]
S23	Demographic factors in cyber security: An empirical study	[21]
S24	Understanding human factors in cyber security as a dynamic system	[49]
S25	Integrating cultural factors into human factors framework and ontology for cyber attackers	[50]
S26	Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions	[51]
S27	Factors that influence Information Security behavior: An Australian web-based study	[52]

References

[1]. Mustonen-Ollila, E.L., Kalle, How organizations adopt information system process innovations: A longitudinal analysis. European Journal of Information Systems, 2004. 13: p. 35-51. DOI:10.1057/palgrave.ejis.3000467

[2]. Uma, M. and P. Ganapathi, A Survey on Various Cyber Attacks and their Classification. Int. J. Netw. Secur., 2013. 15: p. 390-396. DOI:10.6633/IJNS.201309.15(5).09

[3]. Limba, T., et al., Cyber security management model for critical infrastructure. Entrepreneurship and Sustainability Issues, 2017. 4(4): p. 559-573. DOI: 10.9770/jesi.2017.4.4(12)

[4]. Sasse, M.A., S. Brostoff, and D. Weirich, Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal,

2001. 19(3): p. 122–131. https://doi.org/10.1023/A:1011902718709
[5]. Glaspie, H.W. and W. Karwowski. Human Factors in Information Security Culture: A Literature Review. 2018. Cham: Springer International Publishing. https://DOI: 10.1007/978-3-319-60585-2_25
[6]. Metalidou, E., et al., The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences, 2014. 147: p. 424-428. https://doi.org/10.1016/j.sbspro.2014.07.133
[7]. Im, G.P. and R.L. Baskerville, A longitudinal study of information system threat categories: the enduring problem of human error. SIGMIS Database, 2005. 36(4): p. 68–79. https://doi.org/10.1145/1104004.1104010
[8]. Proofpoint, The Human Factor 2019 Report. Available at https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf. 2019.
[9]. Liginlal, D., I. Sim, and L. Khansa, How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Computers & Security, 2009. 28(3): p. 215-228. 10.1016/j.cose.2008.11.003
[10]. Cain, A.A., M.E. Edwards, and J.D. Still, An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 2018. 42: p. 36-45. https://doi.org/10.1016/j.jisa.2018.08.002
[11]. Safa, N.S., R.v. Solms, and L. Futcher, Human aspects of information security in organisations. Computer Fraud & Security, 2016. 2016(2): p. 15-18. https://doi.org/10.1016/S1361-3723(16)30017-3
[12]. Jeske, D. and P. van Schaik, Familiarity with Internet threats: Beyond awareness. Computers & Security, 2017. 66: p. 129-141. https://doi.org/10.1016/j.cose.2017.01.010
[13]. Hadlington, L., Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 2017. 3(7): p. e00346. DOI:10.1016/j.heliyon.2017.e00346
[14]. Niazi, M., Do Systematic Literature Reviews Outperform Informal Literature Reviews in the Software Engineering Domain? An Initial Case Study. Arabian Journal for Science and Engineering, 2015. 40(3): p. 845-855. https://doi.org/10.1007/s13369-015-1586-0
[15]. Kitchenham, B. and S. Charters, Guidelines for performing systematic literature reviews in software engineering. 2007: Keele University.
[16]. de Bruijn, H. and M. Janssen, Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly, 2017. 34(1): p. 1-7. https://doi.org/10.1016/j.giq.2017.02.007
[17]. Anwar, M., et al., Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 2017. 69: p. 437-443. https://doi.org/10.1016/j.chb.2016.12.040
[18]. Choi, K.-s., K. Choo, and Y.-e. Sung, Demographic variables and risk factors in computer-crime: an empirical assessment. Cluster Computing, 2016. 19(1): p. 369-377. https://doi.org/10.1007/s10586-015-0519-8
[19]. Jang-Jaccard, J. and S. Nepal, A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 2014. 80(5): p. 973-993. https://doi.org/10.1016/j.jcss.2014.02.005
[20]. Chan, H. and S. Mubarak, Significance of Information Security Awareness in the Higher Education Sector. International Journal of Computer Applications, 2012. 60(10): p. 23-31. DOI: 10.5120/9729-4202
[21]. Mittal, S. and P.V. Ilavarasan. Demographic Factors in Cyber Security: An Empirical Study. 2019. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-29374-1_54
[22]. Alotaibi, M., S. Furnell, and N. Clarke. Information security policies: A review of challenges and influencing factors. in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). 2016. 10.1109/ICITST.2016.7856729
[23]. Hibshi, H., T.D. Breaux, and S.B. Broomell. Assessment of risk perception in security requirements composition. in 2015 IEEE 23rd International Requirements Engineering Conference (RE). 2015. DOI: 10.1109/RE.2015.7320417
[24]. Slovic, P. and E. Peters, Risk Perception and Affect. Current Directions in Psychological Science, 2006. 15(6): p. 322-325. https://doi.org/10.1111/j.1467-8721.2006.00461.x
[25]. Schneier, B. The Psychology of Security. 2008. Berlin, Heidelberg: Springer Berlin Heidelberg. DOI: 10.1007/978-3-540-68164-9_5
[26]. Oltramari, A., et al., Towards a Human Factors Ontology for Cyber Security, in In Semantic Technology for Intelligence, Defense, and Security (STIDS 2015). 2015. p. 26-33.
[27]. Gutzwiller, R.S., et al., The Human Factors of Cyber Network Defense. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2015. 59(1): p. 322-326. DOI:10.1177/1541931215591067
[28]. Aldawood, H. and G. Skinner, Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, 2019. 11(3): p. 73. https://doi.org/10.3390/fi11030073
[29]. Kassicieh, S., V. Lipinski, and A.F. Seazzu. Human centric cyber security: What are the new trends in data protection? in 2015 Portland International Conference on Management of Engineering and Technology (PICMET). 2015. DOI:10.1109/PICMET.2015.7273084
[30]. Caputo, D.D., et al., Going Spear Phishing: Exploring Embedded Training and Awareness. IEEE Security & Privacy, 2014. 12(1): p. 28-38. DOI:10.1109/MSP.2013.106
[31]. Mackenzie, A. and M. Maged, Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review, 2015. 5(1). DOI:10.22215/timreview/861
[32]. Hoonakker, P., N. Bornoe, and P. Carayon, Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2009. 53(6): p. 459-463. https://doi.org/10.1177/154193120905300605
[33]. Gyunka, B.A., Christiana, and A. Oluwakemi, Analysis of human factors in cyber security: A case study of anonymous attack on Hbgary. Computing & Information Systems, 2017. 21(2): p. 10-18.

[34]. Pollock, T., Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). 2017.
[35]. Micaela, D. Human factor in cyber security : link between attitude towards security and intention to perform security related behavior. 2018.
[36]. Proctor, R. and J. Chen, The Role of Human Factors/Ergonomics in the Science of Security. Human factors, 2015. 57. https://doi.org/10.1177/0018720815585906
[37]. Wang, Z., L. Sun, and H. Zhu, Defining Social Engineering in Cybersecurity. IEEE Access, 2020. 8: p. 85094-85115. DOI: 0.1109/ACCESS.2020.2992807
[38]. Kovačević, A., N. Putnik, and O. Tošković, Factors Related to Cyber Security Behavior. IEEE Access, 2020. 8: p. 125140-125148. DOI: 0.1109/ACCESS.2020.3007867
[39]. Jeong, J., et al. Towards an Improved Understanding of Human Factors in Cybersecurity. in 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC). 2019. DOI: 10.1109/CIC48465.2019.00047
[40]. Lee, M.G. Securing the human to protect the system: Human factors in cyber security. in 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012. 2012. DOI: 10.1049/cp.2012.1519
[41]. Nowakowska, M. and K. Świderski. Information systems and ways of communication with regard to human factor in the face of the challenges posed by modern battlefield. in 2017 International Conference on Military Technologies (ICMT). 2017. DOI: 10.1109/MILTECHS.2017.7988786
[42]. Widdowson, A.J. and P.B. Goodliff. CHEAT, an approach to incorporating human factors in cyber security assessments. in 10th IET System Safety and Cyber-Security Conference 2015. 2015. DOI: 10.1049/cp.2015.0298
[43]. Neupane, A., et al., Neural Markers of Cybersecurity: An fMRI Study of Phishing and Malware Warnings. IEEE Transactions on Information Forensics and Security, 2016. 11(9): p. 1970-1983. DOI 10.1109/TIFS.2016.2566265
[44]. Colwill, C., Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, 2009. 14(4): p. 186-196. https://dl.acm.org/doi/10.1016/j.istr.2010.04.004
[45]. Gratian, M., et al., Correlating human traits and cyber security behavior intentions. Computers & Security, 2018. 73: p. 345-358. DOI:10.1016/j.cose.2017.11.015
[46]. Henshel, D., et al., Trust as a Human Factor in Holistic Cyber Security Risk Assessment. Procedia Manufacturing, 2015. 3: p. 1117-1124. https://doi.org/10.1016/j.promfg.2015.07.186
[47]. Li, L., et al., Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 2019. 45: p. 13-24. https://dl.acm.org/doi/abs/10.1016/j.ijinfomgt.2018.10.017
[48]. Corradini, I. and E. Nardelli. Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. 2019. Cham: Springer International Publishing.
[49]. Young, H., et al. Understanding Human Factors in Cyber Security as a Dynamic System. 2018. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-60585-2_23
[50]. Henshel, D., et al. Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers. 2016. Cham: Springer International Publishing. DOI: 10.1007/978-3-319-41932-9_11
[51]. Sheng, S., et al., Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2010, Association for Computing Machinery: Atlanta, Georgia, USA. p. 373–382. https://doi.org/10.1145/1753326.1753383
[52]. Pattinson, M., et al., Factors that Influence Information Security Behavior: An Australian Web-Based Study, in Proceedings of the Third International Conference on Human Aspects of Information Security, Privacy, and Trust - Volume 9190. 2015, Springer-Verlag. p. 231–241. DOI: 10.1007/978-3-319-20376-8_21