EasyChair Preprint

№ 2032

# Towards an Improved Understanding of Human Factors in Cybersecurity

Jongkil Jeong, Joanne Mihelcic, Gillian Oliver and Carsten Rudolph



November 25, 2019

# Towards an Improved Understanding of Human Factors in Cybersecurity

Jongkil Jay Jeong
*Faculty of Information Technology*
*Monash University*
Melbourne, Australia
jay.jeong@monash.edu

Joanne Mihelcic
*Faculty of Information Technology*
*Monash University*
Melbourne, Australia
joanne.mihelcic@monash.edu

Gillian Oliver
*Faculty of Information Technology*
*Monash University*
Melbourne, Australia
gillian.oliver@monash.edu

Carsten Rudolph
*Faculty of Information Technology*
*Monash University*
Melbourne, Australia
carsten.rudolph@monash.edu

***Abstract* – Cybersecurity cannot be addressed by technology alone; the most intractable aspects are in fact sociotechnical. As a result, the 'human factor' has been recognised as being the weakest and most obscure link in creating safe and secure digital environments. This study examines the subjective and often complex nature of human factors in the cybersecurity context through a systematic literature review of 27 articles which span across technical, behavior and social sciences perspectives. Results from our study suggest that there is still a predominately a technical focus, which excludes the consideration of human factors in cybersecurity. Our literature review suggests that this is due to a lack of consolidation of the attributes pertaining to human factors; the application of theoretical frameworks; and a lack of in-depth qualitative studies. To ensure that these gaps are addressed, we propose that future studies take into consideration (a) consolidating the human factors; (b) examining cyber security from an interdisciplinary approach; (c) conducting additional qualitative research whilst investigating human factors in cybersecurity.**

***Keywords - cybersecurity; human factors; personality; culture; demographics***

## I. INTRODUCTION

Half of cybersecurity breaches associated with routine processing of confidential electronic information and technical implications are due to human errors [1]. Previous attempts at addressing this issue have often focused on physical and/or technical solutions.

Unfortunately, it is becoming increasingly apparent that algorithms, systems and processes alone are not able to keep digital systems secure as evident from the ever-increasing number of cybersecurity related incidents that are being reported globally. For instance, a recent report suggested that in 2018 alone, cybersecurity related incidents were reported to cost close to $600B USD to the global economy [2].

As it has become more apparent that the human side of cybersecurity poses as much of a risk as the technical aspects, research has started to shift towards understanding the various human factors that affect cybersecurity. In studies to date, a person's demographic attributes such as gender and age; one's own inherent personality; as well as cultural contexts have all been identified as key determinants on an individual's attitude and behaviour towards cybersecurity [3].

The highly subjective and complex nature of these human factors require innovative approaches to fully understand their impact on cybersecurity. However, the technical view of human factors and cybersecurity still dominates the majority of research [4]. As such, this highlights the need for an inclusive look into cybersecurity that captures the multidimensionality and interdisciplinary nature of the field that is now emerging.

As a first step towards improving our understanding of these human factors, we conducted a systematic review of literature with the objective of establishing the baseline of current knowledge in information sciences and to identify the current gaps in the literature. Our review examines 27 key studies across different peer-reviewed publications from the past decade (2009-2019), which have focused on the human factors that affect cybersecurity. These studies were selected from a broad spectrum of high-quality publications, to ensure that the human factors could be defined from an interdisciplinary perspective. Analysis of these studies identified three significant gaps: (1) lack of consolidation of attributes of human factors in cybersecurity; (2) limited qualitative studies despite the subjective and complex nature of the subject matter; and (3) a lack of interdisciplinary research to address the complexity and multi-dimensional nature of human behaviour.

The results from our literature review analysis are salient and have informed our definitions of human factors in cybersecurity for upcoming projects that are scheduled in the next twelve months.

The first project is a qualitative research project based on focus group data collected as part of national cybersecurity reviews in the Pacific region. The aim of this study is to identify human factors that influence an individual's perception and behaviour towards a nation's cybersecurity strategy.

The second project is an exploratory ethnographic study involving experts from archival, information and computer sciences. The aim of this project is to improve our understanding of how individual perceptions of safety in digital environments influences the work they do.

The third project is examining the national culture dimensions that impact cybersecurity maturity levels of a country. We aim to explore how national culture factors (based on Hofstede's Cultural Dimensions) affect the day-to-day activities pertaining to cybersecurity which in turn may impact a countries overall cybersecurity maturity / capacity level.

The structure of this paper is as follows. The following section explains the literature search methodology used to

identify the key studies on human factors and cybersecurity. Then, we present our findings and analyse the results based on the categorisation of core themes identified in the literature. Next, we discuss the three main knowledge gaps identified through this study, and how these may be addressed. In the final section of this paper, we outline the contributions of this study to positioning human factors in relation to cybersecurity. We point out limitations of the study while identifying future research directions for information sciences.

## II. Literature Search Methodology

To summarise, synthesise and integrate existing knowledge on the human factors in cybersecurity, we conducted a comprehensive literature review. Rigour is important when conducting research and therefore, in this section we describe how our literature review was conducted based on a number of steps as recommended by Cooper [5].

First, we conducted an extensive database search (i.e. IEEE Xplore; JSTOR; Science Direct, EBSCO) which was accessed via the University of Melbourne library discovery search (http://lib.unimelb.edu.au). Only studies that we had access to the full text (either digitally or physically) were considered. Second, due to the rapid pace that cybersecurity related studies have developed and evolved, we set the time frame for our search to the past decade (2009-2019). Next, only studies which explicitly defined cybersecurity or information security were included in the literature search to ensure that the boundary and scope of the study was fixed. Finally, only studies published in English were considered. In total, 539 studies were identified based on the following Search String:

***(cybersecurity OR "cyber security" OR "information security") AND ("human factors" OR "personal factors")***

From the results of the preliminary search, a four-step filtering process was carried out to ensure that only highly relevant studies were selected for further analysis.

**The first step** ensured that studies which were not peer-reviewed journal or conference papers (e.g. reports; magazines etc.) were removed. This also involved eliminating research-in-progress and follow-up studies. This step filtered out a total of 168 studies, resulting in a total of 371 studies remaining.

The **second step** involved eliminating studies which did not include the cybersecurity and human factor related keywords in the abstract of the paper. This was to ensure that papers that merely referenced or highlighted cybersecurity or personal factor issues were removed. This step eliminated another 255 papers, leaving us with 116 studies.

The **third step** removed another 54 studies because they were follow-up studies which included a significant part of the content from a prior study (e.g. Henshel, et al. [6], Oltramari, et al. [7] vs. Henshel, et al. [3]) or were considered to be focused on a cybersecurity related topic with minimal overlap with human factors despite adhering to the conditions set in the prior two steps (and vice versa). A total of 62 papers remained after this third filtering process.

Out of the remaining 62 studies, the **final step** was a manual process of carefully selecting paper based on the quality of the publication as well as their citation count numbers. This was necessary due to the size and scope of this particular paper, which was limited to 8 pages. The final papers that are selected represent a variety of disciplinary backgrounds that address our initial objective of exploring the notion of cybersecurity from an interdisciplinary perspective. Not only did this selection of articles represent well known computer science and information system journals and conferences, but also extended to operations; management; social sciences; human resources; psychology; and life sciences.

Based on these steps, a total of 27 studies were selected to be included in this particular literature review; we then created a study profile card for each article using the guidelines recommended by King and Torkzadeh [8]. As per the example provided in Table III, each study profile card presented a summary of the (a) research objective; (b) main findings; (c) main keywords; (d) research methodology; and (e) theoretical framework used.

The content from all 27 profile cards were then synthesised into Table IV (pg. 4). It must be noted that the focus area of a particular study fit into three broad categories: Personality (P); Demographics (D); and Culture (C). These categories were determined based on overarching focus areas that were identified through the literature review conducted.

TABLE III. Example Study Profile Card

| **[#] Author / Publication** | **Research Objective** |
|---|---|
| #11 Shropshire et al. (2015)<br><br>Computers & Security | To incorporate personality constructs (conscientiousness and agreeableness) into a conceptual model of security software use. |
| | **Summary of Findings** |
| | 1. Findings suggest that computer users have perceptions of security software which differ from perceptions of other information technologies, and that the attitudes included in the technology adoption model do not fully reflect user motivation to adopt security software.<br>2. The majority of the sample population indicated an intention to adopt the security measure, but less than a quarter actually followed through on their intentions.<br>3. Moderating effect of personality greatly increases the amount of variance explained in actual use. |
| **Keywords:** Attitudes; Personality traits; Information security behaviour; **Research Methodology:** Survey (n=196)<br>**Theoretical Framework(s):** Technology Acceptance Model | |

These three factors are investigated in further detail as per Section III which follows.

## III. Literature Analysis and Findings

Below, we present the analysis and findings of our literature review based on the summary outlined as per Table IV. The specific studies that are referenced in the subsections below are indicated by the numerical order specified and represented by a #.

TABLE IV. SUMMARY OF HUMAN FACTORS IN CYBERSECURITY

| # | Author(s) / Year | Publication | Discipline | Focus Area | | | Theoretical Framework | Methodology |
|---|---|---|---|---|---|---|---|---|
| | | | | P | D | C | | |
| 1 | Myyry et al. (2009) | European Journal of Information Systems | Information Systems | X | | | Motivational Types of Values; Cognitive Moral Development | Questionnaire (n=132) |
| 2 | Da Veiga and Eloff (2010) | Computers & Security | IT Security | | | X | Organisational Culture | Survey (n=1085) |
| 3 | Sheng, et al. (2010) | CHI 2010 | Human-Computer Interaction | | X | | Phishing Susceptibility | Roleplay Survey (n=1001) |
| 4 | Luo, et al. (2011) | Information Resources Management | Information Systems | X | | | Diffusion of Responsibility; Chance for ingratiation; | Conceptual |
| 5 | Sun et al. (2011) | Industrial Management & Data Systems | Operations Management | X | | | Information Security Readiness; Technology Acceptance Model | Experimental (n=109) |
| 6 | Uffen, et al. (2012) | IS Security and Privacy | IT Security | X | | | Planned Behaviour | Survey (n=174) |
| 7 | Metalidou, et al. (2014) | Social and Behavioral Sciences | Social Sciences | | | X | Information Security Awareness | Conceptual |
| 8 | Farooq, et al. (2015) | IEEE Trustcom | Computer Science | | X | | Information Security Awareness | Survey (n=614) |
| 9 | Pattinson, et al. (2015) | Human Aspects of Information Security, Privacy and Trust | Human-Computer Interaction | X | X | | N/A | Survey (n=500) |
| 10 | Proctor and Chen (2015) | Human factors | Human-Computer Interaction | X | | | Risk perception | Conceptual |
| 11 | Shropshire, et al. (2015) | Computers & Security | IT Security | X | | | Technology Acceptance Model | Survey (n=196) |
| 12 | Evans, et al. (2016) | Security and Communication Networks | Network Security | X | | | Assurance Methods | Literature Review |
| 13 | Henshel, et al. (2016) | Advances in Human Factors in Cybersecurity | IT Security | | | X | Hofstede's Cultural dimensions | Conceptual |
| 14 | Klimoski (2016) | People and Strategy | Human Resources | | X | | People and Strategy | Survey (n=113) |
| 15 | Neupane et al. (2016) | IEEE Transactions of Information Forensics and Security | IT Security | X | | | Phishing Detection | Neuroimaging (n=25) |
| 16 | Öğütçü, et al. (2016) | Computers & Security | IT Security | X | X | | Information Security Awareness | Survey (n=881) |
| 17 | Burns et al. (2017) | Computers in Human Behaviour | Psychology | X | X | | Psychological Capital; Protection Motivation | Survey (n=377) |
| 18 | Anwar, et al. (2017) | Computers in Human Behaviour | Psychology | | X | | Cybersecurity Behaviour Model | Survey (n=579) |
| 19 | Hadlington (2017) | Heliyon | Life Science | X | X | | Abbreviated impulsiveness; Online Cognition; | Survey (n=515) |
| 20 | Ki-Aries and Faily (2017) | Computers & Security | IT Security | X | | | Personas | Case Study |
| 21 | McCormac, et al. (2017) | Computers in Human Behaviour | Psychology | X | X | | Information Security Awareness; | Survey (n=505) |
| 22 | Menard et al. (2017) | Journal of Management Information Systems | Information Systems | X | | | Protection Motivation; Self Determination | Survey (n=547) |
| 23 | Dawson and Thomson (2018) | Frontiers in Psychology | Psychology | X | | X | Cybersecurity Workforce; Schwartz Values | Literature Review |
| 24 | Lau, et al. (2018) | Human Factors and Ergonomics Society | Human-Computer Interaction | | X | | N/A | Expert Panel (n=6) |
| 25 | Sawyer and Hancock (2018) | Human Factors | Human-Computer Interaction | X | | | Prevalence Effect | Email Testbed (n=33) |
| 26 | Jones, et al. (2019) | CHI 2019 | Human-Computer Interaction | | X | | Text analysis | Survey (n=503) |
| 27 | Li, et al. (2019) | International Journal of Information Systems | Information Systems | X | X | | Protection Management; | Survey (n=579) |

***P = Personality; D = Demographics; C = Culture;***

### A. Personality

Personality has long been used to explain an individual's cognitive process, attitudes and behavioural outcomes [14, 19]. It is considered an important part of human factors as an individual's personality type remains relatively stable throughout a person's lifetime [34]. Based on the studies examined in Table II, 18 out of the 25 studies highlighted the fact that inherent personality traits had a significant impact on the behaviours and attitudes demonstrated by an individual towards cybersecurity (Table IV).

TABLE V. PERSONALITY AND CYBERSECURITY

| Study | Key Findings |
|---|---|
| # 1, 5, 6, 11, 16, 17, 19, 20, 25, 27 | An individual's perception, attitudes and behaviours towards information / cyber security are influenced by their personality. |
| # 4, 9, 10, 12, 15, 19 | Inherent personality traits affect the overall level of cybersecurity risk an individual faces. |
| # 19, 20, 21, 27 | Personality traits determine the level of compliance towards cybersecurity related policies and training. |
| # 23, 27 | Specific cybersecurity roles and skills may suit workers with certain personality and social traits. |

In ten of the studies, the focus was on how individual perceptions, attitudes and behaviour towards cybersecurity were determined based on an individual's personality type. For instance, Uffen, et al. [8] through a survey of 174 Information Security (IS) executives found evidence to suggest that multiple facets of an IS executive's personality had an impact on his/her attitude towards selecting certain IS management activities for their organisation. Their study suggests that certain personality traits such as conscientiousness and openness were positively associated with attitude towards technical, compliance and strategic aspects of information security management. These studies suggest that there is a strong connection between the behavioural patterns demonstrated towards information and cyber security related management, and the cognitive processes driven by specific personality types.

In six studies, the focus was on whether individuals with a certain type of personality trait were more likely to be susceptible to cybersecurity related risk. For instance, Pattinson, et al. [17], investigated the five-factor personality model through a survey of 500 employees which found that employees who were more agreeable; less impulsive; more conscientious and more open were **less** likely to be involved in cybersecurity related attacks. These studies highlight the fact that inherent personality traits are influential in how an individual may demonstrate safe or risky cybersecurity attitudes and behaviours.

In four of the studies, the emphasis was on investigating the connection between an individual's personality and the degree of awareness they had in regard to cybersecurity related policies and training. For instance, Hadlington [25] in their study found that certain personality traits such as impulsivity (attentional and motor) led to a decrease in compliance - towards cybersecurity training and policies. Their study goes on to suggest that an improved understanding of individual differences pertaining to good governance of cybersecurity related practices are needed to ensure more effective training and awareness mechanisms.

Two of the studies focused on how individuals with certain personality types may be more suitable for certain cybersecurity related roles and tasks. In a study by Dawson and Thomson [29], they argued that social fit in a highly complex cybersecurity workforce was critical to ensure alignment between the cybersecurity workforce, and the individuals entering and training to work within it. They recommended that on top of the technical skillset, the next generation of cybersecurity experts also needed to be measured on social and cognitive measures to accurately gauge performance levels.

### B. Demographic Attributes

Demography encompasses the size, structure and distribution of a population [35]. The importance of demographic features lies in its ability to help society better prepare and deal with specific issues such as the ever-increasing risk posed by cybersecurity and hacking incidents. Based on the literature review conducted, 10 out of the 27 studies reviewed had investigated the connection between an individual's gender, age and level of education with cybersecurity as per Table IV below.

TABLE IV. DEMOGRAPHICS AND CYBERSECURITY

| Factor | Study | Key Findings |
|---|---|---|
| Gender | # 3, 18 | Gender could be associated with cybersecurity related risks and incidents. |
| | # 8 | Males had better knowledge and awareness over cybersecurity related matters. |
| | # 21 | Females had better knowledge and awareness over cybersecurity related matters. |
| Age | # 3, 8, 9, 16 | The younger the participant, the higher the risk factor associated with cybersecurity. |
| | # 8, 21 | Increase in age resulted in improved knowledge and awareness in relation to cybersecurity. |
| | # 26 | There are age-related differences (i.e. language) in relation to cybersecurity. |
| Education / Training | # 3, 16 | Cybersecurity related training reduces and/or mitigates risk. |
| | # 10, 18, 26 | Different individuals and groups require specific cybersecurity training and interventions. |
| Experience | # 3, 14, 16, 24, 27 | Prior experience positively affects awareness over cybersecurity related issues. |

#### 1) Gender

In four of the studies, the **gender** of the study participant was the focus of research. Prior research have suggested that the difference in gender not only caused different perceptions around technology, but also how it was adopted and used as well [24].

In two of the studies, women were believed to be at more risk to cybersecurity related attacks and risks. For instance, Sheng, et al. [11] found that women clicked on links in phishing emails more and also gave out information to these websites more than men. However, there were conflicting results about which gender had greater awareness and knowledge of cybersecurity. Farooq, et al. [16] concluded that males were considered to be more knowledgeable, whereas in the study by McCormac, et al. [27], there was a small significant difference found in favour of females. This was despite both studies using the same theoretical lens (Information Security Awareness) and a statistically significant sample size for their surveys (n=614 vs. n=505).

*2) Age*

In four of the studies, the focus was on the **age** of the participant. Age was considered to be an important factor when differentiating between individuals due to the fact that people at different life stages bring distinct and diverse social, organisational and environmental contexts and challenges [32].

Results from all four studies suggest that the youngest groups of individuals (ages 18-25) had more risk factors; less awareness and knowledge of cybersecurity related matters. The rationale was that younger people were more at risk due to their frequency of internet usage (especially social networks and media) and the fact that younger people are inclined to take more risk.

In two of the studies, an increase in age was attributed towards improved knowledge and awareness in relation to cybersecurity. For instance, McCormac, et al. [27] through their survey of 505 individuals found that older adults had higher Information Security Awareness (ISA) scores when compared to younger adults. They also found that this relationship was fairly linear; as individuals got older, their ISA scores increased.

In a study by Jones, et al. [32], they found that the concept and language used to describe cybersecurity differed between age-groups. They highlight that these differences occur due to the different cybersecurity risks that each age group are likely to face. For instance, those in adolescence may be more likely to associate social media and cyber bullying factors as primary risks, whereas those at a working age may be more concerned about financial transactions etc.

*3) Education and Training*

Five out of the 27 studies focused on the connection between the level of **education and training** received by an individual and its influence on cybersecurity. The premises for these studies was that the level of education and training received by an individual is known to significant boost situational awareness and general ability [22].

In two of these studies, higher levels of education and with less riskier actions and higher levels of compliance with cybersecurity related activities. For instance, Öğütçü, et al. [22] found that employees who received education and training in regard to cyber / information security had improved awareness of potential threats and risks, which led to less risky behaviour to be undertaken by individuals.

In the other three studies, it highlighted the importance of ensuring that cybersecurity training and intervention programs were tailored made to suit different individuals and groups. Proctor and Chen [18] for example argued that humans all have difference processes of assimilating information and making decisions towards cybersecurity practices, and therefore requires systematic training based on a case-by-case. Anwar, et al. [24] also highlighted the need for gender-specific cybersecurity training as well due to the gap between males and females when it comes to security self-efficacy.

*4) Experience*

Five of the studies focused on how prior cybersecurity **experience** affected the overall awareness levels of individuals. Experience is considered to be an important attribute as it sculpts how an individual reacts to a particular artefact through the perception and beliefs that have been formulated through it [36].

All four studies suggest that prior experience has a positive impact on the overall awareness and ability to deal with cybersecurity related risks. Li, et al. [33] found that those with higher levels of 'action experience' were able to cope with cybercrime related activities than those who did not have similar experiences. This is because experience becomes a source of information, which in turn made them better in practicing cybersecurity related activities and measures. Klimoski [20] also suggests that prior experience is a critical component of a CISO's reputation and credibility due to the same reasons as per outlined above.

*C. Cultural Context*

Four of the studies examined focused on cultural factors and their impact on cybersecurity. As a means of addressing the complexities and difficulties in understanding the notion of culture, scholars have proposed that the concept should be broken up into more manageable categories and parts [37, 38].

The research into human factors in cybersecurity that we found in the literature has focused on two distinct categories of culture. All two of these distinctly different 'cultural' levels were found to be influential. Table V provides the summary findings.

TABLE V. CULTURAL FACTORS AND CYBERSECURITY

| Culture Type | Study | Key Findings |
|---|---|---|
| National | # 13 | Assessment of cybersecurity risk may differ based on national cultural dimensions. |
| Organizational | # 2, 7 | Organisations need to cultivate and manage a cybersecurity culture which reduces unintentional harm done by individuals. |
| | # 23 | Cybersecurity personnel requirements differ between organisational culture. |

*1) National Culture*

National Culture refers to a culture specific to a group of people within a specific geographical location [39]. Henshel, et al. [3] in their study argued that the national culture of a particular individual affected their efficacy, performance and contribution to cybersecurity risk. Their study proposed that the effects of culture on individuals pertaining to

cybersecurity can be used to predict cybersecurity threats and attacks, and also customise cyber defences.

*2) Organisational Culture*

Organisational Culture refers to culture that is associated with a particular business and/or work organisation [40]. There were three studies identified through the literature review which suggests how cybersecurity is perceived differently between organisations, and the measurements are drastically different due to this.

In the study by Metalidou, et al. [15], they suggest that organisations need to cultivate and maintain a culture where positive security functions are meaningful and easy to follow whilst being as least intrusive to the end user as possible. By creating such an organisational culture, they suggest that the unintended harm caused by employees by falling victim to cybersecurity attacks such as malware and social engineering attacks can be mitigated.

Dawson and Thomson [29] found that one of the greatest challenges that organisations will face in relation to cybersecurity is ensuring that they hire cybersecurity experts that fit within their organisational culture. For instance, police will need to hire individuals with cyber capabilities that fit within the organisational culture of law enforcement agencies, whereas hospitals may need to hire individuals who are able to navigate the complexities surrounding health care networks and can interact with non-technical medical professionals.

## IV. Discussion

In this study, a systematic review and analysis of the human factors within cybersecurity has been presented. In almost all of the studies examined, researchers have highlighted the importance of human factors in relation to cybersecurity topics and activities. However, our analysis of the literature also highlights three significant gaps, which we identify below and provide recommendations as to how these gaps might be addressed in future research.

### *A. Consolidating the Human Factors in Cybersecurity*

Each study in our review focused on a specific attribute, with only seven out of the 27 studies exploring a combination of factors. The literature reported differences in personality type, demographic attributes and cultural context were all influential in motivating differences in behaviours. Differentiation is important, but at the same time human factors cannot be fully understood in isolation.

Therefore, future studies may be able to gain invaluable insight by taking into consideration all of the human factors identified in this study, as opposed to investigating each factor independently. For instance, one of our proposed studies will aim to investigate how an individual's personality, demographic attributes and cultural context impact how they devise national cybersecurity related policies and create certain information security cultures within their organisations.

### *B. Towards an Integrated Research Approach to Human Factors and Cybersecurity*

The literature review also suggests that there is considerable fragmentation of the disciplinary background which therefore leads to a plethora of different theories used to shed light on human factors in cybersecurity. For instance, a quick analysis of the theories used identified:

- Behavioural based theories (n=9)
- Information Security based theories (n=6)
- Information Systems based theories (n=2)
- Cultural based theories (n=2)
- Psychology Based Theories (n=2)
- Other (n=7)

While this research highlights the different angles that research on human factors in cybersecurity that needs to be covered, it also results in difficulties in creating strategic and evidence-based approaches due to the difficulties in comparing and contrasting results from studies with different disciplinary backgrounds. An interdisciplinary approach to cybersecurity has the potential to provide a more holistic view that would consider the complexity of personal characteristics and cultural contexts.

### *C. The Need for Additional In-Depth Qualitative Studies*

Despite the subjective and complex nature of the themes identified in this literature review, there were only two qualitative studies out of the 27 studies investigated. The first qualitative study was a case study conducted by Ki-Aries and Faily [26] to identify the human factors and security risks pertaining to businesses through the use of personas, and how awareness activities can be designed and developed to combat these risks. In Lau, et al. [30], they facilitated a panel interview with experts from different industry sectors (Healthcare; Computer technology; Automotive; Higher education) to characterise how human factors related to security differ from industry to industry.

One approach towards improving behaviours and culture is with the application of on-going awareness activities. This paper presents an approach for identifying security related human factors by incorporating personas into information security awareness design and implementation. The personas, which are grounded in empirical data, offer a useful method for identifying audience needs and security risks, enabling a tailored approach to business-specific awareness activities. As a means for integrating personas,

- Surveys (n=16)
- Conceptual studies (n=4)
- Experimental (n=3)
- Literature Review (n=2)
- Other (n=2)

Although there are clear benefits of having quantifiable evidence which backs up the conceptual framework and/or hypotheses, human factors in cybersecurity is still a relatively under-explored topic, and therefore additional qualitative studies carried out in different contexts will help enrich our current understanding of this topic.

## V. Conclusion

This study demonstrates how human factors, in information sciences and associated fields or disciplines, are being increasingly reported in relation to cybersecurity. While this study is limited due to the sample size of the literature reviewed, it is focused on quality papers which foreground innovations in research and thinking within the discipline.

Future studies will endeavour to add to the current list of studies examined to ensure that a more comprehensive sample set of studies that represent human factors and cybersecurity is presented.

Furthermore, this study did not differentiate the human factors based on the various roles that humans can take on in relation to cybersecurity (e.g. attacker; defender; user etc.) as the purpose of this paper was to first establish a baseline on what human factors entailed with regard to cybersecurity.

These carefully selected papers report the importance of three key categories of human factors: personality, demographic attributes and cultural context. All three categories influence how people, their behaviour and attitudes are fundamental in both ameliorating risks and generating opportunities in creating cyber secure systems.

While human factors include demographics, they are also described in relation to nuanced cultural contexts and highly subjective states of being and behaviour. The study of human culture and behaviour is deeply embedded in a range of other disciplinary contexts including psychology, anthropology, and social sciences.

There is emergent literature within these human sciences which also address concerns regarding the human relationship to technology and cyber space in diverse societal contexts. As such, this study recommends that research conducted within other disciplinary contexts around human factors and cybersecurity to be considered in future studies. Moving forward, the results from this study may be used to further explore the consolidated human factors their impact on cyber security. This in turn will give us a more accurate picture of the human factors that are currently impacting the cybersecurity landscape in different areas of culture and society.

## REFERENCES


[1] 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.

[2] D. Palmer. "Cybercrime drains $600 billion a year from the global economy, says report." https://www.zdnet.com/article/cybercrime-drains-600-billion-a-year-from-the-global-economy-says-report/ (accessed 2019-02-19 11:06:23, 2019).

[3] D. Henshel, C. Sample, M. Cains, and B. Hoffman, "Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers," in *Advances in Intelligent Systems and Computing*, Cham, 2016: Springer International Publishing, in Advances in Human Factors in Cybersecurity, pp. 123-137.

[4] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review,* vol. 4, no. 10, 2014.

[5] H. M. Cooper, *Synthesizing research: A guide for literature reviews*. Sage, 1998.

[6] D. Henshel, M. Cains, B. Hoffman, and T. Kelley, "Trust as a human factor in holistic cyber security risk assessment," *Procedia Manufacturing,* vol. 3, pp. 1117-1124, 2015.

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

[8] W. R. King and G. Torkzadeh, "Information systems offshoring: Research status and issues," *MIS quarterly,* vol. 32, no. 2, pp. 205-225, 2008.

[9] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance, "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems,* vol. 18, no. 2, pp. 126-139, 2009.

[10] A. Da Veiga and J. H. Eloff, "A framework and assessment instrument for information security culture," *Computers & Security,* vol. 29, no. 2, pp. 196-207, 2010.

[11] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "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: ACM, pp. 373-382.

[12] X. R. Luo, R. Brody, A. Seazzu, and S. Burd, "Social Engineering," *Information Resources Management Journal,* vol. 24, no. 3, pp. 1-8, 2011.

[13] J. Sun, P. Ahluwalia, and K. S. Koong, "The more secure the better? A study of information security readiness," *Industrial Management & Data Systems,* vol. 111, no. 4, pp. 570-588, 2011.

[14] J. Uffen, N. Guhr, and M. H. Breitner, "Personality traits and information security management: An empirical study of information security executives," presented at the International Conference on Information Systems, 2012.

[15] 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.

[16] 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: IEEE, pp. 352-359.

[17] 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: Springer, pp. 231-241.

[18] R. W. Proctor and J. Chen, "The Role of Human Factors/Ergonomics in the Science of Security:Decision Making and Action Selection in Cyberspace," *Human Factors,* vol. 57, no. 5, pp. 721-727, 2015, doi: 10.1177/0018720815585906.

[19] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Computers & Security,* vol. 49, pp. 177-191, 2015.

[20] R. Klimoski, "Critical success factors for cybersecurity leaders: Not just technical competence," *People and Strategy,* vol. 39, no. 1, p. 14, 2016.

[21] A. Neupane, N. Saxena, J. O. Maximo, and R. Kana, "Neural markers of cybersecurity: an fMRI study of phishing and malware warnings," *IEEE Transactions on information forensics and security,* vol. 11, no. 9, pp. 1970-1983, 2016.

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

[23] A. Burns, C. Posey, T. L. Roberts, and P. B. Lowry, "Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals," *Computers in Human Behavior,* vol. 68, pp. 190-209, 2017.

[24] 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.

[25] 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.

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

[27] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Computers in Human Behavior,* vol. 69, pp. 151-156, 2017.

[28] P. Menard, G. J. Bott, and R. E. Crossler, "User motivations in protecting information security: Protection motivation theory versus self-determination theory," *Journal of Management Information Systems,* vol. 34, no. 4, pp. 1203-1230, 2017.

[29] J. Dawson and R. Thomson, "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance," *Frontiers in psychology,* vol. 9, 2018.

[30] N. Lau, R. Pastel, M. R. Chapman, J. Minarik, J. Petit, and D. Hale, "Human Factors in Cybersecurity – Perspectives from Industries," *Proceedings of the Human Factors and Ergonomics Society*

*Annual Meeting,* vol. 62, no. 1, pp. 139-143, 2018, doi: 10.1177/1541931218621032.

[31] B. D. Sawyer and P. A. Hancock, "Hacking the Human: The Prevalence Paradox in Cybersecurity," *Human factors,* vol. 60, no. 5, pp. 597-609, 2018.

[32] S. Jones, E. Collins, A. Levordashka, K. Muir, and A. Joinson, "What is' Cyber Security'?: Differential Language of CyberSecurity Across the Lifespan," in *CHI 2019-Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019: Association for Computing Machinery.

[33] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *International Journal of Information Management,* vol. 45, pp. 13-24, 2019.

[34] M. McBride, L. Carter, and M. Warkentin, "Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies," *RTI International-Institute for Homeland Security Solutions,* vol. 5, p. 1, 2012.

[35] R. L. Baskerville and M. D. Myers, "Design ethnography in information systems," *Information Systems Journal,* vol. 25, no. 1, pp. 23-46, 2015.

[36] Y. Chen, K. Ramamurthy, and K.-W. Wen, "Impacts of comprehensive information security programs on information security culture," *Journal of Computer Information Systems,* vol. 55, no. 3, pp. 11-19, 2015.

[37] R. Gregory, M. Prifling, and R. Beck, "The role of cultural intelligence for the emergence of negotiated culture in IT offshore outsourcing projects," *Information Technology & People,* vol. 22, no. 3, pp. 223-241, 2009.

[38] D. Avison and P. Banks, "Cross-cultural (mis) communication in IS offshoring: understanding through conversation analysis," *Journal of Information Technology,* vol. 23, no. 4, pp. 249-268, 2008.

[39] N. Schmidt, B. Zöller, and C. Rosenkranz, "The Clash of Cultures in Information Technology Outsourcing Relationships: An Institutional Logics Perspective," in *International Workshop on Global Sourcing of Information Technology and Business Processes*, 2016: Springer, pp. 97-117.

[40] T. Moon, "Organizational cultural intelligence: Dynamic capability perspective," *Group & Organization Management,* vol. 35, no. 4, pp. 456-493, 2010.