The Human Factors and Cybersecurity Policy

Alya A. Qashqari Asmaa M. Munshi Haifaa A. Alturkstani Hadeel T. Ghwati Dalia H. Alhebshi
aqashqari0001.stu@uj.edu.sa ammunshi@uj.edu.sa halturkstani.stu@uj.edu.sa
hghawati.stu@uj.edu.sa dalhbshi.stu@uj.edu.sa
Department of Cybersecurity Collage of Computer Science and Engineering
University of Jeddah, Saudi Arabia

Abstract
Computer security is not limited to technology and systems; it also includes the humans and processes that use and depend on it. Even with strong computer security policies, humans are the weakest link in information security, even if people are aware of the policies, they may not act accordingly, leading to error. This paper presents studies that illustrate how human factors affect the cybersecurity, and explains the demographic features, such as gender, age, personality, and cultural background that are key determinants of an individual's attitude and behavior toward cybersecurity. Based on this review the paper discusses the concept of "insider threat" and how its potential impact on cybersecurity policies. its then proposes recommended solutions to handle insider threats and provides cybersecurity awareness and explains the importance of ensuring training and intervention programs on cybersecurity.

Keywords
cybersecurity awareness, human behavior, insider threat, policy.

1. Introduction

Human behavior is defined as individual acts that differ from person to person; it is unlikely for common behavior to be predictable. Human behavior can threaten security and destroy all an organizau8tion's protection systems, devices, and infrastructure. It is hard to understand how individuals think, which could reduce or avoid negative behaviors. To avoid bad behavior, internal security controls, such as policies and procedures, need to be identified. Policies and procedures for safety and operational controls are standard countermeasures to protect organizational assets from attacks and vulnerabilities, but without accounting for human behavior, the design and execution of countermeasures could be ineffective[1]. This paper is organized as follows. First, it illustrates how human factors affect cybersecurity. Second, it provides a brief background and summary of findings in related work. Then, it presents the conceptual overview of the research, exploring the malicious insider threat. Finally, it recommends the developed solution based on the review affect cybersecurity. Second, it provides a brief background and summary of findings in related work. Then, it presents the conceptual overview of the research, exploring the malicious insider threat. Finally, it recommends the developed solution based on the review.

Understanding Human Factors in Cybersecurity

Studying human behavior toward cybersecurity is an important topic for organizations, given its scarcity. Since it has become obvious that the human aspects of cybersecurity pose as many hazards as the technological aspects, studies have started to turn toward understanding the various human factors that impact cybersecurity. Recent studies have established demographic attributes, such as gender, age, individual personalities, and cultural contexts, as key determinants of an individual's attitude and behavior toward cybersecurity [2].

Personality: Studies prove that inherent personality characteristics have a major effect on an individual's behaviors and attitudes toward cybersecurity.

- People's perceptions, attitudes, and actions toward information cybersecurity are affected by their personalities.

A study was conducted on Information Security (IS) executives; it found evidence that several aspects of IS executives' personalities affected their attitudes toward choosing certain IS management practices for their organizations. The study indicates that attitudes toward technological, regulatory, and strategic aspects of IS management were positively correlated with certain personality traits, such as "conscientiousness and openness" [2].

- Cybersecurity risk level is affected by inherent personality traits.
- Personality characteristics define the level of compliance regarding cybersecurity policies and training.
- Specific roles and skills in cybersecurity can match staff with certain personal and social characteristics [2].

Demographic Attributes: Demography "concerns the size, structure, and distribution of a population" [2]. The importance of demographic features lies in their ability to help society better plan for and address specific problems, such as the ever-increasing risk presented by cybersecurity and hacking incidents. Studies investigate the connection between an individual's age, gender, experience, and education level with cybersecurity, as shown below.

Gender: Female considered to be at higher risk of cybersecurity-related attacks and threats. For example,

Manuscript received April 5, 2020
Manuscript revised April 20, 2020

female clicked more on links in phishing emails and provided more data than male to those websites.

Age: Since humans carry distinct and complex social, organizational, and environmental backgrounds and challenges depending on their life stages, age is a significant factor when differentiating between individuals. The study shows younger people (ages 18–25) were more at risk because of their level of internet use (especially social networks and media) and because they have less knowledge and awareness of cybersecurity-related issues.

Education level: Studies focus on the connection between an individual's education and training level and cybersecurity. The rationale for these studies is that an individual's level of education and training is known to significantly improve situational awareness and overall skills, resulting in higher education rates having less risky behavior and higher compliance with cybersecurity-related activities. For instance, employees who received cyber/information security education and training had greater knowledge of possible threats and risks, resulting in individuals who participate in fewer risky activities.

Experience: This study focuses on how previous cybersecurity experience impacts individuals' overall knowledge and awareness. The study suggests that previous experience has a positive effect on the general understanding and willingness to resolve threats associated with cybersecurity [2].

Cultural Context: The study focuses on two distinct categories of culture.

National Culture: This refers to a culture that is specific to a population group within a certain geographic place. Culture's impact on cybersecurity could be used to presume cybersecurity threats and attacks and adapt cyber defenses.

Organizational Culture: This refers to the culture related with a specific business or organization. Organizations need to develop a culture of practical, easy-to-follow positive security features while being as nonintrusive as possible to the end-user. By establishing such an organizational culture, they indicate that the unintentional harm done by staffs falling victim to cybersecurity threats, such as ransomware and threats on social engineering, can be mitigated [2].

2. Background

In cybersecurity, the study of human factors explores how humans interact with computers. Human conduct is usually unexpected, which is why human factors are considered a challenging problem. First, it is critical to control human security conduct to secure all systems. After enforcing a control mechanism on human conduct, computer security is guaranteed. To ensure compliance with these controls, it is important to consider security policies. In general, a security policy within an organization is a group of rules and laws that illustrate what is prohibited and what is permitted; they are different from one organization to another, according to the organization's requirements. For example, in 2016, a study on IS policies stated the phrase "security policy" is applied to assign scopes for organizations to save their properties and achieve their objectives. On the other hand, a 2013 study on policy framework, named A Policy Framework for Information Security, states that security policies are "generally high-level, technology-neutral, concern risks, set directions and procedures, and define penalties and countermeasures if the policy is transgressed, and must not be confused with implementation-specific information, which would be part of the security standards, procedures, and guidelines". These guidelines, standards, and procedures are intended to preserve the integrity, availability and confidentiality of data and, therefore, protect the organization [3].

Some IS researchers assume that one of the significant techniques for making IS efficient in an organization is constraining negative user conducts and raising positive user conducts. Different studies gauge human conduct in security policies; one of these studies is summarized in the following section [3].

In 2004, a study analyzed user security conducts on employees in the United States from various fields, including communication, health, government, and financial. The research examined the impact of user conduct upon security efficacy within an organization. This research ended with the security conduct elements, which are related to password choices and recurrence of passwords changes [4]. The research concentrated on asking users about a group of items that contained three items relating to password management conduct, such as recurrence of password changes; three points relating to password participating conduct, such as participating passwords with others in a group of work; and three points relating to organizational boost of security conduct, such as how an organization prepares training courses to support staff develop their awareness and knowledge of data security and computer [4].

The research showed 48.5% of users had not altered their passwords in the previous months, 23% users showed their passwords to other users within their workgroup in the organization, 7% shared passwords outside their workgroup, 4.1% shared passwords outside the organization, 62.5% of users were not using punctuation or numbers in their passwords, 27.9% of users noted their password in the previous six months to remember it, 34.9% of users worked without learning how monitor computer activity, 19.9% of users worked in an organization that does not require an reasonable use policy, and 35% of users never received security training. The researchers proposed that organizations must have a framework that includes a human reliability evaluation, a cybersecurity human-part

vulnerability scoring system, and statistical quality control [4].

Other studies are summarized in the following. In 2016, the Office of National Statistics evaluated that online fraud was costing firms an evaluated £193 bn. Also, the study mentioned that 5.8 million individual cybercrime cases occurred between 2015 and 2016; these cases were divided into fraudulent internet activities, such as email fraud and credit card fraud, and computer misuse – data misuse and unauthorized copying, hacking, viruses, etc. In 2015, the Business Crime Survey mentioned a 55% growth in reported internet fraud between 2014 and 2015. In the same study, the increase of insider threat – individuals' threat – in an organization was one of the main concerns raised [5].

A large amount of attention is provided to developing the present security structure to save organizations and businesses against the threat of cybercrime and fraud by providing legal security against different types of threats through developing network security in technical ways, such as intrusion detection and firewalls. However, these procedures presume that all threats to an organization's security come from an external attacker [5].

Some cybersecurity researchers have perceived that one of the greatest impediments to making effective IS strategies within organizations is the human factor; cybersecurity is affected by human conduct errors [5].

3. Insider Threat Indicators

The following section presents a brief overview of the research exploring the malicious insider threat and discusses the psychology behind the manipulative insider, focusing on a limited number of case studies that capture the inside threat. In contrast, organizations overlook the human factor; a factor that relies on technology for security is often falsely perceived as the immediate response to cybersecurity problems [5].

"Hadlington" defined an insider threat as a person who exploits or intends to exploit their authorized access to an organization's assets for unauthorized purposes. Several researchers have addressed a four-core indicator of human behavior likely to become an insider threat, listed below

1. Negative Life Experiences:

In this instance, the person expresses his anger at failures in his life through open flashes of anger directed at both peers and authority figures. The individual also has a low frustration threshold, which is often expressed directly through aggressive explosions [5].

2. Lack of Awareness:

This is related to a lack of general knowledge of attacks, as "Nobles" [6] presented. An example of a lack of awareness could be that users do not know how important it is to choose a strong password; therefore, they cannot secure themselves from credit card fraud and social engineering.

3. Lack of Conscientiousness

This involves people who disregard existing rules and practices. They disregard the tasks and responsibilities in the working environment and exhibit a lack of professionalism and a lack of judgment and concentration [5].

4. Manipulative:

These employees use persuasive techniques to get their way and create relationships that help cultivate their self-interest. They often take social roles that help fulfill their needs, such as being polite and in line with those in control [5].

5. Sense of Entitlement:

Insiders have a sense of entitlement, usually granted through special privileges or access rights they have been allowed to exercise in their duties [5].

There is a direct connection between the challenges faced by many organizations and the lack of IS awareness and training [7].

To reduce human insider threat, it requires a security awareness training and including psychologists' human factors experts to analyze and evaluate the behavior of end-users in cyber operations. If an organization has a comprehensive and efficient IS culture and users implement it, it makes a difference.

4. Finding and Recommended Solution

Insider threats in cybersecurity need to be managed and handled carefully. Presented here several solutions to handle insider threats.

1. The Big Five personality traits:

The first step to managing insider threats starts with employee recruitment. The paper Towards an Improved Understanding of Human Factors in Cybersecurity stated, "Personality is a Major Effect in an Individual Behavior" [2]. We recommend adding the Big Five personality traits test as a job requirement. The Big Five personality traits test is a psychology test to present the personality in five deferent domains – Openness to Experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism or OCEAN. This delivers a meaningful classification for studying individual behaviors and variances [8]

- Openness to Experience: This domain includes being Ambition (creativity, insistence, motivation, and impulsive) and Sociability (friendly, attention-seeker, and communicative) [8].
- Conscientiousness: This domain includes being cautious, detailed, responsible, organized, planful, thorough, achievement-oriented, and determined [8].
- Extraversion: This domain includes being creative,

educated, curious, unique, open-minded, smart, and artistically sensitive
- Agreeableness: This domain includes being polite, flexible, trusting, easy-going, supportive, merciful, soft-hearted, and accepting [8].
- Neuroticism: This domain includes being nervous, miserable, angry, ashamed, sensitive, anxious, and insecure [8].

2. Employee satisfaction:

The second step for managing insider threats is ensuring employees are satisfied. Organizations will benefit from satisfied employees. They will benefit from the high performance that leads to a productive organization, the professionalism that leads to a better work environment, skill improvements that lead to self-satisfaction, and, most importantly, it will gain employees' trust and loyalty, which will lead to employees following the organizational policies and standards, including IS policies and standards, protecting the organization from any possible threats [9]. Also, employee satisfaction leads to positive energy, which leads to a positive individual [8].
Employee satisfaction can be met in several ways: [10]

- **Employee orientation**: ensure all employees have a clear understanding of organization policies and standards, plus their rights and responsibilities.
- **Positive work environments**: ensure to provide a positive and productive work environment to all employees in the organization
- **Competitive benefits**: provide employees with benefits like health insurers, paid holidays, flexible schedule and annual salary raise
- **Recognition and rewards**: provide an employee of the month program or employee of the year program to motivate and appreciate employees
- **Job satisfaction tracking**: provide surveys to learn how employees feel about different things in the organization and tackle all problems immediately
- Workforce engagement: ensure to involve all employees in the organization by taking their opinion and recommendation under consideration
- **Commuting stress reduction**: in case of employee emergency provide the option of working from home

3. Cybersecurity awareness and training:

- The traditional methods of providing cybersecurity awareness and training, including brochures, posters, courses, and lectures, have failed to reach their goal [11].
- Stengel et al. (2016) proposed a new method to provide cybersecurity awareness via mobile applications. To benefit from the rapid development of mobile applications, a new simulation mobile game was developed to provide cybersecurity awareness and training for end-users. However, more professional cybersecurity awareness mobile gaming applications have not yet been developed [12].
- Cybersecurity awareness was proposed by escape rooms. The concept of an escape room game is a group of people trying to exit the room by solving puzzles and getting clues to find the master key to the room. This concept can be applied to spread cybersecurity awareness. The effect of experiencing security threats has a greater impact than reading about it or listening to a talk about it [13].
- **Table 1** present the relationship between the recommended solution and the human factor threats.

Table 1: the relationship between recommended solution and the human factor threats

Recommended Solution	Human Factor Threats				
	Negative Life Experiences	Lack of Awareness	Lacks Conscientiousness	Manipulative	Sense of Entitlement
Big Five Personality Traits Test	●			●	●
Employee Satisfaction			●		●
Cybersecurity Awareness and Training		●	●		●

5. Conclusion

This paper discussed the threats deriving from the human factor in the cybersecurity world, which is affected by an individual's personality, background, gender, age, and experience. It also discussed how to address them, starting with the Big Five personality traits test to know an individual's personality and behavior, improving the employee's relationship with the organization and satisfying him to ensure his trust and loyalty to the organization. Finally, it discussed spreading cybersecurity awareness in new and innovative ways like mobile applications or escape room games. Future work could be achieved by presenting new ideas to spread cybersecurity awareness; as it has been mentioned in the paper, the traditional methods are lacking and ineffective.

References

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

[2] J. Jeong, J. Mihelcic, G. Oliver and C. Rudolph, "Towards an Improved Understanding of Human Factors in Cybersecurity," in 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles,CA, 2019.

[3] Alissa, K.A., Alshehri, H.A., Dahdouh, S.A., Alsubaie, B.M., Alghamdi, A.M., Alharby, A. and Almubairik, N.A., "An Instrument to Measure Human Behavior Toward Cyber Security Policies," 21st Saudi Computer Society National Computer Conference (NCC), no. IEEE, pp. 1-6, 2018.

[4] K. R. Stam, J. M. Stanton, P. Mastrangelo and J. Jolton, "Analysis of end user security behaviors," Computers & security.4(2), pp. 124-133, 2005.

[5] L. Hadlington, "The "human factor" in cybersecurity: Exploring the accidental insider. In Psychological and Behavioral Examinations in Cyber Security," IGI Global, pp. (46-63), 2018.

[6] C. Nobles, "Botching human factors in cybersecurity in business organizations," HOLISTICA–Journal of Business and Public Administration, pp. 71-88, 2018.

[7] Alotaibi, M., Furnell, S. and Clarke, N., "Information security policies: a review of challenges and influencing factors.," 2016.

[8] M. R. BARRICK and M. K. MOUNT, "The big five personality dimensions and job performance: a meta-analysis," Personnel psychology, vol. 44, no. 1, pp. 1-26, 1999.

[9] A. S. Bin, "The relationship between job satisfaction, job performance and employee engagement: An explorative study. Issues in Business Management and Economics," Issues in Business Management and Economics, vol. 4, no. 1, pp. 1-8, 2015.

[10] K. Faber and D. McKonkie, "Innovation Management," 2018. [Online]. Available: https://innovationmanagement.se/2018/06/08/simple-ways-to-increase-employee-satisfaction/. [Accessed 28 March 2020].

[11] K. Korpela, "Improving cyber security awareness and training programs with data analytics," Information Security Journal: A Global Perspective, vol. 24, no. 1-3, pp. 72-77, 2015.

[12] I. Stengel, M. Papadaki, S. Furnell and F. Alotaibi, "A Review of Using Gaming Technology for Cyber-Security Awareness," International Journal for Information Security Research (IJISR), vol. 6, no. 2, pp. 660-666, 2016.

[13] E. D. Oroszi, "Security awareness escape room a possible new method in improving security awareness of users," in 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019.