Cultural Influences on Information Security

Henry Collier[1], Charlotte Morton[2], Dalal Alharthi[3] and Jan Kleiner[4]
[1]Norwich University, Northfield, VT, USA
[2]University of Chester, Chester, UK
[3]The University of Arizona, Tucson, AZ, USA
[4]Masaryk University, Czech Republic

hcollier@norwich.edu
0818685@chester.ac.uk
dalharthi@arizona.edu
jkleiner@mail.muni.cz

Abstract: Humans are by far the weakest link in the information security chain. Many in the information security industry advocate for a technical solution to this problem. Unfortunately, technology does not hold the answer to solving the human problem. Instead, it is important to better understand the problem and find new ways of training individuals, so they have a better security mindset and make better security minded decisions. The security challenges associated with human factors have been widely studied in previous literature and different research groups. Prior research has shown that both human behavioural factors and social media usage factors can be used to better assess a person's susceptibility to cybercrime. We know that humans are multi-faceted beings who are swayed by many factors. In addition to behavioural factors and social media factors, humans are predisposed by cultural influences. This paper begins the process of understanding how culture influences a person's ability to make positive cybersecurity decisions in a world that is full of data being thrown at them. The end goal of this research is to use culture, along with behaviour and social media usage as new metrics in measuring a person's susceptibility to cybercrime. This information can then be used by information security practitioners and researchers to better prepare individuals to defend themselves from cyber threats. This paper is the start of the research process into how culture impacts a person's susceptibility to cybercrime. It shows the significance of identifying what specific aspects of culture impact how someone makes a decision. This can help mitigate social engineering attacks by better understanding the influencing factors which control an end user. The authors will continue their work on this project to develop new Information Awareness (IA) training programmes that work to modify an individual's behaviour, while taking into consideration their behaviours, social media usage and culture.

Keywords: cybersecurity, resilience, susceptibility, culture, social engineering, behaviours

1. Introduction

Humans are the front door to most computer networks and nefarious threat actors open this doorway with precision and ease. The nefarious actors open the human doorway easily because they understand that humans are the weakest link in the chain of information security (Collier, 2021) (Collier & Collier, 2020) (Hallas, 2018) (Hadnagy, 2018) (Schroeder, 2017). To open this door, the threat actors simply need to use the end user's behaviours against them (McIlwraith, 2006).

Historically speaking, researchers have tried to find a technical way to prevent social engineering. Add to this, industry has approached cybersecurity through technology and policy, neglecting the cultural and behavioural dimensions (Bernal, 2021). However, behaviour and awareness are some of the most critical issues that needs to be addressed in best practice guidelines and protective tools (Zwilling, et al., 2020). Unfortunately, people circumvent every technical measure created to protect them because these methods make their lives more difficult (Collier, 2021) (Collier & Collier, 2020) (McIlwraith, 2006) (Zinatullin, 2016). A 2019 study investigated the reasons people most often resist cybersecurity policies; it found that if the policies are overly complex or punitive in nature, the end user will work to find a way around the policy, while giving the appearance of compliance (Mehri & Ahluwalia, 2019). Moreover, when people are subjected to rules and norms that are not robustly justified to them, their reflexivity towards these rules suffers, or they tend not to follow them at all (D´Agostino et al., 2021). Coles-Kemp et al. (2018) predicted a similar ramification if people´s desires and needs are not taken into consideration. These are some of the underlying aspects of the social contract theory which

has been increasingly applied to cybersecurity (see, e.g., Abrams et al., 2016; Liaropoulos, 2020) and which is closely tied to culture.

Research into the reasons why a person makes a poor information security decision has increased during the last five years, but more needs to be done. One of the perspectives that has been considered is working on making the security mindset more prevalent amongst end users. A cybersecurity mindset was defined by (Dutton, 2017) as, "a set of attitudes, beliefs and values that motivate individuals to continually act in ways to secure themselves and their network of users, such as by acquiring technical skills, new practices or changing their behaviour online". By choosing a framework approach to cybersecurity that is bottom up, cybersecurity practices will be socially supported (Dutton, 2017), rather than a top-down approach, which is often associated with a fear driven concept. Fear is negative in nature and does not result in long term positive outcomes. Fear feeds into the concept of a toxic workplace and toxicity often results in employees second guessing themselves (Hassandoust & Techatassanasoontorn, 2018) (Mehri & Ahluwalia, 2019) (Collier, 2021). Research has shown that using punishment as a means of behavioural modification is ineffective compared to positive reinforcement (Dynes, et al., 2020) (Durrant & Ensom, 2012). To develop a cybersecurity mindset, it is important not to create a culture of fear (Dutton, 2017) but for organisations to think of the human layer of defence, differently. Instead of putting end users in a position where they might try to conceal a potential breach out of fear of reprisal, the cybersecurity community needs to shift its perspective and work to identify breaches sooner by encouraging employees to notify the information security team of a suspected breach, or if they have fallen for a social engineering scheme. If a security breach is identified sooner, the security team can implement a recovery strategy quicker, stopping the damage faster. Stopping the exfiltration of data quicker will result in less information being lost, and reduces the overall damage done by the threat actor. This lower level of data loss will not only reduce the financial burden of the company that was targeted, but also reduces the risk of long-term negative impacts on the customers that the company serves.

Zimmerman & Renaud (2019) proposed a mindset called 'Cybersecurity, Differently'. This approach changes the human from being the weakest link in cybersecurity to being part of the solution, looking through the lens of the socio-technical system (STS). STS considers the interconnectedness of hardware, software, people, and communities. The human is widely blamed by governments and industry as the weakest link in cybersecurity. For example, IT would be blamed for a successful cyber-attack if a hacker exploits an unpatched system, while the user would be blamed for not paying enough attention during the training sessions if they fell for a phishing email (Zimmerman & Renaud, 2019). In both cases, the blame is on the human, not the technology.

The current defence against the human problem in cybersecurity is the annual cybersecurity awareness training and assessment used by most companies to "train" their employees on cyber issues. Cybersecurity awareness training programmes teach end users about the risks associated using networked systems. It is imperative that organizations ensure their employees understand the risks of cybercrime, and to be prepared to not fall victim to it (Alharthi & Regan, 2021). Unfortunately, knowledge is not enough because the current methods of IA training do not change a person's behaviour, nor do they require a person to learn the material, the individuals are only required to achieve a certain score on the quiz (Schroeder, 2017) (Collier, 2021). Acknowledging the concepts that end users need to be aware of is not enough to make a significant difference (Schroeder, 2017). People also face the problem of information overload and fatigue (Hallas, 2018). Cybersecurity awareness can be defined as 'the degree of understanding of users about the importance of information security and their responsibility and acts to exercise sufficient levels of information security control to protect the organisation's data and networks' (Shaw, et al., 2009). Hackers will seek out the most vulnerable end user (Zwilling, et al., 2020). 'Netizens,', people who use the internet, lack an acceptable level of awareness of the different types of cybersecurity threats, in this study 'threats' is defined as 'cyber hazards' (Zwilling, et al., 2020). These go from the very simple spam emails or texts and calls to organised cyber-crime 'people'. One of the recommendations is that training programmes should be developed from an international position related to an individual's behaviour, rather than based on local or cultural expressions (Zwilling, et al., 2020).

The result of a breach associated with a person falling victim to cybercrime is the termination of the person who fell victim from their employment (Collier, 2021). When an organization is breached, regardless of the reason why, one of the first victims is the Chief Information Security Officer (CISO) and sometimes the entire C-suite is impacted. Target, Capitol One, Equifax, Uber, and JP Morgan each suffered breaches in which the CISO, CIO and/or CEO were terminated due to mishandling of the incident or simply because the breach occurred (Swinhoe, 2020). If one considers that it is not if, but when, an organization falls victim to a breach, then the idea

that an organization immediately terminates an employee or member of the executive team is counterproductive in the long term. More needs to be done to understand why someone becomes a victim to cybercrime and to identify and develop new ways of defending against such breaches. Collier, in his 2021 study used additional metrics to evaluate a person's susceptibility to social engineering (Collier, 2021). The results showed that when factors like behaviours and social media usage were calculated into a susceptibility algorithm, it was possible to assess someone's susceptibility to cyber-crime in a more finite manner (Collier, 2021). However, behaviours and social media usage factors are only a couple of the metrics that need to be assessed when calculating a person's susceptibility level. People are multifaceted beings, influenced by many factors, most of which are unmeasurable. The goal of research needs to be to identify which influential factors impact the decision-making process and affect security minded decisions. If it is possible to better understand the people who are falling victim to cybercrime and what influencing factors impacted their cognitive ability and decision-making process, then it will be possible to develop new methods and techniques to prevent future breaches.

This paper is a first look into how culture plays a role in a person's decision-making process and whether culture impacts the security mindset of individuals. As the culture´s role in an individual´s decisions regarding cybersecurity has not yet been investigated much by scholarly literature, the aim here is to employ an exploratory investigation (as conceptualised by Stebbins, 2001) to lay down the foundations for further empirical and theoretical works. The remainder of this paper is structured as follows. Section 2 highlights how culture plays a role in the decision-making process and how it impacts the security mindset. Cultural influence on cybersecurity decision-making is addressed in Section 3. The paper then addresses a proposed solution to the research problem in Section 4 and concludes by addressing future research venues in Section 5.

2. Culture/decision-making process/security mindset

To understand how culture plays a role in the decision-making process and how it impacts the security mindset, we need to understand what culture is, what the decision-making process is, and what a security mindset is. Once these aspects are better understood, it is important to identify how they are linked and how one influences another.

2.1 Culture

Simonson, et al., (2000) propose that "cultures endow individuals with different rules or principles that provide guidance for making decisions, and a need to provide reasons activates such cultural knowledge" and imply that culture is something that is manipulated by societal rules, which means that culture is learned and changes over time. Since culture is learned, it is consequently guided by societal rules (Whiten, et al., 2011). Culture is by default abstract or fuzzy in nature (Causadias, 2020). Due to the ambiguous nature of culture, it is difficult to define exactly what culture is (Causadias, 2020). Culture is sophisticated and influenced by a set of distinct and similar individuals who are connected on various levels, all related to behavioural expectations, religious beliefs, morals, values, language, symbolism, and ethics. In other words, culture is social in nature (Causadias, 2020). One important thing that needs to be understood is that "culture is not an insignificant or marginal object" (Breznik, 2013).

Müller, et al. (2009) notes that "numerous studies have been conducted on cultural differences and commonalities, showing the differences in values and behaviour of people from different national cultures." Culture can be placed in one of two modalities—individualism and collectivism (Müller, et al., 2009) (Darwish & Huber, 2003) (LeFebvre & Franke, 2013). Individualism is where people are more concerned with themselves and their family members, and less concerned with others within their community (Darwish & Huber, 2003). Conversely, collectivism is where people are more concerned about their community, versus themselves or close family members (Darwish & Huber, 2003). This paper does not judge either individualism or collectivism as being the right way to approach culture, but rather reinforces that culture is not simple in nature. From an information security perspective, individualism and collectivism impact the decision-making process differently and could result in a vastly different outcome. When looking at culture from a worldly perspective, North America and Europe tend to be individualistic cultures, while East Asia and Middle Eastern countries tend to be collective cultures (Darwish & Huber, 2003).

The current statistical information regarding which countries have the most incidents of cybercrime vary depending on the source and is therefore unreliable when assessing if individualism or collectivism is better when it comes to the information security mindset. What is consistently seen when looking at this information is that these incidents span across both individualistic and collective cultures, so neither culture is immune. With most cyber incidents involving social engineering, it is imperative that we understand how culture plays a role in individuals becoming victims to social engineering (Collier, 2020) (Bada, et al., 2019) (Dupuis & Khadeer, 2016).

What we have learned so far about culture is that it is something that is complex in nature, learned through experiences and social group interactions, it is flexible, and most importantly, culture is not insignificant. This creates a problem when trying to determine a method of assessing the risk associated with culture and the information security decision making process.

2.2 Decision-making process

The decision-making process is a process whereby an individual makes a choice based on available data and assessing multiple options. The decision-making process is influenced by knowledge, information, and resources, to include past experiences and skills possessed by the decision maker. The decision maker's psychology, behaviours, and emotional state, also affect the decision maker (Collier, 2021). The basis of the decision-making process is that there is a goal, there are choices and there are selection criteria being considered (Wang & Ruhe, 2007).

Decision-making is part of the cognitive process that separates humans from other mammals. Humans can take detailed amounts of data into consideration and have the ability to think beyond the moment. The decision-making process occurs in both the conscious mind and subconscious mind (Wang & Ruhe, 2007). When conducted in the conscious mind, the individual making the decision will apply a logical approach to the decision-making process. However, in the subconscious mind, behaviours and emotions get involved and the decision-making process becomes muddled and loses some, if not all, of its logic, which may result in a bad decision. For example, logic would dictate that an adult human being could easily step on or remove an insect from their house without harm. However, if the human suffers from entomophobia, logic goes out the window and the decision-making process is heavily influenced by the fear of the insect. Fear, like many other human emotions and behaviours, can be significant influencing factors when it comes to the decision-making process.

Decision-making, like culture, has been studied for centuries by philosophers, but has a shorter history with experimental psychology (Slovic, et al., 1988). Although many different models have been developed over the decades of research that attempt to define the decision-making process, these models are not predictive in nature. They might explain how a decision was made, but when applied to a new decision, there is no data that supports the models that can predict the outcome of the decision with statistical significance (Slovic, et al., 1988). This is because each decision is unique and shaped by many things (Slovic, et al., 1988). For example, when two people are given the same data, do they come up with the same decision every time? Of course not, because each of the decision-makers is a unique individual with different psychological make ups, emotions, knowledge, desires, and cultural influences. It is these unique attributes which make humans wonderful, but at the same time puts them in a position of risk when it comes to the information security decision making process. When you take into consideration all the inputs that impact a decision, it is clear why and how social engineers are as successful as they are. Humans are flawed, as is their security-minded decision-making process.

2.3 Security mindset

The security mindset is a state of mind whereby an individual who is deciding, consistently considers the security outcome of that decision. Since the advent of the computer and the Internet, humans have become more connected than ever. This constant connectedness comes with many benefits, but also many detriments. From a business perspective, the lightning speed of the Internet allows for the near immediate transferal of data, this input of data in such an available manner makes business decisions faster and more accurate. However, this comes with a flaw and that is there is a ton of information available at the touch of a few keys. Much of this data is meant to be kept secret, but often it falls into the hands of nefarious actors. Since humans are the front line of any organization's network, one would think they are well prepared to defend the network and to secure the data. This concept is about as far from the truth as one can get. Humans are imperfect, and their weaknesses are the reason why humans are the number one entry point into a secure network.

If an organization works to foster a security mindset within the population of employees, then it is working to build a more secure border to its network. However, it is important to realize that if not properly developed, the security mindset can be utilized too much, or not utilized enough (Dutton, 2014). The cybersecurity industry understands that more needs to be done to focus people's attention on "attitudes, beliefs and practices" (Dutton, 2017). Unfortunately, the cybersecurity industry and most cybersecurity researcher's response is to push for the development of new technical measures to close the hole in the human firewall (Collier, 2021). As each new technical measure is created, a human will figure a way around it, to circumvent it because it is inconvenient. Instead of finding a technical measure to solve the human problem, we propose understanding the human better to strengthen the human firewall. One of the most important things that we can do to solve this issue is to work to better understand why someone becomes a victim of cybercrime. From here, we need to work to have end users on our systems take ownership of the security and work to develop a security- mindset.

"The security mindset is not only essential but critical for all individuals who design/develop/deploy/upkeep/use digital systems" (Siraj, et al., 2021). Instead of hoping that your company's cyber team is going to catch all attacks and exploits, it is time that end users take responsibility for their own actions. Developing a security mindset has the potential to go beyond the existing technical measures and redefine how a person behaves (Hann, 2022).

3. Cultural influence

From a security perspective, there are three main types of threats to a network. The first is the malicious outsider threat (MOT), that black hat hacker/nefarious threat actor who is trying to get into your network and steal your data or encrypt it. The second is the malicious insider threat (MIT), that disgruntled employee who wants to damage the company because their egos have been bruised and they feel as though they have been wronged by the people they work with or the organization itself. These first two are not what this research is about. Rather, this research is about the third type, the non-malicious insider threat (NMIT) who doesn't want to hurt their organization but does because they fall victim to social engineering. The NMIT threat is the threat that can be prevented by understanding the human element better and then helping them develop a better security mindset.

Collier (2021) conducted research into the NMIT and worked to better understand how human behaviours and social media usage impacted the NMIT. As part of his research, Collier determined that there are 128 different human behaviours which lead to a person making a poor information security decision, resulting in them becoming a victim of social engineering. Collier (2021) developed a new Dynamic Adaptable Information IA Training Assessment tool that utilized questions based on these behaviours and questions related to social media usage to assess one's susceptibility to cybercrime in a more precise manner. This study is an extension of what Collier did with his Dynamic Adaptable IA Training Assessment Tool in that we are working to determine how culture influences a person's information security decision-making process and to see if we can assess and measure it effectively.

In section 2.1, we demonstrate that culture is something that is integrated into a person from birth. Like morals and ethics, culture influences the decision-making process. For example, if a person's culture is that of collectivism, then the person will tend to make decisions that benefit their community over themselves. While on the contrary, someone from an individualistic culture, will tend to make decisions that benefit themselves, over their community at large. Regardless of which form of culture one is associated with, it is clear culture impacts the decision-making process. The question then becomes how does culture influence the information security decision-making process, and can it be measured? We also need to ask if it is possible to develop a set of questions that can be used to generalize culture or is culture so unique that it needs to be applied in a homogeneous manner based on where the tool is being used.

There is no global IA training assessment tool that truly assesses the unique susceptibility each person has. Currently things are artificially grouped together to meet a requirement to train and assess. The current methodologies do not consider human behaviours, culture, or external influencing factors like social media. The cliché about insanity from Albert Einstein states doing the same thing over and over and expecting a different result is insanity may be one of the most overused quotes in history. However, when it comes to the way the cybersecurity industry approaches IA training and assessment, the statement isn't far off. The current IA training and assessment models do nothing to truly change a person's behaviour, and part of the reason is because these methods were not designed around the person, their behaviours, or cultural influences.

To be more effective at changing a person's behaviour, IA training and assessment needs to be reformatted to include psychological techniques like Cognitive Behavioural Therapy (Collier, 2021). Furthermore, these training and assessment programmes need to utilize behavioural and cultural data sets to make the training more international in nature (Zwilling, et al., 2020) (Collier, 2021).

4. The social contract theory, governance, polity, and culture

The social contract theory (SCT) and cybersecurity governance are only a step away from decision-making. In fact, these two often overlap. Note that governance does not need to be solely connected to the state level but also to the organizational one. The SCT represents centuries of political philosophy thinking, from ancient first fruits through Hobbes, Rousseau, or Locke to Rawls, Buchanan or Scanlon. Despite its many branches and particular theories, its basic model comes down to representatives (e.g. politicians or other decision-makers) choosing rules, norms, or principles in a deliberative setting for individuals who are to be guided by these rules and adhere to them. Both these groups must share reasons and norms for the sake of compliance and reflexivity (D´Agostino et al., 2021). Moreover, such principles must be robustly justified and reach a sufficient level of publicity (Gaus, 2021).

The justification process can vary significantly based on many factors. One of them is polity which Carr (2007) links with political (or institutional) culture. Within, the political system plays a huge role. To demonstrate, let us stay with democracy, which can be broadly grasped as a process (procedure) or content (generated rules and laws). If democracy as a procedure is sufficiently justified, its products (contents) are, too (Swift, 2014). In such a context, we use the term legitimacy. The concrete democratic justification then stands on rather different foundations than the undemocratic one, for instance, the Chinese communist or Iranian theocratic polities. Moreover, the contractualist strain of the SCT represented by Kant, Rawls, Scanlon and others cannot be used outside the democratic scope as they emphasize freedom, justice, property rights etc. (Lessnoff, 1990).

Finally, the concept of the Four Internets developed by O´Hara and Hall (2021) loosely connects the recognition of democratic and non-democratic regimes as a part of the culture and the cyber realm. The authors distinguish four internet governance approaches - Silicon Valley´s open, [Washington] DC´s commercial, Brussels´ burgeois, and Beijing´s authoritarian, plus Moscow´s spoiler model. Hence, even within the democratic scope, we have sub-clusters that emphasize openness, commercial exploitation, data and user protection. The similar applies to undemocratic ones.

In sum, governance on state and organizational levels is closely tied with or even constitutive of culture and probably vice versa. To theoretically grasp these phenomena, we employ the social contract theory - one of the most potent branches of political philosophy that has been increasingly applied to the cyber(security) realm. Here, we must reckon with political systems as well as they provide different foundations for one of the core SCT concepts - justification of rules, norms, and principles. This applies not only to the basic distinction between democratic and undemocratic ones but also to a deeper recognition of various strains located within these two traditions. Finally, by adding this discussion to our mix, we are then able to formulate cybersecurity governance implications.

5. Moving forward

We must understand how culture plays a role in the information security decision-making process as it relates to changing how the end user works to protect their organization's data. To do this, we need to identify what specific aspects of culture impact how someone makes a decision. The first step was to understand what culture is, and this part of the study has given us valuable information about culture and how it is going to be unique depending on where in the world someone is from. These differences can be between countries, between regions, and could even be different between villages/towns. The following steps should thus test these confounding variables and look for other ones via both qualitative and quantitative empirical investigations. The complexity that culture is, is certainly going to make determining how culture impacts the information security mindset a bit more difficult. However, this research needs to be completed in order for the fight against the social engineers to be successful.

Now that we have a better understanding of what culture is we will work to establish a series of questions that demonstrate how culture influences the decision-making process. From these questions, we will work to refine

the questions to specific questions that impact the information security decision making process. Once the questions have been developed, we will test their efficacy using the Dynamic Adaptable IA Training Assessment Tool developed by Collier (2021) to determine if culture can be used to predict someone's susceptibility to cybercrime more accurately.

The current susceptibility algorithm used by Collier in his Dynamic Adaptable IA Training and Assessment Tool will be modified to include culture as one of its quantitative values. The proposed algorithm will be (QrTotal/Hb+SM+C)*1000)/2 where QrTotal is the average of the responses to the seven topics of cybersecurity questions, where Hb is the score associated with the human behavioural questions, where the SM score is related to the social media usage questions and where C is the value assigned based on the responses to the cultural assessment questions. The results of this algorithm will fall within the scale of 0-100, with 0 having the highest risk of becoming a victim, and 100 having the least risk.

Upon completion of this test, the results will then be used as part of an interdisciplinary team effort to develop new IA training programmes that work to modify an individual's behaviour, while taking into consideration their behaviours, social media usage and culture.

Acknowledgements

We would like to thank Norwich University student, Emily Collado for her work as a research assistant on this project.

References

Abrams, B., Barrack, S., Bew, R., Brown, J., Buonomo, J., Clinton, L., Connelly, J., Cotton, A., Crisp, D., Daly, K., Doucet, T., Estlick, D., Flannery, B., Fleming, M., Hermanson, S., Humbert, L., Khona, M., Jainchill, C., McAlum,

Alharthi, D. & Regan, A., 2021. *Social Engineering InfoSec Policies (SE-IPs).* Zurich, CICT.

Bada, M., Sasse, A. M. & Nurse, J. R., 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. *CoRR,* Volume abs/1901.02672.

Breznik, m., 2013. And Culture?. *Journal of Arts and Humanities / Journal of Arts and Humanities,* 7(1), pp. 21-29.

Causadias, J. M., 2020. What is culture? Systems of people, places, and practices. *Applied Developmental Science,* 24(4), pp. 310-322.

Coles-Kemp, L., Ashenden, D., & O'Hara, K. 2018. Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. Politics and Governance, 6(2), 41–48. https://doi.org/10.17645/pag.v6i2.1333

Collier, H., 2020. *Social Media: A Social Engineer's Goldmine.* Reading, Academic Conferences and Publishing International Limited.

Collier, H., 2021. *Enhancing Information Security by Identifying and Embracing Executive Functioning and the Human Behaviours Related to Susceptibility.* Colorado Springs: ProQuest.

Collier, H., 2022. *Including Human Behviors into IA Training Assessment: A Better Way Forward.* Reading, Academic Conferences International Limited.

Collier, H. & Collier, A., 2020. *The Port z3R0 Effect!: Human Behaviours Related to Susceptibility.* Copenhagen, AIRCC Publishing Corporation, p. 5.

D´Agostino, F., Gaus, G., & Thrasher, J. 2021. Contemporary Approaches to the Social Contract. https://plato.stanford.edu/archives/win2021/entries/contractarianism-contemporary/

Darwish, A.-F. E. & Huber, G. L., 2003. Individualism vs Collectivism in Different Cultures: a cross-cultural study. *Intercultural Education,* 14(1).

Dupuis, M. & Khadeer, S., 2016. *Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat.* Boston, s.n.

Durrant, J. & Ensom, R., 2012. Physical Punishment of Children: Lessons from 20 Years of Research. *CMAJ,* 184(12), pp. 1373-1377.

Dutton, W. H., 2014. *Fostering a Cybersecurity mindset.* [Online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490010 [Accessed 30 01 2023].

Dutton, W. H., 2017. Fostering a cyber security mindset. *Journal of Internet Regulation,* 6(1).

Dutton, W. H., 2017. Fostering a cyber security mindset. *Internet Policy Review Journal on Internet Regulation,* 6(1).

Dynes, M. et al., 2020. Impact of Education about Physical Punishment of Children on the Attitudes of Future Physicians,. *Children's Health Care,* 49(2), pp. 218-231.

Hadnagy, C., 2018. *Social Engineering: The Science of Human Hacking.* Indianapolis: Wiley.

Hallas, B., 2018. *Rethinking the Human Factor.* s.l.:The Hallas Institute.

Hann, H., 2022. Using Complexity Theory to Identify K-12+ Pedagogical Misalignment with a Security mindset. *Journal of The Colloquium for Information Systems Security Education ,* 9(1).

Hassandoust, F. & Techatassanasoontorn, A. A., 2018. *Understanding User's Information Security Awareness and Intentions: A Full Nomology of Protection Motivation Theory.* Yokohama , s.n.

LeFebvre, R. & Franke, V., 2013. Culture Matters: Individualism vs. Collectivism in Conflict Decision-Making. *Societies,* Volume 3, pp. 128-146.

Liaropoulos, A. 2020. A Social Contract for Cyberspace. Journal of Information Warfare, 19, 1–11.

McIlwraith, A., 2006. *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness.* Burlington : Gower Publishing Company.

Mehri, M. I. & Ahluwalia, P., 2019. Examining the Impact of Deterrence Factors and Norms on Resistance to Information Security Systems. *Computers in Human Behaviour,* Volume 92, pp. 37-46.

Müller, R., Spang, K. & Ozcan, S., 2009. Cultural differences in decision making in project teams. *International Journal of Managing Projects in Business,* 2(1), pp. 70-93.

O'Hara, K., & Hall, W. 2021. Four Internets. Oxford University Press. https://doi.org/10.1093/oso/9780197523681.001.0001

Schroeder, J., 2017. *Advanced Persistent Training: Take your Security Awareness Programmes to the Next Level.* Edinburgh: Apress.

Shaw, R. S., Chen, C. C., jarros, A. L. & Huang, H.-J., 2009. The impact of information richness on information security awareness training effectiveness. *Computers & Education,* 52(1), pp. 92-100.

Simonson, I., Morris, M. & Briley, D., 2000. Reasons as Carriers of Culture: Dynamic versus Dispositional Models of Cultural. *Journal of Consumer Research,* 27(2), pp. 157-178.

Siraj, A. et al., 2021. Is there a Security mindset an Can it be Taught?. *CODASPY '21: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy,* pp. 335-336.

Slovic, P., Lichtenstein , S. & Fischhoff, B., 1988. Decision Making. In: Wiley, ed. *Steven's Handbook of Experimental Psychology.* New York: Wiley.

Stebbins, R. A., 2001. *Exploratory research in the social sciences.* SAGE.

Swinhoe, D., 2020. *CSO.* [Online] Available at: https://www.csoonline.com/article/3510640/7-security-incidents-that-cost-cisos-their-jobs.html [Accessed 14 01 2023].

Wang, Y. & Ruhe, G., 2007. The Cognitive Process of Decision Making. *International Journal of Cognitive Informatics and Natural Intelligence.*

Whiten, A., Hinde, R. A., Laland, K. N. & Stringer , C. B., 20011. Culture evolves. *Philosophical Transactions of the Royal Society B,* 366(1567).

Zimmerman, V. & Renaud, K., 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies,* Volume 131, pp. 169-187.

Zinatullin, L., 2016. *The Psychology of Information Security.* Cambridgeshire: IT Governance Publishing.

Zwilling, M. et al., 2020. Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study. *Journal of Computer Information Systems,* 62(1), pp. 82-97.