Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P. 17247-17257

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

User behaviour's contribution to better Cyber Security Management

Quang-Vinh Dang

British University Vietnam, Hung Yen, Vietnam
vinh.dq4@buv.edu.vn
ORCID: 0000-0002-3877-8024

How to cite this article: Quang-Vinh Dang (2024) User behaviour's contribution to better Cyber Security Management. *Library Progress International,* 44(3), 17247-17257.

ABSTRACT

According to theoretical and empirical knowledge, cybersecurity awareness is a crucial issue in cyber security. The main actors in cyber security are people, and one way to reduce risk in cyberspace is to increase knowledge of security concerns. Companies lose money as a result of data breaches and production losses brought on by cyberattacks. Consequently, there has been a surge in research endeavours aimed at comprehending the cybersecurity behaviours of users. The benefit of knowing user behaviours is that researchers and security professionals may utilize this information to start altering behaviours for the sake of cybersecurity. Similar cybersecurity behaviours have been categorized by several research, while the naming systems used vary. Sanctions, a decline in customer loyalty, and damage to one's brand may all arise from data breaches. Business continuity is also impacted by cyberattacks, which make it difficult for organizations to maintain constant production. This paper aims to demonstrate that, in addition to computer science research, behavioural sciences that study user behaviours can offer useful strategies to improve cyber security and lessen the impact of attackers' social engineering and cognitive hacking tactics (i.e., disseminating misleading information). Thus, in this study, we provide fresh insights on the psychological characteristics and individual variances of computer system users that account for their susceptibility to cyberattacks and crimes. Our investigation shows that different computer system users have different cognitive capabilities, which affects their ability to defend against information security threats. In order to improve network and information security, we identify research gaps and suggest possible psychological techniques to help computer system users follow security requirements.

Keywords: Cyber Security, Data Breaches, Computer System, Security Policies, Cognitive Hacking, Social Engineering, Vulnerabilities, Attacks and Crimes, Information Security, Psychological Methods.

I. INTRODUCTION

In 2019, 73.4% of Serbians were connected to the internet, while more than fifty percent of the world's population (58.8%) used the Internet. These days, it is hard to imagine life without information technology. According to a poll conducted by Serbia, 99.2% of those aged 16 to 24 use machines, and 98.2% use the Internet every day or almost every day [1]. Recent technological developments have had a big influence on people's lifestyles. However, this development also has a drawback: the Ponemon Institute estimates that the global economic impact of security breaches was almost fifty million dollars in 2017 [1, 2], and the cost of breaches of information is increasing yearly [2, 3]. Security incidents are becoming increasingly complicated and dangerous, and their frequency is steadily increasing [3, 4]. In recent decades, as information technology has become more widely used, the end-user characteristics has changed as well [3, 4].

The average IT user lacks technical expertise and most likely has never taken a cyber security course in school [2, 4]. Cyber security is a computer-based discipline that uses people, technology, information, and processes to safeguard operations from illegal access or attack [4, 5]. Although they are somewhat knowledgeable about the security risks, most users do not know how to take action to achieve cyber security [4, 5]. For instance, some consumers are not sure how to recognize the problem or react appropriately to phishing, even if they have heard of it. Human error is the primary problem with secure information, according to several publications [5, 6], thus

it's critical to understand how individuals act while utilizing security technologies [6, 7].

Gurucul behaviours analytics offers some advantages over traditional security techniques [6, 7]. For example, it can detect attacks by people using compromised credentials and insider threats that traditional security systems are unable to detect (Fig. 1) [6, 7]. By monitoring user behaviours and identifying unusual activity, behaviours analytics can issue alerts for dubious insider behaviour's, such as unauthorized data access, privilege abuse, or data exfiltration [7, 8].

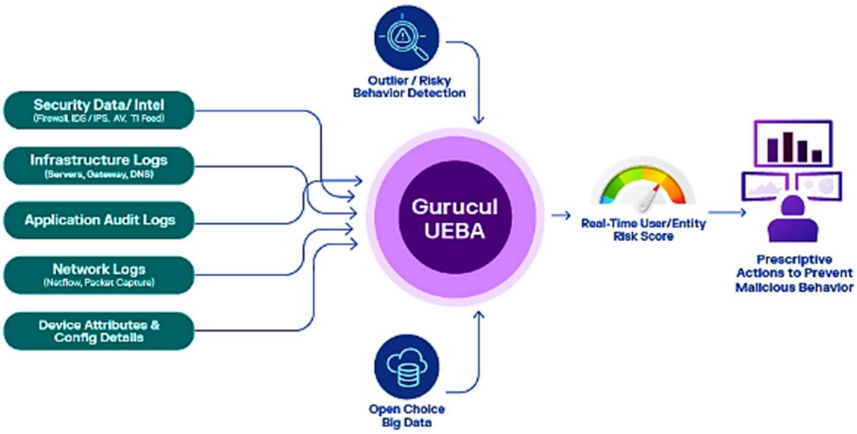

Fig. 1 Gurucul Analytics of Behaviour. [8, 9]

Many security issues are caused by ignorance or unsafe behaviours (e.g., sharing passwords or clicking on unsafe links in emails) [8, 9]. Protecting oneself online is crucial these days [9, 10]. NIST Special Publication 800-16 provides the following definition of security awareness.

> *''Awareness is not training [11, 12]. The purpose of awareness presentations is simply to raise awareness of security [12]. Giving individuals the ability to recognize IT security threats and take the necessary action is the aim of awareness presentations [13].*

Just being aware of such threats is only one part of awareness [13]; putting security procedures into place is another.

The National Initiative for Cyberspace Employment and Studies defines cybersecurity as [14],

> *'The method, skill, [14, 15] or circumstance that protects communication and information infrastructures and the data they hold against damage, unlawful use or change, or exploitation [15].'*

Cyber and network systems require at least four components:

- Computer system users, [15],
- Security system analysts,
- Cyber attackers,
- Computer systems.

Cybercriminals often attempt to get, modify, [15, 16], or hold onto unlawful data. The bulk of cybersecurity research has focused on improving computer network systems because many people believe that software development and technological developments are the main ways to improve information security [16]. Fewer studies have focused on improving the situational awareness and cognitive skills of system analysts. However, by [16], hackers may also affect users' ideas rather than the computer system itself by [16, 17]. To infiltrate a network or computer system, for example, they may use social engineering (e.g., tricking people to get information, such as passwords) and cognitive hacking (e.g., spreading misleading information) [18]. Social engineering attacks account for 28% of all cyber security threats, while phishing accounts for 24% [18, 19].

According to Cyber Edge Reports, more than 70% of social engineering attacks have been successful in recent years [19]. According to Telstra's 2018 and 2019 surveys, human error is the largest cybersecurity threat [19, 20]. The most common attacks, according to the research, were phishing (and spear-phishing) efforts, which tricked victims into installing malware or visiting fraudulent websites to get their login credentials by using deceit and partial social engineering [19, 20].

The victims of these attacks sometimes get emails or texts that seem to be notifications from the financial institution or social networking site, a software update, a current storm or catastrophe, or a third-party provider, among other things [20, 21]. Users of computer systems not only fall for phishing schemes but also commit other cyber security errors, such sharing passwords with friends and family as well as failing to update software. It is important to keep in mind that different computer system users have different approaches to following security procedures.

Numerous studies have shown that individual differences in postponement, impulsivity, geared toward the future thinking, and risk-taking behaviour's may account for variances in adherence to security standards [21, 22]. Importantly, given that human error may still impact network security, we will discuss the use of psychological approaches to improve adherence to security laws [22]. Using novel polymorphic security alarms, rewarding and penalizing both good and bad online behaviours, and promoting reflection on the long-term consequences of one's actions are some examples of these psychological strategies [22, 23].

Cybercrime has grown in popularity all around the globe once people realized how susceptible the global network was. Even while buying a laptop and setting up an internet connection are cheap, and using technologies like a VPN and proxy servers makes it easy to be anonymous online, the number of cyberattacks has been steadily increasing [23]. These evil intentions may be motivated by political [23, 24] considerations, economic gain, or—above all—the destruction of a country's critical infrastructure. As communities become more dependent on information technology, the vulnerability of key infrastructures in cyberspace poses a severe concern [24]. For instance, a new malware called Stuxnet was released to the world in 2012. It was intended to target Iranian nuclear installations and cause significant damage to uranium enrichment-related industrial equipment [24, 25].

1.1 Cybersecurity Behaviour

The conditions around a behaviour make up its context. Behaviour is influenced by context [10]. One example pertaining to CSB is that social engineering assaults could be more successful at certain seasons of the year, such the holidays. This section discusses the CSB in relation to the home and workplace.

- **Cybersecurity Behaviour at Work:** Policies and regulations primarily control the CSB of workers. When employees violate the organization's policies or engage in wrongdoing, they are held responsible [1, 11, 12]. Additionally, ICT departments help users follow policy by banning harmful or unsuitable websites, reminding users about software upgrades, and providing information on emerging dangers and recommended practices [9].

Blythe made an effort to comprehend CSB within an organizational context [13]. Cybersecurity is often assessed in an organizational context in relation to compliance [14, 15]. Bad CSB is seen in an organization as a violation of the established rules. Behaviour is more involved than this, Blythe said. According to the research, the assessment of compliance is constrained as it only looks at a restricted number of rules and processes. The behaviours is influenced by both internal and external factors, among other behavioural variables. Similar to the objectives discussed in [9], internal factors include drive or self-motivation, whilst external impacts include elements like the surroundings [13].

- **Cybersecurity Behaviour at Home:** People of all ages who use computers or mobile devices with Internet access are known as home users. Users are usually in charge of managing their CSB alone in the home setting [22, 23]. Since home users are not exposed to training programs, it is expected that their cybersecurity knowledge, awareness, and abilities are much lower [19]. This presumption was subsequently shown to be incorrect by [20], who discovered that home users actually possess cybersecurity expertise. Although the behaviours at home is different, the information may be acquired in other settings, such as the workplace [11, 21, 22, 24].

Finally, some home users do adhere to cybersecurity principles in their homes. The research by Catherine et al. used the term "cybercitizens." Home users who are proactive in being aware of cybersecurity and using cybersecurity skills in their surroundings are referred to as cybercitizens [19]. In order to encourage more users to become cybercitizens, the research provides treatments that centre on the intents of cybercitizens. Cybercitizen behaviours include downloading and upgrading antivirus software, being wary of emails and their attachments, and, finally, creating strong, memorable passwords [19].

A six-element taxonomy to classify CSB in organizations. The behaviours were grouped using the dependent

variables, which were,

(1) The level of skill needed to execute the behaviours, and
(2) The purpose of the behaviours with regard to the organization.

Intentional destruction, risky tinkering, conscious assurance, damaging usage, naïve blunders, and basic cleanliness were the six categories of the taxonomy [9].

Nearly 2.7 billion workers, or about 81% of the global workforce, are impacted by full or partial lockdown measures, according to the International Labour Organization's (ILO) Monitor, which was released on April 7, 2020 (ILO Monitor:COVID-19 and the world of work. Second edition 2020). In the second quarter of 2020, the COVID-19 pandemic is predicted to eliminate 6.7% of working hours worldwide, or 195 million full-time employees. Therefore, it is predicted that losses across various income categories are greater than the impact of the financial crisis of 2008–2009.

Businesses who have put effort, time, and money into their digitization have been less impacted by this unprecedented crisis and have even benefited from it in certain situations. Stated differently, those who have successfully integrated information technology into their daily operations are able to go on without interruption. Although these firms are better off than their less technologically advanced competitors, they still have to deal with the less obvious COVID-19 side effect of a rise in cybercrime.

In order to capitalize on online trends and behaviours, cyber risks are always changing. This is also true in the COVID-19 pandemic. Criminals have used the coronavirus to launch pandemic-themed social engineering attacks and disseminate different malware packages since the start of the COVID-19 disaster. Shai Alfasi, a vulnerability researcher at Reason Labs, disclosed on March 9, 2020, that hackers were gaining access to user-stored personal data (credit card numbers, passwords, etc.) by creating phony copies of decease distributed maps. (Trend Analysis Report 2020; COVID-19, Info Stealer & the Map of Threats). In March 2020, there was a 400% spike in complaints of fraud connected to coronaviruses, which cost their victims more than 800,000 pounds in a single month, according to the UK National Fraud & Cyber Security Centre.

The discovery of Stuxnet has shown that viruses, or hostile software as some call them, may really harm people physically [24, 25]. Governments now invest billions of dollars on information security due to past cyber catastrophes. The top information technology research and consultancy firm in the world estimates that businesses spent $75.4 billion on information security in 2015 [25, 26]. Information security is still a contentious issue for consumers, companies, and countries since it encompasses not just the protection of knowledge resources but also other assets, such persons [25, 26]. However, a secure environment cannot be created just by technological information security measures. Thus, a more comprehensive strategy that considers organizational, social, national, and technological issues is needed to protect data management [25, 26].

Since human ignorance and lack of knowledge are often linked to a company's security risk, experts claim that nothing can ensure the security of any system and that human engagement is required. Nowadays, maintaining a safe online environment depends on people's information security practices [25, 26]. Supporting people's information security behaviours may benefit both individuals and businesses [26, 27]. But maintained that,

> *"The importance of human components in information security cannot be overstated [27, 28]."*

In this context, identifying the contextual and/or personal factors that support or enable people's information security behaviour is essential [28, 29]. However, research on how to promote appropriate information security behaviour is still in its early stages [28, 29]. This research adopts a more thorough method to identify the organizational and/or individual factors that impact people's information security behaviour [29, 30].

Additionally, this study aims to provide a more thorough approach to information security administration, [30], taking into consideration both organizational and human elements, in light of this advice in previous research, [29, 30]. The current study aims to empirically examine the relationships between information security behaviour and individual and organizational factors, such as self-efficacy, organizational policy regarding information security [31,32], data regarding security share [30,31], and the intention to attend security training, building on the significant works [30,31].

This investigation is organized as follows [31, 32]. We begin by discussing studies and initiatives related to compliance with security standards. Secondly, we discuss the many cyber security errors that many users of computer systems do, including exchanging passwords, falling for phishing schemes, and neglecting to update software. Third, we discuss personality differences including absences, impulsivity, risk-taking, and geared

toward the future thinking that influence cyber security behaviour's in computer system users [33, 34]. Lastly, we provide psychological techniques that might be used to sway user behaviour toward safer practices [21, 22].

II. ADHERING TO SECURITY GUIDELINES

Following security guidelines is a crucial behaviour to protect computer and network systems. There aren't many studies on the psychology of security policy compliance. Noncompliance with security rules may pose a major threat to information security. For example, many studies have shown that computer system users often ignore security warnings [22, 24]. To measure these individuals' security-related behaviour's, the Security Behaviour Intentions scale was developed [25].

The scale evaluates general security attack knowledge [23], password choices [25], regular software upgrades, and attitudes toward device security. The scale has sixteen questions, including,

(a) I open my laptop or tablet using a password or passcode, [25, 30]
(b) I open my laptop or tablet using a password or passcode, [30, 31]
(c) When I leave my computer, I manually lock the screen, [30], and
(d) If I find a security flaw, I keep working on it because I figure someone else will take care of it.

The scale itself illustrates basic components of protection and security mitigation plans [30]. As we discuss below, this scale has been used in several studies to measure the different types of security errors made by computer system users [30, 31].

III. ERRORS IN HUMAN CYBERSECURITY

This section explains the many cyber security errors that many computer system users make. According to many publications [33], which have also been backed by more recent investigations [31, 32], humans are believed to be the most security-vulnerable group. A study found that 95% of network and cyberattacks are caused by human mistake. In our scenario, persons are either security analysts or computer system users, despite the fact that most research in this area focuses on errors made by computer system users [22]. The weakest link in preserving system security is the company's workforce (see also for discussion and analysis) [25, 31].

Fig. 2 Errors in Human Cybersecurity. [22]

Password sharing, excessive social media sharing, accessing dubious websites, using unapproved external media, carelessly clicking links, using the same passwords repeatedly, opening email messages from unreliable sources, sending confidential information over cell phone networks, failing to update software, and not physically securing personal electronic gadgets are just a few examples of human error in cyber and network security [25, 26]. Accordingly, one of the fundamental issues underlying information and cyber security is the difficulty of making a network or data more usable and accessible while preserving security [26]. In an effort to increase security, organizations usually require users of computer systems to create complex passwords, which makes usability difficult [26].

- **Being a phishing victim:** Some phishing research has used a laboratory-based phishing experiment. According to a recent research, the use of lab-based phishing trials is connected to actual phishing [26, 27]. According to one study, over 30% of government employees click on a questionable link in this phishing email, and many of them have provided their credentials [27, 28]. In another study that used a similar phishing experiment, over 60% of college students clicked on a questionable link in a phishing email. As a result, some studies [28] suggest that while researching cyber and network security, behavioural, psychological, and human factors research be included. In another study, Columbia University staff and students replied to phishing emails [28], and they reported that it took them around four rounds to recognize that they were receiving phishing emails [29].

- **Sharing passwords:** Sharing passwords with friends, relatives, and even total strangers is a typical example of human cyber security failures [29, 30]. Older adults with good self-monitoring and perseverance scores are more likely to share their passwords. Password sharing may lead to financial exploitation, one of the most common forms of abuse among older people [30, 31]. The reason for this is that many older people have a high level of trust in strangers, especially those they encounter online. Similar to older people, younger people often share passwords, especially for streaming services [31, 32]. Younger users, who had grown up with computers, saw security as a hurdle they had to solve [32].
- **Setting up software upgrades:** One common error that underpins cybersecurity behaviour's is installing software upgrades slowly or not at all. An experimental behavioural decision-making study suggests that certain people's updating software installation behaviour's may be explained by their risk-taking tendencies. More risk-takers, in particular, choose to delay downloading upgrades to their software. While phishing and password sharing have received a lot of attention in the area [31], installing software updates has not [33].

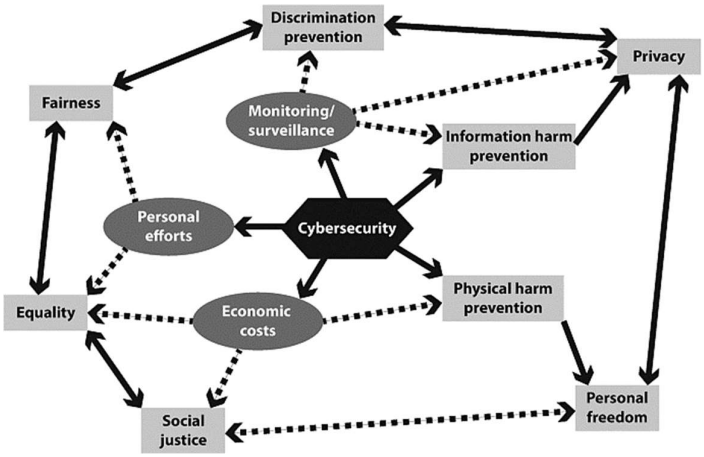

Fig. 3 Cybersecurity's Core Values and Value Conflicts: Going Beyond Privacy vs. Security. [33]

IV. PERSONAL DIFFERENCES BUNDED BY CYBER SECURITY ACTIONS

Individual differences in personality, cognition, and behaviour are linked to cybersecurity behaviour's. Individual differences in cognitive abilities and personality factors may be important for effectively protecting computer and information systems [33, 34]. Below, we discuss some of these psychological traits [34].

- **Procrastination:** Complying with security standards may be linked to cognitive processes such as exerting significant effort to achieve a goal. A scale known as "the need for cognition" is used to assess working hard, appreciating, and doing activities that require effort and thinking [34]. As a result, performance on the Security Behaviour Intentions Scale is associated with the Need for Cognition (NFC), which indicates a tendency to expend cognitive effort [34, 35]. Interestingly, a recent study developed a procrastination scale for kids and teens that is suitable for the increasing number of young people using the internet. As a result, [34], conscientiousness (i.e., doing things accurately and thoroughly) [35] and the desire to follow information security rules are related. Furthermore, procrastinators are less likely to follow security standards, as shown by their performance on the Security Behaviour Intentions Scale using the General Decision-Making Style (GDMS) scale [35, 36]. This is understandable considering the inverse relationship between delaying and active task completion [36].
- **Impulsivity:** Compliance with security standards may also be impacted by individual differences in impulsive behaviour's [36, 37]. Performance on the Security Behaviour Intentions Scale was shown to be correlated with Barratt Impulsiveness Scale scores. Another research found that internet addiction and impulsivity influence dangerous cyber behaviour's [37].
- **Future Thinking:** Crucially, following security standards may also be associated with forward-thinking and taking into account how present actions may impact future results. In other words, those

that care more about the future might make sure their computer system is safe in the future by adhering to security recommendations [37, 38]. Consequently, performance on the Security Behaviour Intentions Scale is linked to Consideration for Future Consequences (CFC) [37, 38]. The following items on this scale are very relevant to cyber security behaviour's: [38],

'I think about how things could turn out in the future and attempt to affect such things via my daily actions,

'Even though a terrible consequence won't happen for many years, I believe it is crucial to heed warnings about it',

and

'When I make a choice, I consider the potential long-term effects [28, 39].

- **Risk-taking actions:** Another facet of psychology that is connected to cyber security is risk-taking behaviour's. Numerous studies suggest that high-risk computer users may be more susceptible to cybercrimes [39, 40]. Risk is the act of doing something that has an uncertain outcome, usually with the goal of gaining more. For example, it's risky to steal from a bank since you can get jailed [40]. Ignoring security rules is risky because, while there are benefits to avoiding additional work, such software updates, there is also a chance of falling victim to phishing and other cybercrimes [40, 41].

The Big Five Scale has also been used in cybersecurity and psychological studies [40, 41]. Extraversion, diligence, transparency, neuroticism, and agreeableness are the five components of the Big Five Scales [42]. But we found that the literature only mentions neuroticism, extraversion, and openness [42, 43]. Instead of analysing the precise differences between the Big Five Scales and the triad's limited approach, we have extracted the multi-dimensional features of the dark triad. For example, impulsivity is a component that is present in all of the measurement indicators [43, 44, 45]. The additional components are grouped in Table 1. To sum up, this section included earlier studies showing the connection between personality traits and cyber security behaviour's as well as individual differences in procrastination, impulsivity, and risk-taking behaviour's [45].

V. ENHANCED SECURITY ACTIONS THROUGH PSYCHOLOGICAL METHODS

As discussed earlier, hackers often use social engineering and cognitive hacking methods to get access to computer systems or networks [45, 46]. Some computer system users may have psychological traits that make them more susceptible to phishing [46, 47]. Giving users of computer systems that are vulnerable to security breaches the resources they need to mitigate these effects is thus essential. This section discusses a number of psychological techniques to increase compliance with security regulations [46].

- **Making use of new polymorphic security alerts**: Most consumers ignore internet security notifications out of habit [46, 47]. In psychology, a reduced response to repeated exposure to the same stimuli over time is referred to as habituation. To put it another way, we tend to overlook things that we see often. Most warnings are similar to other message dialogs [44].

Table 1 An overview of each individual trail found in relevant ideas and tools. [44]

Individual Trait	Test/Theory	Instruments
Procrastination	Big Five:	Procedure for Hunter and Schmidt Meta-Analysis
	Neuroticism	Scale of Academic Procrastination
	Dark Triad:	The Adult Procrastination Inventory
	Machiavellianism and Psychopathy	Inventory of Aitken Procrastination
		Questionnaires on Decisional Procrastination
		Scale of General Procrastination
		Scale of Procrastination Assessment
		Procrastination Log Behaviour of Students
		Inventory of Procrastination Self-Statement
		Questionnaire on Test Procrastination
Impulsiveness	Dark Triad:	Hadlington's Analysis
	Psychopathy	Scale of Abbreviated Impulsivity
	Narcissism	Barratt's Scale of Impulsivity
	Big 5 Scales:	Scale of Security Behaviours and Intentions (SeBIS)
	Openness	Momentary Ecological Assessment
	Extraversion	The Dickman's Dysfunctional Impulsivity subscale
Future Thinking		Inventory of Impulsivity
		Test of Internet Addiction
		Scale of Wishful Thinking
		Questionnaire on Automatic Thoughts
		ESE scale for Entrepreneurial Self-Efficacy
Risk taking		Measure of Attitudes Toward Cyberbullying
		Scale of Cybersecurity Attitudes
		Scale of Security Behaviour Intentions
		Scale of Domain-Specific Risk Taking
		Scale of Dangerous Cybersecurity Behaviours

- **Rewarding and punishing both positive and negative online conduct:** Both positive (such as prizes) and bad (such as losses, penalties, etc.) experiences in day-to-day living may teach us anything [36]. People are often motivated to do certain things in order to get rewards and avoid negative outcomes. On the other side, the advantage of cyber security behaviour's is that nothing bad will happen; users' computer systems won't be attacked if they adhere to security rules [34]. In other words, following cyber security procedures is an example of negative reinforcement, in which doing certain behaviour's (such adhering to cyber security regulations) prevents a negative outcome [34, 35].
- **A greater consideration of the effects of actions in the future**: As mentioned earlier, disregard for possible consequences is one of the primary characteristics of disobedience with cyber security legislation [38, 48]. Thinking about the future has been shown to be associated with careful planning and decision-making, and it may lessen impulsive behaviour, which is connected to risky online behaviour as we previously discussed [49, 50]. Given this, using psychological strategies to increase reflection on the long-term consequences of choices may improve reflective decision-making and, thus, improve cyber security procedures [50].

VI. CONCLUSION AND FUTURE WORK

According to our study, a lack of consideration for cyber and network security standards is associated with specific personality traits, including impulsivity, risk-taking, and an incapacity to consider the long-term effects of activities. Future studies should concentrate on creating a set of assessments that include personality traits and mental processes associated with network and cyber security behaviours into a single, cohesive framework. The cognitive abilities covered above, such as impulsivity, risk-taking, and considering the long-term effects of decisions, must be tested. Here, we also demonstrate how a range of psychological techniques can promote pro-security behaviours, such as through the use of creative polymorphic security alerts, the reward and punishment of security-related behaviours, and psychological techniques that promote contemplation of the potential long-term effects of actions. Furthermore, there are cognitive training techniques, such working memory training that may help the general public become less impulsive, risk-taking, and procrastinating. Techniques for cognitive training may be able to improve cybersecurity behaviours and change certain behavioural characteristics.

Computational cognitive models are employed in cybersecurity and may be used to forecast how attackers or users of computer systems would behave. Neural network models, for instance, are used to identify social engineering assaults. Call logs and other data from phone calls were used to evaluate the model. Date, time, call origin and end location, and conversational details are all included in each record. The language was analysed using the model to spot any efforts at social engineering or infiltration. Additionally, it was shown via cognitive modelling that an over-reliance on frequency and regency is associated with cyberattacks. Computational models

should be used in future research to more thoroughly examine the connection between cybersecurity behaviours and cognitive processes.

VII. REFERENCES

[1] Fornell, C. and Larcker, D.F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error', Journal of Marketing Research, Vol. 18, No. 1, pp.39–50.

[2] Furnell, S. and Clarke, N. (2012) 'Power to the people? The evolving recognition of human aspects of security', Computers & Security, Vol. 31, No. 8, pp.983–988.

[3] Galba, T., Solic, K. and Lukic, I. (2015) 'An information security and privacy self-assessment (ISPSA) tool for internet users', Acta Polytechnica Hungarica, Vol. 12, No. 7, pp.149–162.

[4] Gartner (2015) Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to reach $75.4 Billion in 2015, 23 September.

[5] Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010) Multivariate Data Analysis: International Version, Pearson, New Jersey.

[6] Han, J., Kim, Y.J. and Kim, H. (2017) 'an integrative model of information security policy compliance with psychological contract: examining a bilateral perspective', Computers & Security, Vol. 66, No. 3, 52–65.

[7] Herath, T. and Rao, H.R. (2009) 'Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness', Decision Support Systems, Vol. 47, No. 2, pp.154–165.

[8] D. Jeske and P. van Schaik, ''Familiarity with Internet threats: Beyond awareness,'' Comput. Secur., vol. 66, pp. 129–141, May 2017.

[9] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, ''Correlating human traits and cyber security behavior intentions,'' Comput. Secur., vol. 73, pp. 345–358, Mar. 2018.

[10] S. Egelman and E. Peer, ''Scaling the security wall: Developing a security behavior intentions scale (SeBIS),'' in Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst. (CHI), 2015, pp. 2873–2882.

[11] A. Moallem, Cybersecurity Awareness among Students and Faculty. Boca Raton, FL, USA: CRC Press, 2019.

[12] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, ''Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q),'' Comput. Secur., vol. 42, pp. 165–176, May 2014.

[13] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, ''Individual differences and information security awareness,'' Comput. Hum. Behav., vol. 69, pp. 151–156, Apr. 2017.

[14] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, ''Gender difference and employees' cybersecurity behaviors,'' Comput. Hum. Behav., vol. 69, pp. 437–443, Apr. 2017.

[15] A. A. Cain, M. E. Edwards, and J. D. Still, ''an exploratory study of cyber hygiene behaviors and knowledge,'' J. Inf. Secur. Appl., vol. 42, pp. 36–45, Oct. 2018,

[16] K. Olmstead and A. Smith, ''Americans and cybersecurity,'' Pew Res. Center, Washington, DC, USA, Tech. Rep., 2017.

[17] K. Olmstead and A. Smith, ''what the public knows about cybersecurity,'' Pew Res. Center, Washington, DC, USA, Tech. Rep., 2017.

[18] M. Anderson and E. Vogels, ''Americans and digital knowledge,'' Pew Res. Center, Washington, DC, USA, Tech. Rep., 2019.

[19] IBM SPSS Statistics for Windows, version 22.0, IBM Corp, Armonk, NY, USA, 2013.

[20] D. Florencio and C. Herley, ''A large-scale study of Web password habits,'' in Proc. 16th Int. Conf. World Wide Web (WWW), Banff, AB, Canada, 2007, p. 657.

[21] G. Notoatmodjo and C. Thomborson, ''Passwords and perceptions,'' in Proc. 7th Australas. Inf. Secur. Conf. (AISC), Wellington, New Zealand, 2009, pp. 71–78.

[22] McBride, M., Carter, L., and Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. RTI Int. Inst. Homel. Secur. Solut. 5:1.

[23] Mishra, S., and Dhillon, G. (2006). "Information systems security governance research: a behavioral perspective," in Proceedings of the 1st Annual Symposium on Information Assurance, academic track of the 9th Annual 2006 NYS Cyber Security Conference, New York, NY.

[24] Mohebzada, J., El Zarka, A., BHojani, A. H., and Darwish, A. (2012). "Phishing in a university community: Two large scale phishing experiments," in Proceedings of the Innovations in Information Technology (IIT), International Conference, (Piscataway, NJ: IEEE), 249–254.

[25] Rajivan, P., and Gonzalez, C. (2018). Creative persuasion: a study on adversarial behaviors and strategies in phishing attacks. Front. Psychol. 9:135.

[26] Rankin, C. H., Abrams, T., Barry, R. J., Bhatnagar, S., Clayton, D. F., Colombo, J., et al. (2009). Habituation revisited: an updated and revised description of the behavioral characteristics of habituation. Neurobiol. Learn. Mem. 92, 135–138.

[27] Regier, P. S., and Redish, A. D. (2015). Contingency management and deliberative decision-making processes. Front. Psychiatry 6:76.

[28] Rodriguez-Enriquez, M., Bennasar-Veny, M., Leiva, A., Garaigordobil, M., and Yanez, A. M. (2019). Cybervictimization among secondary students: social networking time, personality traits and parental education. BMC Public Health 19:1499.

[29] Rosenbaum, G. M., Botdorf, M. A., Patrianakos, J. L., Steinberg, L., and Chein, J. M. (2017). Working memory training in adolescents decreases laboratory risk taking in the presence of peers. J. Cogn. Enhanc. 1, 513–525.

[30] Sadkhan, S. B. (2019). Cognition and the future of information security. Paper presented at the 2019 International Conference on Advanced Science and Engineering (ICOASE).

[31] Saleme, D., and Moustafa, A. A. (2020). "The multifaceted nature of risk-taking in drug addiction," in Cognitive, Clinical, and Neural Aspects of Drug Addiction, ed. A. A. Moustafa (Amsterdam: Elsevier).

[32] Saleme, D. M., Kluwe-Schiavon, B., Soliman, A., Misiak, B., Frydecka, D., and Moustafa, A. A. (2018). Factors underlying risk taking in heroin-dependent individuals: Feedback processing and environmental contingencies. Behav. Brain Res. 350, 23–30.

[33] Ifinedo, P. (2014). Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf. Manag. 51, 69–79.

[34] Jacobs, N., Goossens, L., Dehue, F., Völlink, T., and Lechner, L. (2015). Dutch cyberbullying victims' experiences, perceptions, attitudes and motivations related to (coping with) cyberbullying: focus group interviews. Societies 5, 43–64.

[35] Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. (2007). Social phishing. Commun. ACM 50, 94–100.

[36] Jakobsson, M., and Ratkiewicz, J. (2006). "Designing ethical phishing experiments: a study of (ROT13) rOnl query features," in Proceedings of the 15th International Conference on World Wide Web Feature, Scotland

[37] Joireman, J., Shaffer, M. J., Balliet, D., and Strathman, A. (2012). Promotion orientation explains why future-oriented people exercise and eat healthy evidence from the two-factor consideration of future consequences-14 scale. Pers. Soc. Psychol. Bull. 38, 1272–1287.

[38] Jones, A., and Colwill, C. (2008). "Dealing with the Malicious Insider," in Proceedings of the 6th Australian Information Security Management Conference, (Perth,WA: Edith Cowan University).

[39] Kar, K., Moustafa, A. A., Myers, C. E., and Gluck, M. A. (2010). "Using an animal learning model of the hippocampus to simulate human fMRI data," in Proceedings of the 2010 IEEE 36th Annual Northeast Bioengineering Conference (NEBEC), New York, NY.

[40] Keller, U., Strobel, A., Wollschläger, R., Greiff, S., Martin, R., Vainikainen, M., et al. (2019). A need for cognition scale for children and adolescents: structural analysis and measurement invariance. Eur. J. Psychol. Assess. 35, 137–149.

[41] King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., and Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Front. Psychol. 9:39.

[42] Moustafa, A. A., Cohen, M. X., Sherman, S. J., and Frank, M. J. (2008). A role for dopamine in temporal decision making and reward maximization in Parkinsonism. J. Neurosci. 28, 12294–12304.

[43] Moustafa, A. A., Keri, S., Herzallah, M. M., Myers, C. E., and Gluck, M. A. (2010). A neural model of hippocampal-striatal interactions in associative learning and transfer generalization in various neurological and psychiatric patients. Brain Cogn. 74, 132–144.

[44] Moustafa, A. A., Keri, S., Polner, B., and White, C. (2017). Drift diffusion model of reward and punishment learning in rare alpha-synuclein gene carriers. J. Neurogenet. 31, 17–22.

[45] Moustafa, A. A., Keri, S., Somlai, Z., Balsdon, T., Frydecka, D., Misiak, B., et al. (2015). Drift diffusion model of reward and punishment learning in schizophrenia: modeling and experimental data. Behav. Brain Res. 291, 147– 154.

[46] G. Notoatmodjo and C. Thomborson, ''Passwords and perceptions,'' in Proc. 7th Australas. Inf. Secur. Conf. (AISC), Wellington, New Zealand, 2009, pp. 71–78.

[47] A. Adams and A. M. Sasse, ''Users are not the enemy,'' Commun. ACM, vol. 42, pp. 40–46, Apr. 1999.

[48] R. W. Rogers, ''A protection motivation theory of fear appeals and attitude Change1,'' J. Psychol., vol. 91, no. 1, pp. 93–114, Sep. 1975.

[49] M. Ovelgönne, T. Dumitraş, B. A. Prakash, V. S. Subrahmanian, and B. Wang, ''Understanding the relationship between human behavior and susceptibility to cyber-attacks: A data-driven approach,'' ACM Trans. Intell. Syst. Technol., vol. 8, no. 4, pp. 51:1–51:25, Mar. 2017.

[50] G. A. Grimes, M. G. Hough, E. Mazur, and M. L. Signorella, ''Older adults' knowledge of Internet hazards,'' Educ. Gerontol., vol. 36, no. 3, pp. 173–192, Feb. 2010.