# Cybersecurity policy compliance in higher education: A theoretical framework

## Abstract

Higher education institutions (HEIs) are open in their nature, decentralized, rich in population and private data, home to some ground-breaking research and innovations. As such, HEIs attract quite a substantial threat and cyberattacks due to their heavy reliance on the Internet. However, there is poor cybersecurity culture and low awareness that are motivated by generational differences that are characterised by “digital natives” and “digital residents” and gaps in technology savviness impacting cybersecurity compliance in a specific higher education environment. Whilst technologies to prevent and response to cyberattacks have been inevitable, their effectiveness lie extensively rather on heterogeneous human factors in enforcing their principles in the context of compliance. Thus, the objective of this study was to develop a theoretical framework for effective cybersecurity compliance strategy in HEIs. To do this, we would focus on critical factors such as cybersecurity and organizational cultures into compliance theory and protected motivated theory (PMT) respectively to help in understanding how cybersecurity compliance can be achieved in HEIs.

**Keywords: Cybersecurity, Higher Education Institution, Cybersecurity culture, Organizational culture, Compliance Theory, Protected Motivated Theory**

## Introduction

The birth of the “Es” as in “Electronics” has seen unprecedented accessibility to services and resources across industries and across continents around the globe. “Electronic” could not be any more useful especially in such situations as Covid-19 pandemic where social distancing and face-masking prove to be the panacea to contain the spread of the virus. The recent innovations and digital development have played critical role in these regards. One of such industries that have been remodelled, taking advantage of the Internet and internet of things (IoTs) is education, specifically Higher Education (HE) through e-Learning[1] platforms, a term first used by Elliott Masie in his presentation in TechLearn Conference at Disneyworld in November 1999. Since its inception in November 1999, there has been sustained increase in the reliance on e-Learning platforms as with their evolving functionalities but not without challenges, particularly with cyberattacks, threats and incidents. For example, higher education institutions, universities for that matter now have the capabilities of Wi-Fi support, online teaching and learning software, virtual classrooms, and digital libraries, on the one hand. On the other hand is the increased exposure to cybersecurity vulnerabilities and attacks (Ajaero, 2020, Suciu et al.). To say the least, these platforms on web infrastructure for digital learning infrastructure provide both state and non-state cyberattacks a safe haven (Udroiu, 2017) as the Higher Education sector continue to expand and explore additional potential of information systems and computer networks to meet the growing diverse nature of teachers and learners expectations who demand more than just traditional classroom-based experiences (Bandara et al., 2014). This makes Internet an important resource component in the higher education in modern times “to meet the demands of the present-day diversified learners, higher education sector has been extensively seeking the help of the information systems and technology in their classrooms and also for the online learning systems as well” (Singar and Akhilesh, 2020).

Also known as the complete online delivery of course, program or degree, e-Learning is learning that utilizes electronic technologies to access educational curriculum outside of a traditional classroom (Ibrahim et al., 2020). E-learning systems are complicated and comprise computing systems and networks of the Internet cohort. They have the objective of ensuring rich experience for teaching and learning process (Rjaibi et al., 2012). To enhance online

[1] In this study, e-Learning, Online learning, and m-learning will be used interchangeably to imply Internet-related learning

learning, a myriad of eLearning and online course management systems have been designed. Parallelly, models of cyberattacks/cybercrimes have also evolved (Ibrahim et al., 2020).

Given their complex and open nature as with being heterogeneous and broad in scope, not only are the cybersecurity threats heightened but also varied (Bandara et al., 2014). As such any hope for an agile post-pandemic pedagogy capable of responding to the turbulence of switching between face-to-face and online would need to refocus its energies on the desecuritization of face-to-face schooling for the future possibility of “emancipatory” pedagogy, whether face-to-face or online (Murphy, 2020). Desecuritization in this context would implicitly require the netting in of a wider community and initiatives involving partners in the business sector, higher education and end users (students) during the development of learning product/service is one way to keep up-to-date of advancements in relevant technologies (Villikka, 2018) and the continue adoption and use of Internet of Things (IoTs) as they evolve. Alongside the adoption of relevant advanced Internet technologies is increased exposure to cyberattacks. Scholarship agree that technical aspects of cybersecurity is not a full panacea to securing information systems asserts and preventing cyberattacks. The rest of cybersecurity issues rest with human factors in the context of compliance (Donalds and Osei-Bryson, 2020, Donalds and Osei-Bryson, 2017, Reddy and Rao, 2016, Alshaikh, 2020).

However, in the higher education, there are differing levels of online exposure, experience, and cybersecurity awareness. For example, a study on the attitudes of business students in cybersecurity awareness highlighted the need for training for improving cybersecurity awareness  The gap between those Prensky (2001) refers to as “digital natives” and “digital migrants” demonstrated the importance of developing an Internet-based cyber education/training system (Kim et al., 2017a, Dodel and Mesch, 2017) given the potential cybersecurity risk these groups. Digital natives are the younger generations as the digital natives given the availability of technology to digital natives and their ubiquitous usage as such speak digital language of computers. Digital migrants are the people born prior to the ‘80s who “may learn to use new technologies but will still be in some way located within the past, unable to fully understand the natives” (Prensky, 2001). Cybersecurity compliance have been challenged by human factors (Algarni et al., 2018, Zimmermann and Renaud, 2019, Evans et al., 2016, Maglaras et al., 2018), and more so, inside attacks (Guitton, 2017, Sanders et al., 2019, Wang et al., 2017, Corradini, 2020, Kim et al., 2017b). We argue that framing a theory around compliance and compliance and human factors could help improve understanding of cybersecurity compliance and human factors thereby leading to the formulation of more effective cybersecurity compliance strategies in HEIs. Thus, the aim of this study was to develop a theoretical framework for this subject matter.

## Higher Education (HE)

HE is one of the four sectors of the formal education. The other three are early childhood education, primary education, and secondary education. The HE is largely provided by universities, with some vocational education training (VET) and private higher education practitioners (HEPs) also offering bachelor and associate degrees in low student numbers compared with universities. There are some institutions that are both a university and vocational (Gale and Parker, 2013).

HE institutions (HEIs) are rich in population and private data and attract quite a substantial and various forms of attacks. HEIs house not only large and important biographical data, financial data but also data on cutting-edge research and development of emerging and new technologies (Gearhart et al., 2019, Aliyu et al., 2020). Whilst universities are positioning themselves at the forefront of technological advancement on the one hand, on the other hand, the increased access to the advanced technologies also increases their vulnerabilities in computing environment with increased security threat (Joshi and Singh, 2017). For example, the University of Queensland (Challener, 2020) and the Oxford University in partnership with AstraZeneca have been at the forefront of developing Covid-19 vaccines (Lane, 2020) due for trial in various countries (Mahase, 2020, Makoni, 2020). This is coupled with poor cybersecurity infrastructure and poor attack response preparation to any attack or breaches as with their open and transparency culture that encourages them to report any breaches. Millions of data breaches are reported from multinational companies, the theft or exposure of academic data is not widely publicised (Chapman, 2019). Grama (2014) disagrees that the HEI openness make them susceptible to attacks and data breaches arguing that other industries do not report breaches due to loss of competitiveness and lack of investor confidence. For example, Beaudin (2015) asserts that there have been over 700 data breaches involving educational institutions publicly recorded between 2005 and 2014 in a report by Chronology of Data Breaches. The answer to the question of whether cyberattacks on HEIs is higher or there is transparent reporting of incidents is mixed. Either way, one thing is certain. Colleges and universities have a complex mix of private and public areas, secure and open networks, and have a vast amount of personal and intellectual property information that make them increasingly vulnerable to hacker attacks. HEI as industry is equally competitive and needs to remain competitive to attract quality students, faculty, and non-faculty members. For example, in a 2016 report written by Center for Digital Education, Milford, executive director of the Research and Education Networking Information Sharing and Analysis Center at Indiana University, was quoted as saying "Perhaps even more significant than potential financial losses, cyberattacks pose a grave threat to a university's reputation and the safety of its students" (Campbell, 2020).

## e-Learning, e-Examination, and cybersecurity

HEIs have adopted online study modes to extend their offerings and expand their user/student population base globally (Butler-Henderson and Crawford, 2020). Academics and administrations in HEIs have questioned ways in which e-Learning could contribute in keeping up the excellence of the didactic in their institutions whilst also looking at different conditions that make learning the key for the "co-creation and co-delivery of knowledge of knowledge and training (Dell'Acqua, 2017, Bovill, 2020). However, with emerging alliances such as University of Stanford and University of Pennsylvania on "Coursera", MIT and Harvard collaborating on "EdX", founded by Mellon Foundation, Bill and Belinda Gates Foundation are leading and living the concept (Dell'Acqua, 2017). In cases that were studied in Arcada and Expert College in Finland and Pearson in Netherlands, students' feedback emphasized the need for support with digital scaffolding (platform/framework) and the need for a structured approach to digitalization and eLearning (Villikka, 2018). On some occasions, student would need to bring in additional content from external sources. Whether the external contents compound or alleviate students' challenges, there is exposure to risk of cyberattack and threats through malicious software. As several systems are accessed by many over several networks and managed through the Internet, securing e-Learning systems presents a huge cybersecurity challenge at all times (Bandara et al., 2014).

The future of e-learning is greatly attributed to the credibility of e-Examinations through authentication and security to prevent cheating and cyberattacks. For example, although Butler-Henderson and Crawford (2020) note the availability and inclusion of e-Examinations, the authors also acknowledged their implementation and use are limited. e-Invigilation systems are also needed to complement e-Learning. e-Invigilation for monitoring students activities through biometric methods that provide security against external and internal threats and offers scalable management, storage, retrieval and processing of biometric samples (Iwasokun et al., 2019, Ketab et al., 2016). Whilst biometric authentications have been most efficient, they still are vulnerable to cyberattacks (Sabbah, 2017). "Biometric authentication is any form of human biological measurement or metric that can be used to identify and authenticate an authorized user of a secure system”. Biometric authentication can include fingerprint, voice, iris, facial, keystroke, and hand geometry (Coronado, 2012) in (Kowtko, 2014). Other notable e-Examination authentication methods include Face, Fingerprint, keystroke dynamic authentication, Video matching algorithm, proctored-Only scheme, video monitoring, and Webcam monitoring (Sabbah, 2017).

## Higher Education and Cybersecurity

HEI with huge population relies heavily on Internet for its operations. Hackers with differing motivation are interested in the theft/or adulterating valuable data generated from day-to-day operations for further fraud activities. 61% of data breaches in higher education are the results of hacking and malware (Grama, 2014). Data breach is "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure." (The Identity Theft Research Centre, 2015) The proliferation of multiple modes of teaching and learning have made higher education grown increasingly complex with the evolution, use  and management of a plethora of technologies to remain viable to community as education or training service provider (Gearhart et al., 2019). These technologies, which depend largely on the Internet are continuum of interconnected devices.  However, the very nature of the core business and clientele of higher education for that matter make them open environments both physically and academically and it is important they retain that open culture.

In 2014, cybersecurity breaches in higher education sector accounted for 10% (31) of the global breaches and with some 1,359,190 identities exposed (De Kock and Futcher, 2016). In fact, Karl E Weick described universities as “loosely coupled systems” (Weick, 1976, p.1), thus open. This make them susceptible to all sorts of attacks – from physical to cyber, necessitating a sense of balance between openness and safety (Chapman, 2019, Singar and Akhilesh, 2020, Zalaznick, 2013). Elsewhere, a study by  Kaspersky (2013) found an increased cyberattacks on corporate IT infrastructure and those of higher education whilst remain deficient in the context of security remains a target for threat actors  (Aliyu et al., 2020).

Security threats have shown to have a negative impact not only on the assets associated with an organization but also on its reputation (Zwilling et al., 2019, Dodel and Mesch, 2017). When an institution suffers a full network outage from a Distributed Denial of Service (DDoS) attack disrupting teaching and learning (Chapman, 2019), it endures a dent on its status. Cybersecurity threats and incidents have proved to have negative impact not only on cyber infrastructure, digital assets associated with organizations and individual but also their reputations. Particularly, an attack during examination when students across an institution are using the Virtual Learning Environment revision and to write their examination. As more and more higher education institutions continue to establish/or integrate and institutionalise e-Learning into their programs/curriculum, so are the rise in cyberattacks on their systems.

The pace at which applications that utilize Internet when activated evolve is unprecedented as HEI tend to be information intensive. These applications and their storage such as Cloud make them prone to cyberattacks. Cloud computing poses privacy concerns because the security of data on this platform is available to a huge viewership making it susceptible to the ill-minded cyber criminals/hackers (Alajmi and Sadiq, 2016). Poremba named five higher education information security[2] threats that needs to be known. They are as Phishing, ransom, and malware, Password problems, Wi-Fi, Card Not Present Transactions, and BYOD. In a research by the Centre for Digital Education Chief information security officers (CISOs) cited eight major cyber security challenges HE. They are Phishing, User education, Cloud Security, High-profile information security strategy, Next-Generation security technology planning, identity and access management, governance over data security, unsecure personal devices (Roscorla, 2016). We expound on a few common threats below.

### Phishing, ransom, and malware

Human factor in cybersecurity breaches still dominates the threats. Phishing, for example uses fraudulent emails and links to obtain authorised or sensitive personal information such as electronic account user/login details, credit information via disguised emails. Victims are sent, for example, an email that redirects to an infested site that steals victims information (Vayansky and Kumar, 2018).

Ransomware attack first occurred in 1989 in the healthcare domain (Ferreira, 2018). A study by Martens et al. (2019) estimated that WannaCry infected an estimated 10,000 organization with 200,000 computers in more than 150 countries via phishing email and a user visiting a malware infected website (Sammons and Cross, 2017). Ransomware is a “malicious software that once loaded on a victim system encrypts the hard drive and issues a warning that unless a ransom is paid within 24–48 hours, all the data will become unrecoverable” (Winkler and

[2] Whilst Information systems security and Cybersecurity are not necessarily the same, in this study, they are used synonymously/interchangeably

Gomes, 2017). The malware, once installed on computer has the potential to prevent the running of app, stop keyboard from working as with the potential to blocking the desktop leading to inaccessibility of the taskbar (Sammons and Cross, 2017). Ransom demanded is usually between $250 and $1000 (Winkler and Gomes, 2017).

Whilst the healthcare domain remains atop of the ransomware attack list of industries, ransomware has infiltrated into other industries including the HE given its rich and diverse data. HEI and students as young adults are vulnerable to these types of cybercrimes given their active engagement with Internet related activities as part of carrying out their academic work and given that they are lenient in terms of cybersecurity.

**Password problems**

Protecting information with password remains the dominant method. However, it has drawbacks when not strong or poor as they are easy to break by for example, brute force and malware. Educational institutions have much of the usual data security concerns of other organizations including sensitive employee data and operating revenues (Coffey et al., 2018). HEI is a great place for password-related cybercrime. This is all because of the habit of higher education students and perhaps researchers using the same password and username/email for everything/every account to enable them keep track of accounts to various resources (Poremba, 2014). This habit also offers a reason to look at authentication beyond password. The lack of awareness of the security vulnerabilities of giving emails and password information upon request from both known and unknown sources is worrying. For example, a decoy by Greening (1996) requesting Sydney's undergraduate computer science students usernames and password under the disguise of intrusion detection and computer information system upgrade saw 47% of the students succumbing to it. Information security awareness and management remain low and challenging in Australian Universities (Chan and Mubarak, 2012).

**BYOD**

Bring your own device (BYOD) is a concept that originated from Intel as a cost cutting strategy whilst improving productivity motivated by the proliferation and adoption of IoTs/smart devices. "BYOD in education is an ICT mediated 1:1 mobile learning (m-learning) model that encourages learners to bring their own personal device(s) with various apps and embedded features/functions to school to use them for learning (and teaching) purposes" (Safar, 2018). BYOD is about the use of personally owned devices and related technologies that allow authorised members of an organization or institution to connect to and access their corporate and institutional network and data to complete tasks (Afreen, 2014). Gartner also defined BYOD as "an alternative strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data" (Gartner, 2013).

In the higher education environment, BYOD is the practice of allowing students and teachers to use their own mobile computing devices such as laptops, tablets, personal digital assistants (PDAs) and more recently, tablets and smartphones during lectures or classes (Singh et al., 2017). Primarily, BYOD enable students, lecturers and other authorised staff to access course and other educational materials and resources online and to interact with course activities.

Even with its vulnerabilities and threats (Herrera et al., 2017) given the general unregulated use of personal devices, BOYD is predicted to increase in the domain of education as with increased utilization of Internet resulting in increased risk to information and data security risks that effect on a higher educational institutions given increased plethora of connected devices (Singar and Akhilesh, 2020, De Kock and Futcher, 2016). In Australia as with other advanced economies, nearly all HEIs allow both students and non-students to use their devices on their network (Bradford Network, 2013) in (De Kock and Futcher, 2016). Whilst the BYOD initiative have been hailed and widely adopted, there are obvious security concerns given the open nature of HEI physically, educationally, and virtually. Cybersecurity concerns range from potential installation of malicious software on BYODs from social media and social networking apps such as Facebook, Instagram, Twitter, YouTube, etc. Malware downloaded do not only infects the individual devices but also the entire organization.

## Information security awareness in higher education

There is evidence that "suggest that greater awareness of security risks and controls contributes to improvements in both control development (i.e., design and implementation) and performance" (Spears and Barki, 2010, p.518). Similarly, as with Chan and Mubarak (2012) and Bulgurcu et al. (2010), Yeo et al. (2007) also found in their information security risk assessment strategies of an Australian University that information security awareness is an important component which must be assessed as integral component of the University's overall risk program. Additionally, Alotaibi et al. (2016) also note that management policy, dissemination, user awareness and user behaviour in the context of human and organizational factors significantly impact on user information security compliance behaviour. The authors posit that the security of information transmitted through a continuum of devices not only depends on technological and technical infrastructure and policies put in place, but also on human factors and awareness issues in terms of the understanding of importance of using devices and associated information and cybersecurity (Herrera et al., 2017). For example, a BYOD policy should not only be accessible but also easy to understand by all institutional members (Herrera et al., 2017). However, Rajab and Eydgahi (2019) claim that the Chief of Information Security Office at the University of Wisconsin-Madison is of the view that students and non-students members of higher education lack adequate levels of information and cyber security awareness due to their busy schedules.

## Cybersecurity and policy in higher education

An information security policy is any official document that clearly stipulates guidance on the DOs and DON'Ts behaviours when dealing with information assets of an organization or institution that are expected to be complied (Alotaibi et al., 2016). It provides fundamental assurance to information security and a violation of such policy amounts to non-compliance, resulting in some actions. It is achieved through technical and non-technical solutions resulting in security culture in an organization. Depending on the organization, information security may vary substantially. However, the human behaviour  and organizational culture are key drivers of compliance in the context of ensuring that users adhere to security policies to ensure institutional resources safety (Hina and Dominic, 2018). In their study on violations of information security measures, which is any kind of information security policy, Alshare et al. (2018) found procedure justice, distributive justice, severity and celerity of sanction, privacy, responsibility and organizational culture as predictors. As such ISPC interventions should be designed to encompass these predictors in the context of how they contribute to behavioural intention at individual levels (Hina and Dominic, 2018). Literature has confirmed that the ISC developed in organizations can reduce the risk of security breaches and potential incidents, as compliance with rules and regulations becomes a habit. For example, about a third of HEI users access emails and other links that contain some sort malware (Brumfield, 2016).  Information security compliance has a huge potential in reducing and mitigating risk to information assets. It can neutralize and bring some level of agreement of internal individual intentions and ideologies towards unified front against threats. Literature trend in this domain indicates that ISPC can be achieved at three levels defining the information security components that impact information security behaviour (Da Veiga and Eloff, 2010). However, the people or human factor aspect, which executes ISPC through compliance is yet to fully be understood. There is evidence in literature suggesting that awareness, education, and training programs have been instrumental in improving cybersecurity compliance. See for example, (Alshaikh et al., 2020, Aldawood and Skinner, 2019, Vasileiou and Furnell, 2019, He and Zhang, 2019). For example, more recently cybersecurity maturity models are built on assessing broader compliance to cybersecurity programs/or policies and HE is not different.

## Cybersecurity maturity assessment in Higher education

Information and cyber-risk assessment is a methodology for establishing the level of exposure of information security assert or asserts in the context of being lost, taken over, unauthorised changes (Fay, 2018). There are various models used in assessing the overall risk value of a setting, employing both qualitative and quantitative methodologies. For example, the Operationally, Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) for information security assessment and planning by defining information security assets/resources that includes but are not limited to people, hardware, software and as well as information and systems (Joshi and Singh, 2017). Other assessment frameworks are National Institute of Standards and Technology's Risk Management Framework (NIST RMF), Treat Agent Risk Assessment (TARA) and Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) (Aliyu et al., 2020). Each of these frameworks has their weakness as elucidate (Joshi and Singh, 2017). Using the identified weaknesses of existing assessment frameworks, Joshi and Singh proposed a risk assessment framework that is an objective of assessing an objective of assessing open networks in the context of Universities through "recursive mechanism that collects input regarding vulnerabilities and threats and produces quantitative risk level that can be measured and treated" (Joshi and Singh, 2017, p.129). Whilst Capability Maturity Models can enable organisations to benchmark current maturity levels against best practices (Aliyu et al., 2020), this is generally achievable through broader compliance.

## Cybersecurity in Higher education and theoretical framework

Technology alone is not sufficient to assure information security Even with the advancement in technical measures, attacks on digital assets have not stopped and have become heterogeneous and complicated because with adequate level of user **cooperation** and **knowledge**, many security techniques are liable to be misused or misinterpreted by users (Van Niekerk and Von Solms, 2010).

Compliance is human factor oriented. It means following established rules that help in meeting set requirements. There is emphasis on the role of human factor in majority of cyber-attacks/data breaches as cybersecurity policies are perceived as guidelines as opposed to rules.

In cybersecurity, compliance implies establishing a program that offers risk-based controls to protect information assets. As with cyber culture, several human behaviour related theories/frameworks have been used to evaluate employee behaviour viz-a-viz compliance in cybersecurity measures. Popular among them include Protection Motivation Theory (PMT), predicting two cognitive processes – threat and coping appraisals respective by (Rogers, 1983); General deterrent Theory GDT) (Jervis, 1978), Theory of Planned Behaviour (Ajzen, 1991), Health Belief Model (Rosenstock, 1960), and Organizational Theory (OT).

Culture is the way people live. It is "a set of basic tacit assumptions about how the world is and ought to be that a group of people share and that determines their perceptions, thoughts, feelings, and, to some degree, their overt behaviour" (Schein, 1996, p.11). Culture can also be said to be social behaviours, knowledge, beliefs and norms that are acquired through everyday activities (Tylor, 1958). The group be any group of people or an organization. Organizational culture describes the environment in which people work for a common goal. The organizational environment has influence on how people think, act and experience work (Warrick et al., 2016). At any level, culture can differ significantly. As posit….culture demonstrates itself at three levels: the level of deep tacit assumption and beliefs, that represent the essence of the culture, the level of espoused values that are often reflect what a group wishes ideally to be, and the way it wants to present itself to the public (Schein, 1996).

In the domain of information security and cybersecurity, culture is a new concept and an aspect of organizational culture that is gaining traction. It is "*contextualized to the behaviour of humans in an organizational context to protect information processed by the organization through compliance with the information security policy and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives"* (da Veiga et al., 2020, p.19). Although many factors drive culture, cybersecurity culture is driven by organizational culture and leadership. Thus, Cybersecurity culture in organization is deduced to efforts by organization toward securing positive and acceptable behaviour, perception, assumption, beliefs, norms, and values of people towards cybersecurity when processing information with the help of information technologies. In other words, the development of a CSC is meant to achieve a change in mindset, fosters security awareness and risk perception and maintains a close organisational culture, rather than attempting to coerce secure behaviour. Overarchingly, the goal of cybersecurity culture in organizations is to address the culture of the organisation, the culture of groups and individuals to get organizational members to comply with cybersecurity policies. It involves the creation of and sustained awareness and education on cybersecurity. CSC therefore perceive culture as a concept that can be changed and managed (Enescu, 2019) to achieve cybersecurity policy compliance by organization. We discuss compliance theory next.

## Compliance Theory

The general lack of cybersecurity awareness and involvement has led to increased ignorance, negligence, apathy, mischief, and resistance (Safa et al., 2016, p.2). Organizations have been classified in accordance with the type of power they use to direct the behaviour of their members and the type of their involvement (Lunenburg, 2012) to get them comply with policies. Compliance theory was developed by Etzioni (1975) as an approach to organizational structure. The theory comprises three types of power with three accompanying involvements that organizations use to direct behaviours. They are coercive power with alienative involvement, utilitarian power with calculative involvement, and normative power with moral involvement (Lunenburg, 2012). As alientative involvement is generally an intense and negative orientation usually practice in prisons for inmates, calculative involvement designates positive and negative low orientations that are applied to business relationships (Lunenburg, 2012).

Generally, most schools tend to be normative organizations as coercive and utilitarian power with teachers and students may lead to dysfunction (Lunenburg, 2012). Coercive power is based on force and fears. Like the custodian model, Utilitarian power is based on remunerations or extrinsic reward to control lower-level organizational members. Unlike utilitarian, the normative power manages members through intrinsic rewards such as job satisfaction and continuous development, identification of goals. Recognitions and awards and influence the distribution of acceptance and positive response in the organization and attractive many professionals. HEI is an example of the organizations that employ normative power. The success of these powers largely depends on the extent to which participants are involved. Involvement is “the orientation of a person to an object, characterized in terms of intensity and direction” (Lunenburg, 2012). Involvement allienative, which is usually intense and negative; calculative is low in intensity with either positive or negative orientation. The last involvement, the moral, is positive orientation of high intensity (Lunenburg, 2012).

We contend that given the decentralised and open nature of HEI, positive orientation of high intensity educates and motivates members of a HEI to undertake protective behaviour motivated by threat appraisal and copying appraisal (Tsai et al., 2016, White, 2017, Towbin, 2019), thereby complying with cybersecurity policies. We discuss protective motivated theory (PMT) later on. Clearly, in the settings of HEI normative power and moral involvement are perceived to be more applicable. Moral involvement in the context of positive orientation such "involvement, such as information security knowledge sharing, collaboration, intervention and experience, as well as attachment, commitment, and personal norms that are important elements positive orientation" (Safa et al., 2016, p.2). Positive orientation encompasses a positive attitude – self-satisfaction, optimism, self-esteem in (Kupcewicz et al., 2019). It mirrors the positive relationship between one's self-efficacy and self-esteem drawn from past experienced and positive future expectations and experiences. These promote a higher level of commitment to life with the potential to result in positive impact on the individuals, their social groups, and creates a significant personal resource which is important in the context of workplace environment (Tisak, 2019, Caprara et al., 2019).

**Protective Motivated Theory (PMT)**

Several cybersecurity studies have employed PMT to understand the motivation for individuals to embark on cyber-related protective behaviour. PMT is based on the theory of reasoned action (TRA) (Fishbein and Ajzen, 1977) and has two fundamental contructs - threat appraisal and coping appraisls. Each of these cardinal constructs help individuals assess level of risk they encounter whilst processing information and take action as a protection cover. The theory questions the motive for individuals practicing protechtive behaviour (Rogers, 1975) when interacting with cyberspace. "Threat appraisals are determined by perceived vulnerability and susceptibility to risks, as well as rewards associated with unsafe behaviours (Tsai et al., 2016). Coping appraisals are based on coping self-efficacy, response efficacy, and response costs associated with safe or adaptive behaviours (Tsai et al., 2016). One the one hand, the authors also defined coping self-efficacy is the belief that individuals can successfully carry out protective behaviors and response efficacy as the belief in the effectiveness of the protections, on the other hand (Tsai et al., 2016).

Li et al. (2019) operationalized PMT, Health Belief Model to investigate the impact of cybersecurity policy awareness on employee's cybersecurity behaviour. Towbin (2019), (Fishbein and Ajzen, 1977) applied PMT in the healthcare domain to showcase that individuals are not likely to implement recommended threat mitigation strategy unless three conditions are met: the threat must be sufficiently severe, threat must likely to affect the individual, and if the two conditions were met, the third, individual expect the solution to be effective. Tsai et al. (2016) employed PMT in a cross-sectional survey of Amazon Mechanical Turk users to determine how classical and new PMT factors predicated security intentions. Their findings suggest strong coping appraisal as predictor of online safety intention. Elsewhere, the results of a study that proposed a model for understanding smartphone security behaviours showed that perceived vulnerability and perceived severity correlated strongly with the outcome variable of perceived vulnerability (Verkijika, 2018). In a related study using PMT, Miraja et al. (2019) demonstrated that self-efficacy and response efficacy had significant relationships with the behavioural intention of "digital natives" to comply with educational software anti-piracy laws. The findings of a study by Liang and Xue (2010) suggest factors of perceived susceptibility and severity (threat appraisals) and safeguard effectiveness, safeguard cost, and self-efficacy (coping appraisals) significantly correlated with computer threat avoidance behaviours.

## Discussion

The issue of cyber-security and threats in higher education and are not debatable. Higher education openness in terms of network accessibility has expanded its cybersecurity vulnerabilities and risks. But there must be a struck in the balance between openness and cyber safety. Already, higher education institutions such as universities are less confident of their cybersecurity programs (Chapman, 2019) due to increasing adoption of BYOD and expanded online and blended learning modules and lack of standard cybersecurity maturity assessment models. For example, a study the results a study on cyber security behaviour among university students was mostly disappointing in malware, password usage, phishing, social engineering, and online scam (Muniandy et al., 2017). Given its invaluable and heterogenous data ranging from cutting-edge research and innovation, affiliations, through to tens of thousands of students, cybersecurity threats in the higher education are legion, including thieves, insiders, fraudsters, and list goes on (Susskind, 2014).

Unlike cybersecurity compliance analysis, which is methodologically structured (Furfaro et al., 2018), human compliance of cybersecurity polices is cognitive-based and depend on a range of behavioural factors. Vulnerabilities are multiplying too, thanks to increasingly interconnected people and businesses, as well as the expanding "Internet of Things" (Susskind, 2014). Cybersecurity awareness and education has been argued as one of widely used for the prediction of compliance with cybersecurity policies and procedures, though empirical evidence is inconclusive(Reddy and Rao, 2016). The implication of this is that cybersecurity compliance predictors need to expand to embed behavioural theories that can ascertain and test relevant cognitive and behavioural factors without excluding organizational cultural factors.

## Conclusion and future work

Like many other industries, the use of Internet in higher education is well felt with the integration and institutionalization of e-Learning and IoTs motivated initiatives such a BYOD resulting in increased HEI user population across the globe, diversifying human factor. HEIs have a complex mix of private and public areas, secure and open networks, and have a vast amount of personal and intellectual property information that make them increasingly vulnerable to a continuum of cyberattacks. This has complicated the decentralised nature of HEI and increased accessibility by users. HEIs are homes to some ground-breaking research and innovations. Our findings suggest that whilst most HEIs do have cybersecurity policies in place, there are challenges with compliance behaviour, as a consequence of low cybersecurity awareness in HEI and poor response strategies to attacks. Even with some acceptance levels of cybersecurity maturity and awareness, the human behaviour and organizational culture remain key drivers of cybersecurity policy compliance to ensure institutional resource safety.

Organizational culture and cybersecurity culture are candidate variables that have the potential to help in understanding how cybersecurity compliance can be achieved when integrated with other potential variables from other relevant theories/models. In this study, we have demonstrated a trajectory of integrating cybersecurity and organizational cultures into compliance theory and protected motivated theory respectively as demonstrated in our discussion through this review.

Cybersecurity interventions must focus mainly on prevention and backup/restoring procedures, which are related to sociotechnical solutions that can manage and understand users' awareness, workflow, behaviours and needs (Ferreira, 2018). It is important to adapt information security interventions and awareness programs to suit different stakeholders to foster a culture of compliance. For example, in HE environment, there are user/member generational differences that is characterised by "digital natives" and "digital residents" and technology savviness, which has the propensity to impact cybersecurity compliance. As such, gaining knowledge and perception of generational differences can assist in the development of more robust collaborative work environments by leveraging on the strength of differing generational members.

## Reference

AFREEN, R. 2014. Bring your own device (BYOD) in higher education: Opportunities and challenges. *International Journal of Emerging Trends & Technology in Computer Science,* 3**,** 233-236.

AJAERO, C. 2020. *Behavioral Characteristics Computer Users Need to Minimize Ransomware Exposure.* Capella University.

AJZEN, I. 1991. The theory of planned behavior. *Organizational behavior and human decision processes,* 50**,** 179-211.

ALAJMI, Q. & SADIQ, A. What should be done to achieve greater use of cloud computing by higher education institutions. 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016. IEEE, 1-5.

ALDAWOOD, H. & SKINNER, G. 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet,* 11**,** 73.

ALGARNI, M., ALMESALM, S. & SYED, M. Towards Enhanced Comprehension of Human Errors in Cybersecurity Attacks. International Conference on Applied Human Factors and Ergonomics, 2018. Springer, 163-175.

ALIYU, A., MAGLARAS, L., HE, Y., YEVSEYEVA, I., BOITEN, E., COOK, A. & JANICKE, H. 2020. A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences,* 10**,** 3660.

ALOTAIBI, M., FURNELL, S. & CLARKE, N. Information security policies: a review of challenges and influencing factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016. IEEE, 352-358.

ALSHAIKH, M. 2020. Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security,* 98**,** 102003.

ALSHAIKH, M., MAYNARD, S. & AHMAD, A. 2020. Applying Social Marketing to Evaluate Current Security Education Training and Awareness Programs in Organisations. *Computers & Security***,** 102090.

ALSHARE, K., LANE, P. & LANE, M. 2018. Information security policy compliance: a higher education case study. *Information & Computer Security*.

BANDARA, I., IORAS, F. & MAHER, K. 2014. Cyber security concerns in e-learning education.

BEAUDIN, K. 2015. College and university data breaches: Regulating higher education cybersecurity under state and federal law. *JC & UL,* 41**,** 657.

BOVILL, C. 2020. Co-creation in learning and teaching: the case for a whole-class approach in higher education. *Higher Education,* 79**,** 1023-1037.

BRUMFIELD, J. 2016. *Verizon's 2016 data breach investigations report finds cybercriminals are exploiting human nature* [Online]. Verizon. Available: http://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-0 [Accessed 31/10 2020].

BULGURCU, B., CAVUSOGLU, H. & BENBASAT, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly,* 34**,** 523-548.

BUTLER-HENDERSON, K. & CRAWFORD, J. 2020. A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity. *Computers & Education***,** 104024.

CAMPBELL, S. 2020. *Cybersecurity in Higher Education: Problems and Solutions* [Online]. Toptal. Available: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education [Accessed 1/11 2020].

CAPRARA, G., ALESSANDRI, G. & CAPRARA, M. 2019. Associations of positive orientation with health and psychosocial adaptation: A review of findings and perspectives. *Asian Journal of Social Psychology,* 22**,** 126-132.

CHALLENER, C. 2020. Can Vaccine Development Be Safely Accelerated?

CHAN, H. & MUBARAK, S. 2012. Significance of information security awareness in the higher education sector. *International Journal of Computer Applications,* 60.

CHAPMAN, J. 2019. How safe is your data? Cyber-security in higher education. *HEPI Policy Note,* 12**,** 1-6.

COFFEY, J., HAVEARD, M. & GOLDING, G. 2018. A case study in the implementation of a human-centric higher education cybersecurity program. *Journal of Cybersecurity Education, Research and Practice,* 2018**,** 4.

CORONADO, A. 2012. Corporate Computer and Network Security. Taylor & Francis.

CORRADINI, I. 2020. Security: Human Nature and Behaviour. *Building a Cybersecurity Culture in Organizations.* Springer.

DA VEIGA, A., ASTAKHOVA, L., BOTHA, A. & HERSELMAN, M. 2020, p.19. Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security,* 92**,** 101713.

DA VEIGA, A. & ELOFF, J. 2010. A framework and assessment instrument for information security culture. *Computers & Security,* 29**,** 196-207.

DE KOCK, R. & FUTCHER, L. Mobile device usage in higher education institutions in South Africa. 2016 Information Security for South Africa (ISSA), 2016. IEEE, 27-34.

DELL'ACQUA, S. eLearning in Higher Education and Excellence: When, Where and How It Is Possible. Conference Proceedings. The Future of Education, 2017. libreriauniversitaria. it Edizioni, 47.

DODEL, M. & MESCH, G. 2017. Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human behavior,* 68**,** 359-367.

DONALDS, C. & OSEI-BRYSON, K.-M. 2020. Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management,* 51**,** 102056.

DONALDS, C. & OSEI-BRYSON, K. Exploring the impacts of individual styles on security compliance behavior: A preliminary analysis. SIG ICT in Global Development, 10th Annual Pre-ICIS Workshop, Seoul, Korea, 2017.

ENESCU, S. The concept of cybersecurity culture. The Fourth Annual Conference of the National Defence College Romania in the New International Security Dynamics, 2019. " Carol I" National Defence University Publishing House, 176-191.

ETZIONI, A. 1975. A comprehensive analysis of complex organizations (rev. ed.). *New York, NY: Free Press. Evans, G.(2004). The environment of childhood poverty. American Psychologist,* 59**,** 77-92.

EVANS, M., MAGLARAS, L., HE, Y. & JANICKE, H. 2016. Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks,* 9**,** 4667-4679.

FAY, J. 2018. Contemporary Security Management Fourth Edition. Elsevier Ltd.

FERREIRA, A. Why ransomware needs a human touch. 2018 International Carnahan Conference on Security Technology (ICCST), 2018. IEEE, 1-5.

FISHBEIN, M. & AJZEN, I. 1977. Belief, attitude, intention, and behavior: An introduction to theory and research.

FURFARO, A., GALLO, T., GARRO, A., SACCÀ, D. & TUNDIS, A. 2018. Cybersecurity compliance analysis as a service: Requirements specification and application scenarios. *Concurrency and Computation: Practice and Experience,* 30**,** e4289.

GALE, T. & PARKER, S. 2013. Widening participation in Australia in higher education.

GARTNER, I. 2013. *"Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes"* [Online]. Available: http://www.gartner.com/newsroom/id!2466615 [Accessed 31/10 2020].

GEARHART, G., ABBIATTI, M. & MILLER, M. 2019. Higher education's cyber security: Leadership issues, challenges and the future. *International Journal on New Trends in Education and Their Implications,* 10**,** 11-18.

GRAMA, J. 2014. Just in Time Research: Data Breaches in Higher Education. *EDUCAUSE*.

GREENING, T. 1996. Ask and ye shall receive: a study in "social engineering". *ACM SIGSAC Review,* 14**,** 8-14.

GUITTON, C. 2017. *Inside the Enemy's Computer: Identifying Cyber-attackers*, Oxford University Press.

HE, W. & ZHANG, Z. 2019. Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce,* 29**,** 249-257.

HERRERA, A., RON, M. & RABADÃO, C. National cyber-security policies oriented to BYOD (bring your own device): Systematic review. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), 2017. IEEE, 1-4.

HINA, S. & DOMINIC, P. 2018. Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*.

IBRAHIM, H., KARABATAK, S. & ABDULLAHI, A. A Study on Cybersecurity Challenges in E-learning and Database Management System. 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020. IEEE, 1-5.

IWASOKUN, G., AKINYOKUN, O. & OMOMULE, T. Design of E-Invigilation Framework Using Multi-Modal Biometrics. 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 2019. IEEE, 1-6.

JERVIS, R. 1978. Deterrence theory revisited. *World Pol.,* 31**,** 289.

JOSHI, C. & SINGH, U. 2017. Information security risks management framework–A step towards mitigating security risks in university network. *Journal of Information Security and Applications,* 35**,** 128-137.

JOSHI, C. & SINGH, U. 2017, p.129. Information security risks management framework–A step towards mitigating security risks in university network. *Journal of Information Security and Applications,* 35**,** 128-137.

KASPERSKY, G. 2013. Global Corporate IT Security Risks: 2013. *Kaspersky Lab: Moscow, Russia*.

KETAB, S., CLARKE, N. & DOWLAND, P. The value of the biometrics in invigilated e-assessments. Conference Paper, 2016.

KIM, B., KIM, K., HONG, S. & OH, S. 2017a. Development of cyber information security education and training system. *Multimedia Tools and Applications,* 76**,** 6051-6064.

KIM, H., SON, H., KIM, J. & KANG, H. 2017b. Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants. *Reliability Engineering & System Safety,* 167**,** 290-301.

KOWTKO, M. Biometric authentication for older adults. IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014, 2014. IEEE, 1-6.

KUPCEWICZ, E., SZYPULSKA, A. & DOBOSZYŃSKA, A. 2019. Positive Orientation as a Predictor of Health Behavior during Chronic Diseases. *International journal of environmental research and public health,* 16**,** 3408.

LANE, R. 2020. Sarah Gilbert: carving a path towards a COVID-19 vaccine. *Lancet (London, England),* 395**,** 1247.

LI, L., HE, W., XU, L., ASH, I., ANWAR, M. & YUAN, X. 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management,* 45**,** 13-24.

LIANG, H. & XUE, Y. 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems,* 11**,** 1.

LUNENBURG, F. 2012. Compliance theory and organizational effectiveness. *International journal of scholarly academic intellectual diversity,* 14**,** 1-4.

MAGLARAS, L., KIM, K.-H., JANICKE, H., FERRAG, M., RALLIS, S., FRAGKOU, P., MAGLARAS, A. & CRUZ, T. 2018. Cyber security of critical infrastructures. *Ict Express,* 4**,** 42-45.

MAHASE, E. 2020. Covid-19: Oxford team begins vaccine trials in Brazil and South Africa to determine efficacy. British Medical Journal Publishing Group.

MAKONI, M. 2020. COVID-19 vaccine trials in Africa. *The Lancet Respiratory Medicine,* 8**,** e79-e80.

MARTENS, M., DE WOLF, R. & DE MAREZ, L. 2019. Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior,* 92**,** 139-150.

MIRAJA, B., PERSADA, S., PRASETYO, Y., BELGIAWAN, P. & REDI, A. 2019. Applying Protection Motivation Theory to understand generation z students intention to comply with educational software anti piracy law. *International Journal of Emerging Technologies in Learning (iJET),* 14**,** 39-52.

MUNIANDY, L., MUNIANDY, B. & SAMSUDIN, Z. 2017. Cyber Security Behaviour among Higher Education Students in Malaysia. *J. Inf. Assur. Cyber Secur,* 2017**,** 1-13.

MURPHY, M. 2020. COVID-19 and emergency eLearning: Consequences of the securitization of higher education for post-pandemic pedagogy. *Contemporary Security Policy***,** 1-14.

POREMBA, S. 2014. *5 Higher Education Information Security Threats You Should Know Before Your Child Leaves For College* [Online]. Forbes. Available: https://www.forbes.com/sites/sungardas/2014/11/05/5-higher-education-information-security-threats-you-should-know-before-your-child-leaves-for-college/#2549e1e91239 [Accessed 21/10 2020].

RAJAB, M. & EYDGAHI, A. 2019. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security,* 80**,** 211-223.

REDDY, D. & RAO, V. 2016. Cybersecurity skills: The moderating role in the relationship between cybersecurity awareness and compliance.

RJAIBI, N., RABAI, L. B., AISSA, A. & LOUADI, M. 2012. Cyber security measurement in depth for e-learning systems. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),* 2**,** 107-120.

ROGERS, R. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology,* 91**,** 93-114.

ROGERS, R. 1983. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook***,** 153-176.

ROSCORLA, T. 2016. *8 Cybersecurity Challenges Facing Higher Education* [Online]. Centre for Digital Education. Available: https://www.govtech.com/education/higher-ed/8-Cybersecurity-Challenges-Facing-Higher-Education.html [Accessed 1/11 2020].

ROSENSTOCK, I. 1960. What research in motivation suggests for public health. *American Journal of Public Health and the Nations Health,* 50**,** 295-302.

SABBAH, Y. 2017. Security of Online Examinations. *Data Analytics and Decision Support for Cybersecurity.* Springer.

SAFA, N., VON SOLMS, R. & FURNELL, S. 2016, p.2. Information security policy compliance model in organizations. *computers & security,* 56**,** 70-82.

SAFAR, A. 2018. BYOD in Higher Education: A Case Study of Kuwait University. *Journal of Educators Online,* 15**,** n2.

SAMMONS, J. & CROSS, M. 2017. Cybercrime. *J. Sammons, & M. Cross, The Basics of Cyber Safety. Amsterdam: Elsevier***,** 87-116.

SANDERS, G., UPADHYAYA, S. & WANG, X. 2019. Inside the insider. *IEEE Engineering Management Review,* 47**,** 84-91.

SCHEIN, E. 1996. Three cultures of management: The key to organizational learning. *Sloan management review,* 38**,** 9-20.

SCHEIN, E. 1996, p.11. Three cultures of management: The key to organizational learning. *Sloan management review,* 38**,** 9-20.

SINGAR, A. & AKHILESH, K. 2020. Role of Cyber-security in Higher Education. *Smart Technologies.* Springer.

SINGH, M., CHAN, C. & ZULKEFLI, Z. 2017. Security and privacy risks awareness for bring your own device (BYOD) paradigm. *International Journal of Advanced Computer Science and Applications,* 8**,** 53-62.

SPEARS, J. & BARKI, H. 2010, p.518. User participation in information systems security risk management. *MIS quarterly***,** 503-522.

SUCIU, G., ANWAR, M. & ISTRATE, C. The 15th International Scientific Conference eLearning and Software for Education Bucharest, April 11-12, 2019.

SUSSKIND, N. 2014. Cybersecurity compliance and risk management strategies: What directors, officers, and managers need to know. *NYUJL & Bus.,* 11**,** 573.

THE IDENTITY THEFT RESEARCH CENTRE. 2015. *Data Breaches* [Online]. Available: http://www.idtheftcenter.org/id-theft/data-breaches.html [Accessed 21/10 2020].

TISAK, M. 2019. The association of positive orientation with health and psychosocial adaption. *Asian Journal of Social Psychology,* 22**,** 140-142.

TOWBIN, R. 2019. *A Protection Motivation Theory Approach to Healthcare Cybersecurity: A Multiple Case Study.* Northcentral University.

TSAI, H., JIANG, M., ALHABASH, S., LAROSE, R., RIFON, N. & COTTEN, S. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security,* 59**,** 138-150.

TYLOR, E. 1958. [1871] Primitive Culture. *Boston: Estes and Lauriat*.

UDROIU, A. The cybersecurity of elearning platforms.  Conference proceedings of» eLearning and Software for Education «(eLSE), 2017. " Carol I" National Defence University Publishing House, 374-379.

VAN NIEKERK, J. & VON SOLMS, R. 2010. Information security culture: A management perspective. *Computers & security,* 29**,** 476-486.

VASILEIOU, I. & FURNELL, S. 2019. *Cybersecurity Education for Awareness and Compliance*, IGI Global.

VAYANSKY, I. & KUMAR, S. 2018. Phishing–challenges and solutions. *Computer Fraud & Security,* 2018**,** 15-20.

VERKIJIKA, S. 2018. Understanding smartphone security behaviors: an extension of the protection motivation theory with anticipated regret. *Computers & Security,* 77**,** 860-870.

VILLIKKA, D. 2018. Developing eLearning in Higher Education: A Critical Review.

WANG, A., LIANG, R., LIU, X., ZHANG, Y., CHEN, K. & LI, J. An inside look at IoT malware. International Conference on Industrial IoT Technologies and Applications, 2017. Springer, 176-186.

WARRICK, D., MILLIMAN, J. & FERGUSON, J. 2016. Building high performance cultures. *Organizational Dynamics,* 1**,** 64-70.

WEICK, K. E. 1976, p.1. Educational organizations as loosely coupled systems. *Administrative science quarterly***,** 1-19.

WHITE, J. 2017. *Impact of Protection Motivation Theory and General Deterrence Theory on the Behavioral Intention to Implement and Misuse Active Cyber Defense.* Capella University.

WINKLER, I. & GOMES, A. 2017. Chapter 5-how to hack computers. *Advanced Persistent Security***,** 41-46.

YEO, A., RAHIM, M. M. & MIRI, L. 2007. Understanding factors affecting success of information security risk assessment: the case of an Australian higher educational institution. *PACIS 2007 Proceedings***,** 74.

ZALAZNICK, M. 2013. Cyberattacks on the rise in higher education. *University Business*.

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

ZWILLING, M., LESJAK, D., NATEK, S., PHUSAVAT, K. & ANUSSORNNITISARN, P. How to deal with the awareness of cyber hazards and security in (Higher) education. Thriving on future education, industry, business and society. Proceedings of the Makelearn and TIIM International Conference, 2019. 433-439.