INCREASING SECURITY AWARENESS THROUGH LENSES OF CYBERSECURITY CULTURE

Alina ANDRONACHE[1,2]

Abstract: *Recent years have shown that the expansion of digitalisation implies an extension of what needs to be protected. While businesses invest in technology to protect against cyber-attacks, one of the top vulnerabilities remains the human element. This questions the centrality of the human role, something which often pertains cybersecurity policy, awareness, and training. Thus, it is imperative to understand if such approaches remain good strategies in protecting an organisation's information, assets, and people. To portray the current state, this paper takes into account prior developments in the study of Security Awareness and in addition, it explores the relevance of Cybersecurity Culture. Accordingly, the proposed approach aspires to delve into the value proposition of combining the two. The research determines that attaining organisational resilience differs on how employees perceive formal (awareness and cybersecurity policy) and informal rules (i.e., culture). Further research is required to determine the long-term effects in enriching Cybersecurity Awareness in context of Cybersecurity Culture.*

Keywords: *Security Awareness, Cybersecurity Culture, Behaviour; Organisational Resiliency*

1. Introduction

To date, it is known that cybercrimes are affecting the global digital economy, organisations, and users alike [1],[2]. This matter has been investigated in many ways hence digitalisation implies a paradox of progress meaning that apart from benefits, it has exposed organisations to cyber threats as well [3], [4], [5]. Equally, cybersecurity has been gaining importance due to its vital role in protecting the growing digital infrastructure [6], [7].

This has impacted on risk response, security technologies, practices, and staff behaviour. Consequently, even though the cybersecurity is an evolving approach, failures demonstrate that efficiency is yet to be achieved. Whilst businesses invest in technology to protect against cyber-attack, one of the top vulnerabilities remains, the human element [8]. Evidence shows that security remains a twofold socio-technical challenge [9]. Technology has become inadequate in ensuring security and so the human intervention is needed in order to render a stronger response to risk; hence threats are not constant and instead require continuous adjustment [10].

[1] Affiliation during research: Brunel University
[2] current affiliation: University of the West of Scotland, alina.andronache@partner.uws.ac.uk

The challenge in today's context is that humans are more exposed, more vulnerable, and less motivated [2], [4], [8], [11].

As a result, there are growing appeals for transforming existing human capabilities and behaviours to help avoid potential disruption of a potential cyberbreach [1], [12]. A common strategy used to address the human side in security was addressed by prior literature under security awareness. Antecedents of security awareness research are believed to have been driven by prescriptive factors such organisational context, standards, regulations, policy compliance requirements, and knowledge gap. Traditionally, awareness has been applied in isolation, acknowledged as insufficient in shaping organisational risk culture [13]. Taken together, these factors demonstrate that managing human behaviour and culture remains to be understood [14].

On the other hand, cybersecurity culture is found to influence organisational risk response performance. So, proper cultivation could protect an organisation against loss [15]. On these premises, factors such as employees' beliefs, values, and attitude in the context of cybersecurity can either be a risk or a foundation to increase organisational effectiveness and resiliency [5]. It is known that human error or lack of motivation can lead to substantial consequences for any organisation; and where the foundation is missing, the long term effects can be problematic. Fortunately, taking steps to instil good behaviour and getting prepared for a response to threats can diminish the extent of fragility and consequences.

This questions whether attaining organisational resilience varies on how employees perceive formal (i.e., awareness and cybersecurity policy) and informal factors (i.e., culture). To portray the current state, this paper takes into account prior developments in the study of Security Awareness and in addition, it explores the Cybersecurity Culture relevance.

Accordingly, the proposed approach aspires to delve into the value proposition of combining the two, enriching Cybersecurity Awareness through lenses of Cybersecurity Culture paradigm.

In the next section, an analysis of prior research is presented, followed by section 3, which covers the theoretical framework. Then, section 4 covers the research finding, and finally, the conclusion is presented in section 5.

2. Literature review

Exploiting human flaws has become a risk and this raises the need for a more secure culture of awareness to guide compliant behaviours [5], [16]. Recent years have shown that the risk of incidents materialising is higher, and so the human factor has become an essential component in maintaining secure organisation practice [17]. On the other hand, employee negligence, whether deliberate or not, push organisations to demand stronger security policy and requirements [18].

2.1 Security awareness

The scope of security awareness emerged as a necessity to prevent breaches and help employees understand the importance of maintaining vigilant practice towards threats [11]. Habitually, organisations develop policies, procedures, and guidelines to reduce human risks [19]. In the broad sense, under Cybersecurity Management, this is encouraged to be an acknowledgement in protecting confidentiality, integrity, and availability (CIA) of information assets [8].

2.2 Organisational culture

Culture is defined as being a meaningful way to sum up a range of behaviours. The conceptual background of culture pertains to dimensions of cognitive, behavioural, attitudinal, and normative aspects [17] along with other key components such as group ethics, communication, customs, assumptions, and responsibilities [19].

Thus, developing culture can be defined as a way to increase the level of awareness, norms, knowledge, attitudes, behaviours, intentions, beliefs, shared values and a framework of ethical behaviour [17].

2.3 Cybersecurity culture as a sub-culture

In the context of cybersecurity, having a good understanding of what culture implies could become a strong prevention strategy [20] and a way to positively influence individuals' perceptions and habits towards an expected behaviour [21]. The resulting behaviour would be a more robust capability and mindset to protect information, assets, and people.

A key argument is that every organisation is different, with their own goals, risk appetite, specific practices, context, and often other sub-cultures that can trigger different results. Consequently, solutions to tackle security culture vary and are often challenging for organisations. In turn, they need to adjust and find a suitable practice in line with the organisation's overall culture [22],[23].

It is essential to acknowledge that cybersecurity culture definition is still undefined, and even though it implies the influence of fast pacing digitalisation, it seems a concept that is hard to change [21]. One of the key reasons is that culture is not understood and more concerning subcultures within business units play an influential role on the overall results.

The importance of keeping peace with cybersecurity has been defined by some as risk culture; hence motivating employees to follow procedures or learn protective skills has been acknowledged as a people-centric approach. Conversely, this ingrains fear that insecurity has become a sensitive matter. Beyond the outlined approaches, having a good cybersecurity culture is not all about setting the right policies or procedures or checking effects. It implies setting strategic risk awareness beyond mitigating controls and getting collective responsibility that has a significant impact on daily activities [3], [24].

With increased hyperconnected environments, employees face higher risks of falling victim [25], [18] and as such, organisations which seek to nurture cybersecurity culture help avoid a siloed approach of awareness and instead encourage training that highly relies on competencies and knowledge. A cultural approach would consider the effects of a secure culture of awareness in the context of perceptions and respectively behaviour. [26] highlighted that culture within an organisation is a key determinant for cybersecurity management and its security performance. It was suggested that a security-aware culture indirectly guides the protection of information and assets as well as raising awareness of risk and responsibilities. We can draw the conclusion that the unwritten practice of sub-culture impacts at various levels across an organisation as well as on the secure course of actions [26].

This widens the debate of how every employee can affect cybersecurity practice and how non-conformance can lead to vulnerability, thus highlighting how important it is to start internally with a substantial baseline, adequate policies, and behaviour monitoring [9].

It is argued that that technical and administrative control within a cybersecurity function should imply a uniform and a confirmed approach. Beyond technology and documentation, the human aspect plays a significant role in the successful application of direction of expected controls and behaviours. Thus, how to tackle a cybersecurity culture strategically and instil employee's commitment remain a challenge [9].

This could be problematic because it emphasises dependencies on long-term effects on how security is collectively perceived in a workplace. A challenging problem is that it has a causal relationship to the overall organisational security posture. It is assumed that the cultivation of cybersecurity culture in an organisational environment could influence behaviour and attitudes among individuals [27]. Thus, cybersecurity culture aspires to tweak the group mindset towards consciousness of risk as well as adherence to internal policies [28]. In addition to generic research findings, literature emphasises different dimensions of culture that overlap, namely behaviour, perception, assumptions, knowledge, commitment, accountability, awareness, attitude, communication, norms, responsibilities, or values [27],[28],[29]. All the aforementioned are believed to be predisposed by artefacts (i.e., procedures) and exposed values (i.e., guidelines) [30]. Previous studies have based their criteria on selecting a few elements and have articulated either a top-down approach or mid-level approach (i.e., operational), while some other studies focused more on awareness and emphasised a bottom-up approach. On the other hand, organisational culture is expected to constantly strengthen ethical and appropriate risk appetite. To portray this further, the standardised approach of the institutional side of culture was even described as programmed behaviour, although it is most probably a pattern under a form of expected behaviour.[30],[31].

2.4 Linking practices

Cybersecurity culture is recommended to be anchored in organisation culture and objectives [32]. Marrying the two concepts (organisation culture and cybersecurity culture) has the potential to invoke an intuitive response, change mindset, instil a readiness concept to risk, and embed all this in daily practices. In addition, if this is supported with awareness and training, among many behavioural aspects, it could lead towards greater security culture. 'Cultivating' (i.e., preventing) and not 'prescribing' (i.e., curing) as security awareness does invokes an intentional acknowledgement that technology alone is not sufficient and everyone has a role to play. Nonetheless, literature shows such approaches have been overlooked in the past [26]. Whilst cyber risks are acknowledged [4], the cyber threats still contextualise, and the human side is still one top reason a cyber breach occurs. Nevertheless, no matter how sophisticated technology and policies are, the employees' behaviour is not always expected. Too many organisations security policies do not always work, or employees do not pay interest, whilst tending to underestimate cybersecurity risks. Given the two sides of a risk, the insider threats remain amongst top 'threat agent' of breaches, either if occurs intentional or unintentional [4].

However, on other occasions, some organisations lack sufficient resources or knowledge [5],[28],[33]. To support the message and prompt regular discussion about cybersecurity, organisations review policies and expect to drive uniform behaviour. Nonetheless, uncompliant habits or misuse remain a difficult aspect to control [5].

2.5 Factors

Identifying factors that affect users' intentions to comply with cybersecurity policies is of utmost importance. Tackling this issue has a sense of urgency due to its causal relationship to motivate, determine and drive the engagement of an employee. Policies are frequently cited as the ones that guide good behaviours and drive the norms but remain prescriptive in its nature.

Nevertheless, culture in context of awareness is suggested to be a moderator and a driver for effective implementation [34]. Thus, tackling human factors require finesse due to the systemic implications and the fact they change over time. Moreover, the problem pinpointed is that the literature lacks clarity around how to enhance cybersecurity behaviour and employees' threat perception without creating security fatigue [33]. Another aspect that came to the surface is that change behaviour could be superficially tacked as awareness if deployed through presentations, policies, or one-time action [35]. How an organisation can ensure consistent and long-term results remains dependent on the influence of key determinants as outlined in Table 1.1.

Table 1.1 Determinants of cybersecurity behaviour

Key determinants of security culture		
Strategic influence	Leadership	[5], [36]
	Policies	[9], [19], [28]
	Compliance and conformity	[38], [39]
	Sanctions	[5]
	Organisation culture	[37]
	Awareness and training	[28], [35], [49], [58
	Response cost	[45]
	Reward and Recognition	[4], [45]
	Engagement and communication	[11]
Social influence	Group or co-workers' behaviours	[5], [16], [17], [21]
	Security fatigue	[33]
	Cultural differences	[36], [37]
	Group habits	[5]
Individuals' perception	Vulnerability and probability	[21]
	Efficacy in dealing with security threats	[4], [45]
	Experience/awareness	[53]
	Personality and values	[27], [46]
External rules	Regulation	[40]

Nonetheless, as observed in Table 1.1., there are key determinants which can play a role in influencing behaviour when a threat occurs. To put it another way, cultural variables can both enhance or impede behavior dependent on the interrelationship bewtwen variables [36]. For example, cultural differences are variables that can affect managerial control as well as individual evolution and input. That is to say that strategic decisions must acknowledge these variables and interrelated effects [36].

Practically, at the basis of a projected compliant behaviour are policies, procedures and guidelines. However, these findings suggests that the missing link is that each individual and organisation are unique. The organisation's vision and mission define its main goal, whilst people bring their own perspectives. Thus, approaching cybersecurity as an instrument [24] can help determine suitable patterns and approaches for awareness [28].

Notably, an organisation's core values, norms, traditions or philosophy may possibly provide understanding how risks are understood, addressed, and mitigated [37].

3 Theoretical lenses

As literature showed that culture incorporates strategic influence, social influence, individuals influence and external influence, the debates about what build good security culture remain unanswered. [33] emphasise that despite significant theoretical contribution, translating such approaches in practice might not always successfully influence risky behaviour.

To combine the cognitive variables, a model that combines variables of Protection Motivation Theory, and Institutional Theory is presented in Figure 1.1. and includes:

Institutional Theory (ITT) ─ considers the value, normative rules, legitimacy, beliefs, principles, practices, structures, processes, obligations, behaviour, ethics, and social systems establishing command and assigning responsibilities. The external rules, also known as 'rationalised myths' (traditional conformity) can influence an organisation through isomorphism [38], [39]. There are various interpretations regarding institutional views, hence the response of academics focusing on various aspects. Institutional Theory posits how mimetic, coercive, and normative pressures affect the interdepartmental linkage compliance on daily work practices [40]; including variables such as External Rules, Coercive Isomorphism, Normative Isomorphism, and Homogeneity Rules Influence.

- Coercive isomorphism describes to the informal and formal pressures an organisation gets from several sources and the resultant organisational behaviour [41]. The concept of coerciveness is about external action and the rendered effect, comparable to other organisations. Most often seen as a recognised as a professional expectation in the form of a norm, obligation, moral, standard or duty [41]. This can include, for example, the effect of peer organisations, competitors, regulatory bodies [40], political impact, control from supervisory authorities, and economic factors [42], among many others.
- Normative isomorphism reports the collective effect of professionalisation [42] and concentrates on normative social expectations to control specialist positions categorisations [39] that order responsibilities. Some examples of normative influences are professional interactions at events (e.g., conferences, professional associations meetings) among specialists [43].
- Mimetic isomorphism questions the cognitive influence of others' success to be emulated and taken granted as a solution to thrive and be recognised as legitimate [38], [42]. It analyses what leads to specific organisational decisions taken in specific practices [39] mechanism or structures [41].

Protection Motivation Theory (PMT) ─ explores the cognitive process of an individual when it is exposed to a threat [44]. The theory considers an individual

behaviour under variables such as motivation, probability, severity, vulnerability, response efficacy, self-efficacy, response cost, reward [45]. The utility of this theory is to understand to what extent threat perception triggers a positive or negative response [4]. The likelihood of such variables to materialise in predicting secure behaviour and policy compliance are incremental when implementing security measures.

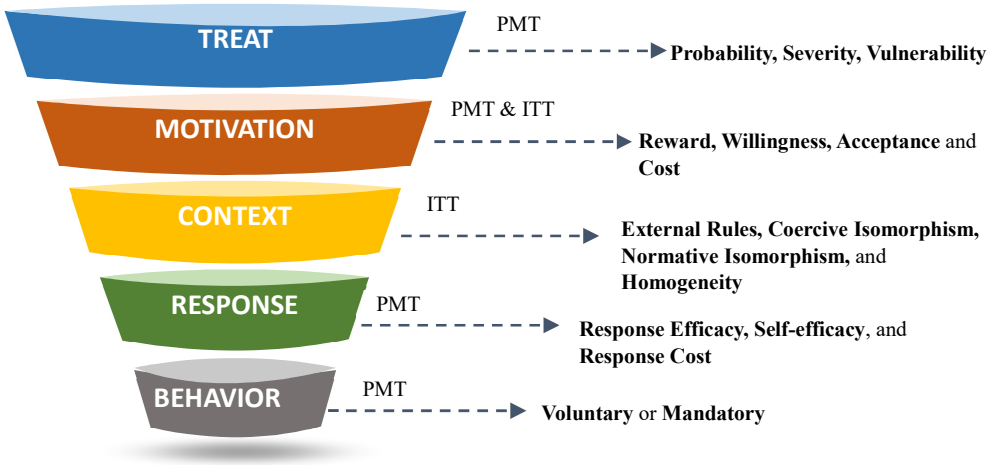

Figure 1.1 Cybersecurity culture model

As seen above, the two theories are funneling down a social system that subconsciously perceives through cognitive variables, processes, constructs and relationships that influence response and behaviours [46]. Security culture relationship with cybersecurity management is unclear within literature [47]. On the other hand, the effects of security awareness on security culture seem evident yet only help with segregated understanding and some degree of responsibility [45], [47].

This research thus proposes to include cultural aspects of cognitive behavioural responses (Protection Motivation Theory) and conformity (Institutional Theory) to security awareness programmes, so it can position an organisation to have better resilience. Organisational culture, on the other hand, is unique to every organisation and could have multiple layers from prescriptive rules to ideal behaviours. Breaking this down, the way organisations plan to mitigate risk can be expanded by understanding that norms, behaviours, attitudes and beliefs can sustain the performance of an organisation holistically. It can lead to a multi-layered approach that implies lenses of psychology, change management, and strategic management. Fostering a security mindset through the view of organisational culture, avoids limitation in implementing measures, and instead of

placing focus on the procedural side, it could expand on a broader view, incorporating perception and enculturation.

4. Data analysis and results

This research was exploratory and interpretative in nature to investigate challenges in the financial industry. The paper utilised qualitative data from 26 semi-structured interviews to investigate if cybersecurity awareness remains a sufficient strategy in protecting an organisation resiliency.

The Human factor is identified as a category that inhibits implementation relates to people-centric rapport, meaning that 30.95% of respondents reported concerns related to the ability to recognise problems and avoid human error. This finding is in line with prior research which reported that people-related risks are a common challenge for organisations [48].

A breakdown of human factors is detailed below:

(1) Skills deficiencies (13.04%) - investment in skills and knowledge of employees was reported to be another factor that affects compliance behaviour.

(2) Lack of awareness (17.91%) - investment in skills and knowledge of employees is a factor mentioned. The literature indicates that security awareness is a component of culture bearing influence over organisational effectiveness [49].

When questioning why cybersecurity controls fail, the evidence from interviews highlights that many inhibitors are people-centric and refers to human capabilities. Briefly, the respondents emphasised that there could occur a domino effect if skills deficiencies and lack of awareness are missing. The concerning result is that these two people-centric inhibitors it can affect an organisation ability to deploy suitable response. Given these facts, it is acknowledged that this can leads to difficulties in reaching effectiveness and cybersecurity maturity. Accordingly, lack of skills or awareness can deter appropriate lines of responsibility, accountability, and knowledge, all of which are essential element of cybersecurity [50].

Governance factor

(3) Inappropriate governance was pinpointed by 10.14% of respondents as being an inhibitor. Failure to understand cultural context and governance need was indicated by respondents as being detrimental for organisations. For instance, poor governance it can be hindering policy applicability, disengage business units, or even have contradictory interpretations for risk. In addition, unclear accountability (responsibility) sustains deficiencies. The readiness to overcome governance weaknesses depends on the organisation's acceptance to change, the cost involved, and the availability of resources [51], [52].

(4) Lack of management commitment (11.59%) in translating how strategy aligns to security culture makes it difficult to understand how prioritise risk.

Inadvertently, respondents believe executive ignorance it can imply a spreadable effect on employee behaviour, resistance to change and/or non-acceptance.

(5) Cultural deficiencies factor (11.59%) was found to be one of many components that could impact an organisation security organisational posture. The findings indicate concerns of respondents in this regard. Traditionally, within the literature the risk culture concept is a compound of values, past experiences, philosophy, and behaviours [53]; in addition, same author specifies that materialise in a form of pattern of conduct [53]. Detailed examination of risk culture showed that culture deficiencies are predictable and define repeatable behaviour. Much of the literature identified internal values, beliefs, knowledge, and understanding as number of limitations. Therefore, most scholars suggests that that risk culture involves two main strands: (1) organisational attitude and (2) people's behaviour under risk pressure. Accordingly, other findings show that culture deficiencies could be influenced by key elements such as leadership, strategy, adaptability, coordination, and relationship [54], [55].

Resource factor

(6) Cost - 11.94% agreed that the cost of security awareness implementation is an inhibitor. One noticeable aspect is that the intrinsic investment's purpose is to avoid cost instead of producing income [57]. The literature suggests that many organisations have challenges when intending to invest due to such perception in the latency of results [57].

To summarise the results, the findings give clarity around the fact that multiple elements interrelate. Interestingly, education, awareness, skills set, and communication were perceived as different by respondents; This result is somewhat the opposite of literature which shows that all of the above compound elements of culture. The findings also offer insight into the following:

- Cybersecurity culture depends on governance (33.32%), people (30.95%) and resource (11.94%). All interrelate, and play a significant role, thus ingraining cybersecurity culture means adopting a bottom-up approach (resources, people, technology and governance) [5]. Prioritising its effort as a community and increase resilience also means delivering security awareness, and additionally considering cultural characteristics and pain points as a whole. It fosters an environment that encourages compliance behaviours as an informal measure.

- Where cultural deficiencies remain undressed, the security awareness is unsustainable to proactively support compliant behaviour.

- Security awareness programmes are still yet to mature whilst other organisations lack a formal programme. Likewise, within the research field is believed that has not reach maturity [58].

These empirical results and the reported findings within the literature, suggest that planning and instilling a risk culture requires consideration of knowledge, behaviour, and culture characteristics. The Researcher concludes that if the concept of cybersecurity culture is embraced within a Security Awareness programme, it can lead to relevant, understandable, and personalised content and delivery which can motivate compliant behaviours (conformity) through cognitive lenses.

4. Conclusion

The research proposed to validate if Security Awareness is a sufficient strategy in current context in order to determine what other factors can help an organisation limit human-related risk. Poor behaviours demand a change of mindset in order to keep pace with technological transformations and implications whilst complacency reigns.

By answering the research question, this paper validates that Security Awareness strength can be increased through the lenses of culture concept. Additionally, this paper contributes by challenging the conceptual shift of cybersecurity awareness towards a more integrative approach. This supports the idea that both domains, culture and awareness share common dependencies and interdependence. For instance, they rely on expanding knowledge as well enforcing good practice.

Overall, this paper expands on challenges posed by how security culture is perceived due to various interpretations and consequential inconsistent outcomes. It thus proposes to include cultural aspects of cognitive behavioural responses (Protection Motivation Theory) and conformity (Institutional Theory) to security awareness programmes, so it can position an organisation to have better resilience.

Considering the pace at which digitalisation evolves, the findings are relevant for the time of writing this paper. Further research exploration is required to determine the long-term effects and implications of the cybersecurity culture paradigm. It is recommended that future research should imply more considerable empirical evidence that might determine further insight into potential trends and developments.

Another avenue of further research could be the effects of fostering cybersecurity culture across organisations through formal programmes in order to determine their sustainability in practice.

5. References

[1] Singh Lallie, Harjinder, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. *Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic*, 2020;

[2] Strupczewski, *Grzegorz. Defining cyber risk*. Safety science 135, 105143, 2021;

[3] Pupillo, Lorenzo. *EU Cybersecurity and the Paradox of Progress*. CEPS Policy Insights No 2018/06, 2018;

[4] Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. *Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior*. International Journal of Information Management 45, 2019;

[5] Huang, Keman, and Keri Pearlson. *For what technology can't fix: Building a model of organizational cybersecurity culture*. In Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019;

[6] Rahman, M., and Shannon E. *Donahue. Convergence of corporate and information security*. arXiv preprint arXiv:1002.1950, 2010;

[7] Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. *Defining cybersecurity.* Technology Innovation Management Review 4, no. 10, 2014.

[8] Khando, Khando, Shang Gao, Sirajul M. Islam, and Ali Salman. *nEnhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review*. Computers & Security, 102267, 2021;

[9] McEvoy, Thomas Richard, and Stewart James Kowalski. *Deriving Cyber Security Risks from Human and Organizational Factors–A Socio-technical Approach*. Complex Systems Informatics and Modeling Quarterly 18, 47-64, 2019;

[10] Tang, Mincong, and Tao Zhang. *The impacts of organizational culture on information security culture: a case study*. Information Technology and Management 17, no. 2, 179-186, 2016;

[11] Hadlington, Lee, Jens Binder, and Natalia Stanulewicz. *Exploring role of moral disengagement and counterproductive work behaviours in information security awareness*. Computers in Human Behavior 114,106557, 2021;

[12] Qureshi, Shahana Gajala, and Shishir Kumar Shandilya. *Advances in Cyber Security Paradigm: A Review.* In International Conference on Hybrid Intelligent Systems, pp. 268-276. Springer, Cham, 2019;

[13] Dojkovski, Sneza, Sharman Lichtenstein, and Matthew J. Warren. *Fostering information security culture in small and medium size enterprises: an interpretive study in Australia*, 2007;

[14] Hassan, Noor Hafizah, and Zuraini Ismail. *A conceptual model for investigating factors influencing information security culture in healthcare environment*. Procedia-Social and Behavioral Sciences 65, 1007-1012, 2012;

[15] Veiga, A. Da, and Jan HP Eloff. *An information security governance framework. Information systems management.* 24, no. 4, 361-372, 2007;

[16] Gangire, Yotamu, A. D. Veiga and M. Herselman. *Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory.* HAISA, 2020;

[17] Orehek, Špela, and Gregor Petrič. *A systematic review of scales for measuring information security culture.* Information & Computer Security, 2020;

[18] Ali, Rao Faizan, P. D. D. Dominic, Syed Emad Azhar Ali, Mobashar Rehman, and Abid Sohail. *Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance*. Applied Sciences 11, no. 8, 3383, 2021;

[19] Georgiadou, Anna, Spiros Mouzakitis, and Dimitris Askounis. *Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis.* International Journal of Network Security & Its Applications (IJNSA) Vol 13, 2021;

[20] Corradini, Isabella, and Enrico Nardelli. *Building organizational risk culture in cyber security: the role of human factors*. In International Conference on Applied Human Factors and Ergonomics, pp. 193-202. Springer, Cham, 2018;

[21] Da Veiga, Adele, Liudmila V. Astakhova, Adéle Botha, and Marlien Herselman. *Defining organisational information security culture—Perspectives from academia and industry*. Computers & Security 92, 101713, 2020;

[22] Hanson, E. Mark. *School management and contingency theory: An emerging perspective*. Educational Administration Quarterly 15, no. 2, 98-116, 1979;

[23] Rubino, Michele. *A comparison of the main ERM frameworks: how limitations and weaknesses can be overcome implementing IT governance*. International Journal of Business and Management 13, no. 12, 203-214, 2018;

[24] Da Veiga, Adéle. *A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument*. In 2016 SAI Computing Conference (SAI), pp. 1006-1015. IEEE, 2016;

[25] Ramluckan, Trishana, and Brett van Niekerkand Isabel Martins. *A Change Management Perspective to Implementing a Cyber Security Culture*. In ECCWS 2020 20th European Conference on Cyber Warfare and Security, p. 442. Academic Conferences and publishing limited, 2020;

[26] AlHogail, Areej, and Abdulrahman Mirza. *Information security culture: a definition and a literature review.* In 2014 World Congress on Computer Applications and Information Systems (WCCAIS), pp. 1-7. IEEE, 2014;

[27] Nasir, Akhyari, Ruzaini Abdullah Arshah, Mohd Rashid Ab Hamid, and Syahrul Fahmy. *An analysis on the dimensions of information security culture concept: A review*. Journal of Information Security and Applications 44, 12-22, 2019;

[28] ENISA. *Cyber Security Culture in organisations*. Available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations, 2020;

[29] Korovessis, Peter, Steven Furnell, Maria Papadaki, and Paul Haskell-Dowland. *A toolkit approach to information security awareness and*

education. Journal of Cybersecurity Education, Research and Practice, no. 2, 2017;

[30] Von Solms, Rossouw, and Johan Van Niekerk. *From information security to cyber security. computers & security* 38, 97-102, 2013;

[31] Al Sabbagh, Bilal, Marihan Ameen, Tove Wätterstam, and Stewart Kowalski. *A prototype For HI 2 Ping information security culture and awareness training.* In 2012 International Conference on E-Learning and E-Technologies in Education (ICEEE), pp. 32-36. IEEE, 2012;

[32] Sabillon, Regner, Jordi Serra-Ruiz, and Victor Cavaller. *An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada.* Journal of Cases on Information Technology (JCIT) 21, no. 3, 26-39, 2019;

[33] Bada, Maria, and Jason RC Nurse. *Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs).* Information & Computer Security, 2019;

[34] Shao, Zhen. *Interaction effect of strategic leadership behaviors and organizational culture on IS-Business strategic alignment and Enterprise Systems assimilation.* International Journal of Information Management 44, 96-108, 2019;

[35] Ramirez, Robert, and Nazli Choucri. *Improving interdisciplinary communication with standardized cyber security terminology: a literature review*. IEEE Access 4, 2216-2243, 2016;

[36] Tosi Jr, Henry L., and John W. Slocum Jr. *Contingency theory: Some suggested directions*. Journal of management 10, no. 1, 9-26, 1984;

[37] RIMS. *Transitioning to enterprise risk management.* Available at: https://rims.org/RiskKnowledge/RISKKnowledgeDocs/transitioningtoerm_4192017_122623.pdf, 2014;

[38] van der Velden, Claus. *Organization Theory: Tension and Change*, 332-336, 2001;

[39] Lawrence, T. B. and Shadnam, M. *Institutional Theory*. In: Donsbach, Wolfgang, (ed.) The International Encyclopedia of Communication. Blackwell Publishers, Oxford, pp. 2288-2293. ISBN 978-1-4051-3199-5, 2008;

[40] Teo, Hock-Hai, Kwok Kee Wei, and Izak Benbasat. *Predicting intention to adopt interorganizational linkages: An institutional perspective*. MIS quarterly, 19-49, 2003;

[41] Daft, R. L., Murphy, J. and Willmott, H. *Organization theory and design: An international perspective.* 2nd edn. London, United Kingdom: Cengage Learning EMEA, 2014;

[42] Hsu, Carol, Jae-Nam Lee, and Detmar W. Straub. *Institutional influences on information systems security innovations.* Information systems research, 23, no. 3-part-2, 918-939, 2021;

[43] Hu, Qing, Paul Hart, and Donna Cooke. *The role of external and internal influences on information systems security–a neo-institutional perspective*. The Journal of Strategic Information Systems 16, no. 2, 153-172, 2007;

[44] Mills, Annette, and Natasha Sahi. *An empirical study of home user intentions towards computer security*. In Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019;

[45] Haag, Steffi, Mikko Siponen, and Fufan Liu. *Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future*. ACM SIGMIS Database: the DATABASE for Advances in Information Systems 52, no. 2, 25-67, 2021;

[46] Sommestad, Teodor, Henrik Karlzén, and Jonas Hallberg. *A meta-analysis of studies on protection motivation theory and information security behaviour*. International Journal of Information Security and Privacy (IJISP) 9, no. 1, 26-46, 2015;

[47] Chen, Y. Ramamurthy, and Kuang-Wei Wen. *Impacts of comprehensive information security programs on information security culture.* Journal of Computer Information Systems 55, no. 3, 11-19, 2015;

[48] Blacker, Keith, and Patrick McConnell. *People Risk Management: A practical approach to managing the human factors that could harm your business*. Kogan Page Publishers, 2015;

[49] Braumann, Evelyn C. *Analyzing the role of risk awareness in enterprise risk management.* Journal of Management Accounting Research 30, no. 2, 241-268, 2018;

[50] Majdalawieh, M. and Gammack, J. *An Integrated Approach to Enterprise Risk: Building a Multidimensional Risk Management Strategy for the Enterprise*, International Journal of Scientific Research and Innovative Technology, 4(2), pp. 95-114, 2017;

[51] Prioteasa, Adina-Liliana, and Carmen Nadia CIOCOIU. *Challenges in implementing risk management: a review of the literature*. In Proceedings of the INTERNATIONAL MANAGEMENT CONFERENCE, vol. 11, no. 1, pp. 972-980. Faculty of Management, Academy of Economic Studies, Bucharest, Romania, 2017;

[52] Merhi, Mohammad I., and Punit Ahluwalia. *Examining the impact of deterrence factors and norms on resistance to information systems security*. Computers in Human Behavior 92 (2019): 37-46;

[53] Carretta, Alessandro, Vincenzo Farina, and Paola Schwizer. *Risk culture and banking supervision*. Journal of Financial Regulation and Compliance (2017);

[54] Smit, Jakobus. *The Relationship between Organizational Culture and Innovation. In 25th Annual Conference of the International Information Management Association* (IIMA), 2014;

[55] Silvius, AJ Gilbert, Jakobus Smit, and Heidy Driessen. *The Relationship between Organizational Culture and the Alignment of Business and IT*. In AMCIS, p. 186, 2010;

[56] Power, Michael, Simon Ashby, and Tommaso Palermo. *Risk culture in financial organisations: A research report*. CARR-Analysis of Risk and Regulation, 2013;

[57] Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. *Empirical evidence on the determinants of cybersecurity investments in private sector firms*. Journal of Information Security 9, no. 02, 133, 2018;

[58] Gjertsen, Eyvind Garder B., Erlend Andreas Gjære, Maria Bartnes, and Waldo Rocha Flores. *Gamification of Information Security Awareness and Training*. In ICISSP, pp. 59-70, 2017.