International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

Check for updates

A methodological framework for fostering cybersecurity mindsets and behaviour

Austin Oguejiofor Amaechi *

Department of Information and Communication Technology, The ICT University, Cameroon.

International Journal of Science and Research Archive, 2025, 15(02), 1799–1810

Publication history: Received on 21 April 2025; revised on 27 May 2025; accepted on 30 May 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.2.1659

Abstract

The continuously growing attack surfaces and artificial intelligence-enabled attacks have increased the overwhelming nature of the cybersecurity challenge. The result is that to some organizations, no amount of preparedness can guarantee immunity from cyber-attacks. Cybersecurity preparedness is an ongoing process and incentivizing the right behaviour is an essential characteristic of a human-centered whole-of-enterprise approach to cybersecurity. While there are many techniques developed to improve and understand cybersecurity decision making, there is a lack of design methodologies to allow cybersecurity design teams to systematically tackles creation of conditions that stimulate and sustain desired level of cybersecurity mindsets in an organization. To bridge this gap, we propose the Human Centered Methodological Cybersecurity (HCMC) framework to address this gap. This human-centered approach is based on the fundamental premise that the unpredictable nature of human behaviour and actions make humans an important element and enabler of the level of cybersecurity. Fostering sustainable cybersecurity mindset is a design problem. This study uses framework formulated from the Design Science Research (DSR) approach. The evaluation of the framework was done using different groups of cybersecurity experts, professionals, and general users. HCMC enables cybersecurity teams to surface and explore complex cybersecurity behaviour fostering issues specific to their organization and stimulate thinking from the perspective of different groups of stakeholders systematically, which might potentially be overlooked otherwise.

Keywords: Cybersecurity Behaviour; Cybersecurity Influence; Behaviour Change; Cybersecurity Awareness; Shared Responsibility

1. Introduction

Cybersecurity is a complex dynamic field, and the production of cybersecurity is a knowledge-intensive task [1]. According to National Initiative for Cybersecurity Careers and Studies definition, “cybersecurity is the activity or process, ability, or capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation”. In another definition, Schiliro said that “cybersecurity is the collection and concerting of resources including personnel and infrastructure, structures, and processes to protect networks and cyber enabled computer systems from events that compromise the integrity and interfere with property rights, resulting in some extent of loss” [2]. Organizations are under continuous pressure to update existing and acquire novel knowledge to keep up with the evolution of cyber-threats [3]. According to a 2023 study, the heightened threat landscape has engendered a mounting interest in organisations ensuring that staff are compliant with cybersecurity procedures and practices [4]. The effectiveness of a security program requires ongoing voluntary compliance from cybersecurity users; meaning that it is important that the organizational and human factors that motivate self-regulated maintenance of cybersecurity compliance are identified and included in any security training and communication program [5]. In addition, contemporary users are prone to reject cybersecurity systems that offer an inadequate user experience (UX), making UX a prerequisite for system adoption [6]. Hence, organizations must “adopt human-centred design to design technologies capable of

[*] Corresponding author: Austin Oguejiofor Amaechi

competing successfully in a saturated global market" [7]. An ever-important question often asked is: Can the cybersecurity mindset be developed?

This led us to our research question: How can a targeted, actionable, doable cybersecurity mindsets user-centered cybersecurity methodological framework be appropriately designed? This paper is based on a diverse set of existing frameworks, theories, and previous studies designs a human centred cybersecurity change methodological framework capable of promoting more effective cybersecurity behaviour and sustaining those changes over time. The framework is based on the understanding that strong cybersecurity behavioural habits and mindsets can be created. In addition, the problem of cybersecurity human errors and behaviours has been identified to include cybersecurity fatigue, non-adherence to cybersecurity behavioural guidelines, lack of appropriate knowledge, information security ignorance, and absence of organizational support [8]. The framework proposed is also firmed on the understanding that personal responsibility and establishment of communities of practice (COP) are dynamic ways of fostering cybersecurity mindsets. According to Hong & Furnell [9], to form a habit, "a Behaviour must be practiced in the presence of cues that are strong enough to elicit previously learned responses to stimuli". Dutton [10] define security mindset as "a set of attitudes, beliefs and values that motivate individuals to continually act in ways to secure themselves and their network of users, such as by acquiring technical skills, new practices or changing their behaviour". Dweck in another study [11] sees mindset as a set of beliefs about the world that motivates the adoption of different behaviours and ways of thinking. The individual using the constructed solution must have a high level of belief in successfully reaching the desired outcome.

The remainder of this paper is organized as follows: in Section 2, the conceptual background formulated for this study are presented; in Section 3 an in-depth description of the methodology of this study are presented; in Section 4, the results of the analyses are presented in form of framework for cybersecurity behaviour change; and in Section 5, the conclusions and implications of the study are delineated.

2. Conceptual Background

2.1. Characteristics of Cybersecurity

Cybersecurity is a broad concept, which encompasses the "technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor" [12]. Thus, cybersecurity is a complex area, covering multiple fields, such as sociology, psychology, information technology, etc. The cybersecurity issues are stemmed from these fields and are affected by the combination of factors that can lead to errors, risks, and unprotected vulnerabilities ([13], [14]). Cybersecurity is also defined as the "convergence of people, processes and technology to protect organizations, individuals or networks from digital attacks" [15]. One of the main research directions in "cybersecurity relates to human behaviour and its underlying drivers (i.e., human traits, attitudes, motivations, and preconditions shaping cybersecurity behaviour)" [16]. Other authors (e.g., [17], [18], [19]) have argued that human-centered perspective emphasizing behaviour and, especially, efforts to strengthen it have rarely gained systematic support from organizations. Human centric cybersecurity [HCCS] is "an approach that emphasizes the significance of the human element in designing, implementing, and managing cybersecurity systems" ([20],[21]). According to [21], "HCCS involves all aspects of cybersecurity with a particular focus on the human involvement in the system and processes. That is, understanding how humans represent value, but also risk to an organization; understanding how humans and computer interact and what risks are introduced because of these interactions." Hong & Furnell argues that human behaviour toward cybersecurity and reasons for behaviour is a concern for both end-users and organizations. This is because most cybersecurity incidents are caused by human mistakes or inadequate knowledge [9]. Chowdhury et al opinion that "promoting cybersecurity behaviour is essential to protecting organizations and individuals from security threats" [19]. According to Khan et al [22], "Behavioural cybersecurity also known as the human factor presents the social scientific perspective, and a number of topics are being covered under cybersecurity behavioural research includes awareness, behaviour, policy compliance and cybersecurity culture". Human factors such as personality, beliefs, expectations, emotions affect human behaviour. behaviour change, according to [23] is "any modification of human behaviour through some type of intervention". Guiding individuals to form good cybersecurity habits can help to reduce their cybersecurity vulnerability both effortless and efficiently [24]. Creating a better methods fostering good cyber hygiene. 'Cyber hygiene' in this context, refers to various steps that "individuals and organisations can take to reduce cybersecurity risks, such using strong passwords and multifactor authentication, installing security updates, and limiting the number of users with administrator access to systems and networks". These backgrounds are the guiding motivation in this research.

2.2. Factors influencing Cybersecurity Behaviour

Finding a proper balance between cybersecurity and the cybersecurity users' Behaviour liberty is a dynamic challenge in fostering cybersecurity. All cybersecurity users are susceptible to unauthorised access and interference. Behavioural cybersecurity can be "preventive, reactive, or adaptive". Preventive behaviours, according to Tempestini et al, "mitigate risks before an incident occurs, reactive Behaviours respond to an incident after it occurs, and adaptive behaviours involve changing practices based on past incidents or new information about potential threats" [25]. Generally, Behavioural cybersecurity research and measures aim to understand and protect information systems by the "use of psychological, social, cognitive, and emotional factors as data" [26]. Behavioural cybersecurity is described by Stanton et al as "the complexes of human action that influence the availability, confidentiality, and integrity of information systems" [27]. It also represents actions individuals or organizations take to protect their information systems and networks from security incidents, breaches, or attacks [22]. According to Lahcen et al recent study, a key research direction in cybersecurity relates to "human behaviour and its underlying drivers (i.e., human traits, attitudes, motivations, and preconditions) shaping cybersecurity behaviour" ([28], [29]). The Cybersecurity Behaviour phenomenon has been studied, examined and analyzed from different angles and in different contexts. For instance, Chowdhury et al [19] study classified task characteristics (e.g., complexity, involvement), user characteristics (e.g., their personality or role), or workplace characteristics (e.g., colleagues in their workplace) that can impact cybersecurity-related behaviour. Given the research focus of this study, we valued the Zimmermann and Renaud [30] study which suggest the "adoption of a human-as-solution mindset in organizations". Kioskli et al study looked at improving cybersecurity behaviour with varying actions such as "creating and managing strong passwords, avoiding suspicious emails or websites, regularly updating and patching software, using secure networks, and backing up data" [31]. Factors such as "individuals' knowledge, differences in personality, cognitive and behavioural traits, attitudes, and perceptions of threat and vulnerability as well as organizational culture, policies, and training" have been found to influence cybersecurity behaviour ([22], [33], [33], [34]) can thus be fostered. Creating conducive environment for cybersecurity user's attitude and behaviour change is another important human-as-solution mindset. Possible solution can include, sharing information about security issues with the audience [35], generating interest and engaging the audience for participation [36], making clear appeals for doable actions [35], and evoking emotion through positive enforcement to act the way it has been suggested [37]. According to Paul Moritz Wiegmann et al [38], "understanding how people formulate preconceptions and beliefs, how socio-psychological, economic, and other factors (for example, cognitive and cultural biases, demographics, personality traits, and risk-taking propensity) impact people's decision-making processes, and what roles different motivation techniques (e.g., persuasion techniques, teaching and learning techniques)" can enhance cybersecurity attitudes and behaviour change." Various research articles have investigated the factors which influence human behaviour and thus cybersecurity behaviour change, including:

- The "individual's knowledge, skills and understanding of cybersecurity as well as their experiences, perceptions, attitudes, and beliefs are the main influencers of their behaviour" ([39], [40])
- Sunil Chaudhary [41] summarised a number of attributes that could motivate cybersecurity behaviour adoption and change to include "obtain senior management support and participation in cybersecurity awareness activities; consider cybersecurity awareness as a continuous process that needs to be updated and improved on a regular basis; cultivate and spread 'cybersecurity' as a norm in the organisation; encourage cybersecurity activities and behaviours through incentives; craft and use persuasive cybersecurity awareness messages; employ innovative and effective approaches to disseminate cybersecurity awareness messages; and recommend security activities that are achievable and pertinent for the audience".
- Harper [42] review study concludes that training, employee awareness of cyber-related threats, robust security metrics, policy development, and a holistic culture of cybersecurity awareness have a significant role in mitigating human behaviour that can open up organizations and individuals to cyberattacks
- Baltuttis et al [43] developed a taxonomy of six dimensions to understand employees' cybersecurity behaviour, namely "(1) attention & diligence, (2) environment & experience, (3) work-life blurring, (4) trusting mindset, (5) resilience & self-confidence, and (6) goodwill & personal impact".
- MINDSPACE framework [44] summarized a number of important factors that drive all behaviour, and they include "messenger, incentives, norms, defaults, salience, priming, affect, commitments, and ego".

2.3. Selected Theories/Models in Cybersecurity Behaviour

The Behaviour development process of an individual can be mapped and managed under many existing behavioural models, theories and frameworks. Several systematic literature reviews on cybersecurity behaviour have been conducted. Michie et al [45] describe in detail no fewer than 83 systematic attempts to understand and influence human behaviour interventions. While some models and theories centered "on beliefs about what people think about a given behaviour and then the intervention focuses on changing those beliefs by targeting the constructs within that model;

others consider the degree of motivation that people have for changing behaviour". Among these models and theories considered are:

- Knowledge-attitude-behaviour (KAB) model formulated by Kruger and Kearney [46] has been used to explain "cybersecurity awareness and behaviours" (e.g., [47], [48], [49]). The KAB model definitions assumes that "the users' knowledge impacts their attitude and, in turn, promotes changes in behaviour" [43]. The main proposition of KAB is "while knowledge can change behaviours, attitude is often a necessary mediator between the two factors. In other words, increased knowledge improves attitude, which then results in better behaviours" [50].
- In the Broaden and Build Theory of Positive Emotions framework, emotions play a significant role in human behaviour [51]. Positive emotions are believed to increase actions and thoughts. This means they increase opportunities to consider the many factors logically with situational responses and consequently promote adaptive reactions to the environment. Positive emotions indicate not only current mindsets but also enhance future mindsets. Positive emotions may encourage employees to defend their information technology assets against outside and inside threats [52]. According to Alshammari et al [53], negative emotions such as anger, fear, and sadness affect interpersonal interactions and predict people's behaviours.
- The fullness of Capability, Opportunity, Motivation, Behaviour (COM-B) model is described in ([45], [54],[55]). COM-B model provides "a comprehensive framework for understanding behaviour, as well as designing Behaviour change interventions". The COM-B model posits that behaviour change as a function of three inter-related components; the person's psychological and physical Capability, the extent to which they have the physical and psychological Opportunity to perform the behaviour, and combined, these two factors impact one's Motivation to perform the behaviour. The application of the COM-B behaviour development process results in a behavioural environment, in which a behavior is produced from the interaction between people, processes and physical environments. Thus, the "behaviour development process of an individual can be mapped and managed under the framework of the COM-B model".
- Concept of Nudge theory and choice architecture. Nudging according to [56] is a "framework frequently used in behavioural science and behavioural economics, which asserts that subtle and indirect changes in the environment are effective means to change people's behaviour and decision-making". As a psychological intervention technique, nudging influences behaviour by creating changes in the environment, aimed at guiding people towards more desirable behaviours. Nudges are "indirect suggestions to influence the behaviour and decision-making of an individual" [57]. The key idea therefore is that people can be persuaded to act in particular ways where solutions are arranged with user behaviour as a principal guiding principle. According to Thaler and Sunstein [56] 'choice architectures' can be designed to "help nudge people towards make better choices without forcing certain outcomes upon anyone".

A review of the above theories and model shows that human-centered cybersecurity Behaviour is greatly influenced by range of factors.

3. Research Methods

Fostering sustainable cybersecurity mindset is a design problem. From the perspective of human centeredness, this paper approach is that a more effective approach to cybersecurity is designing solutions or technology that work securely for human interaction. The goal of our methodological framework is to develop a 'theoretically grounded and industrially relevant method' capable of fostering sustainable cybersecurity behaviour and enabling the relevant users with "the right skills and knowledge, competency to undertake the relevant behaviour, and have the motivation to adopt the behaviour". Cybersecurity behaviours are actually "design artifacts" that are created by people and sustain by people. By seeing sustainable cybersecurity behaviour change as a design problem, this study offers a human centered design perspective. This study uses framework formulated from Design Science Research (DSR) approach to attain the key objective of this paper. Design science research involves "the creation of an artefact, framework, model, or theory in which the current state of practice can be improved together with the existing knowledge" ([58], [59]). Our use of DSR thinking follows a 'constructive approach', and the developed framework is 'consequentialist' as defined in [60], assuming behaviour to involve planning ahead, based on outcome expectations. The DSR element is relevant for the defined objective because it reconciles real-world issues with theoretical knowledge to create relevant artifacts. The 'constructive design journey' presented in this paper illustrates how our practical method and consequentialist' vision can turn empirical cybersecurity perceptions into pragmatic cybersecurity behaviour improvement design principles.

4. Our approach to Fostering HCCS Training and Communication Program

Human Centered Methodological Cybersecurity (HCMC) framework is the result of this study. The “human-centred design” framework involves considering people’s cybersecurity needs and limitations - the way we think, behave, and interact with technology when designing and building software and applications. HCMC provides a robust framework that allows cybersecurity teams to deliver cybersecurity behaviour value incrementally, react quickly to changes, and continuously refine their processes. The key steps lies in “understanding the sources of the behaviours involving the people in the process, communicating clearly and frequently, decreasing or increasing the knowledge requirements for using cybersecurity controls, provision of necessary support and incentives (better opportunity) to behave safely or discourage unsafe behaviour, efficient management of behaviour expectations and ongoing risks through motivation construct such as influencing cybersecurity users’ behaviour by restructuring their presented choices”. According to Brennan et al., study to “encourage and lead users to regularly practice cybersecurity compliance, an organization needs an approach that helps to build understanding of employees’ motivations and behaviours within the social system” [61]. The main steps in our approach are presented in Figure 1. The cybersecurity framework was designed to be “organization focused”. The HCMC process enables the compliance with relevant standards and regulations ensuring that the designed solution is secure and meets the necessary requirements. The following subsections elaborate on each design dimension and associated constructs.

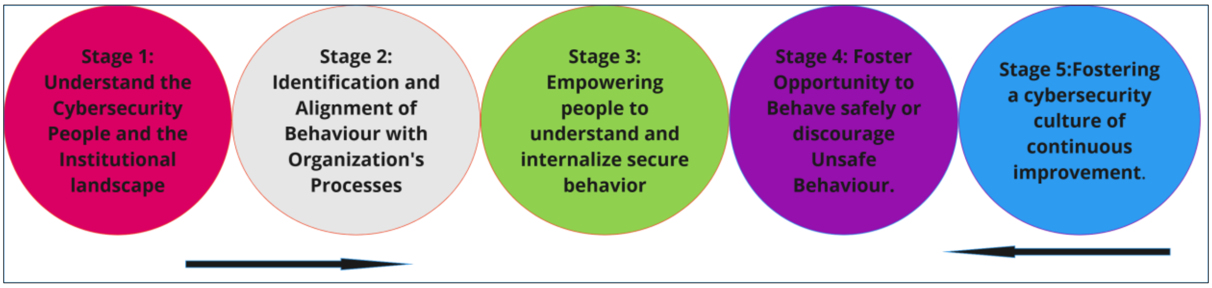
Stage 1: Understand the Cybersecurity People and the Institutional landscape
Stage 2: Identification and Alignment of Behaviour with Organization's Processes
Stage 3: Empowering people to understand and internalize secure behavior
Stage 4: Foster Opportunity to Behave safely or discourage Unsafe Behaviour.
Stage 5:Fostering a cybersecurity culture of continuous improvement.

Figure 1 Multilevel Representations of influences on Human-Centric Cybersecurity Behaviour Change. (Source: Own elaboration, 2025)

5. Stage 1: Understand the Cybersecurity People and the Institutional landscape.

The first stage in the human centered cybersecurity behaviour change journey is to understand cybersecurity users and cybersecurity landscape of the organization. In this step, the socio-technical cybersecurity needs to be understood as placed within, and influenced by, the environment in which the behaviour occurs. In proposing this stage, we acknowledge the existing fact that there are cybersecurity users who only change their behaviour when adequately informed, and there are users who only perform the intended behaviour under coercion, and there are population that falls between the two extremes. It is important that all the groups are considered in cybersecurity behaviour change design and human risk management. Individuals’ cybersecurity habits influence the individual cybersecurity behaviours. Thus, understanding the target group or individuals including their specific job roles, education, work experience, preferred training methods, current knowledge level, decision styles, personality traits, beliefs, interests, and goals which influence their cybersecurity usage is important. Knowledge is the key indicator. Both the KAB and the COM-B model of behaviour change suggests that to “engage in a behaviour, a person needs to have the capability, opportunity and motivation to perform that behaviour, so any behaviour change will require modifying at least one of those components” [62]. According to Yao et al [63], the “most important factor around which all strategies work for the growth of any organisation is ’knowledge’”, thus, organizations grow, remain competitive, and achieve their goals by leveraging their knowledge as a foundation [64]. Human-centered design as a “problem-solving technique”, puts real “people at the center of the development process”, thus cybersecurity mindsets designers must develop “empathy with cybersecurity users to truly understand their experiences and needs”. Users’ involvement across all stages of behaviour change design is extremely important to ensure that the intervention strategies is acceptable, practical, relevant, and appropriate. to reliably obtain each person's behaviour. To assess or extract individuals' behaviours and attitudes when they interact with the cybersecurity solutions, a validated constructs proposed in Baltuttis et al [43] can be employed. The Baltuttis et al model consists of a questionnaire of 32 constructs structured along five categories: personality and attitude; cybersecurity background, knowledge, and skills; cybersecurity behaviour; organizational environment, and way of working.

6. Stage 2: Identification and Alignment of Behaviour with Organization's Processes

Change is hard. Thus, fostering cybersecurity mindsets or changing cybersecurity behaviour requires understanding what the problematic and target Behaviours are, understanding the expectations of the cybersecurity stakeholders, and understanding how success will be measured. Repeated unsafe cyber behaviours should be identified. Focus should be on the behaviours that needs to change and to what they are changing to. It is important to capture the various poor security Behaviours within the organization and understand the possible cybersecurity Behaviour change processes and finally the cybersecurity behaviours or mindsets we wish to foster. The desired new mindsets must be identified or created and that is the recipe to sustained success. The basis is that in order to succeed in a behaviour change at any given moment, the individual or target group from the perspective of COM-B model must have sufficient levels of “capability (individual having the awareness, knowledge, and skills to enact the behaviour) to do it, motivation (beliefs and attitudes that drive enthusiasm, or lack of it) to do it, and an opportunity (external factors like having the time, resources, tools, money, and access to enact the desired behaviour) to do it”. For effective outcome, it is recommended that one or two behaviours are targeted at a time. Current and target cybersecurity mindsets or Behaviours are best sourced from integration of user experience activities, namely expert review and prototyping workshops, document reviews, interviews, focus groups, direct observation, and questionnaires. It is important that the desired cybersecurity mindsets or Behaviours are achievable and pertinent, and the change processes designed in ways that make the cybersecurity users feel in control.

7. Stage 3: Empowering people to understand and internalize secure Behaviour

Cybersecurity user’s behaviour is what “creates or reduces cyber-based vulnerability”. Many interesting intervention formulas have been studied and published. We reasoned in this study that what is required in a cybersecurity Behaviour improvement program is a “learn, practice and maintain knowledge” construct. Implementation of the practices of threat modeling is an essential step towards adaptation of a cybersecurity-focused mindsets. Though a context specific formula, threat modeling is considered an essential first step for "secure by design" development [65]. The aim should be creation of desirable emotions, guidelines, and growth of practical knowledge as well as professional competence. This requirement aligns greatly with COM-B notion of psychological capability construct. There should be a decrease of the knowledge requirements for using cybersecurity controls or increase in the cybersecurity user’s knowledge. Knowledge about desirable cybersecurity behaviours and change initiatives should be shared with individuals taking their level of education into consideration, and they should be trained in the skills required to adopt, use, and to sustain the new behaviours. Desired cybersecurity behaviour can be built over time to build cybersecurity behaviour resiliency. The following user experience questions based on COM-B model categories are capable of fostering and sustaining the desired cybersecurity mindsets: “Do people need to know more about the behaviour? Do the people need to understand why the behaviour is important? Do people find the behaviour easy to do” Do people have the time to do the behaviour? Are there triggers in the environment to prompt the behaviour? Do people need special tools to do the behaviour? Do people have the social support required to do the behaviour? Do other people encourage or discourage the behaviour? Does the behaviour align with people’s goals and values? Do people have plans in action to achieve the behaviour?” The use of reinforcement learning and practice is advocated. Negative emotions are detrimental to cybersecurity behaviour. Therefore, it is important that positive emotions are fostered. According to Dennison (2024] eliciting emotions is key to persuasion because attitudes have a cognitive and emotive component. Emotions influence “people’s views, mindsets, and actions”. We assert that fostering positive emotions (such as being excited, increased job satisfaction, feeling hopeful, being optimistic) are good for acceptable cybersecurity behaviours, as it increases actions and thoughts. As Schwartz ([67], [68]) stated, both “situational and individual factors probably influence awareness of consequences and ascription of responsibility in choice situations”. In this research we have postulated that “sufficient cybersecurity awareness of consequences and ascription of responsibility positively affects personal norms”. Therefore, the organization must ensure that users are aware of the benefits of the cybersecurity behaviour transformation and how it will impact their work and the organization. Rezaei et al., [69] argued that when “individuals are aware of the negative consequences of not adopting a behaviour and feel a personal responsibility because of these adverse consequences, they may feel a personal moral obligation to engage in a certain behaviour”. Thus, growth of personal norms according to [70] is a winning intervention strategy in a successful adoption of the new behaviour.

8. Stage 4: Foster Opportunity to Behave safely or discourage Unsafe Behaviour.

If cybersecurity users construe a cybersecurity threat confronting him to be positive, negative and moral choice, relevant norms he holds about cybersecurity are likely to be activated and affect the person’s intention and Behaviour. Previous authors (e.g. [67], [68], [71], [72]) argues that “problem awareness, awareness of consequences and ascription of responsibility influence an individual’s personal norm. Schwartz [68] explains that “through awareness of consequences, individuals build an acknowledgement of responsibility". Generation of multiple creative personal norm solutions is a first crucial step. Cybersecurity behavioural mechanisms encouraging cybersecurity users to make certain choices - deliberate interventions should be designed (such as notifications, incentivization/nudging, empowering messages, education, technology regulation, and prompts) which can nurture the operational capabilities of the cybersecurity users. Operational capabilities in this context refers to the "abilities and systems within the cybersecurity systems that allow for immediate, coordinated, and effective response to cyberspace crises". In addition, organisations should try to make it easier for cybersecurity users to behave in the desired manner by better supporting user's business goal-oriented behaviour in the design of cybersecurity controls (for instance use of the fingerprint authentication procedure versus password passphrase to gain access to devices or services). The concept of techno-regulation and nudging are also important theoretical and practical frameworks in fostering desired behaviours. Van den Berg and Leenes [73] defined techno-regulation as the "intentional influencing of individuals' behaviour by building norms into technological devices". Nudging concept is an acclaimed good behaviour motivating intervention. The challenge with nudging concept is that different cybersecurity users will need different nudges, depending on their psychological and personality profiles. The cybersecurity behaviour policymaker or choice architect must take these differences into consideration. This research therefore reasoned that adding explanatory information to a 'prompts nudging' will be beneficial and more empowering. The nudging cybersecurity behaviour targeted approaches, however, should empower rather than paternalize cybersecurity users. According to Hartwig and Reuter [74] study, nudging in cybersecurity is helpful as long as the "nudges are transparent, sources are trustworthy, and they appear only occasionally". Van Steen & De Busser emphasis that "nudging ensure that the way in which cybersecurity choices are offered is the optimal method from the choice architect's point of view, leading to the highest level of compliance without the need for punishment, or restriction of freedom of choice" [75]. On the other hand, the authors stated that techno-regulation suggests that security can be forced by taking away the freedom to act differently. This means not "merely making it easier for people to behave in the desired manner but preventing cybersecurity end-users from doing anything that is not the preferred option". Hence, techno-regulation offers opportunities to have policy enforced in a strict sense.

9. Stage 5: Fostering a cybersecurity culture of continuous improvement.

Human centered cybersecurity behaviour change is a dynamic and evolving process. Creating a resilient and sustainable strong cybersecurity organizational culture (i.e., common norms, values, attitudes, and beliefs of individuals within the organization) requires a commitment from organization leadership, education, positive reinforcement, adaptable policies, regulations, and processes. Fostering a dynamic cybersecurity culture is both a management and technical issues and requires attention to leadership, faculty development, enabling Communities of Practice, reflection and dialogue. In addition, continuous improvement of user centered cybersecurity requires that responsibilities of users (shared responsibility and personal responsibility) are clearly defined, maturity evaluation instruments informed by educational theory, and all relevant stakeholders get a voice. This study agreed to a combination of rule oriented and goal oriented organisational cybersecurity culture ([76], [77]). User's cybersecurity intellectual skills, procedural knowledge, and competences must be acquired and maintained. Just like Kam et al [78] findings that different motivation factors fostered learning persistence and performance, we believe that cybersecurity users will greatly benefit from sustained motivation. In addition, establishment of cybersecurity communities of practice (CoPs) can further educational enhancement as they foster an exchange of expertise and ideas for innovation [79]. Finally, a continual creation of awareness and evaluation of the interventions are important factors to maintain desired behaviours. Cybersecurity users need to be aware about the consequences that may derive from their negative Behaviour (e.g., scam emails can lead to phishing); as such, awareness can lead them to feel responsible which would lead them to a pro-cybersecurity behaviour. Equally an application of evaluation formula (e.g., APEASE criteria evaluation (affordability, practicability, effectiveness, acceptability, side-effects and safety and equity) assessing the impact of any intervention strategies are important. [45].

10. Conclusion

Cybersecurity is a mindset, and it involves fostering a culture of cybersecurity behaviour. Cybersecurity behaviour refers to the "individual practices that attenuate or minimize the risk and likelihood of cyber threats". There is a significant gap between the "attitudes and behaviours" among cybersecurity users. Such gaps have resulted from either internal factor, such as the level of user knowledge, technical skills or personal experience or external factors, such as organizational culture and complexity of the cybersecurity process [80]. The formulated methodological framework is grounded in concept of complex adaptive systems principles and behavioural change theories. Our study has several important implications for practice. The study has proposed a new process that can be used by organisations to foster an effective cybersecurity culture where personal and shared responsibilities are important success factors. The study has also provided practical guidance to organisations on how to use the framework to develop their individual cybersecurity programs.

A static analysis and descriptive evaluation were carried out. A team of knowledgeable persons in a workshop examined the structure of the developed artefact for static qualities and judged it dynamic. In addition, there is “adequate information in the knowledge base to assure users and researchers of the external and internal validity of the artefacts”. The framework is capable of systematically guiding the identification of target cybersecurity users and cybersecurity landscape, understanding the vulnerable behaviours and desired behaviours, enable the users learn the necessary behaviours and put the learned cybersecurity behaviour knowledge into practice. Our methodological framework is not context specific. In conclusion, we believe this methodology is implemented to foster collaboration between multiple teams and enables users to be involved in the design and development process. HCMC framework is about designing for people and the way people think, behave, and interact with the technology. Organisation must provide cybersecurity support to their people and enable the approach of pushing cybersecurity information rather than expecting the users to seek out cybersecurity information on their own. For further research, it might be needful to explore the possibility of reiterating the design quality and evaluation framework.

References

[1] Ben-Asher Noam, Gonzalez Cleotilde. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behaviour, 48 (2015), pp. 51-61

[2] Francesco Schiliro. Towards a Contemporary Definition of Cybersecurity. 5 Feb 2023.

[3] Dimitri Percia David, Marcus Matthias Keupp, Alain Mermoud, Knowledge absorption for cyber-security: The role of human beliefs, Computers in Human Behaviour, Volume 106,2020, 106255, https://doi.org/10.1016/j.chb.2020.106255.

[4] Chen, X; Tyran, CK. A framework for analyzing and improving ISP compliance. J. Comp. Inf. Syst. (2023), pp. 1-16, https://doi.org/10.1080/08874417.2022.2161024

[5] Pham, C.H., El-den, J. and Richardson, J. (2016), “Stress-based security compliance model-an exploratory study”, Information and Computer Security, Vol. 24 No. 4, pp. 326-347.

[6] ISO. (2019). Ergonomics of human-system interaction — part 210: Human-centred design for interactive systems.

[7] Djamasbi, S., & Strong, D. (2019). User experience-driven innovation in smart and connected worlds. AIS THCI, 11(4), 215–231.

[8] Fosoh Holiness Nikel & Austin Oguejiofor Amaechi, 2022. "An Assessment of Employee Knowledge, Awareness, Attitude towards Organizational Cybersecurity in Cameroon," Network and Communication Technologies, Canadian Center of Science and Education, vol. 7(1)

[9] Yuxiang Hong, Steven Furnell, Understanding cybersecurity Behavioural habits: Insights from situational support, Journal of Information Security and Applications, Volume 57, 2021, 102710, https://doi.org/10.1016/j.jisa.2020.102710.

[10] William H. Dutton. (2018). Fostering a cybersecurity mindset. Zenodo. https://doi.org/10.5281/zenodo.1186288

[11] Dweck C. Mindset: Changing the way you think to fulfil your potential. Constable & Robinson 2017;1:3–264.

[12] Clark, D., Berson, T., & Lin, H. S. (Eds.) (2014). At the nexus of cybersecurity and public policy. Computer Science and Telecommunications Board, National Research Council, Washington DC: The National Academies Press

[13] Dawson, J., and Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. Front. Psychol. 9:744. doi: 10.3389/fpsyg.2018.00744

[14] Nobles, Calvin. "Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem" HOLISTICA – Journal of Business and Public Administration, vol.13, no.1, 2022, pp.49-72. https://doi.org/10.2478/hjbpa-2022-0003

[15] S. Hasan, M. Ali, S. Kurnia, R. Thurasamy. Evaluating the cyber security readiness of organizations and its influence on performance J. Inf. Secur. Appl., 58 (2021), Article 102726, 10.1016/j.jisa.2020.102726

[16] M. Lahcen, R. Ait, B. Caulkins, R. Mohapatra, M. Kumar. Review and insight on the Behavioural aspects of cybersecurity Cybersecur. (Singap), 3 (1) (2020), p. 10, 10.1186/s42400-020-00050-w

[17] R.S. Dalal, D.J. Howard, R.J. Bennett, C. Posey, S.J. Zaccaro, B.J. Brummel. Organizational science and cybersecurity: abundant opportunities for research at the interface. J. Bus. Psychol., 37 (1) (2022), pp. 1-29, 10.1007/s10869-021-09732-9

[18] A. Pollini, T.C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, D. Guerri. Leveraging human factors in cybersecurity: an integrated methodological approach. Cogn. Technol. Work, 24 (2) (2022), pp. 371-390, 10.1007/s10111-021-00683-y

[19] Noman H. Chowdhury, Marc T.P. Adam, Timm Teubner, Time pressure in human cybersecurity Behaviour: Theoretical framework and countermeasures, Computers & Security, Volume 97,2020,101963,https://doi.org/10.1016/j.cose.2020.101963.

[20] S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis, S. Bonacina, Influence of human factors on cyber security within healthcare organisations: A systematic review, Sensors (Basel, Switzerland) 21 (2021) 5119–.

[21] Grobler M, Gaire R and Nepal S (2021) User, Usage and Usability: Redefining Human Centric Cyber Security. Front. Big Data 4:583723. doi: 10.3389/fdata.2021.583723

[22] Naurin Farooq Khan, Amber Yaqoob, Muhammad Saud Khan, Naveed Ikram, The cybersecurity Behavioural research: A tertiary study, Computers & Security, Volume 120, 2022, 102826, https://doi.org/10.1016/j.cose.2022.102826.

[23] Mersinas, Konstantinos and Bada, Maria and Furnell, Steven, Cyber Behaviour Change: An Ethical Framework for Behavioural Interventions in Cybersecurity. Available at SSRN: https://ssrn.com/abstract=4743156 or http://dx.doi.org/10.2139/ssrn.4743156

[24] E. Lindbladh, C.H. Lyttkens. Habit Versus Choice: The Process of Decision-Making in Health-Related Behaviour. Social Science & Medicine, 55 (3) (2002), pp. 451-465

[25] Tempestini, G.; Rovira, E.; Pyke, A.; Di Nocera, F. The Cybersecurity Awareness INventory (CAIN): Early Phases of Development of a Tool for Assessing Cybersecurity Knowledge Based on the ISO/IEC 27032. J. Cybersecur. Priv. 2023, 3, 61–75.

[26] W. Patterson, C. Winston, L. Fleming Behavioural cybersecurity: human factors in the cybersecurity curriculum Advances in Human Factors in Cybersecurity, Springer International Publishing (2016), pp. 253- 266, 10.1007/978-3-319-41932-9_21

[27] J.M. Stanton, K.R. Stam, P. Mastrangelo, J. Jolton Analysis of end user security Behaviours. Comput. Secur., 24 (2) (2005), pp. 124-133, 10.1016/j.cose.2004.07.001

[28] Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro, Cyber security: State of the art, challenges and future directions, Cyber Security and Applications, Volume 2, 2024, 100031, https://doi.org/10.1016/j.csa.2023.100031.

[29] Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insighton the behavioural aspects of cybersecurity. Cybersecurity, 3(1).https://doi.org/10.1186/s42400-020-00050-w

[30] V. Zimmermann, K. Renaud. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. Int. J. Hum. Comput. Stud., 131 (2019), pp. 169-187, 10.1016/j.ijhcs.2019.05.005.

[31] Kioskli, K.; Fotis, T.; Nifakos, S.; Mouratidis, H. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Appl. Sci. 2023, 13, 3410. https://doi.org/10.3390/app1306341

[32] Alshaikh M, Naseer H, Ahmad A, Maynard SB (2019) Toward sustainable behaviour change: an approach for cyber security education training and awareness. In: In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden

[33] Almansoori, A.; Al-Emran, M.; Shaalan, K. Exploring the Frontiers of Cybersecurity Behaviour: A Systematic Review of Studies and Theories. Appl. Sci. 2023, 13, 5700.

[34] Kannelønning, K. and Katsikas, S.K. (2023), "A systematic literature review of how cybersecurity-related Behaviour has been assessed", Information and Computer Security, Vol. 31 No. 4, pp. 463-477. https://doi.org/10.1108/ICS-08-2022-0139

[35] A. Christiano, A. Neimand. Stop Raising Awareness Already. Standford Social Innovation Review (2017), pp. 34-41

[36] L. Spitzner, "Top 3 Reasons Security Awareness Training Fails," 01 January 2019. [Online]. Available: https://www.sans.org/blog/top-3-reasons-security-awareness-training-fails/. [Accessed 2 May 2025].

[37] Hoxhunt, "How to create Behaviour change with security awareness training?," n.d.. [Online]. Available: https://www.hoxhunt.com/ebooks/how-to-create-Behaviour-change-security-awareness-training. [Accessed 2 May 2025].

[38] Paul Moritz Wiegmann, Madis Talmar, Sjoerd Bastiaan de Nijs, Forging a sharper blade: A design science research approach for transition studies, Environmental Innovation and Societal Transitions, Volume 48, 2023,100760, https://doi.org/10.1016/j.eist.2023.100760.

[39] Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672 (2019)

[40] Moustafa AA, Bello A and Maurushat A (2021) The Role of User Behaviour in Improving Cyber Security Management. Front. Psychol. 12:561011. doi: 10.3389/fpsyg.2021.561011

[41] Sunil Chaudhary, Driving behaviour change with cybersecurity awareness, Computers & Security, Volume 142, 2024, 103858, https://doi.org/10.1016/j.cose.2024.103858.

[42] J. W. Harper, Cybersecurity: a review of human-based Behaviour and best practices to mitigate risk. Issues in Information Systems Volume 24, Issue 4, pp. 247-254, 2023 https://doi.org/10.48009/4_iis_2023_119

[43] Dennik Baltuttis, Timm Teubner, Marc T.P. Adam, A typology of cybersecurity Behaviour among knowledge workers, Computers & Security, Volume 140, 2024, 103741, https://doi.org/10.1016/j.cose.2024.103741.

[44] P. Dolan, M. Hallsworth, D. Halpern, D. King, R. Metcalfe, I. Vlaev, Influencing behaviour: The mindspace way, Journal of Economic Psychology, Volume 33, Issue 1, 2012, Pages 264-277, https://doi.org/10.1016/j.joep.2011.10.009.

[45] S. Michie, L. Atkins and R. West, The Behaviour Change Wheel, a Guide to Designing Interventions, 1st edn, Silverback Publishing, Great Britain, (2014) , pp. 1003–1010.

[46] H. Kruger, W. Kearney. A prototype for assessing information security awareness. Computers & Security, 25 (4) (2006), pp. 289-296

[47] Agata McCormac, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius, Malcolm Pattinson, Individual differences and Information Security Awareness, Computers in Human Behaviour, Volume 69, 2017, Pages 151-156, https://doi.org/10.1016/j.chb.2016.11.065.

[48] X. Li; Qin An; Wilson Hong; Zhang Yunfeng; Kimberly Kolletar-Zhu; Xiaoshu Xu Undergraduates' KAB Towards the Disclosure of Personal Data Online in China. July 2023 DOI: 10.3233/FAIA230168 In book: Modern Management Based on Big Data IV

[49] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and Behaviour: A comparative study. Journal of Computer Information Systems, 1–16. https://doi.org/10.1080/08874417.2020.1712269

[50] Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R. and Jerram, C. (2015), "The influence of organizational information security culture on information security decision making", Journal of Cognitive Engineering and Decision Making, Vol. 9 No. 2, pp. 117-129, doi: 10.1177/1555343415575152.

[51] Fredrickson BL. The broaden-and-build theory of positive emotions. Philos Trans R Soc Lond B Biol Sci. 2004 Sep 29;359(1449):1367-78. doi: 10.1098/rstb.2004.1512. PMID: 15347528; PMCID: PMC1693418.

[52] Zhen, J., Xie, Z., & Dong, K. (2020). Positive emotions and employees' protection-motivated behaviours: A moderated mediation model. Journal of Business Economics and Management, 21(5), 1466–1485.

[53] Alshammari, A., Benson, V. and Batista, L. The Influences of Employees' Emotions on Their Cyber Security Protection Motivation Behaviour: A Theoretical Framework. In Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS 2024) - Volume 2, pages 524-531 DOI: 10.5220/0012681600003690

[54] West, R., and S. Michie. 2020. "A Brief Introduction to the COM-B Model of Behaviour and the PRIME Theory of Motivation." Qeios, 1–6. doi: https://doi.org/10.32388/ww04e6.2.

[55] GCS Behavioural Science Team. The Principles of Behaviour Change Communications https://gcs.civilservice.gov.uk/publications/the-principles-of-behaviour-change-communications/

[56] Thaler, R.H.; Sunstein, C.R. Nudge: Improving Decisions about Health, Wealth, and Happiness; Penguin: London, UK, 2008.

[57] Kosters, M.; J. Van der Heijden; "From Mechanism to Virtue: Evaluating Nudge Theory," Evaluation, vol. 21, iss. 3, 7 July 2015, p. 276–291, https://journals.sagepub.com/doi/abs/10.1177/1356389015590218

[58] E. Achampong and C. Dzidonu, "Methodological Framework for Artefact Design and Development in Design Science Research," researchgate.net, 2017, Accessed: August. 27, 2024. [Online].

[59] Jan vom Brocke, Alan Hevner, and Alexander Maedche, Introduction to Design Science Research. In book: Design Science Research. Cases. September 2020. DOI: 10.1007/978-3-030-46781-4_1

[60] Loewenstein, G. F., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. Psychological Bulletin, 127, 267–286.

[61] Brennan, L., Binney, W., Parker, L. and Nguyen, D., A., T. (2014), "Theories and their uses in social marketing", in Social Marketing and Behaviour Change: Models, Theory and Applications, Glos GL50 2JA, Edward Elgar Publishing, Cheltenham, pp. 7-14.

[62] Michie, S., van Stralen, M.M. & West, R. The behaviour change wheel: A new method for characterising and designing behaviour change interventions. Implementation Sci 6, 42 (2011). https://doi.org/10.1186/1748-5908-6-42

[63] Y. Yao, E. A. Patterson, and R. J. Taylor, "The influence of digital technologies on knowledge management in engineering: A systematic literature review," IEEE Transactions on Knowledge and Data Engineering, 2023

[64] B. Kogut and U. Zander, "Knowledge of the firm, combinative capabilities, and the replication of technology," Organization science, vol. 3, no. 3, pp. 383–397, 1992

[65] R. E. Thompson, M. McLaughlin, C. Powers, and D. Votipka."There are rabbit holes I want to go down that I'm not allowed to go down": An Investigation of Security Expert Threat Modeling Practices for Medical Devices. In 33rd USENIX Security Symposium, pages 4909–4926, 2024.

[66] James Dennison, Emotions: functions and significance for attitudes, behaviour, and communication, Migration Studies, Volume 12, Issue 1, March 2024, Pages 1–20, https://doi.org/10.1093/migration/mnad018

[67] Schwartz, Shalom H. Awareness of Consequences and the Influence of Moral Norms on Interpersonal Behaviour. Sociometry, vol. 31, no. 4, 1968, pp. 355–69. JSTOR, https://doi.org/10.2307/2786399.

[68] Schwartz, S. H. (1977). Normative Influence on Altruism. In L. Berkowitz (Ed.), Advances in Experimental Social Psychology, 10, (pp. 221-279). New York: Academic Press. http://dx.doi.org/10.1016/s0065-2601(08)60358-5

[69] Rezaei, R.; Safa, L.; Damalas, C.A.; Ganjkhanloo, M.M. Drivers of farmers' intention to use integrated pest management: Integrating theory of planned Behaviour and norm activation model. J. Environ. Manag. 2019, 236, 328–339

[70] Chwialkowska, A.; Bhatti, W.A.; Glowik, M. The influence of cultural values on pro-environmental Behaviour. J. Clean. Prod. 2020, 268, 122305.

[71] Nabsiah Abdul Wahid, Sharifah Fairuz Syed Fadzil, Shaizatulaqma Kamalul Ariffin (2022). .Influences of Problem Awareness, Awareness of Consequences and Ascription of Responsibility on Consumer's Personal Norm to Prevent Water Wastage Behaviour. Environment and Ecology Research, 10(2), 275 - 283. DOI: 10.13189/eer.2022.100217.

[72] Setiawan, Budi; Afiff, Adi Zakaria; and Heruwasto, Ignatius (2021) "PERSONAL NORM AND PROENVIRONMENTAL CONSUMER BEHAVIOUR: AN APPLICATION OF NORM ACTIVATION THEORY PDF," ASEAN Marketing Journal: Vol. 13 : No. 1 , Article 3. DOI: 10.21002/amj.v13i1.13213

[73] Van den Berg, B.; Leenes, R.E. Abort, retry, fail: Scoping techno-regulation and other techno-effects. In Human Law and Computer Law: Comparative Perspectives; Springer: Dordrecht, The Netherlands, 2013; pp. 67–87.

[74] Katrin Hartwig and Christian Reuter. 2021. Nudge or Restraint: How do People Assess Nudging in Cybersecurity - A Representative Study in Germany. In European Symposium on Usable Security 2021. ACM, Karlsruhe Germany, 141--150. https://doi.org/10.1145/3481357.3481514

[75] Van Steen, T. & De Busser, E. (2021). Security by Behavioural design: A rapid review. Technical report. Leiden University.

[76] Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences, 43(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

[77] Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. Journal of Enterprise Information Management, 34(4), 1203–1228. https://doi.org/10.1108/JEIM-08-2019-0217

[78] Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. Computers & Security, 96, 101875.

[79] de Carvalho-Filho MA, Tio RA, Steinert Y. 2020. Twelve tips for implementing a community of practice for faculty development. Med Teach. 42(2):143–149.

[80] Pham, H.C., Brennan, L., Parker, L., Phan-Le, N.T., Ulhaq, I., Nkhoma, M.Z. and Nhat Nguyen, M. (2019), "Enhancing cyber security Behaviour: an internal social marketing approach", Information and Computer Security, Vol. 28 No. 2, pp. 133-159. https://doi.org/10.1108/ICS-01-2019-0023