Proceedings of the
35th International Conference on Information Technologies (InfoTech-2021)
IEEE Conference, Rec. # 52438, 16-17 September 2021, Bulgaria

PEOPLE-CENTRIC SECURITY AWARENESS PROGRAM

Federico Giovannetti

Doctor of Business Administration Program
Muma College of Business, University of South Florida, Tampa
e-mail: fgiovannetti@usf.edu
United States of America

Abstract: Information Security departments are continuously challenged and frustrated by the lack of employee compliance with established security policies. Several studies have shown causal factors for this type of employee behavior. However, few have recommended management level interventions that can be used as a solution framework by security practitioners. Based on constructs such as tailored communication messages, leadership influence, and peer ambassadors, this article presents a People-centric Information Security Awareness Program that can help security practitioners improve the Information Security Culture of their organization.
Key words: Information security culture, employee compliance, tailored messaging, leadership, ambassadors.

1. INTRODUCTION

Information security departments protect the information assets of their organizations by mostly executing on two main tasks: 1) Implementing and deploying technical tools to safeguard the confidentiality, integrity, and availability of their information assets, and 2) Crafting policies, standards, guidelines and procedures that all employees must follow [1]. Fortunately, with respect to the first task, technical tools have reached a high level of maturity and are very effective in protecting against current security threats. On the other hand, the second task depends heavily on the rest of the organization's compliance with policies and other artifacts dictating information security governance [2]. Problems abound regarding human behavior influencing lack of compliance, from carelessness and human error [3] to a significant list of motivational factors including convenience, perceived effort, and perceived risk, among others [4]. The result is that despite the advancement of

technical tools that safeguard information assets, employees are estimated to be the largest source of security incidents [5].

Information Security departments, typically led by a Chief Information Security Officer (CISO), are continuously challenged and frustrated by the lack of compliance with established security policies by the rest of the organization. Employees tend to believe that information security is the responsibility of the security department alone. However, in the same way employees are the largest source of security incidents, they can also help the security department implement and maintain appropriate security controls in a significant way. In other words, employees' behaviors can directly influence the information security safeguards of an organization in both negative and positive ways [6]. This concept has been studied by scholars as the "information security culture" of an organization [7]. The question about how to improve it has been addressed before, but it still seems open to further research.

The goal of this article is to present an Information Security Awareness Program which objective is to drive improvements in the information security culture of an organization.

Motivation

As stated in Mahfuth et al. [7], there are several definitions in the literature for information security culture. A common theme appears to be that information security culture relates to the behaviors of individuals towards compliance with information security policies (ISP). In that sense, several of these studies propose frameworks aimed at consistently changing individuals' behaviors, including techniques rooted in psychology such as persuasion and influencing [1]. Some authors explicitly argue that security awareness education, viewed purely as a knowledge acquisition exercise, does not by itself accomplish the desired results regarding compliance, and should be complemented with behavioral change techniques in order to be effective [1][8]. In fact, even the most recent security awareness training material based on instructional technology (videos, games, simulations, etc.) is widely viewed by employees as just another compliance activity to check mark.

How do you change employee behavior towards security compliance? Many researchers have studied the factors that influence this behavior, as well as related interventions to modify it. Most of these studies are rooted in theories from the Psychology sciences, such as the Theory of Planned Behavior [9], the Protection Motivation Theory [10], and the Deterrence Theory [11]. To that extent, many of the causal factors studied in the literature revolved around explaining individual behavior. Although this is an important angle to understand, the challenge is that interventions become quite difficult to devise and implement at an individual level. At best, one can only implement interventions that would address the most common

individual behaviors. Even then, affects (moods, feelings, etc.) are known to have an additional daily effect on individuals' attitude towards compliance [12].

As seen thus far in this discussion, this is a people's problem. Employee behaviors, namely their lack of compliance with information security policies, are making the security posture of the organization weaker. At times, it seems as though some employees try to outright bypass information security safeguards in favor of accelerating their business objectives, causing tremendous frustration for security practitioners. On the other hand, as security practitioners assume a policy enforcement role, the rest of the company increasingly sees them as an obstacle to achieving their main objectives. This creates unproductive reinforcing behaviors where the two parties increasingly grow further apart, making it very difficult to achieve the goals related to improving the information security posture of the organization. Ultimately, the goal of the CISO department is to protect the confidentiality, integrity, and availability of the information assets of the organization. For this reason, a program that reduces the risks associated with employees' lack of compliance should be a welcome addition to their tool chest.

2. THE PROBLEM SPACE

The problem space was validated by studying the existing environment and knowledge base.

2.1. Existing Environment

Much of the existing environment has been already described in the previous section, and it is summarized in Table 1 below using three interrelated constructs: People, Organization and Tools. People are the different actors or personas that are part of the existing environment. Organization contains issues intrinsic to the inter-relations of the actors within the context of this study. Tools are the tactics and/or artifacts currently being used to deal with the organization-level issues.

Table 1. Existing Environment

People	Organization	Tools
1. **InfoSec Office (practitioners)**: Main role is to safeguard the information assets of the organization. 2. **Employees:** Belong to different business units with diverse roles. 3. **Senior Management:** Provide leadership, strategic direction, and tactical execution to all employees.	• Information Security Culture relates to the behaviors of employees towards compliance with information security policies. • Employees' lack of compliance increases vulnerabilities. • Negative reinforcing cycle when infosec practitioners become enforcers and employees see them as an obstacle to achieving their business objectives.	• Security Basics Training • Security Awareness Training • Communications o Advisories o Newsletters • Deterrence (penalties) o Block account o Deny access

	• Business objectives are dictated by senior management	• Cross-functional collaboration

2.2. Existing Knowledge Base

A review of the literature on information security culture and employee compliance with information security policies shows a remarked emphasis on individual behavior. Furthermore, scholars study the causal factors that explain different types of deviant or non-compliance behavior. Table 2 summarizes the most common factors studied.

Table 2. Causes of employees' non-compliance with Infosec policies

Category	Cause/Factor	References
Individual	Self-Efficacy: the belief of the individual about their own skills to implement a certain task	[13] [14] [15] [16] [12] [17]
Individual	Lack of knowledge regarding the infosec policy	[18] [15] [16]
Individual	Lack of knowledge regarding general infosec concepts	[15] [16]
Individual	Unintentional: stress, mood and other affects, operator error, etc.	[18] [12]
Individual	Inertia: The manifestation of an employee's reluctance to change their current behavior	[19]
Individual	Perception of Cost vs. Benefit of compliance	[15] [12] [20] [17]
Individual	Perception of the severity and certainty of monitoring and sanctions	[15] [19] [12] [20] [17]
Individual	Perception of the severity, vulnerability, and probability of security incidents	[15] [16] [21] [17]
Organizational	Normative Beliefs: "perceived social pressure" from executives and peers who are considered as a reference point in compliance to information security policies. Some authors explore the "positive" influence from peers while others explore "negative" influences in terms of ISP compliance	[14] (positive influence) [22] (negative influence) [12] (positive influence) [17] (positive influence)
Organizational	Leadership support of Infosec governance. Employees tend to trust leaders with respect to policy security controls	[16]
Organizational	Conflicting goals. Productivity vs. Infosec compliance. Compliance seen as impediment of business goals	[23] [22] [12] [17]
Organizational	Organizational commitment. How committed is the employee to the organization	[24] [17]

Most of the factors listed in Table 2 relate to the Theory of Planned Behavior [9], which links cognitive beliefs, behavioral intention, and behavior. The cognitive beliefs include attitude, subjective norm, and perceived control, as seen in ***Fig. 1***.

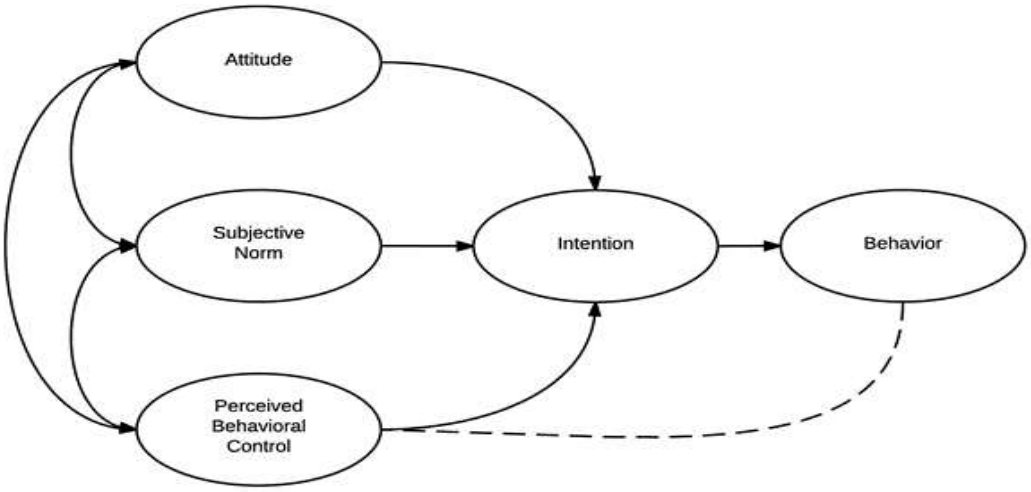

Fig. 1. Theory of Planned Behavior (TPB)

Variations of these constructs can be seen in the Causes/Factors column in Table 2, especially those that have solely an individual origin (although group dynamics affect individuals in specific ways). According to the TPB, these factors shape the intention of an individual towards the behavior (in this case compliance with the information security policy) which in turn drives the actual behavior.

Other articles use constructs from the Protection Motivation Theory (PMT) [10], which revolves around how humans process and react to fear appeals in terms of adopting behaviors that protect themselves from the perceived threat (***Fig. 2***). Self-efficacy, for example, is a causal factor included in quite a few articles.

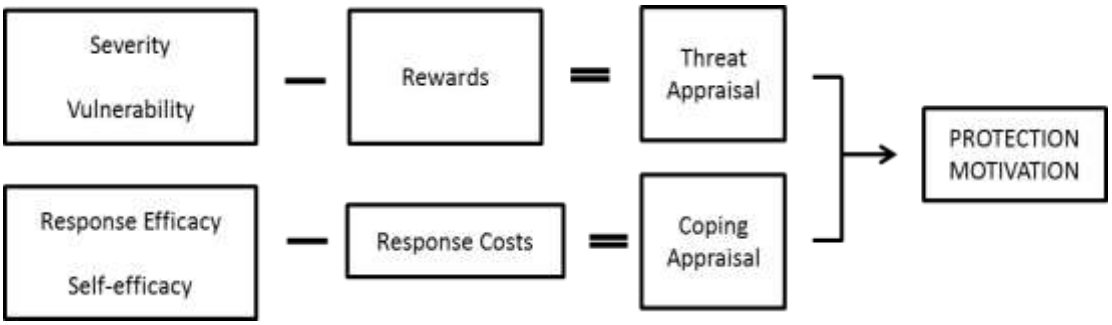

Fig. 2. Protection Motivation Theory (PMT)

These two theories, in addition to others cited to a lesser extent such as Deterrence Theory [11], are all rooted in the psychology science. To that extent, many of the causal factors studied in the literature revolve around explaining individual behavior. In such cases, a follow up with a corresponding intervention was not common. This is validated in a comprehensive meta-analysis article that explores the most common causes of ISP non-compliance in the literature [25]. Referring to the top 3 categories found, they state: *"These categories are closely linked with the psychological and ethical characteristics of employees, rather than other, lower-*

ranked categories, such as punishment, threats, and rewards, which are typically associated with managerial actions." Regrettably, they conclude that it follows, as a contribution to practice, that organizations should emphasize hiring employees with the right psychological makeup in order to increase ISP compliance, instead of concluding that there is not enough research related to how managerial actions can influence the employees already hired.

It is important to note that interventions at the individual level are not practical to implement in an organizational context to make any significant impact. Only a few articles found in the knowledge base complemented the individual behavior (psychology) factors with group and organizational dynamics (sociology). They focus on peer influence and to some extent the role of leadership and/or senior management within the organization. In fact, several authors assert that information security culture should be treated as part of the larger organizational culture [8, 26-28]. More specifically, that employee compliance with security policies should be based on "espoused values" and "shared tacit assumptions", which are largely driven by the founders and leaders of the organization, complemented with "artifacts" and "information security knowledge" that allow the basic understanding of what must be done [28]. In yet another interesting view of the relationship between organizational culture and information security culture, D'Arcy and Greene [26] argue that the latter can be conceptualized by three dimensions: top management commitment to security, security communication and computer monitoring. All these concepts illustrate how important the leaders of an organization are in influencing the information security culture.

3. THE SOLUTION SPACE

This study aims to understand causal factors at an individual level but to devise interventions at an organizational level. In other words, to empower information security practitioners and managers with an effective program that can improve the information security culture of their organization and therefore increase compliance with information security policies. It is worth noting that many practitioners believe that compliance can be improved via enforcement and penalization. This proposal does not argue the merits of that approach and leaves aside any "carrot versus stick" debate. However, since it approaches the compliance issue from an information security culture point of view, it aims to rely on employee self-judgement. This is, an environment where employees, independently, make everyday decisions within their areas of responsibility that are aligned with the information security policies of the organization.

The proposed solution is a novel "People-centric Security Awareness Program" whose foundational elements are presented in Table 3. Each element listed is linked to a causal factor(s) presented in the problem space, and a short description of the corresponding intervention addressing the causal factor(s) is presented.

Table 3. Foundational Elements of Security Awareness Program

Element	Causal Factor addressed	Intervention
Education	Lack of understanding of Information Security concepts	Training and simulation modules
Communication Messaging	Lack of knowledge regarding the ISP Perception of Cost vs. Benefit of compliance Perception of the severity, vulnerability, and probability of security incidents Self-efficacy, Inertia	Messaging tailored to show "utility" to the target audience and therefore engage them with the program
Leadership buy-in	Leadership support of Infosec governance. Normative Beliefs	Message tailored to leadership to engage them to have an active role (see next item)
Leadership Message	Conflicting goals: Productivity vs. compliance. Perception of Cost vs. Benefit of compliance	Espoused values and clear direction and priorities well communicated to organization
Ambassadors	Self-efficacy Normative Beliefs Organizational commitment	Recruit the most engaged participants in the program to spread the word within their groups

To summarize the table above, the proposed People-centric Security Awareness Program (PCSAP) uses open and engaging communications to talk to employees about what matters to them, personally and professionally, in their language. The desired effect of the program is that it becomes popular and sought after, as opposed to feared and avoided, which in turn motivates champions/ambassadors to spread the word. The conceptual model that represents this design is depicted in *Fig*. 3. The relationships between constructs in this diagram are considered positive (increases or improves) as shown left to right. An explanation of the conceptual model follows the diagram.

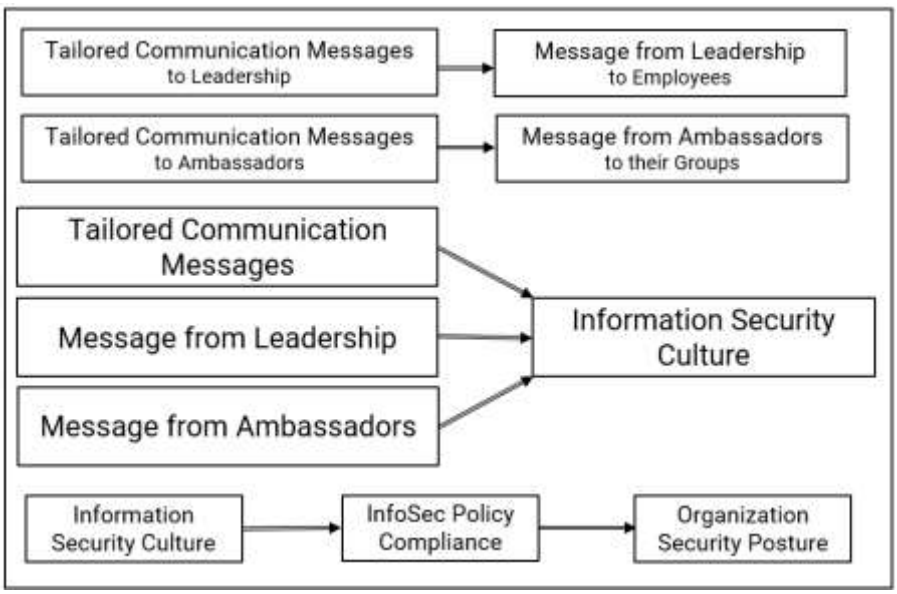

Fig. 3. Conceptual Model supporting proposed program

The key concept in this model is Tailored Communication Messaging. It refers to a communications technique that takes the targeted audience into account when crafting the message. For example, when conveying the benefits of healthy foods, it would make sense to utilize different messages for different age groups. How are messages tailored? What makes a message effective when it is sent to a targeted audience? According to Informing Science research, a message must pass several bias filters before it can be effectively received by the audience [29]. These bias filters include attention, information, cognition, and motivation, among others. The information and motivation filters, which combined can be thought of as the "utility" of the message to the receiver [30], are very important conceptual elements in the proposed solution. In other words, the message must be useful to the recipient.

The PCSAP is meant to be implemented by the CISO department within an organization. However, it relies heavily on the participation of the organization's leadership for support and to help communicate the appropriate message to all employees. To that extent, it incorporates tailored messaging to the leadership team itself in order to make them part of the program. Once this is accomplished, the leadership team will deliver the "message from leadership" to the rest of the organization.

The same concept is applied to recruit peer ambassadors into the PCSAP. Ambassadors are employees outside of the CISO department that can influence their peers towards better compliance. They are an invaluable extension of the PCSAP team in the process of improving the information security culture. For illustration purposes, a potential ambassador can be a software developer. A tailored message to them would be that a software developer that understands and solves security vulnerabilities is more valuable in the job market. The software developer becomes interested in learning more about writing secure code and reaches out to the CISO department, becoming the ambassador that will then bring the tailored security awareness message to their peers.

Summarizing the utilization of Tailored Communication Messages in the design of the PCSAP, it is used first to recruit leadership and peer ambassadors, and then it is used to deliver tailored messages to other segmented audiences within the organization. These messages are delivered by the PCSAP team, as well as the individuals recruited, with the sole purpose of improving the Information Security Culture of the organization.

Finally, although not the only contributing factor, an improvement in the Information Security Culture will improve InfoSec Policy Compliance, which in turn improves the security posture/profile of the organization, as has been previously discussed.

The PCSAP therefore consists of a collection of components. Each component is intended for a target audience and uses tailored messaging specific to that audience. The most important factor in this design is the believe that awareness that drives individual decision making is key to improving the information security

culture. According to the Merriam-Webster dictionary, awareness is defined as *"knowledge and understanding that something is happening or exists"*. Based on the author's own experience as a practitioner, "understanding" is a key word in this definition, and something that can only be accomplished if the communication message can pass through the several bias filters that we experience as individuals. By creating different components of the program, the audience is segmented in a way the utility of the message is specific to that audience. In other words, the goal is to pass through the information and motivation filters by communicating information relevant to the audience so that the "understanding" part of awareness is cemented. This program helps each audience better understand information security and becoming aware of the importance of complying with its policies.

The segmentation of targeted audiences, as well as the tailored messages to each, is likely to be different amongst organizations. Therefore, the PCSAP director must customize the program to their specific environment. As a way of example, a few representative components are presented next:

3.1. Private Citizen Component

This component is key for building trust and popularity of the PCSAP, as individuals will be interested in the utility of the communication at a personal level. It consists of organizing discussion and information sessions regarding popular topics of concern to private citizens. For example:

- Identity theft education
- Popular scams: craigslist, email solicitations, government calls, etc.
- Social media privacy protection tutorials
- Online banking risks and recommendations
- Personal security hygiene
    - Password risks and password managers
    - Personal computers' antivirus recommendations
    - Laptops, tablets, and smartphones risks
    - Wi-Fi hotspots

3.2. Application Developers Component

Buy-in from development teams and/or individual developers is critical. Pursue having developers teaching developers about secure coding.

- Tailored recruiting message: who has more job market value?
    - Software developer
    - Software developer with cybersecurity skills
- Help developers start a secure SDLC program
    - OWASP based workshops:
        - Top 10 vulnerabilities
        - Top 10 security controls

- Secure code review methodologies
- Introduce developers to secure testing tools
  - SAST, DAST
  - Vulnerability scans

3.3. Product/Sales/Marketing Component

Help Product/Sales/Marketing audience build and sell security-aware products by incorporating security insights into their interactions with customers.

- Lunch and learn sessions:
  - Basic concepts: Threats, Vulnerabilities, Risk Management, Controls
  - Advanced concepts: Data Classification & Protection, Network Security, Logging/Monitoring, Application Security, Cloud Security
- Market insights workshops
  - Highlight customers' expectations regarding security
  - Security jargon to convince and impress
  - Customer mockup sessions (role play security-aware customer)

3.4. Executive Leadership Component

Specifically tailored to garner support for the program form the leaders of the organization, including actionable contributions.

- Prepare program metrics from all components
- Executive Leadership specific topics (their language)
  - Liability, fiduciary duty updates
  - Revenue impact examples
    - Customers' expectations (market research)
    - Regulatory landscape
  - Weekly executive news summary, state of the industry
  - Product/features opportunities
- Conduct research on specific topics, taking requests from individual members of the Executive Leadership team

3.5. PCSAP lifecycle

In addition to all the different program components that should be created for each targeted audience, the PCSAP should also have a consistent lifecycle that includes:

- Reward and recognize employees for
  - Making the right decisions
  - Reporting incidents or discovered vulnerabilities
  - Spreading the message
- Build Community
  - Create discussion groups.

    - Introduce like-minded employees to each other
- Keep educational materials current and engaging

4. CONCLUSION

This article presented a proposal for a People-centric Security Awareness Program that utilizes tailored communication messages as well as the participation of leadership and peer ambassadors to influence employees to understand and internalize information security and to comply with the information security policies of the organization. The design of the program is based on a review of the existing environment and knowledge base studying employee behavior towards compliance and seeks to elevate the information security culture of the organization.

The contribution to the information security practice can be broad. Practitioners should be able to deploy the program based on their initial assessment regarding audience segmentation and tailored messaging, then continue to refine both parameters based on observations of the reception and desired results. The theoretical foundation supports such continuous refining cycles.

REFERENCES

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

[2] Mishra, S. (**2015**). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security,*.

[3] Beautement A. and A. Sasse (**2009**). The economics of user effort in information security. *Computer Fraud & Security*, vol. 2009, no. 10, pp. 8-12.

[4] Coventry, L., P. Briggs, J. Blythe, and M. Tran (**2014**). Using behavioural insights to improve the public's use of cyber security best practices. *Gov. UK report*.

[5] PricewaterhouseCoopers (**2016**). Key findings from The Global State of Information Security Survey (available at: https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf)

[6] Da Veiga, A. and J.H.P. Eloff (**2010**). A framework and assessment instrument for information security culture, *Computers & Security*, Article vol. 29, no. 2, pp. 196-207

[7] Mahfuth, A. et al. (**2017**). A systematic literature review: Information security culture. *In 2017 International Conference on Research and Innovation in Information Systems (pp. 1-6). IEEE*.

[8] Sherif, E., S. Furnell, and N. Clarke (**2015**). Awareness, behaviour and culture: The ABC in cultivating security compliance. *10th International Conference for Internet Technology & Secured Transactions (ICITST)*, p. 90.

[9] Ajzen, I. (**1991**). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211.

[10] Rogers, R. W. (**1975**). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1), 93-114.

[11] D'arcy, J. and T. Herath (**2011**). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems,* vol. 20, no. 6, pp. 643-658.
[12] D'Arcy, J. and P. B. Lowry (**2019**). Cognitive- affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, Article vol. 29, no. 1, pp. 43-69.
[13] Yoo, C. W. , G. Jahyun, and H. R. Rao (**2020**). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. *MIS Quarterly,* vol. 44, no. 2, pp. 907-931.
[14] Kaymaz, K. (**2020**). THE ANALYSIS OF THE RELATIONS AMONG NORMATIVE BELIEFS, SELF-EFFICACY AND INTENTION TO COMPLY WITHIN THE FRAME OF INFORMATION SECURITY POLICIES. *Is, Guc: The Journal of Industrial Relations & Human Resources*, vol. 22, no. 1, pp. 1-20.
[15] Tsohou, A. and P. Holtkamp (**2018**). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology & People,* vol. 31, no. 5, pp. 1047-1068.
[16] Koohang, A. et al. (**2020**). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, vol. 120, no. 1, pp. 231-247.
[17] Herath, T. and H. R. Rao (**2009**). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,* vol. 18, no. 2, pp. 106-125.
[18] Alotaibi, M. J., S. Furnell, and N. Clarke (**2019**). A framework for reporting and dealing with end-user security policy compliance. *Information and Computer Security,* vol. 27, no. 1, pp. 2-25.
[19] Malimage, K. et al. (**2020**). Impact of Deterrence and Inertia on Information Security Policy Changes. *Journal of Information Systems*, vol. 34, no. 1, pp. 123-134.
[20] Aurigemma, S. and T. Mattson (**2017**). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security,* vol. 25, no. 4, pp. 421-436.
[21] Zhang, J., B. J. Reithel, and H. Li (**2009**). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security,* vol. 17, no. 4, pp. 330-340.
[22] Hwang, I. et al. (**2017**). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review,* vol. 41, no. 1, pp. 2-18.
[23] Mayer, P. et al. (**2017**). Productivity vs security: mitigating conflicting goals in organizations. *Information and Computer Security,* vol. 25, no. 2, pp. 137-151.
[24] Johnston, A. C. et al. (**2019**). Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. *Decision Sciences,* vol. 50, no. 2, pp. 245-284.
[25] Cram, W. A., J. D'Arcy, and J. G. Proudfoot (**2019**). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly,* vol. 43, no. 2, pp. 525-554.
[26] D'Arcy, J. and G. Greene (**2014**). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security,* vol. 22, no. 5, pp. 474-489.
[27] Marchand-Niño, W. R., & B. P. G. Fonseca (**2019**). Social Engineering for Diagnostic the Information Security Culture. *2019 IEEE 39th Central America and Panama Convention.* pp. 1-6.
[28] Okere, I., J. van Niekerk, and M. Carroll (**2012**). Assessing information security culture: A critical analysis of current approaches. *2012 Information Security for South Africa,* p. 1.
[29] Gill,T. G. (**2008**). The Single Client Resonance Model: Beyond Rigor and Relevance. *Informing Science,* vol. 11, pp. 281-310.

[30] Gill,T. G. (**2008**). A Psychologically Plausible Goal-Based Utility Function. *Informing Science*, vol. 11, pp. 227-252.