EasyChair Preprint

№ 15791

Towards a Cybersecurity Culture Framework: a Literature Review of Awareness and Behavioral Transformation in Telecommunications Organizations

Esther Endjala, Hanifa Abdullah and Mathias Mujinga

February 3, 2025

Towards a Cybersecurity Culture Framework: A Literature Review of Awareness and Behavioral Transformation in Telecommunications Organizations

Esther Endjala[1], Hanifa Abdullah[2], and Mathias Mujinga[3]

[1] University of South Africa, Pretoria, South Africa
[2] School of Computing, College of Science, Engineering and Technology, University of South Africa, Pretoria, South Africa
e-mails: 45163464@mylife.unisa.ac.za | abdulh@unisa.ac.za | mujinm@unisa.ac.za

Abstract. This paper explores the theoretical and strategic foundations for cultivating a cybersecurity culture within telecommunications institutions. Drawing on established behavioral theories—Social Cognitive Theory (SCT), Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), and Technology Acceptance Model (TAM)—it examines the opportunities for enhancing cybersecurity awareness and transforming employee behaviors into a resilient human firewall. The paper synthesizes existing literature to highlight the role of leadership, employee engagement, training, collaboration, and recognition in fostering a cybersecurity culture. The review further identifies gaps and limitations in the current approaches, proposing a conceptual foundation for developing an effective cybersecurity culture framework tailored to telecommunications institutions.

Appropriate cybersecurity culture is essential in developing the entity and helps protect organizational assets such as data, networks, and systems when technical defenses are quite significant. The section takes into consideration the theoretical aspect of cybersecurity culture and comes out with a derived underlying framework that incorporates aspects like the Social Cognitive Theory, Protection Motivation Theory, Theory of Planned Behavior, and Technology Acceptance Model. The text highlights essential factors for building a strong cybersecurity culture, such as top management commitment, employee engagement, continuous training, and interdepartmental collaboration. Organizations must address challenges like resistance to change, resource limitations, and regulatory barriers. By embedding these elements, cybersecurity can become a core organizational value, leading to increased awareness, compliance, and proactive employee involvement in cybersecurity practices. This paper thus builds the essential critical foundation for further empirical work on embedding cybersecurity culture and informs the essential steps toward strengthening organizational resilience and ensuring a safe digital environment.

Keywords: Cybersecurity Culture, Cybersecurity Framework, Cybersecurity Policy, Cybersecurity Awareness, Cybersecurity Training, Organization Culture, Cyber Threat, Telecommunications.

1 Introduction

The rise of cyber threats poses a significant challenge to organizations, particularly within the telecommunications sector, where customers' sensitive data and critical infrastructure are at constant risk. While technological solutions play a vital role in mitigating these threats, the human element remains a critical vulnerability. This study aims to develop a cybersecurity culture framework to improve awareness and transform employees' behaviors into a resilient human firewall. This paper's objective is to review existing literature on behavioral theories and organizational strategies to establish the foundations for cultivating an effective cybersecurity culture. In this respect, the telecommunication sector has seen revolutionary changes, with seamless connectivity, efficient data transfer, and innovative solutions to help grow modernized economies. These advancements have brought about new, unparalleled weaknesses, as cyber-terrorists leverage those complex, interconnected systems and large amounts of sensitive data maintained by this sector [1].

Telecommunications networks are critical infrastructures linking people, businesses, and governments worldwide. This makes the consequences of cyber security breaches, in which one node is attacked and the effect spreads across the network-paralyzing it, exposing sensitive data, and weakening trust within it much worse [2]. For instance, cybersecurity threats influence this domain in everything from ransomware attacks and distributed Denial-of-Service (DDoS) attack incidents to sophisticated phishing schemes and insider threats. The rapid evolution of cyber threats, fueled by advances in malicious software and the rise of Internet of Things (IoT) devices, demands that organizations adopt proactive and adaptive strategies that exceed traditional defense mechanisms [3].

Such a cybersecurity culture of resilience has turned an important player in dealing with these issues, far beyond technical solutions into the sphere of human behaviors, organizational norms, and shared responsibility. For the latter to develop, cybersecurity principles have to be instilled at an organization's core such as that everyone, from the management level down to the entry-level employees, is informed about their role in security [4].

2 Theoretical Background

The research study is underpinned by a theoretical framework that forms the foundation and perspective through which the research problem is examined. Upon reviewing the various frameworks designed to promote cybersecurity culture, it is evident that organizations have a wealth of resources at their disposal to enhance their cybersecurity measures. The theories selected for this study are the Social Cognitive Theory (SCT), Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), and Technology Acceptance Model (TAM) to analyze the adoption and integration of cybersecurity policies into the organization's culture. Understanding and influencing human behavior is central to cultivating a cybersecurity culture. The following theories provide a robust foundation for this effort:

2.1 Social Cognitive Theory (SCT)

The key focus of the Social Cognitive Theory lies in the perception of safe skills from observation, social modeling, and reinforcement. This theory generates a conceptual framework about how the environment influences learning through the identification of interactions between environmental, behavioral, and personal factors [5]. Within the cybersecurity context, SCT highlights the importance of organizational leadership and policy as enablers of safe behaviors. Leaders who demonstrate a commitment to cybersecurity through actions such as actively participating in training, promoting best practices, and endorsing policies serve as role models, influencing employees to emulate these behaviors [1, 6]. This behavioral modeling fosters an organizational culture where security is a shared value, and employees adopt leadership practices to protect assets and data [4].

SCT states that organizational priorities must be set by the leadership. The organizational leadership shows employees that cybersecurity is an organizational core value by demonstrating a commitment to support cybersecurity initiatives. This can be done by leaders participating actively in training sessions, issuance and approval of security policies, and promotion of best practices [1]. This is because this behavioral modeling dummies the most critical application of security within the organizational setup, thus making the employees imitate their leadership thinking capabilities and commitment. With SCT, it's possible to implement a proactive and resilient cybersecurity culture within an organization whereby individuals can inspire and motivate others to secure the assets and data of the company, simply by adopting this theory with reinforcement practices, such as recognizing compliance with security policies [7].

2.2 Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) approaches how people cognitively appraise threats and develop protection behaviors, conceptualized by Rogers (1975). This theory focuses on an individual's mental consideration of threat appraisals and coping evaluations. Threat appraisal will be assessed with the likelihood and severity of a potential incident on cybersecurity instances, phishing attacks, or data breaches. This evaluation considers the perceived dangers associated with the threat and its potential impact on individual or organizational security [8]. Coping evaluation, conversely, examines the perceived effectiveness of suggested protective actions and an individual's self-assurance in implementing them, often termed self-efficacy. These assessments collectively determine a person's motivation to engage in risk-mitigating behaviors [8, 9].

Organizations can use PMT to institute appropriate interventions for increased motivation among employees to adopt the proper practices. For instance, organizations would use training programs to make the staff more aware of the natural consequences of cyber threats and, therefore, watch out for the hazards. Simultaneously, coping evaluations would be improved, enabling employees to confidently and efficiently take action, if the efficacy of security measures such as using strong passwords, detecting

phishing attempts, or identifying suspicious activities-is shown. Adaptation of such interventions to particular organizational functions will ensure relevance and enhance their potential impact. By applying PMT, organizations can ultimately cultivate a cybersecurity culture where employees are motivated to actively participate in protecting critical assets and systems [9].

2.3 Theory of Planned Behavior (TPB)

The Theory of Planned Behavior (TPB) developed by Ajzen (1980) asserts that three fundamental components influence individuals' intentions to perform particular behaviors: attitudes, subjective norms, and perceived behavioral control [10]. Within the realm of cybersecurity, TPB provides a valuable framework for predicting employees' compliance with security protocols and practices. Attitude involves one general evaluation regarding cybersecurity, including one's perception that following security measures is favorable and vital to the organization's security. The subjective norm can be described as the perceived social pressures to perform or not to perform secure behaviors, and usually influenced by employees, managers, and company expectations. Perceived behavioral control is a person's belief in their capability to execute a security action, such as following password instructions or correctly identifying a phishing attack [6].

Here is a list of the factors that studies have reported as significantly impacting employees' intentions to comply with cybersecurity policies: favorable attitudes towards cybersecurity, coupled with peer support and enough training in this, enhance the likelihood of employees acting securely. On the other hand, those employees who feel capable and empowered to implement cybersecurity measures are likely to comply with organizational guidelines. At this point, TPB can be used by organizations to establish specific interventions that fix attitude, norm, and perceived control deficits. Placing employees within an environment that preaches the importance of cybersecurity, examples of safe behaviors, and resources and training increases compliance. Consequently, TPB functions as a potent theoretical framework for comprehending and encouraging security-oriented behaviors in the workplace [8, 10].

2.4 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) examines perceived usefulness (PU) and Perceived Ease of Use (PEOU) as factors affecting individual adoption of technologies [11]. While PU refers to the belief that the use of a technological component will enhance performance or productivity, PEOU refers to the degree to which the individual perceives the use of technology as effortless. In cybersecurity, TAM provides a useful structure for comprehending employee interactions with security technologies, including encryption programs, two-factor authentication systems, and password management tools [11, 12].

The use will require ease, intuitive interfaces, and making them aware of the benefits coming with cybersecurity tools to ensure acceptance and use. Employees will buy into the concept of security technologies if they find those intuitive and capable of

enhancing their capacity to protect the assets of any given organization. Equipment that is easy to navigate has a short learning curve, reducing resistance while increasing engagement. Moreover, communicating the benefits of these tools, such as enhanced data protection or reduced breach risks, enhances their perceived usefulness and leads employees to adopt these tools within their current workflows. By implementing TAM principles, an organization will be able to develop and deploy cybersecurity tools that match employee expectations, thus enhancing compliance and the security posture of the organization as a whole [11, 12].

Figure 1 illustrates the interconnected theories that move from the broadest down to more specific frameworks addressing behavior, technology adoption, and cybersecurity practices, helping to organize them logically to support the study. This sequence starts with Social Cognitive Theory as the broad foundation, leading into Protection Motivation Theory, which narrows the focus on behavior in response to threats. Then comes the Theory of Protected Behaviour, which further provides insights into why individuals may or may not engage in protective cyber behavior, and finally, the Technology Acceptance Model, which directly addresses the adoption of cybersecurity technologies. Below is the illustration of the theories of cybersecurity culture:

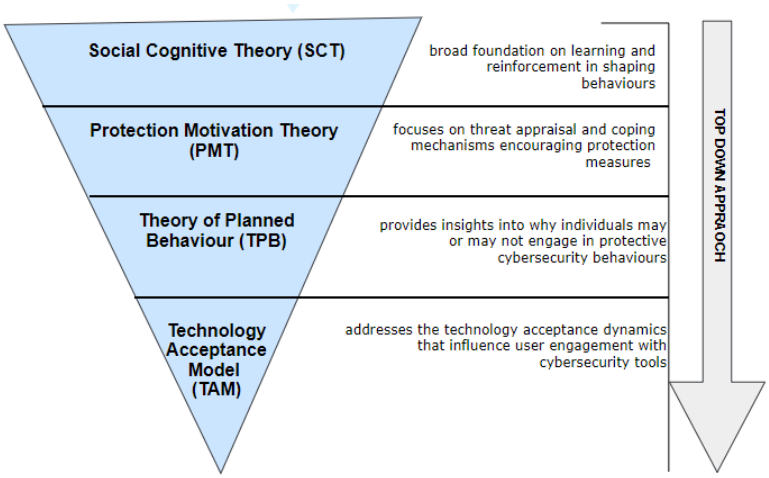

Figure 1: Cybersecurity Theories Integration

Therefore, the illustrated figure indicates the top-down approach, following the sequence of these theories to ensure a logical progression from general principles of human behavior to specific theories regarding security behavior and technology acceptance. These theories collectively establish the basis of the proposed cybersecurity culture framework, addressing individual and organizational behaviors. By connecting theory to practical applications like leadership involvement, tailored training, and technology implementation, the framework provides a unified strategy to integrate cybersecurity practices and enhance resilience against evolving threats.

3 Opportunities for Cultivating Cybersecurity Culture

Establishing a strong cybersecurity culture provides organizations with key opportunities to enhance resilience against evolving cyber threats. Dedicated leadership is crucial; when leaders prioritize cybersecurity through budget allocation, training participation, and endorsement of policies they signal that it is a core organizational value. This visible commitment encourages employees to prioritize security in their daily tasks and promotes shared responsibility [4]. Moreover, transparent communication and early employee involvement in cybersecurity planning can reduce resistance to change, fostering trust and a sense of ownership over the organization's security practices [3, 18]. It encourages cooperation between departments and maintains clear communication, facilitating the integration of cybersecurity practices into the organization's routine workflows.

Smaller organizations with limited resources can benefit from innovative and cost-effective strategies. By utilizing free or low-cost cybersecurity training tools from non-profits and government agencies, they can improve employee awareness without overspending. Leveraging internal expertise to create customized security programs and adopting scalable, cloud-based solutions can help address resource constraints while maintaining efficiency [13]. Additionally, partnerships with industry groups or regulatory bodies provide essential resources and expertise, enabling these organizations to foster a strong cybersecurity culture, even on a tight budget [1].

Organizations across various sectors can tailor cybersecurity culture frameworks to align with local norms and regulations [4]. This flexibility allows them to tackle unique challenges, such as varying technological literacy and sector-specific threats, while upholding core cybersecurity principles. Customized training initiatives can ensure cultural relevance and regulatory compliance. For example, finance and healthcare industries may prioritize regulatory adherence, while manufacturing focuses on operational safety alongside cybersecurity [8, 18].

This paper proposes a cybersecurity culture framework, drawing on benchmarked attributes from authoritative sources, including the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the Center for Internet Security (CIS). Additionally, it incorporates sector-specific insights from frameworks tailored to the telecommunications sector, such as those developed by the European Telecommunications Standards Institute (ETSI), the Telecommunications Industry Association (TIA), and the Global System for Mobile Communications Association (GSMA). These frameworks collectively highlight the critical importance of transforming employee behavior into proactive and consistent cybersecurity practices, ensuring an integrated approach to organizational security [7].

3.1 Leadership Commitment and Support

The dedication of leadership is fundamental for integrating cybersecurity within the cultural framework of an organization. Leaders play a critical role in shaping the strategic approach to cybersecurity by distributing essential resources, instituting comprehensive policies, and promoting a culture of accountability [7]. Management,

by showing serious commitment to cybersecurity, provides an unequivocal tone from the top and makes it the concern of everybody in the organization, not an isolated responsibility of an information technology department [13]. In that way, a commitment at this level would ensure that the decisions and strategies at all levels of the organization include consideration of cybersecurity. It calls for effective leadership that should avail an enabling environment through the provision of training, assurance, and putting in place well-coordinated response mechanisms for the effective takeoff of a cybersecurity framework [1].

The presence of visible leadership support significantly influences the development of a culture in which employees emphasize secure practices [4]. When leaders engage directly in cybersecurity initiatives, including their attendance at awareness programs or their endorsement of security policies, they underscore the significance of cybersecurity and illustrate its connection to the attainment of organizational objectives [3]. The more visibility, the more it leads to an organizational culture among employees regarding cybersecurity and hence builds a shared responsibility for the same [7]. Further, the process of leaders openly acknowledging and appreciating the efforts of the employees toward cybersecurity greatly enhances engagement and compliance with safety [14].

3.2 Employee Engagement and Awareness Campaigns

Initiatives to raise employee awareness are seen as crucial steps in strengthening cybersecurity frameworks inside businesses. These training programs are vital for instructing employees on methods to avert possible risks, such as malware and phishing scams, along with other digital threats [15]. This means that awareness programs reduce risks, making the infrastructure for organizational security stronger by equipping workers with the knowledge and skills to identify such threats. Thus, these programs cultivate a security culture of co-responsibility, meaning cybersecurity is one of those important areas. of responsibility where everyone in the organization is obliged at all levels, not just the IT department alone [16].

Effective Campaigns for Employee Awareness: Indeed, the modes of communication used in effective campaigns for employee awareness tend to hold the attention of participants and ensure their participation. Some of the commonly used methodologies to effectively communicate certain messages intended for different employee demographics include workshops, interactive discussions, email newsletters, and other digital resources [17]. This ensures that the information to be communicated to the employees, who have different technical backgrounds, is relevant and digested with ease. Organizations can enhance employees' understanding of cybersecurity risks and encourage proactive behaviors by integrating concrete examples, practical demonstrations, and engaging platforms. In conclusion, effectively implemented awareness initiatives cultivate a culture of vigilance and responsibility, enabling personnel to serve as the initial line of defense against cyber threats [15].

3.3 Training and Education Programs

The incorporation of various continuing education programs will help equip the employees with the right kind of expertise and experience and thus make them proactive for emerging new threats. These employees can be very crucial in this defensive mechanism by organizing certain training related to the recent cyber threat and strategies that are recommended. Employees who undergo such training will also have the ability to handle data more securely, perform phishing detection, and apply efficient password management [18].

There have been significantly effective custom-made training programs that have improved safe behaviors. The contents are relevant and applicable during the training, as the contents are carefully crafted to match the particular cybersecurity requirements of the organization and the specific roles of its staff [15]. For instance, special training in methods of secure communication for customer-service employees, or teaching IT staff advanced techniques of threat detection, are very contributory to the overall security outcomes. In addition, embedding interactive features such as simulation, practical scenarios, and assessment increases learning motivation [17].

3.4 Collaboration and Communication

The practice of cybersecurity within an organization can be successfully consolidated through interdepartmental collaboration and the establishment of clear lines of communication. The focus shifts from a singular, departmental concern toward a collective concern when there is healthy interaction among departments; this enhances the general effectiveness of the practice of cybersecurity [4]. The combination of these factors means that this collaborative approach is one whereby all arms of the institution-information technology, human resources, and finance know their roles in maintaining security and hence make for a more integrated and coordinated organizational response to threats. Siloed departments in an organization are bound to adopt a shared responsibility culture where each division contributes to discovering vulnerabilities and deploying stringent security measures [4].

What is needed now is the establishment of effective communication channels to further strengthen this collaborative framework. Continuous sharing of information, meetings between departments, and clear lines of reporting in support of effective information flow regarding cybersecurity-related issues and updates would enable rapid detection and mitigation of any potential security incidents well before weaknesses are exploited. Furthermore, customized communication approaches that address the specific requirements and knowledge of various departments guarantee that cybersecurity information is comprehensible and practical for all personnel [15].

3.5 Reward and Recognition

Recognition of security contributions from employees strengthens an organization's security culture and encourages pro-activeness in participation. That is to say, recognition of employees' activities within cybersecurity means only that such activities

were necessary and that they should be more observant in the future. Formal or informal incentives given as means of appreciation for such recognition bring forth a culture of pride and ownership among personnel about their responsibilities in resource protection. This form of positive reinforcement encourages employees to integrate and maintain secure practices as an integral aspect of their professional duties, thereby highlighting the significance of individual contributions to the collective security framework [14].

Incentive programs most definitely go a long way in leveraging employee engagement through tangible rewards for demonstrating outstanding cybersecurity behaviors, such as reporting potential security threats with speed or adherence to predefined security procedures. It will create an atmosphere of competitiveness versus collaboration, focusing directly on security. This allows not just the ability for employees to stay vigilant but also sets the benchmark for good practices across the board. Public recognition of "security champions" should, in turn, drive others toward active engagement in building a cybersecurity-savvy culture. Recognitions and incentives, offered as part of an organization's overall cybersecurity strategy, will achieve shared responsibility across the organization in the longer term [4, 15].

These opportunities highlight the importance of strong leadership, innovation, and the ability to adapt to different contexts to overcome challenges and foster a resilient cybersecurity culture. By turning awareness into actionable behaviors, organizations can empower their workforce to function as a collective human firewall. This collective effort helps protect critical assets and ensures organizational security in an increasingly interconnected world.

4 Limitations

Many challenges to establishing a robust cybersecurity culture remain unverified. The literature highlights issues like resistance to change, resource constraints, and regulatory complexities. Future research should empirically test strategies to address these challenges and facilitate effective implementation within organizations.

5 Conclusion

This paper highlights the importance of cultivating a strong cybersecurity culture to address evolving digital threats. Grounded in SCT, PMT, TPB, and TAM, the proposed framework emphasizes leadership commitment, employee engagement, and continuous training as key enablers of secure behaviors. It addresses challenges such as resistance to change, resource constraints, and regulatory compliance while ensuring adaptability across sectors and organizational sizes. By fostering proactive strategies and tailored solutions, the framework supports the development of a resilient cybersecurity culture that empowers employees as a critical defense against cyber threats.

References

1. Zimba, M., & Keshav, S. (2019). How can the industry help secure the Internet?. Communications of the ACM, 62(3), 46-52.
2. Workman, M., Bommer, W. H., & Straub, D. (2019). Security lapses and the omission of information security measures: A threat control model and empirical test. Journal of the Association for Information Systems, 20(3), 234-266.
3. Woldegebreal, D. Z., & Riedl, R. (2019). Cybersecurity culture in Ethiopia: Analysis and recommendations. In 2019 IST-Africa Week Conference (IST-Africa) IEEE, 1-12.
4. Corradini, I., & Corradini, I. (2020). Building a cybersecurity culture. Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology, 63-86.
5. Martin, J. J., & Guerrero, M. D. (2020). Social cognitive theory. In Routledge Handbook of Adapted Physical Education (pp. 280-295). Routledge.
6. Eloff, M. M., & Eloff, J. H. (2020a). Developing a cybersecurity culture in South Africa: A comprehensive framework. Computers & Security, 92, 101-689.
7. bin Mohammed Almoughem, K. A. (2023). The Future of Cybersecurity Workforce Development. Academic Journal of Research and Scientific Publishing| Vol, 4(45).
8. Fezzey, T., Batchelor, J. H., Burch, G. F., & Reid, R. (2023). Cybersecurity Continuity Risks: Lessons Learned from the COVID-19 Pandemic. Journal of Cybersecurity Education, Research and Practice, 2022(2), 4.
9. Abaidi, S. A., & Al-Sharhan, S. (2019). Cybersecurity training and education in Iran: Challenges and opportunities. Journal of Cybersecurity Education, Research and Practice, 1-14.
10. Abbasi, G. A., Kumaravelu, J., Goh, Y. N., & Singh, K. S. D. (2021). Understanding the intention to revisit a destination by expanding the theory of planned behavior (TPB). Spanish Journal of Marketing-ESIC, 25(2), 282-311.
11. Davis, F. D., Granić, A., & Marangunić, N. (2024). The technology acceptance model: 30 years of TAM. Springer International Publishing AG.
12. Abdel-Basset, M., Chang, V., & Nabeeh, N. A. (2020). Advantages of fostering a cybersecurity culture in Egypt: A case study. International Journal of Information Management, 51, 102-157.
13. Eloff, M. M., & Eloff, J. H. (2020b). Challenges in enhancing cybersecurity awareness and comprehension in South Africa: A study on limited resources. Journal of Information Privacy and Security, 16(1), 38-51.
14. Wessel, R. A., & Heim, T. N. (2023). The Various Dimensions of Cyberthreats:(In) consistencies in the Global Regulation of Cybersecurity. Anales de Derecho.
15. Gallego-Nicasio, E., Alcaraz, S., & Santos, O. C. (2021). The cybersecurity culture in Spain. Computers & Security, 108, 102-223.
16. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.
17. Haney, J. M., & Lutters, W. G. (2019). Motivating cybersecurity advocates: Implications for recruitment and retention. Proceedings of the 2019 Computers and People Research Conference,
18. Al Mehairi, A., Zgheib, R., Abdellatif, T. M., & Conchon, E. (2023). Cyber Security Strategies While Safeguarding Information Systems in Public/Private Sectors. Electronic Governance with Emerging Technologies: First International Conference, EGETC 2022, Tampico, Mexico, September 12–14, 2022, Revised Selected Papers.