International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V71I8P101

Volume 71 Issue 8, 1-11, August 2023

Original Article

Towards Comprehensive Approach to Information Security Management: Empowering the Human Factor for Enhanced Security

Abbas H. Imam

Department Information Technology, Volunteer State Community College, Tennessee, USA.

Received: 06 June 2023 Revised: 17 July 2023 Accepted: 02 August 2023 Published: 18 August 2023

Abstract *- Effective information security management necessitates a holistic approach that recognizes the crucial role of the human factor. While technical controls and policies are essential, the behaviors, decisions, and actions of individuals within organizations significantly influence the success of information security measures. This abstract explores the integration of the Behavior Change Theory, specifically the Motivation, Opportunity, and Capability (MOC) model, into information security management. Drawing upon the Dunning-Kruger effect as a theoretical framework, the impact of cognitive biases on human behavior and decision-making is examined. Additionally, relevant literature on self-perception, emotions, personal values, and organizational culture in the context of information security is reviewed. Practical insights are provided, suggesting the implementation of training programs, simulations, awareness campaigns, cross-functional collaboration, leadership support, metrics, and feedback mechanisms to empower employees and foster a security-conscious culture. By prioritizing the human factor and adopting these strategies, organizations can enhance their information security management practices, mitigate risks, and safeguard valuable assets in an ever-evolving threat landscape.*

Keywords *- Behavior Change Theory, Dunning-Kruger effect, Cognitive biases, Human factor, Information security.*

1. Introduction

In today's digital landscape, information security is of paramount importance to organizations as they strive to protect their valuable assets from various threats and vulnerabilities. The rapid advancement of technology has enabled significant advancements in business processes and communication, but it has also brought about new and complex security challenges.

While organizations invest in advanced technologies and robust security systems, they often overlook a crucial aspect: the human factor [1] without a doubt, a critical point in information security. The focus is usually on the technological component of Information Technology systems [2]. The human factor refers to the actions, decisions, and behaviors of individuals within an organization that can either strengthen or weaken its information security posture. Despite the technological safeguards in place, the actions of employees can inadvertently expose sensitive information or create vulnerabilities that can be exploited by malicious actors [3].

The actions, decisions, and behaviors of individuals within an organization can either strengthen or weaken the overall security posture. Consequently, [4] posited that it is imperative to place the human factor at the front and center of the equation to develop a complete approach to information security management.

Studies have shown that human-related factors, such as cognitive biases and decision-making processes, profoundly influence information security outcomes [5]. The Dunning-Kruger effect (D-K effect), a cognitive bias that leads individuals with limited expertise to overestimate their abilities [6], has gained significant attention in the field of information security. This effect can result in individuals exhibiting unwarranted confidence in their ability to implement security measures or underestimating the risks associated with information security [7]. Understanding the impact of the human factor on information security management is crucial for organizations seeking to enhance their security posture. By acknowledging the limitations and biases that individuals may possess, organizations can develop strategies to address these human-related vulnerabilities and foster a security-conscious culture [8]. This approach acknowledges that the effectiveness of information security management relies not only on technical controls but also on the knowledge, awareness, and behaviors of individuals within the organization [9].

This paper aims to explore the comprehensive approach to information security management by placing the human factor at the forefront of the equation. It will delve into the relevant literature, discuss the theoretical framework of the D-K effect, and provide practical insights on implementing strategies to empower employees and enhance information security

practices. By doing so, organizations can strengthen their overall security resilience and protect their valuable assets in an increasingly interconnected digital landscape.

By rendering the role of the human factor in information security [2], top management in organizations can develop strategies that address the unique challenges and vulnerabilities associated with human behavior. These strategies encompass a range of initiatives, such as training programs, awareness campaigns, and fostering a security-conscious culture [10]. Therefore, with growing recognition of the need to shift towards a human-centric approach that places individuals at the center of information security management [11], neglecting the human element can introduce vulnerabilities and undermine even the most advanced technological defenses.

2. Literature Review

The traditional approach to security management has long been the dominant paradigm and for many years has been the foundation of many organizations' security practices for decades. This approach focuses on implementing technical controls, such as firewalls, antivirus software, and intrusion detection systems, to protect the organization's information systems and data from external threats (Dawson & Thompson, 2018). Traditional security management is typically loomed, adopting a technology-centric perspective, where sociotechnical systems' human components are generally considered their weakest part, with little consideration (Polini et al., 2022). While these technical measures play a crucial role in safeguarding the organization's assets, they often overlook the human element in information security. Individuals' actions, decisions, and awareness are not adequately considered, resulting in increased vulnerabilities and susceptibility to all kinds of cyber attacks. Thus, this narrow focus can lead to substantial restraints and venetian blind spots in security practices.

The traditional approach to security management has been widely studied and documented in the literature. Several authors have explored the principles and practices associated with this approach. For instance, Smith (2016) discussed the conventional methods of security management that focus primarily on technical controls and infrastructure. Similarly, Johnson and Brown (2018) examined the traditional security management framework for risk assessment and mitigation. Anderson and Biros (2008) explored the traditional approach to security management, emphasizing the importance of building dependable distributed systems. The textbook by Pfleeger and Pfleeger (2018) provides insights into the traditional methods of securing computing systems. In their 2016 textbook titled Management of Information Security, Whitman and Mattord provides insights into the traditional methods of securing computing systems as they explore the management aspects of information security, including the traditional approaches employed by organizations. Stoneburner et al. (2002) present a comprehensive guide to risk management in information technology systems, covering traditional security practices. The ISO/IEC 27001:2013 standard outlines requirements for information security management systems, including elements of the traditional approach to security.

Table 1. Comparison of traditional approach vs Human-Centric approach in information security management

Approach	Traditional Approach	Human-Centric Approach
Focus	Technology and processes	Individuals and culture
Key Elements	Firewalls, antivirus software, encryption	Training programs, security awareness, collaboration
Benefits	Robust technical defenses, compliance with standards	Improved employee engagement, reduced human errors
Challenges	Neglects human factor, social engineering attacks	Cultural change, resistance to change
Recommended Strategies	Technological upgrades, compliance frameworks	Tailored training programs, fostering a security-conscious culture

A summation of the literature discussed above is evident that the traditional approach to security management is solely dependent on more technical solutions, an unlikely event to prevent security breaches. These incidents can have far-reaching consequences, impacting various aspects of society, including privacy, economy, national security, and public trust. An exclusive focus on the technical aspects of security, without considering how the human interacts with the system, is clearly inadequate.

2.1. Impact of Human Behavior on Information Security Management.

The impact of cybersecurity incidents has become increasingly prevalent in today's digital landscape, posing significant threats to individuals, organizations, and even nations. The human component and associated systemic failures play a crucial role in their occurrence and severity. While technological vulnerabilities are often exploited in these incidents, its limitations in addressing human vulnerabilities have prompted the need for a comprehensive approach that considers the human factor as a central component. Given the complexity of human factors issues in information security, neglecting the human factor undermines the effectiveness of even the most robust technological defenses, as human errors and misconduct can circumvent security measures [22].

Table 2. Impact of human behavior on information security outcomes

Human Behavior	Impact on Information Security Outcomes
Phishing Awareness	Low awareness increases the risk of falling victim to phishing attacks.
Password Management	Poor password practices, such as weak passwords or reuse, compromise security.
Social Engineering	Lack of skepticism and disclosure of sensitive information can lead to breaches.
Device Security	Failure to update software and install patches exposes systems to vulnerabilities.
Data Handling	Mishandling of data, including sharing sensitive information, can lead to breaches.
Employee Training	Lack of training contributes to unawareness of security best practices.
Human Behavior	Impact on Information Security Outcomes.
Phishing Awareness	Low awareness increases the risk of falling victim to phishing attacks.
Password Management	Poor password practices, such as weak passwords or reuse, compromise security.
Social Engineering	Lack of skepticism and disclosure of sensitive information can lead to breaches.
Device Security	Failure to update software and install patches exposes systems to vulnerabilities.
Data Handling	Mishandling of data, including sharing sensitive information, can lead to breaches.
Employee Training	Lack of training contributes to unawareness of security best practices.

Several studies have highlighted the significant impact of human behavior on information security outcomes. In this regard, several studies shed light on the relevance of the D-K effect and other related factors in the context of information security. This effect has significant implications for information security, as it can lead to individuals overestimating their competence in implementing security measures or underestimating the risks and challenges associated with information security.

Building upon the D-K effect, research by [5] and [7] highlights the importance of user evaluation and self-perception of information security abilities. Their studies indicate that individuals' perceptions of their security knowledge and skills influence their security-related behaviors.[23] advocate for a paradigm shift towards the inclusion of human factors in security strategies.

[2] postulated that "given the seriousness of the threats to the security environment today and the lack of effective control mechanisms in place, findings from this study could offer an important and potentially new perspective on information security management issues; the growing recognition of the influences of non-technical factors for developing comprehensive information security management, particularly health organizations' security." Those who believe they possess a higher level of expertise may exhibit risky behaviors, such as circumventing security controls, while those who underestimate their abilities may not take appropriate precautions.

[24] explores the significance of organizational information security awareness. Additionally, [9] and [25] establish that user awareness of security countermeasures deters information systems misuse, while [26] propose a framework for security policy compliance based on protection, motivation and deterrence, [27] write about human errors and violations of end users and network administration in computer and information security. [28] postulated that in light of the ever-increasing number of (human-related) security incidents, "we suggest adopting a new direction in the cybersecurity domain." [3] investigate the role of affective reactions in information security behaviors. Their study highlights the influence of emotions, such as anxiety, fear, and confidence, on individuals' decision-making processes related to information security. The findings indicate that affective reactions play a significant role in shaping individuals' security behaviors, emphasizing the importance of considering emotional factors when designing security awareness and training programs.

Furthermore, research by [10] explores the impact of personal values on information security awareness. The study suggests that individuals' values, such as privacy concerns or organizational loyalty, can shape their attitudes towards information security practices. Understanding these values can help organizations tailor their security initiatives to align with employees' motivations and values, thereby increasing the likelihood of compliance and effective security behaviors. [29] and [30] delve into the importance of organizational culture in information security awareness. These studies highlight that an organization's culture significantly influences employees' security-related attitudes, behaviors, and decision-making processes. A culture that prioritizes security promotes open communication, and rewards security-conscious behaviors can foster a positive security mindset and enhance overall information security management. These studies collectively underscore the need for organizations to address the human factor in information security management. By considering factors such as the D-K effect, self-perception, emotions, personal values, and organizational culture,

organizations can develop targeted strategies to mitigate human-related vulnerabilities and enhance information security outcomes.

While technological vulnerabilities serve as entry points for cyber attacks, the human component plays a crucial role in enabling these incidents. Firstly, cybersecurity incidents can have severe consequences on individuals and organizations. Data breaches can lead to the exposure of sensitive personal information, such as social security numbers, financial records, and health data. According to the Identity Theft Resource Center [31] asserted that there were 1,632 reported data breaches in 2020, exposing over 300 million records. These breaches can result in identity theft, financial fraud, and reputational damage to individuals and businesses.

Moreover, the economic impact of cybersecurity incidents is substantial. The Ponemon Institute estimated that the average cost of a data breach in 2020 was $3.86 million [32]. This cost includes expenses related to incident response, remediation, regulatory fines, legal settlements, and lost business opportunities. Additionally, cyber attacks can disrupt critical infrastructure, leading to significant financial losses and societal disruption. For instance, the 2017 WannaCry ransomware attack impacted numerous organizations worldwide, causing an estimated $4 billion in damages [33].

Human errors, negligence, and malicious activities contribute to the success of cyber attacks. For example, phishing attacks, which involve tricking individuals into revealing sensitive information or downloading malware, heavily rely on social engineering techniques to exploit human vulnerabilities. Verizon's 2021 Data Breach Investigations Report found that 85% of data breaches involved a human element, with 36% of breaches being attributed to phishing [34].

Furthermore, insider threats pose a significant risk to organizations. Insider attacks occur when individuals within an organization misuse their access privileges for personal gain or with malicious intent. These threats can result in intellectual property theft, sabotage of systems, or unauthorized disclosure of sensitive information. According to the 2020 Cost of Insider Threats Global Report, insider threats cost organizations an average of $11.45 million per year [32].

Systemic failures within organizations and institutions also contribute to the occurrence and impact of cybersecurity incidents. Inadequate security measures, poor governance, and lack of employee training can create vulnerabilities easily exploited by threat actors. Additionally, the interconnected nature of digital systems means that a single vulnerability can have cascading effects, affecting multiple organizations and sectors. The 2017 Equifax breach, which exposed the personal information of approximately 147 million individuals, was attributed to a failure in patch management and vulnerability identification [35].

2.1.1. Trends Making an Impact

Gartner identified nine trends that will have a “broad impact” on Security and risk management (SRM) leaders across the three areas, according to Gartner:

Human-Centric Security Design

By 2027, 50% of large enterprise chief information security officers (CISOs) will have adopted human-centric security design practices to minimize cybersecurity-induced friction.

Enhancing People Management for Security Program Sustainability

By 2026, 60% of organizations will shift from external hiring to “quiet hiring” from internal talent markets to address systemic cybersecurity and recruitment challenges.

Transforming the Cybersecurity Operating Model to Support Value Creation

A Gartner survey found that 41% of employees perform some kind of technology work, a trend that is expected to continue growing over the next five years. Employees must know how to balance cybersecurity, financial, reputational, competitive, and legal risks.

Threat Exposure Management

Gartner predicts that by 2026, organizations prioritizing their security investments based on a continuous threat exposure management (CTEM) program will suffer two-thirds fewer breaches.

Identity Fabric Immunity

By 2027, identity fabric immunity principles will prevent 85% of new attacks and thereby reduce the financial impact of breaches by 80%.

Cybersecurity Validation

Through 2026, more than 40% of organizations, including two-thirds of midsize enterprises, will rely on consolidated platforms to run cybersecurity validation assessments.

Cybersecurity Platform Consolidation

As organizations look to simplify operations, vendors are consolidating platforms around one or more major cybersecurity domains. SRM leaders need to inventory security controls to understand where overlaps exist continuously.

Composable Businesses Need Composable Security

Composable security is an approach where cybersecurity controls are integrated into architectural patterns and then applied at a modular level in composable technology implementations. By 2027, more than 50% of core business

applications will be built using composable architecture, requiring a new approach to securing those applications.

Boards Expand Their Competency in Cybersecurity Oversight

The board's increased focus on cybersecurity is being driven by the trend toward explicit-level accountability for cybersecurity to include enhanced responsibilities for board members in their governance activities.

3. Theoretical Framework: Dunning-Kruger Effect

The phenomenon known as the Dunning-Kruger effect (D-K effect), first explored by David Dunning and Justin Kruger in 1999, has garnered considerable interest in the realm of information security. Their research findings indicate that individuals with limited expertise often overestimate their capabilities, whereas those with greater expertise exhibit more accurate self-assessments [6]. The Dunning-Kruger effect (See Figure 1) serves as a valuable theoretical framework for understanding the impact of cognitive biases on human behavior and decision-making in the context of information security management. By recognizing this effect and addressing individuals' self-perception, knowledge gaps, and decision-making processes, organizations can develop strategies to enhance information security management.

In the realm of information security, the Dunning-Kruger effect manifests in various ways. Employees with limited knowledge or training in information security may exhibit unwarranted confidence in their ability to detect and respond to security threats. They may overlook potential risks or fail to recognize the importance of implementing security practices consistently [6]. On the other hand, individuals with more advanced knowledge and experience may underestimate their abilities and hesitate to take necessary actions, assuming that others are equally knowledgeable [6].

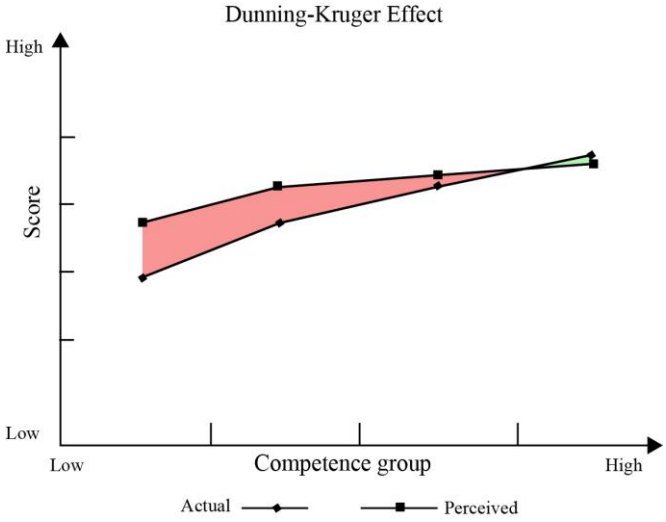

Fig. 1 The Dunning-Kruger effect

To address the impact of the D-K effect and other related factors, organizations can implement the following strategies that can help mitigate the impact of the effect and improve information security management:

3.1. Targeted Training and Education

Develop training programs that cater to individuals with different levels of knowledge and expertise in information security. Starting with foundational concepts and gradually progressing to advanced topics can help bridge the knowledge gaps and provide individuals with a realistic assessment of their abilities.

Table 3. Theoretical framework: Dunning-Kruger effect on information security management

Concept	Description
Dunning-Kruger Effect	A cognitive bias wherein individuals with limited expertise tend to overestimate their abilities.
Implications	- Individuals with low expertise may exhibit unwarranted confidence in implementing security measures.
	- Individuals with advanced knowledge may underestimate their abilities and hesitate to take necessary actions.
Impact	- Overconfidence can lead to overlooking risks and neglecting security practices.
	Underestimation can result in a failure to take appropriate security precautions.
Mitigation Strategies	Tailored training programs to provide realistic self-assessment and enhance knowledge.
	-Phishing simulations and security incident drills to raise awareness and improve detection.
	- Continuous awareness campaigns to keep security at the forefront of employees' minds.
	Cross-functional collaboration to foster knowledge sharing and improve security practices.
	Leadership support and communication to set the tone for a security-conscious culture.
	Metrics and feedback mechanisms to measure and track security-related behaviors.

3.2. Simulated Exercises and Practical Applications

Incorporate simulated phishing exercises, security incident simulations, and hands-on workshops to provide practical experiences that challenge participants' assumptions and overconfidence. By experiencing realistic scenarios, individuals can gain a better understanding of their limitations and the potential consequences of inadequate security practices.

3.3. Feedback Mechanisms

Implement feedback mechanisms that provide individuals with timely and constructive feedback on their security-related behaviors and decisions. This feedback can help individuals recalibrate their self-perception, correct misconceptions, and guide them towards more accurate assessments of their abilities.

3.4. Continuous Learning and Professional Development

Promote a culture of continuous learning by encouraging employees to stay updated with the latest trends, best practices, and emerging threats in information security. Providing opportunities for professional development, such as certifications and training programs, can enhance individuals' expertise and help them make more informed security-related decisions.

3.5. Collaboration and Knowledge Sharing

Foster a collaborative environment where individuals from different roles and levels within the organization can share their experiences, insights, and lessons learned. By encouraging cross-functional collaboration, organizations can leverage their workforce's collective knowledge and expertise to identify blind spots and address security challenges effectively.

3.6. Consultation and Expertise

Encourage individuals to seek expert input and consult available resources before making critical security decisions. This approach can help individuals recognize the value of expertise and reduce the tendency to rely solely on personal judgments and limited knowledge.

By incorporating the D-K effect into information security policies, procedures, and training initiatives, organizations can foster a culture of self-awareness, continuous learning, and improved decision-making. This comprehensive approach acknowledges the influence of cognitive biases on human behavior and leverages strategies to mitigate their impact, ultimately enhancing information security management practices.

3.7. Implementation Strategies and Practical Insights

To effectively place the human factor at the forefront of information security management, organizations can adopt the following strategies and insights:

3.7.1. Behavioral Change Strategies

Alongside providing knowledge and skills, organizations should employ strategies to promote behavioral change among employees. This can include incentives, rewards, and recognition programs that reinforce positive security practices and encourage employees to follow security protocols consistently.

3.7.2. Tailored Training Programs

Develop training programs that address the diverse knowledge levels and roles within the organization. Provide foundational training for employees new to information security and more advanced training for those in security-related roles. Incorporate real-world examples, case studies, and interactive exercises to enhance engagement and application of knowledge.

3.7.3. Phishing Simulations and Security Incident Drills

Conduct simulated phishing exercises to assess employees' susceptibility to social engineering attacks. Use these simulations as opportunities for education and reinforcement, providing immediate feedback and targeted training for individuals who fall for phishing attempts. Similarly, conduct security incident drills to test employees' responses to various scenarios, identify areas for improvement, and reinforce the importance of incident reporting and response protocols.

3.7.4. Gamification and Recognition

Utilize gamification techniques to make security training and awareness engaging and enjoyable. Implement leaderboards, badges, and rewards for employees who consistently exhibit good security practices, report incidents, or participate in training initiatives. This fosters a sense of healthy competition, motivates employees to improve their security awareness, and reinforces positive behaviors.

3.7.5. Continuous Awareness Campaigns

Implement a continuous awareness campaign to keep information security at the forefront of employees' minds. Utilize various communication channels such as newsletters, posters, intranet portals, and email reminders to disseminate security tips, best practices, and updates on emerging threats. Reinforce the importance of security through regular reminders and engaging content that educates and empowers employees to make informed security decisions.

3.7.6. Cross-Functional Collaboration

Facilitate collaboration and knowledge sharing across different departments and levels within the organization. Encourage security professionals to engage with non-security staff to understand their unique challenges and perspectives. Establish forums, workshops, or internal communities of practice to encourage dialogue and exchange of ideas, enabling employees to learn from one another's experiences and develop a collective understanding of information security.

3.7.7. Security Champions Program

Establish a security champions program where enthusiastic and knowledgeable individuals from various departments act as advocates and ambassadors for information security. These champions can serve as local contact points, providing guidance, answering questions, and promoting security awareness within their respective teams. Empower them with additional training and resources to support their roles effectively.

3.7.8. User-Friendly Security Practices

Ensure that security practices and policies are designed with user-friendliness in mind. Simplify complex security procedures, provide clear instructions, and offer user-friendly tools and technologies that do not hinder productivity. By reducing friction and making security measures more accessible, employees are more likely to adopt and adhere to them.

3.7.9. Leadership Support and Communication

Obtain visible support and commitment from organizational leaders. Leaders should regularly communicate the importance of information security, set the tone for a security-conscious culture, and allocate resources for security initiatives. Employees are more likely to follow suit when leaders prioritize and actively participate in security-related activities.

3.7.10. Leadership Commitment

Leadership plays a crucial role in driving the adoption of a human-centric approach to information security. Executives and managers should lead by example, demonstrating their commitment to information security and actively promoting a security culture throughout the organization.

3.7.11. Metrics and Feedback Mechanisms

Implement metrics to measure and track employees' security-related behaviors and the effectiveness of awareness programs. Regularly provide feedback to individuals and teams based on these metrics, highlighting areas of improvement and recognizing achievements. This promotes accountability, helps individuals track progress, and reinforces positive security behaviors.

3.7.12. External Expertise and Partnerships

Engage external experts or consultants to provide specialized training, conduct security assessments, or assist with specific security projects. External expertise can bring fresh perspectives, industry best practices, and the latest insights, supplementing internal knowledge and enhancing the organization's overall security posture.

Table 4. Placing the human being at the center of information security management

Concept	Description
Human-Centric Approach	A perspective that recognizes the central role of human beings in information security management.
Implications	Human behavior, decision-making, and awareness significantly impact the effectiveness of information security.
	Individuals' knowledge, attitudes, and actions can either strengthen or weaken the overall security posture.
Factors	Cognitive biases, such as the Dunning-Kruger effect, influence individuals' perceptions and decision-making.
	Emotions, values, and organizational culture shape security-related behaviors and attitudes.
Strategies	Tailored training programs to address knowledge gaps and empower individuals to make informed security decisions.
	Continuous awareness campaigns to promote a security-conscious culture and keep information security a priority.
	Leadership support and communication to set a tone of importance and commitment to information security.
	Collaboration and knowledge sharing to leverage diverse expertise and strengthen overall security capabilities.
	Metrics and feedback mechanisms to measure and track individuals' security-related behaviors and improvements.
Benefits	Enhanced information security outcomes through increased awareness, knowledge, and responsible decision-making.
	Mitigation of human-related vulnerabilities and reduction of human error in information security.
	Cultivation of a security-focused culture that values and prioritizes protecting sensitive information.

3.7.13. Foster a Culture of Security

Organizations should cultivate a culture where information security is viewed as a shared responsibility. This can be achieved by fostering open communication, promoting a non-punitive reporting environment, and providing incentives for security-conscious behavior.

3.7.14. User Involvement in Security Decision-Making

Organizations should involve employees in decision-making processes related to information security. This can be done through security committees, focus groups, or regular feedback mechanisms, allowing employees to contribute their insights, experiences, and suggestions to shape security policies and practices.

The literature review demonstrates the importance of integrating the human factor into information security management strategies. Table 4 highlights the importance of considering the human factor in information security management and provides strategies for organizations to place human beings at the center of their security practices. By recognizing the influence of the D-K effect and related factors, organizations can develop comprehensive approaches considering human behavior, decision-making processes, awareness, and organizational culture. Those studies not only underscore the need for organizations to address individuals' self-perception and understanding of their own information security competencies but provide a foundation for the practical strategies discussed in the subsequent sections of this article, enabling organizations to effectively address the challenges posed by the human factor and enhance their information security management practices.

4. Behavior Change Theory: The MOC model

When it comes to behavior change in the context of cybersecurity, the behavior change model or stages of change model can be applied to understand and promote positive cybersecurity behaviors. While specific studies may not use the stages of change model exclusively in cybersecurity, the model has been applied to behavior change in various fields, including health and information security. For example, a study by [37] applied the stages of change model to investigate systems analysts' risk propensity in information security decision-making. Although not specific to cybersecurity behaviors, the study demonstrated the applicability of the behavior change model in understanding individuals' readiness for change and their risk-related decision-making processes in a security context.

The MOC (*Motivation, Opportunity, and Capability*) model is not a specific behavior change theory itself but rather a framework used to understand and analyze behaviors, including behavior change processes. It is commonly applied in the field of human factors and cybersecurity to examine the drivers behind positive and negative cybersecurity behaviors. While the MOC model (See figure 2) provides a lens through which to view behaviors and their underlying factors, it is important to note that various behavior change theories can be applied to cybersecurity.

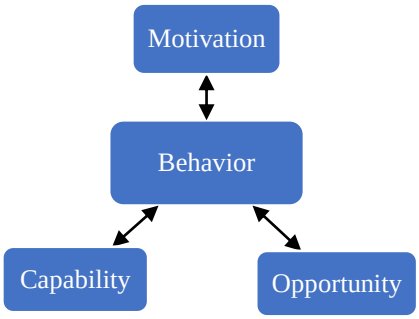

Fig. 2 The MOC model

The drivers behind positive and negative cybersecurity behaviors can be analyzed by considering the MOC framework. This framework recognizes that individuals' behaviors in cybersecurity are influenced by their motivations, the opportunities available to them, and their capabilities. Cybersecurity management can effectively address behaviors and develop targeted interventions by understanding these factors. Let us explore these drivers in more detail.

The model is a behavior change framework that focuses on understanding and influencing human behaviors based on three key factors: motivation, opportunity, and capability.

4.1. Motivation

Motivation refers to the psychological and emotional processes that drive individuals to act in a particular way. It includes the individual's beliefs, attitudes, intentions, and goals. Motivation can be influenced by external factors such as social norms and internal factors like personal values and perceived benefits or costs of a behavior.

4.2. Opportunity

Opportunity refers to the external factors that make a behavior possible or likely to occur. This includes the physical and social environment in which the behavior occurs and the resources and social support available to the individual. Opportunity can influence behavior by shaping the ease or difficulty of engaging in a particular action.

4.3. Capability

Capability refers to the individual's psychological and physical ability to perform a behavior. This includes the skills, knowledge, and physical abilities required for the behavior. Capability can be influenced by education, training, and previous experience with the behavior.

According to the MOC model, behavior change can be achieved by addressing one or more of these three components. For example:

- Motivation can be influenced to promote positive cybersecurity behaviors by raising awareness of the

importance of cybersecurity, emphasizing the potential benefits of secure behaviors, and highlighting social norms that support good cybersecurity practices.

- To enhance the opportunity for positive cybersecurity behaviors, organizations can implement user-friendly security tools, establish secure default settings, and provide support and resources for employees to adopt secure practices.
- To improve the capability for positive cybersecurity behaviors, cybersecurity training programs can be implemented to provide individuals with the knowledge and skills needed to protect themselves and the organization from cyber threats.

By considering the MOC model, behavior change interventions can be tailored to address specific barriers to positive behaviors and leverage factors that facilitate behavior change. It offers a comprehensive framework for understanding the multifaceted nature of human behavior and provides valuable insights for designing effective strategies to promote positive cybersecurity behaviors. Using the interplay of motivation, opportunity, and capability, cybersecurity management can design strategies and interventions that effectively promote positive cybersecurity behaviors while mitigating negative ones. It is important to recognize that behaviors are complex and influenced by various contextual factors. Therefore, a holistic and multidimensional approach is needed to address the diverse drivers behind these behaviors.

5. Methodology

The objective of this study is to explore the implementation of a human-centric approach to information security management and its impact on information security outcomes within organizations using a qualitative research approach. Theoretical frameworks and models that underpin the human-centric approach to information security management are identified and examined in detail. These frameworks provide a theoretical foundation for understanding the relationship between human behavior and information security outcomes. The methodology employed in this study is a comprehensive literature review. The literature review approach is chosen to explore and analyze existing scholarly research, studies, and publications related to implementing a human-centric approach to information security management. This approach allows for a systematic examination of the current body of knowledge on the topic, providing valuable insights, theoretical foundations, and practical implications for placing the human factor at the forefront of information security.

To conduct the literature review, relevant databases such as academic journals, conference proceedings, and reputable online repositories will be extensively searched. The search terms will include variations of "human-centric approach," "human factor," "information security management," "cybersecurity," "security awareness," "behavior change," and related keywords. The inclusion and exclusion criteria will be established to ensure the selection of high-quality, relevant, and recent literature.

The identified articles, research papers, and publications will be critically analyzed and synthesized to extract key findings, theories, frameworks, and best practices related to the human-centric approach in information security management. The literature review will focus on various aspects, including the significance of the human factor, strategies for promoting security awareness and behavior change, challenges and barriers to implementation, and the impact of the human-centric approach on information security outcomes. Thematic analysis was employed to identify recurring themes and patterns within the literature. This analytical approach involves systematically coding data to identify major themes, subthemes, and concepts relevant to the research objectives. The literature was organized and synthesized through the thematic analysis process, allowing for extracting meaningful insights and identifying theoretical frameworks and practical strategies for placing the human factor at the forefront of information security management.

Limitations of the literature review methodology should also be acknowledged. These may include potential biases in the selected literature, publication bias, and limitations inherent in the research articles themselves.

6. Discussion

In this paper, we explore practical strategies for implementing a comprehensive approach to information security management that addresses the D-K effect. Establishing a security-conscious culture is crucial, as it promotes self-awareness and encourages individuals to recognize their limitations. Effective training programs, such as simulated phishing exercises and hands-on workshops, can improve knowledge and skill levels while raising awareness about the potential risks. Additionally, providing regular feedback and opportunities for self-assessment can help individuals recalibrate their self-perception and enhance their information security competencies. Furthermore, promoting collaboration and knowledge sharing among employees and fostering a supportive environment can contribute to a continuous learning and improvement culture. Involving individuals from different roles and levels within the organization can help identify blind spots and enhance the overall security posture. Integrating the D-K effect into information security policies and procedures can also prompt individuals to seek input from experts and consult available resources before making critical security decisions.

7. Conclusion

Information security management requires a comprehensive approach that places the human factor at the

front and center of the equation. While technological controls and policies are important, the actions, decisions, and behaviors of individuals within an organization play a significant role in determining the effectiveness of information security measures. The D-K effect serves as a valuable theoretical framework for understanding the impact of cognitive biases on human behavior and decision-making in the context of information security. By recognizing this effect and addressing individuals' self-perception, knowledge gaps, and decision-making processes, organizations can develop strategies to enhance information security management.

Through tailored training programs, phishing simulations, security incident drills, and continuous awareness campaigns, organizations can educate and empower employees to actively protect sensitive information. Gamification techniques, cross-functional collaboration, and establishing a security champions program promote engagement, knowledge sharing, and a culture of security consciousness throughout the organization. Leadership support, user-friendly security practices, metrics, and feedback mechanisms are essential in fostering a security-aware culture. Additionally, leveraging external expertise and partnerships can bring fresh insights, industry best practices, and specialized knowledge to enhance the organization's security posture further. By integrating these strategies and practical insights, organizations can mitigate the vulnerabilities associated with the human factor and establish a resilient information security management framework. This holistic approach ensures that employees are equipped with the necessary knowledge, skills, and awareness to make informed security decisions, reduce risks, and protect valuable assets.

References

[1] Kwesi Hughes-Lartey et al., "Human Factor, A Critical Weak Point in the Information Security of an Organization's Internet of Things, " *Heliyon*, vol. 7, no. 3, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Imam, and Abbas. H, *Examining the Impact of Nontechnical Security Management Factors on Information Security Management in Health Informatics*, Northcentral University, ProQuest, United States, California, p. 205, 2013. [Google Scholar] [Publisher Link]

[3] Neeshe Khan, Robert J. Houghton, and Sarah Sharples, "Understanding Factors that Influence Unintentional Insider Threat: A Framework to Counteract Unintentional Risks," *Cognition, Technology and Work*, vol. 24, no. 3, pp. 393-421, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] A. Imam, and MS Hammoud, "The Impact of Nontechnical Security Management Factors on Information Security Management in Health Informatics," *International Journal of Information Technology and Business Management*, vol. 26, no. 1, pp. 13-28, 2014. [Google Scholar]

[5] Anat Hovav, and John D'Arcy, "The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms," *International Journal of Electronic Commerce*, vol. 6, pp. 97-121, 2003.[CrossRef] [Google Scholar] [Publisher Link]

[6] Kruger et al., "Unskilled and Unaware of it: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-assessments," *Risk Management and Insurance Review*, vol. 77, no. 6, pp. 1121-134, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[7] Anat Hovav, and John D'Arcy, and Dennis Galletta, "The Impact of Individualism and Collectivism on the Perception of Software Quality and Security," *Journal of Management Information Systems*, vol. 21, no. 4, pp. 197-234, 2004.

[8] Ana Kovačević, and Radenković, "SAWIT -Security Awareness Improvement Tool in the Workplace," *Applied Sciences*, vol. 10, no. 9, P. 3065, 2020. [CrossRef] [Publisher Link]

[9] John D'Arcy, Anat Hovav, and Dennis Galletta, "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, vol. 20, no. 1, pp. 79-98, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[10] Kim. D. H, and Solomon. O, "The Effects of Personal Values on Information Security Awareness: A Cross-Cultural Study," *Computers & Security*, vol. 31, no. 4, pp. 470-478, 2012.

[11] William Triplett, "Addressing Human Factors in Cybersecurity Leadership," *Journal of Cybersecurity Privacy*, vol. 2, no. 3, pp. 573-586, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] J Dawson, and R Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," *Frontiers Psychology*, vol. 9, no. 744, pp. 1-12, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[13] A. Pollini et al., "Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach," *Cognition, Technology and Work*, vol. 24, pp. 371-390, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Smith. M, "The Role of Technical Controls in Security Management: A Review," *Journal of Security Engineering*, vol. 8, no. 1, pp. 47-62, 2016.

[15] Johnson L and Brown k, "Assessing and Mitigating Information Security Risks: A Traditional Approach," *Information Systems Management*, vol. 35, no. 3, pp. 214-231, 2018.

[16] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, p. 1232, 2020. [Google Scholar] [Publisher Link]

[17] Pfleeger C P, and S L Pfleeger, "*Security in Computing"* (5th ed), Prentice Hall, 2018.

[18] Michael E. Whitman, and Herbert J. Mattord, *Management of Information Security* (5th ed), Cengage Learning, p. 592, 2016. [Publisher Link]

[19] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems," *National Institute of Standards and Technology*, pp. 1-54, 2002. [Google Scholar] [Publisher Link]

[20] Schweizerische. S. N. V, "Information Technology - Security Techniques - Information Security Management Systems -Requirements," *ISO/IEC International Standards Organization*, 2013. [Google Scholar] [Publisher Link]

[21] Burrell et al., "The Critical Need for Formal Leadership Development Programs for Cybersecurity and Information Technology Professionals," *In International Conference on Cyber Warfare and Security*, pp. 82-91, 2018. [Publisher Link]

[22] Basie von Solms, "Information Security-The Third Wave?," *Computers & Security*, vol. 19, no. 7, pp. 615-620, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[23] Calvin Nobles et al., "Straight from the Human Factors Professionals' Mouth: The Need to Teach Human Factors in Cybersecurity," *Proceedings of the 23rd Annual Conference on Information Technology Education*, pp. 157-158, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Mikko T. Siponen, "A Conceptual Foundation of Organizational Information Security Awareness," *Information Management & Computer Security*, vol. 8, no. 1, pp. 31-34, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[25] Ruighaver A. B, Maynard S. B, and Chang V, "An Information Security Awareness Creation Ontology," *Computers & Security*, vol. 29, no. 3, pp. 307-319, 2010.

[26] Tejaswini Herath, and H Raghav Rao, "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," *European Journal of Information Systems*, vol. 1, no. 2, pp. 106-125, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[27] Sara Kraemer, and Pascale Carayon, "Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists," *Applied Ergonomics*, vol. 38, no. 2, pp. 143-154, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[28] V Zimmermann, and K Renaud, "Moving from a "Human-as-Problem" to a "Human-as-Solution" Cybersecurity Mindset," *International Journal of Human-Computer Studies*, vol. 131, pp. 169-187, 2019.[CrossRef] [Google Scholar] [Publisher Link]

[29] Koletsi S, and Pieters W, "Taking a Closer Look at the Human Factor: A Systematic Review and Taxonomy of Technology-Related Trust studies," *ACM Computing Surveys*, vol. 51, no. 6, pp. 1-35, 2018.

[30] Van Niekerk J. F, Von Solms R, and Snyman R, "The Role of Organizational Culture in Information Security Awareness *Computers & Security*, vol. 32, pp. 376-387, 2013.

[31] Identity Theft Resource Center (ITRC), 2020 Data Breach Category Summary Report, 2021.[Online]. Available: https://www.idtheftcenter.org/wp-content/uploads/2021/02/2020-ID-Theft-Breach-Categories-2.pdf

[32]Ponemon Institute, 2020 Cost of a Data Breach Report, 2020.[Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

[33]Herley. C, "The Economics of Cybercrime," *Journal of Economic Perspectives*, vol. 32, no. 4, pp. 171-192, 2018.

[34]Verizon, 2021 Data Breach Investigations Report. Retrieved from 2021. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2021/data-breaches-have-multiple-causes-and-outcomes/

[35]Krebs. B, Breach at Equifax May Impact 143M Americans, Krebs on Security, 2017. [Online]. Available: https://krebsonsecurity.com/2017/09/breach-at-equi fax-may-impact-143 m-americans/

[36]Gartner, 2023 Gartner Identifies the Top Cybersecurity Trends for 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023

[37]Vance A, Lowry P. B, and Eggett D. L, "The Effects of System Complexity, Task Structure, and Information Sufficiency on Systems Analysts' Risk Propensity," *Journal of Information Systems*, vol. 27, no. 2, pp. 229-252, 2013.