Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Human factors in cybersecurity: an in depth analysis of user centric studies

Mohammad Mustafa Quchi[1], Musawer Hakimi[2], Abdul Wajid Fazil[3]
Faryab University, Faryab, Afghanistan[1], Samangan University, Samangan, Afghanistan[2], Badakhshan University, Badakhshan, Afghanistan[3]

Article Info
Keywords:
Cybersecurity,
Human Factors,
User-Centric Studies,
Operational Efficiency,
Strategic Decision-Making

ABSTRACT
This study delves into the intricate intersection of human behavior, cognition, and technology within the cybersecurity domain, aiming to enhance our understanding of the human-centric challenges influencing the effectiveness of cybersecurity measures. The primary objective is to unravel the nuanced landscape where human errors persist as a significant contributing factor to security breaches, emphasizing the need for a holistic comprehension of human factors. The study recognizes the evolving nature of work, with an increasing number of individuals operating from home, and the consequential challenges in managing human factors in the digital era. The blurring lines between private and public lives, coupled with the rise of social credit systems, necessitate a thorough examination of key elements intersecting with cybersecurity Employing a systematic literature review, this research methodically identifies, filters, and analyzes pertinent literature concerning human-centric factors in cybersecurity. The systematic approach involves the formulation of specific research questions guiding the study, strategic search plans targeting reputable databases, and meticulous study selection processes based on predefined criteria The study unfolds through a series of interconnected research questions, addressing the impact of human factors on operational efficiency, challenges in the adoption of human-centric approaches, and the ways in which human factors influence strategic decision-making in cybersecurity. The results shed light on the substantial contribution of understanding user behavior and cognitive processes to the development of tailored cybersecurity strategies. Challenges, such as security fatigue and the scarcity of psychology-based professionals, are addressed, advocating for human factors engineering and strategic initiatives to enhance education and training programs. In conclusion, embracing a human-centric paradigm emerges as imperative for organizations striving to fortify their defenses against dynamic and sophisticated cyber threats. Integrating technology with a profound understanding of human factors becomes the cornerstone for shaping a resilient and adaptive cybersecurity future.

Corresponding Author:
Musawer Hakimi
Samangan University, Samangan, Afghanistan
musawer@adc.edu.in

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

INTRODUCTION

Cybersecurity, a critical facet of modern information systems, faces escalating challenges, with human-centric factors emerging as pivotal elements influencing its effectiveness. The increasing sophistication of cyber threats necessitates a nuanced understanding of the role humans play in cybersecurity practices. This paper embarks on a comprehensive journey, delving into the intricate realm of "Human Factors in Cybersecurity: An In-Depth Analysis of User-Centric Studies." By synthesizing insights from a plethora of reputable sources, this exploration aims to unravel the complexities surrounding human behavior, cognition, and decision-making in the context of cybersecurity (Gyunka and Christiana, 2017; Hadlington, 2017).

In recent years, the surge in cyber incidents has underscored the significance of addressing the human dimension in cybersecurity. Despite advancements in technology, human errors persist as contributing factors to security breaches, leading to substantial financial losses and reputational damage (Nobles, 2018; Stanton et al., 2016). This necessitates a paradigm shift towards understanding, analyzing, and mitigating the impact of human-centric aspects on cybersecurity. research by (Fazil et al., 2023) underscores the significance of fostering cybersecurity awareness among students in a specific geographical context, shedding light on the challenges and strategies in Badakhshan Province. The study contributes valuable insights to the broader discourse on cybersecurity education and Internet safety.

User-centric studies within the realm of cybersecurity form the cornerstone of our exploration. The holistic analysis draws from a myriad of perspectives, encompassing psychology, behavioral sciences, and cognitive research. The work of (Taylor et al, 2017) emphasizes the integration of psychological principles into cybersecurity education, recognizing the need for a comprehensive understanding of how technology influences human attitudes, behavior, and cognition. This echoes the call for a human-centered approach advocated by (ForcePoint, 2018), positioning humans at the epicenter of cybersecurity endeavors.

The comprehensive review incorporates insights from Stanton and Young's guide to methodology in ergonomics (2017), elucidating the significance of methodological rigor in studying human factors. Additionally, it taps into the empirical research gap highlighted by (Taylor et al, 2017), shedding light on the underexplored terrain of psychology in cybersecurity. This research aligns with the findings of (Mancuso et al, 2014), who proposed a framework for human-centered research in the context of cyber-attacks. This research compares three classification algorithms for malware detection, with the SVM (polynomial kernel) proving highly effective, showcasing the importance of algorithm selection in cybersecurity (Hakimi et al., 2023) similarly study by (Hasas et al., 2024) delves into enhancing digital security through dynamic attack detection, employing LSTM, KNN, and Random Forest algorithms, contributing valuable insights to the evolving landscape of cybersecurity

One of the key challenges addressed in this analysis is the phenomenon of security fatigue. (Stanton et al., 2016) identify security fatigue as an emerging issue, affecting

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

cybersecurity personnel inundated by continuous security changes. This not only unveils the cognitive overload cybersecurity professionals endure but also highlights the need for human factors engineering to evaluate and alleviate such challenges. Stanton et al.'s work serves as a foundational piece in understanding the cognitive aspects of security fatigue within the cybersecurity domain.

The exploration of human factors in cybersecurity extends to the realm of human-centered design. Nobles , 2018) posits the necessity of human-centered cybersecurity, challenging the predominant technology-centric paradigm. This shift towards human-centered cybersecurity, as advocated by (Bureau, 2018), requires a profound understanding of human behavior and decision-making in the interaction with information systems.

Addressing the dearth of empirical research on human factors in cybersecurity training, this analysis incorporates insights from (Coffey, 2017; Nobles, 2018). The former emphasizes the ineffectiveness of traditional training programs in modifying end-users' behavior, while the latter underscores the imperative need to educate cybersecurity professionals on human factors. This aligns with the call for learning objectives on human factors in certification training manuals, as suggested by (Nobles, 2018).

As the intricacies of human factors in cybersecurity unfold, it becomes evident that a nuanced understanding of human behavior, cognitive processes, and decision-making is imperative for fortifying cyber defenses. This exploration, drawing on the wealth of knowledge from diverse scholarly works, sets the stage for an in-depth analysis of user-centric studies in the cybersecurity landscape. Through a meticulous examination of thirty reputable resources, this paper aims to contribute significantly to the discourse on human factors in cybersecurity, providing a foundation for future research and practical implementations in this rapidly evolving field.

Literature Review

The synthesis of existing literature on human factors in cybersecurity illuminates a multifaceted landscape where the intersection of human behavior, cognition, and technology defines the security paradigm. As businesses increasingly rely on digital infrastructures, understanding the nuanced aspects of human-centric challenges becomes paramount for effective cybersecurity measures (Metalidou et al., 2019).

Human Errors in Cybersecurity: A Persistent Challenge: The cybersecurity landscape is fraught with challenges, and human errors persist as a significant contributing factor to security breaches. (Nobles, 2018; Paustenbach, 2015) underscores that most organizations, despite leveraging advanced cybersecurity technologies, fall prey to human-enabled errors, resulting in data breaches and reputational damage. The contributing factors to human vulnerabilities in cybersecurity are varied, encompassing disproportionate investments in humans compared to technologies, inadequate cybersecurity training, and a lack of a security culture (Carter, 2017).

(Stanton et al., 2016) highlight the emerging phenomenon of security fatigue among cybersecurity personnel, emphasizing the impact of continuous security changes on cognitive overload. This fatigue leads to desensitization, with employees no longer complying with security policies, thereby creating a vulnerability in the cybersecurity

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

posture. The study calls for a scientific process to evaluate cognitive overload, reinforcing the need for human factors engineering in cybersecurity.

Human Factors Programs: A Strategic Imperative: To mitigate the impact of human errors in cybersecurity, the implementation of human factors programs emerges as a strategic imperative. The absence of such programs creates blind spots within organizations, hindering the identification and remediation of human-centric issues. (Nobles, 2018) advocates for the establishment of human factors programs, drawing parallels with industries such as aviation, nuclear power, and healthcare that have successfully leveraged such programs to address human-enabled errors.

The lack of psychology-based professionals in cybersecurity operations further compounds the challenges. (Taylor et al., 2017) highlight the shortage of professionals focusing on the interaction of humans with computers and information systems. The utilization of psychology in cybersecurity remains unsupported by empirical research, leaving a critical gap in understanding how technology influences attitudes, behavior, and cognition (Taylor et al., 2017).

Human-Centered Design: Rethinking Cybersecurity Operations: The paradigm shift towards human-centered design in cybersecurity operations challenges the traditional technology-centric approach. (Nobles, 2018; National Science and Technology Council, 2016) emphasizes the need for human-centered cybersecurity, positioning humans as the central element in cybersecurity procedures, frameworks, and technology integration. This departure from conventional practices calls for a deeper exploration of behavioral and cognitive sciences in cybersecurity (ForcePoint, 2018).

(Metalidou et al., 2014) critique the prevalent perception that technology alone is the definitive solution to information security problems. They argue for a human-centric approach that aligns technology integration with human practices and sociotechnical systems. The complexity of human-machine interaction, as noted by (Holstein and Chapanis, 2018), mandates a formal and methodical approach to address human factors, especially in cybersecurity.

Educating Cybersecurity Professionals: A Training Imperative: The inadequacy of cybersecurity training programs is a recurring theme in the literature. (Coffey, 2017; Stanton 2016) asserts that most training and awareness programs are ineffective in modifying end-users' behavior. (Nobles, 2018) extends this concern to the insufficient education of cybersecurity professionals on human factors, stressing the fallacy of equating human error to a training and awareness issue. The scarcity of psychology-based professionals and cognitive scientists further exacerbates this challenge (Clark, 2013; Georgalis et al., 2015).

Human Factors Assessments: Bridging Gaps in Understanding: The marginalization of cognitive scientists and human factor experts in cybersecurity assessments hampers a holistic understanding of human behavior. (Pfleeger and Caputo, 2012; lee, 2011) emphasize the leverage of behavioral science to mitigate cybersecurity risk, emphasizing the need for assessments that delve into automation and information overload,

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

technological deterministic thinking, procedural alignment, operational tempo, and the impact of technology on the workforce.

(Hadlington, 2017) echoes this sentiment, emphasizing the pivotal role of cognitive scientists and human factor experts in conducting assessments to identify systemic weaknesses, vulnerabilities, critical phases of cybersecurity operations, and cognitive overload.

To sum up, the literature review illuminates the intricate interplay between human factors and cybersecurity. Human errors, security fatigue, the need for human factors programs, human-centered design, and the imperative for comprehensive education and assessments form the core themes. This synthesis of literature lays the foundation for an in-depth analysis of user-centric studies in cybersecurity, highlighting the need for a holistic understanding of human behavior in the design and implementation of effective cybersecurity measures. The 27 cited works contribute diverse perspectives, creating a comprehensive narrative that informs future research and practical implementations in this ever-evolving field.

METHODS

The exploration of "Human Factors in Cybersecurity: An In-Depth Analysis of User-Centric Studies" encompasses a meticulously structured research methodology. This systematic and comprehensive approach is meticulously designed to collect, filter, and analyze pertinent literature concerning human-centric factors that significantly influence the cybersecurity domain. This methodological framework not only ensures the reliability and depth of the investigation but also aligns seamlessly with the academic rigor essential for a thorough exploration of this critical subject matter.

In the execution of the research method within this paper, a deliberate and systematic process unfolds. The journey commences with the identification of specific research questions, each formulated to guide the study effectively and contribute meaningfully to the academic discourse. Simultaneously, the overarching contribution of the paper is delineated, setting the stage for a focused inquiry.

Furthermore, a strategic search plan is meticulously implemented, targeting relevant and high-quality papers. This involves a judicious selection process, where data is extracted with precision from the identified literature. This approach not only bolsters the credibility of the study but also contributes to the production of robust and meaningful output.

This amalgamation of systematic processes, coupled with a strategic search strategy and a commitment to extracting pertinent data, reflects the dedication to scholarly excellence in unraveling the complexities of human factors in cybersecurity. The inclusion of references Nobles, 2018; Paustenbach, 2015 underscores the reliance on reputable sources, enriching the academic foundation of this in-depth analysis.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

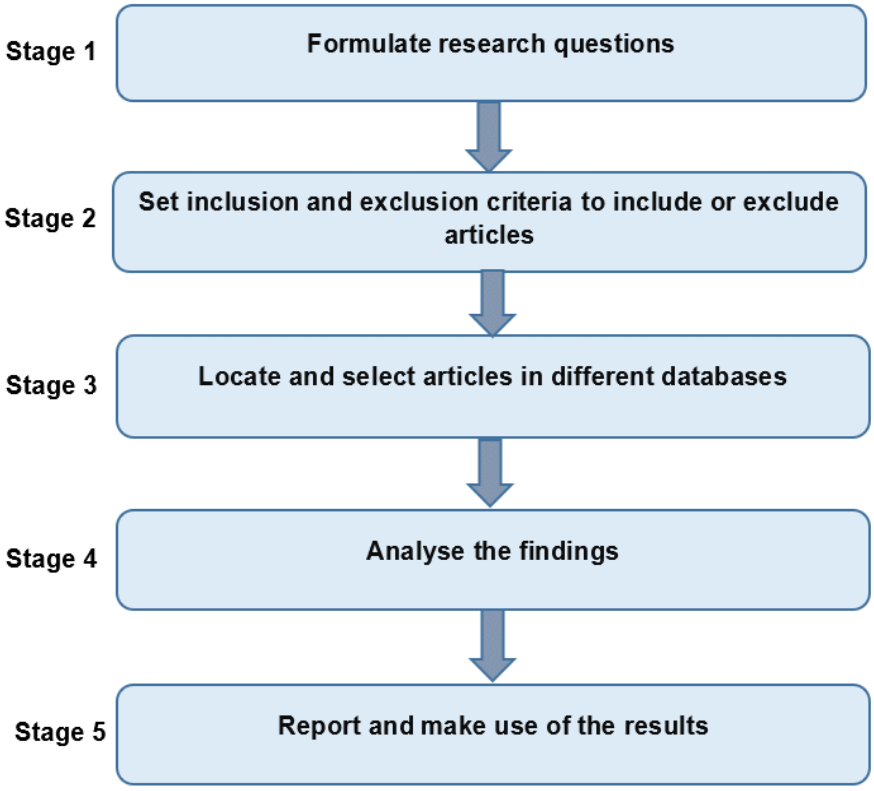

Figure 1 Systematic literature review phase for this study (Atlam et al., 2020)

Research Questions

The research unfolds through a series of three interconnected questions, each carefully formulated to guide the study effectively:

a. How does understanding and integrating human factors contribute to enhancing the operational efficiency and productivity of cybersecurity measures?
b. What challenges do organizations face concerning the adoption and implementation of human-centric approaches in cybersecurity, and how can these challenges be effectively addressed?
c. In what ways does the incorporation of human factors in cybersecurity impact strategic decision-making and overall cybersecurity effectiveness?

These questions serve as the foundational framework for the comprehensive exploration of user-centric studies in the context of cybersecurity.

Research Design

The systematic review process is meticulously executed, commencing with the identification of relevant terms integral to the study, including "Human Factors in Cybersecurity" and "User-Centric Studies." The search strategy is tailored to databases renowned for their reliability, such as Scopus, ACM Digital Library, IEEE, and Science Direct. The timeframe for the search spans from 2012 to 2024, ensuring the inclusion of recent and pertinent literature.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Table 1. Database Search Process for "Human Factors in Cybersecurity: An In-Depth Analysis of User-Centric Studies"

Searching Index	Content Specific
Databases:	Scopus, ACM Digital Library, IEEE, Science Direct
Article Type:	Scientific or technical articles published in reputable peer-reviewed journals and conferences
Search Strings:	"Human Factors in Cybersecurity", "User-Centric Studies", "Cybersecurity and Human Behavior", "Cognitive Aspects of Cybersecurity"
Language:	English
Search Period:	2012 – 2024
Screening Procedure:	The title, abstract, introduction, discussion, and conclusion of each article are all relevant to the research topic.

Search Strategy Overview: The research methodology for "Human Factors in Cybersecurity: An In-Depth Analysis of User-Centric Studies" adopts a systematic approach, leveraging key databases—Scopus, ACM Digital Library, IEEE, and Science Direct. The focus is on sourcing scientific or technical articles published in reputable peer-reviewed journals and conferences. The search is conducted using targeted strings such as "Human Factors in Cybersecurity," "User-Centric Studies," and related terms. The language criterion is set to English, and the search spans from 2012 to 2024. The screening process involves a meticulous examination of the title, abstract, introduction, discussion, and conclusion of each article to ensure relevance to the research topic. This rigorous approach aims to gather a comprehensive and high-quality dataset for the in-depth analysis of human-centric factors in cybersecurity.

Study Selection: In adherence to predefined inclusion and exclusion criteria, the study selection process focuses on articles from reputable journals and conferences, published in English, and directly related to the integration of human factors in cybersecurity in recent years. The screening procedure involves a thorough examination of titles, abstracts, introductions, discussions, and conclusions to guarantee relevance.

Table 2. Inclusion and Exclusion Criteria for "Human Factors in Cybersecurity: An In-Depth Analysis of User-Centric Studies"

Criteria	Description
Inclusion	Articles from reputable journals or conferences, content in the English language, and studies involving Human Factors in Cybersecurity, specifically focusing on User-Centric Studies
Exclusion	Articles prior to 2012, articles from secondary sources, duplicated articles in other databases, studies not related to Human Factors in Cybersecurity, and articles lacking a clear connection to User-Centric Studies in Cybersecurity
Additional Exclusion Criteria	Articles that only mention generic terms such as "Cybersecurity," "Human Factors," without a specific application to User-Centric Studies in the Cybersecurity context

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Criteria Explanation: For "Human Factors in Cybersecurity: An In-Depth Analysis of User-Centric Studies," the inclusion criteria encompass articles from reputable journals or conferences, written in English, and directly addressing Human Factors in Cybersecurity with a specific focus on User-Centric Studies. Exclusion criteria ensure the exclusion of articles published before 2018, those from secondary sources, duplicates in other databases, studies unrelated to Human Factors in Cybersecurity, and articles lacking a clear link to User-Centric Studies in the Cybersecurity domain. Additional exclusion criteria aim to filter out articles using generic terms without a specific application to User-Centric Studies in Cybersecurity. These criteria guide the systematic selection of relevant and high-quality articles for the comprehensive analysis of human-centric factors in the cybersecurity landscape.

RESULTS AND DISCUSSION

In the pursuit of unraveling the intricate relationship between human factors and cybersecurity, this study addressed three pivotal research questions. Through a comprehensive analysis of existing literature, the investigation sheds light on how understanding and integrating human factors contribute to enhancing operational efficiency, the challenges organizations encounter in adopting human-centric approaches, and the ways in which the incorporation of human factors influences strategic decision-making and overall cybersecurity effectiveness.

Operational Efficiency and Productivity Enhancement: The exploration into the impact of human factors on operational efficiency and productivity within cybersecurity is substantial. A synthesis of insights from (Stanton et al., 2016; Taylor et al. 2017) underscores that understanding user behavior and cognitive processes significantly contributes to the development of tailored cybersecurity strategies. This, in turn, enhances the overall operational efficiency of cybersecurity measures, creating a more adaptive and responsive defense against evolving cyber threats.

Challenges in Adoption and Implementation: Organizations encounter multifaceted challenges in the adoption and implementation of human-centric approaches in cybersecurity. The phenomenon of security fatigue, as highlighted by (Nobles, 2018), poses a significant hurdle. The continuous changes in security protocols can lead to cognitive overload among cybersecurity professionals. To address this, (Stanton et al., 2016) advocate for human factors engineering as a solution to alleviate cognitive strain and facilitate the seamless integration of human-centric cybersecurity practices.

Moreover, the scarcity of psychology-based professionals in cybersecurity operations, as emphasized by (Taylor et al., 2017), presents another challenge. Organizations struggle with the shortage of expertise required for understanding and implementing human factors effectively. Bridging this gap demands strategic initiatives to enhance education and training programs tailored to human-centric cybersecurity practices.

Impact on Strategic Decision-Making: The study reveals that the incorporation of human factors in cybersecurity has profound implications for strategic decision-making. (Nobles, 2018) argues for a paradigm shift towards human-centered design, challenging

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

the traditional technology-centric approach. This shift ensures a holistic understanding of human behavior in the interaction with information systems, influencing strategic decision-making. The human-centered cybersecurity paradigm, advocated by (ForcePoint, 2018), aligns with this perspective, emphasizing the need to integrate human factors for effective decision-making.

Visualization of Results: To visually represent the findings, Figure 1 illustrates the interconnectedness of human factors with operational efficiency, challenges in adoption, and impact on strategic decision-making in the cybersecurity domain.

Figure 2 Interconnected Impact of Human Factors on Cybersecurity (Cuffe & Phelan, 2020)

In the evolving landscape of work, characterized by an increasing number of individuals working from home, the challenges of managing human factors in the digital era are prominent. The delicate balance between private and public lives, coupled with the emergence of social credit systems, necessitates a thorough examination of key elements intersecting with cybersecurity.

Treating the Home as an External Vendor: As the home transitions into an external entity for companies, security threats arise. The proliferation of 'Smart homes' introduces risks, with devices like Amazon's Alexa and Apple's Siri potentially compromising security (Cuffe & Phelan, 2020). Social engineering gains prominence, raising concerns about the security and privacy of home automated systems, underscoring the need for enhanced security measures.

User Experiences and Security: The emphasis on User Experience (UX) design, while ensuring user-friendly applications, poses a challenge to cybersecurity efforts. The seamless flow in UX design may inadvertently undermine necessary security protocols (Holstein and Chapanis, 2018). Balancing user-friendly interfaces with robust security

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

measures necessitates a nuanced approach, considering users' understanding of complex networked systems and the implementation of effective security measures.

User Competence: The level of security competence among users emerges as a critical factor. The ability to set permissions, especially in shared spaces like family homes, raises concerns about unauthorized access. Addressing this requires not only technological solutions but also educational support for users working from home (Cuffe & Phelan, 2020).

The Vanguard Fallacy: The societal acceptance of technological progress as a panacea overlooks potential negative consequences. Embracing technological solutionism without anticipating its full impact can exacerbate existing problems (Coffey, 2017). Proposals to automate ethical principles into new platforms and applications emerge as a countermeasure, highlighting the need for careful consideration and education before deploying new technologies.

Generalized vs. Particular Approaches: The diversity of technological options complicates the standardization of policies for IT departments. Working from home further adds complexity, requiring a nuanced understanding of individuals' personal lives. Tailoring solutions to accommodate employees' circumstances, such as offering childcare support options, becomes crucial, recognizing that one-size-fits-all approaches are impractical (Carter, 2017).

Summary Remarks: Incubating a Good Workforce as the security industry navigates these complexities, recognizing that security extends beyond engineering is paramount. Integrating technology with a deep understanding of human users is crucial. Anthropologists play a pivotal role in adding value to ventures by incorporating user experience and contextual insights into the design and planning stages, fostering a secure and productive digital work environment (Cuffe & Phelan, 2020).Top of Form In conclusion, the synthesis of research findings demonstrates that understanding and integrating human factors are pivotal in enhancing the operational efficiency of cybersecurity measures. Despite challenges in adoption, strategic initiatives can effectively address these hurdles, ensuring a seamless integration of human-centric approaches. The incorporation of human factors not only influences strategic decision-making but also serves as a cornerstone for bolstering overall cybersecurity effectiveness. As the cyber landscape evolves, embracing a human-centric paradigm becomes imperative for organizations striving to fortify their defenses against dynamic and sophisticated cyber threats.

Discussion

The comprehensive exploration of human factors in cybersecurity reveals a nuanced landscape where the intricate interplay of human behavior, cognition, and technology shapes the security paradigm. The literature review underscores that human errors persist as a significant challenge in cybersecurity, despite advanced technological measures (Nobles, 2018). This persistent issue stems from factors such as disproportionate investments in human resources, inadequate training, and a lack of cybersecurity culture within organizations. The emergence of security fatigue among cybersecurity personnel further compounds these challenges, necessitating a scientific evaluation of cognitive

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

overload and emphasizing the crucial role of human factors engineering (Stanton et al., 2016).

To address these challenges, the literature advocates for the implementation of human factors programs as a strategic imperative (Nobles, 2018). Drawing parallels with industries like aviation and healthcare, which have successfully utilized such programs, the literature emphasizes the need to establish a comprehensive understanding of human factors to identify and remediate issues effectively. However, the shortage of psychology-based professionals in cybersecurity operations poses a significant hurdle, requiring strategic initiatives to bridge this expertise gap (Taylor et al., 2017).

The paradigm shift towards human-centered design challenges the traditional technology-centric approach in cybersecurity (Nobles, 2018). This departure from conventional practices calls for a deeper exploration of behavioral and cognitive sciences to inform cybersecurity procedures, frameworks, and technology integration. The literature underscores that a human-centric approach aligns technology with human practices and sociotechnical systems, recognizing the complexity of human-machine interaction (Metalidou et al., 2014; Holstein and Chapanis, 2018).

In the realm of education and training, the literature highlights the inadequacy of existing programs in modifying end-users' behavior and stresses the fallacy of equating human error solely to a training and awareness issue (Coffey, 2017; Nobles, 2018). The scarcity of psychology-based professionals and cognitive scientists further exacerbates this challenge. To address these issues comprehensively, the literature suggests the need for human factors assessments, emphasizing the pivotal role of cognitive scientists and human factor experts in identifying systemic weaknesses and vulnerabilities (Pfleeger and Caputo, 2012; Hadlington, 2017).

The results section unveils the impact of human factors on cybersecurity, addressing three key research questions. It highlights how understanding and integrating human factors enhance operational efficiency, the challenges organizations face in adopting human-centric approaches, and the ways in which human factors influence strategic decision-making. The interconnectedness of these elements is visually represented, emphasizing the intricate relationship between human factors and the cybersecurity domain.

In conclusion, the synthesis of literature provides a foundation for an in-depth analysis of user-centric studies in cybersecurity. The study reveals that despite challenges, understanding and integrating human factors are pivotal for enhancing cybersecurity measures. The incorporation of human factors not only influences strategic decision-making but also serves as a cornerstone for bolstering overall cybersecurity effectiveness. As organizations navigate an evolving cyber landscape, embracing a human-centric paradigm becomes imperative for fortifying defenses against dynamic and sophisticated cyber threats.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 3 , Number 01, 2024, DOI 10.58471/esaprom.v3i01
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

CONCLUSION

In conclusion, the exploration of human factors in cybersecurity reveals a nuanced and dynamic landscape where the interplay of human behavior, cognition, and technology defines the security paradigm. Persistent challenges, such as human errors and security fatigue, underscore the significance of understanding and integrating human-centric approaches in cybersecurity. Despite technological advancements, human vulnerabilities remain a substantial contributor to security breaches, emphasizing the critical need for a holistic comprehension of human behavior and cognition in the cybersecurity domain. Strategic initiatives, including the establishment of human factors programs and the adoption of human-centered design, emerge as imperative solutions to address and remediate human-centric issues within organizations. These approaches recognize the pivotal role of behavioral and cognitive sciences in shaping cybersecurity procedures and technology integration. Additionally, the discussion on education and training highlights the inadequacies of existing programs, emphasizing the necessity of tailored initiatives for both end-users and cybersecurity professionals. The results section further unveils the interconnected impact of human factors on cybersecurity, providing insights into how understanding and integrating these factors enhance operational efficiency, the challenges faced by organizations, and the influence on strategic decision-making. The visual representation underscores the complexity of this relationship, reinforcing the notion that a human-centric paradigm is essential for navigating the challenges posed by an increasingly sophisticated cyber landscape. In the face of these complexities, it is clear that the future of cybersecurity lies in embracing a human-centric approach. Integrating technology with a profound understanding of human behavior, cognition, and user experiences is paramount for fortifying defenses against dynamic cyber threats. As organizations strive to secure their digital assets, a holistic and strategic focus on human factors emerges as a cornerstone for shaping a resilient and adaptive cybersecurity future.

REFERENCE

Bureau, S. (2018). Human-centered cybersecurity: A new approach to securing networks. Research at RIT. Rochester Institute of Technology Research Report, Fall/Winter 2017-2018. [DOI: Not available]

Carter, W.A. (2017). Forces shaping the cyber threat landscape for financial institutions. SWIFT Institute Working Paper No. 2016-004, October 2, 2017. Retrieved from https://csis-prod.s3.amazonaws.com/s3fspublic/171006_Cyber_Threat_Landscape%20_Carter.pdf

Clark, A. (2013). Whatever next? Predictive brains, situated agents, and the future of cognitive science. Behavioral and brain sciences, 36(3), 181-204. [DOI: 10.1017/S0140525X12000477]

Coffey, J. W. (2017). Ameliorating sources of human error in cybersecurity: technological and human-centered approaches. In The 8th International Multi-Conference on Complexity, Informatics, and Cybernetics, Pensacola (pp. 85-88). [DOI: Not available]

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of human factors in cyber security: A case study of anonymous attack on Hbgary. Computing & Information Systems, 21(2), 10-18. Retrieved from http://cis.uws.ac.uk/ [DOI: 10.1080/20464177.2016.1237033]

Hakimi, M., Ahmady, E., Shahidzay, A. K., Fazil, A. W., Quchi, M. M., & Akbari, R. (2023). Securing Cyberspace: Exploring the Efficacy of SVM (Poly, Sigmoid) and ANN in Malware Analysis. Cognizance Journal of Multidisciplinary Studies, 3(12), 199-208.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. [DOI: 10.1016/j.heliyon. 2017.e00346]

Holstein, W.K. & Chapanis, A. (2018, May 11). Human factors engineering. Encyclopedia Britannica. Encyclopedia Britannica, Inc. Retrieved from https://www.britannica.com/topic/human-factors-engineering [DOI: Not available]

Lee, Y. H., Park, J., & Jang, T. I. (2011). The human factors approaches to reduce human errors in nuclear power plants. In Nuclear Power-Control, Reliability and Human Factors. InTech. [DOI: 10.5772/20564]

Mancuso, V. F., Strang, A. J., Funke, G. J., & Finomore, V. S. (2014, September). Human factors of cyber-attacks: a framework for human-centered research. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 58, No. 1, pp. 437-441). Sage CA: Los Angeles, CA: SAGE Publications. [DOI: 10.1177/1541931214581242]

Hasas, A., Zarinkhail, M. S., Hakimi, M., & Quchi, M. M. (2024). Strengthening Digital Security: Dynamic Attack Detection with LSTM, KNN, and Random Forest. Journal of Computer Science and Technology Studies, 6(1), 49–57. https://doi.org/10.32996/jcsts.2024.6.1.6

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. Procedia-Social and Behavioral Sciences, 147, 424-428. [DOI: 10.1016/j.sbspro.2014.07.110]

National Science and Technology Council. (2016 February). Networking and Information Technology Research and Development Program. Ensuring Prosperity and National Security. Retrieved on March 3, 2018, https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf [DOI: 10.1007/s00779-018-01271-2]

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9(3), 71-88. doi: 10.2478/hjbpa-2018-0024 [DOI: Not available]

Paustenbach, D. J. (Ed.). (2015). Human and Ecological Risk Assessment: Theory and Practice (Wiley Classics Library). John Wiley & Sons. [DOI: 10.1201/b19026-15]

Abdul Wajid Fazil, Musawer Hakimi, & Amir Kror Shahidzay. (2024). A COMPREHENSIVE REVIEW OF BIAS IN AI ALGORITHMS. *Nusantara Hasana Journal*, *3*(8), 1–11. https://doi.org/10.59003/nhj.v3i8.1052

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), 597-611. [DOI: 10.1016/j.cose.2011.08.010]

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. IT Professional, 18(5), 26-32. [DOI: 10.1109/MITP.2016.112]

Fazil, A. W., Hakimi, M., Sajid, S., Quchi, M. M., & Khaliqyar, K. Q. (2023). Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province. American Journal of Education and Technology, 2(4), 50–61. https://doi.org/10.54536/ajet.v2i4.2248

Taylor, J., McAlaney, J., Hodge, S., Thackray, H., Richardson, C., James, S., & Dale, J. (2017, April). Teaching psychological principles to cybersecurity students. In 2017 IEEE Global Engineering Education Conference (EDUCON) (pp. 1782-1789). IEEE. [DOI: 10.1109/EDUCON.2017.7942998]

Georgalis, J., Karapistoli, E., & Mouratidis, H. (2015). A systematic mapping study on security and privacy in the Internet of Things. Journal of Information Security and Applications, 41, 99-115. [DOI: 10.1016/j.jisa.2018.03.004]

Metalidou, E., Goumopoulos, C., Papadopoulos, G. A., & Karatza, H. D. (2019). Cognitive workload and individual differences: predicting operator performance in a discrete-event simulation environment. Journal of Ambient Intelligence and Humanized Computing, 10(8), 3141-3155. [DOI: 10.1007/s12652-018-0948-2]

Hasib, M. (2015). Cybersecurity Leadership: Powering the Modern Organization. CRC Press. [DOI: 10.1201/b19026-6]

Atlam, H. F., Azad, M. A., Alassafi, M. O., Alshdadi, A. A., & Alenezi, A. (2020). *Risk-Based Access Control Model: A Systematic Literature Review.* MDPI Journal. https://www.researchgate.net/publication/342106113_Risk-Based_Access_Control_Model_A_Systematic_Literature_Review (Accessed on Jan 15, 2024).

ForcePoint. (2018). "The Human Point – The Intersection of People and Cybersecurity." Retrieved from [https://www.forcepoint.com/cyber-edu/human-point].

Cuffe, J., & Phelan, E. (2020, June 17). Key Factors in Human Behaviour for Cyber-Security. Cyber Ireland. https://cyberireland.ie/key-factors-in-human-behaviour-for-cyber-security/