sciendo

Scientific Bulletin
Vol. XXVIII, No. 2(56), 2023

EXPLORING THE NEXUS OF CYBERSECURITY LEADERSHIP, HUMAN FACTORS, EMOTIONAL INTELLIGENCE, INNOVATIVE WORK BEHAVIOR, AND CRITICAL LEADERSHIP TRAITS

Sharon L. BURTON
sharonlburton2@comcast.net
CAPITOL TECHNOLOGY UNIVERSITY, LAUREL, MD, USA

Darrell Norman BURRELL
darrell.burrell@yahoo.com
CAPITOL TECHNOLOGY UNIVERSITY, LAUREL, MD, USA

Calvin NOBLES
drcalvinnobles@gmail.com
ILLINOIS INSTITUTE OF TECHNOLOGY, CHICAGO, IL, USA

Laura A. JONES
prolaurajones@gmail.com
CAPITOL TECHNOLOGY UNIVERSITY, LAUREL, MD, USA

ABSTRACT:

Data shows that 12% of leaders are rated as 'very effective' at leadership. This research emphasizes the importance of understanding human behavior and its impact on leadership effectiveness, innovative work behavior (IWB), and the ability to respond to complex cyber threats, particularly in the realm of cybersecurity leadership. Emotional intelligence (EI), a key human factor, is highlighted as a crucial element that can stimulate cognitive absorption, leading to innovative work behavior and improved innovation efficiency (IE). This underscores the need for leaders to not only be technically proficient but also emotionally intelligent to effectively manage their teams and respond to cyber threats. The article also calls for a shift in leadership education to a more holistic and engaged exploration of key leadership attributes, moving beyond traditional methods that often limit understanding to a single culture or approach. This involves understanding the human factors that influence leadership styles and their effectiveness. Furthermore, the use of a literature review underscores the need for leaders to understand the human elements behind cyber threats. Overall the data suggests that leaders need a comprehensive understanding of leadership principles and an active engagement in its theories to foster innovative thinking within cybersecurity leadership.

KEYWORDS:

Emotional intelligence, human factors, innovation efficiency, innovative work behavior, cybersecurity leadership

DOI: 10.2478/bsaft-2023-0016

© 2023 Sharon L. Burton et al. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

1. Introduction

In the ever-evolving landscape of the modern digital age, where technology permeates every facet of our daily lives, understanding the intrinsic interplay between human factors and critical leadership traits has become paramount. This synergy between human behavior and effective leadership is not merely a matter of academic curiosity but is intrinsically tied to the fabric of our interconnected, technology-driven society. As elucidated by Kunzmann (2019), human factors are the subtle yet pivotal elements that dictate how individuals interact with information systems and how seemingly innocuous actions can inadvertently lead to profound security risks. In an era where our dependence on technology is unprecedented, comprehending these human factors is not just a matter of cybersecurity concern but also has far-reaching implications for the broader spectrum of leadership, both within and beyond the digital realm.

Furthermore, within the realm of leadership itself, certain traits emerge as linchpins of success in navigating the complexities of a *cyber society*. Among these, three qualities stand out as keystones: fairness, consistency, and emotional intelligence. Fairness, consistency, EI, and adherence to justice principles are not just an overall moral compass but a strategic necessity in leadership within a cyber society.

Fairness, as defined by Meyers (2023), is the quality associated with acting just and reasonably, centered around the equitable treatment of others. It entails treating individuals in the proper manner. Moreover, according to Meyers, to garner voluntary followership, leaders must establish trust, which is contingent on being perceived as fair. Perceptions of fairness are subjective; while a leader may believe their actions are fair, it does not guarantee that others share the same perception. Trust relies on a leader's ability to foster positive relationships with individuals and various groups (Zenger & Folkman, 2019). Fairness connects to consistency by fostering trust and predictability. In cybersecurity leadership, this trust enhances IWB and enables an agile response to complex cyber threats (Healthcare Information Management Systems Society (Brooks, 2023; HIMSS, 2021; Lim, 2023). Leaders who consistently treat individuals fairly inspire commitment and facilitate adaptability in security practices.

Consistency, too, emerges as an indispensable facet of leadership. In a world where the pace of technological change can be dizzying, leaders who can maintain steadfastness in their approach while being agile when required are the ones who can steer organizations through the tumultuous waters of the digital age (Chieh-Peng et al., 2020). This information is vital to highlight the significance of consistency in leadership within the context of rapid technological advancements. Moreover, this information underscores how leaders must balance steadfastness with adaptability to navigate the complex and ever-changing digital landscape effectively, a crucial aspect in the study of leadership in a cyber society (Caza & Posner, 2019).

Emotional intelligence, the ability to recognize, understand, manage, and influence emotions has risen to unparalleled prominence (Sehgal, 2023). In a hyper-connected society where human interaction often transcends physical boundaries, the ability to navigate the intricacies of human emotions, individually and collectively, is a hallmark of effective leadership (Sehgal, 2023). This information emphasizes the significance of emotional intelligence in the context of leadership within a hyper-connected society. It underscores that effective leadership hinges on the adept handling of human emotions, which is particularly relevant in the study of leadership's role in addressing cybersecurity challenges, where human factors play a pivotal role.

For several reasons, understanding the symbiotic relationship between human factors and these leadership traits is significant. First and foremost, it is essential to comprehend how to safeguard the security and integrity of the digital infrastructure that underpins our modern world (Healthcare Cybersecurity Coordination Center, 2020; Saunders & Wong, 2020). The knowledge of how human behaviors intersect with technology is crucial for protecting sensitive data, thwarting cyber threats, and ensuring the continuity of critical systems. Beyond cybersecurity, these insights have profound implications for leadership in the broader context. Effective leadership is not limited to technical proficiency but hinges on inspiring, guiding, and empowering individuals in a rapidly evolving digital landscape (Burton, 2022). Understanding these dynamics equips leaders with the tools to forge resilient organizations, foster trust, and propel innovation in a cyber society that demands adaptation and evolution (Burrell, 2021).

According to a survey by the Society for Human Resource Management (SHRM), more than half of employees (55%) have reported leaving a job due to poor leadership. A Gallup study found that managers account for up to 70 % of the variance in employee engagement levels. Fairness, consistency, and emotional intelligence enable leaders to build trust and foster positive relationships, ultimately leading to tremendous success in the cyber society.

This text investigates and clarifies leadership and its impact on behaviors and employee turnovers. Regarding the percentage of leaders who lack traits of fairness, consistency, and emotional intelligence research suggests that it is a prevalent issue. For example, a Harvard Business Review (2021) survey found that only 12% of respondents rated their leaders as “very effective” at managing their own emotions while also considering their employees’ emotions. Further, another study by Development Dimensions International (DDI, 2020) revealed that only 14% of leaders were rated as “very effective” in demonstrating fairness and consistency. In the following pages, this research team will delve deeper into these pivotal concepts, exploring how they intertwine to shape leadership success in our technology-driven world and illuminating the path forward for leaders who seek to navigate this brave new frontier.

2. Background

In cybersecurity leadership, human factors are critical because they encompass the human elements, behaviors, and EI processes significantly influencing an organization's security posture. The problem at hand revolves around the vulnerability of cybersecurity measures to intentional or unintentional human actions, posing significant threats to enterprises, their personnel, and customers (Nobles, 2023). A prevalent issue is the need for more awareness among individuals accessing sensitive data and systems, often oblivious to the associated risks (Nobles, 2023). While nearly 70% of employees express cybersecurity concerns, they often lack the means to address these apprehensions (Gaskell, 2021). Most cyberattacks succeed not solely due to hackers' skills but primarily due to human errors or oversights (Gaskell, 2021). These concerns highlight a pressing need for organizations to empower their employees with the knowledge and tools necessary to actively participate in strengthening cybersecurity defenses and mitigating the impact of human errors and oversights.

Cybersecurity extends beyond IT systems, encompassing how individuals interact with information systems and the actions that can introduce vulnerabilities (Triplett, 2022). Indeed, cybersecurity is a multidimensional issue that requires a comprehensive understanding of not just

the technical aspects but also the human factors involved in using and misusing data, making it a critical component of an organization's overall risk management strategy. A salient problem is that prior to the Biden-Harris Administration's initiatives, organizations were facing a lack of coordination, insufficient long-term investments, and inadequate defense measures, all challenges in cybersecurity. A reckoning is as cyber leaders recognize the significance of human behavior and processes, and collaborate with like-minded individuals, organizations have the opportunity to significantly enhance their strategic cybersecurity approach (Triplett, 2022).

A notable observation is the prevalence of complacent and unintentional behaviors, often facilitated by the lack of awareness among leaders and employees (Burrell, 2021). Inadequate awareness or understanding of potential cybersecurity risks often results in nonchalant and unintentional conduct. An example of such behavior is when an employee inadvertently shares a confidential company document with a competitor by entering an incorrect email address (Cybersecurity & Infrastructure Security Agency, n.d.). Another scenario arises when an individual unintentionally interacts with a malicious file or website embedded in a phishing email, leading to the introduction of a virus (Cybersecurity & Infrastructure Security Agency, n.d.). Consequently, the emphasis on cybersecurity enforcement shifts toward education, awareness, and effective communication strategies (Burrell, 2021).

In the realm of cybersecurity leadership, the backdrop of poor leadership's detrimental effects on employee turnover is particularly pertinent. Human factors, encompassing individual behaviors and responses, play a pivotal role in cybersecurity. Leaders possessing fairness, consistency, and emotional intelligence traits foster a culture of trust and adaptability, which in turn enhances innovative work behavior. In this context, the investment in developing these qualities within cybersecurity leaders is not only about promoting a healthy and productive work environment but also about fortifying an organization's defense against cyber threats, where human errors and actions significantly impact cybersecurity outcomes. This synthesis bridges the gap between leadership qualities and cybersecurity effectiveness, underlining their interconnectedness and importance.

3. Problem statement

According to Gallup's State of the Global Workplace report, only 15% of employees worldwide are engaged in their jobs. Poor leadership is one of the critical reasons for employee disengagement, with up to 70% of employee engagement levels attributed to their managers (Gallup, 2017). A study by the Work Institute found that 77% of employees who left their jobs in 2020 did so voluntarily, and 53% of those voluntary separations were due to poor leadership, lack of career development, and unsatisfactory work-life balance (Work Institute, 2020). These behaviors, in turn, significantly impact employee engagement levels and the overall success of organizations in a rapidly changing digital landscape. Leaders must cultivate fairness, consistency, emotional intelligence, and a deep understanding of cybersecurity risks to build trust and resilience and safeguard their assets and reputation. Furthermore, a survey by the Center for Creative Leadership revealed that only 12% of leaders are rated as 'very effective' at managing their own and their employees' emotions (Center for Creative Leadership, 2016). Harvard Business Review Analytic Services (2021) highlights the need for leaders to move from awareness to action regarding cybersecurity and develop a culture of trust and resilience.

4. Significance of the paper/study statement

The paper highlights the critical importance of effective leadership in cybersecurity in the rapidly changing digital landscape. The lack of understanding of human factors, IWB, EI, and knowledge among leaders can lead to negative behaviors, high employee turnover, decreased productivity and profitability, damage to an organization's reputation, and financial loss. Additionally, poor leadership is a significant reason for employee disengagement, which has a considerable impact on the overall success of organizations. Recent studies have emphasized the need for leaders to develop the critical leadership traits and knowledge necessary to thrive in a cyber society. A study by the Ponemon Institute found that the average cost of a data breach in 2020 was $3.86 million, underscoring the need for leaders to invest in cybersecurity measures to safeguard their assets and reputation (Ponemon Institute, 2021). Another study by McKinsey & Company revealed that a majority of organizations are unprepared for cyber threats, highlighting the need for leaders to build resilience and trust (McKinsey & Company, 2020). A study by the World Economic Forum found that cyberattacks are one of the top five risks to global stability, making it imperative for leaders to understand cybersecurity risks and take proactive measures to address them (World Economic Forum, 2019). To address these challenges, leaders must cultivate an understanding of human factors, IWB, EI, fairness, and a deep understanding of cybersecurity to include risks. They must also move from awareness to action regarding cybersecurity, develop a culture of trust and resilience, and invest in cybersecurity measures to protect their organizations from cyber threats. In conclusion, this paper underscores the critical importance of effective leadership in cybersecurity in a rapidly changing digital landscape. It provides a roadmap for leaders to cultivate the necessary traits and knowledge to safeguard their assets and reputation.

5. Methodology

The methodology used for this research was a literature review. The literature review functioned as a knowledge synthesis, effectively amalgamating the existing body of knowledge and yielding a thorough comprehension of the current state of research (Purdue University, 2023; Snyder, 2019). In the realm of leadership research, particularly within the context of cybersecurity, this methodology entails a meticulous and critical evaluation of the most pertinent, recent, and scholarly works about leadership phenomena in the cybersecurity domain (Kannelønning & Katsikas, 2023; Lloyd, 2018).

6. Applicable theories and research from the literature

Two research theories that could be used for this literature review are the Social Learning Theory and the Unified Theory of Acceptance and Use of Technology. The Social Learning Theory posits that individuals learn from observing, imitating, and modeling the behaviors, attitudes, and emotional reactions of others (Dearden & Parti, 2021). In the context of cybersecurity leadership, this theory was applied to understand how leaders' fairness, consistency, and emotional intelligence traits serve as role models and influence the behavior of employees. A recent illustration of Social Learning Theory in the context of cybersecurity leadership can be found in the research paper titled "Cybercrime, Differential Association, and Self-Control: Knowledge Transmission through Online Social Learning," which was published in the American Journal of Criminal Justice (Dearden & Parti, 2021). This study delves into whether social learning in offline or online settings influences self-disclosed cyber-offending.

A thorough theory that investigates how people and organizations embrace and use technology is called the Unified Theory of Acceptance and Use of Technology. This theory was examined in the context of cybersecurity leadership to determine how traits like fairness, consistency, and emotional intelligence affect how well cybersecurity policies and technology are adopted inside a company. A recent study, "Research: Why Employees Violate Cybersecurity Policies," examined this issue (Posey & Shoss, 2022). According to the study, 67% of participants admitted to breaking cybersecurity regulations at least once throughout the 10 workdays examined, with an average failure-to-comply rate of one out of every 20 job tasks. The top three reasons given by participants when asked why they disregarded security restrictions were "to better accomplish tasks for my job," "to get something I needed," and "to help others get their work done" (Posey & Shoss, 2022) This data implies that if executives enforce cybersecurity regulations fairly and consistently and communicate security issues with emotional intelligence, employees may be more ready to adopt new security solutions and participate in IWB. The theory offers a paradigm for comprehending how human factors, leadership behaviors, and technology adoption interact in the context of cybersecurity. Also, they provide a framework for reviewing the literature to gain in-depth insights.

7. Literature review

The literature review provides a comprehensive overview of cybersecurity and risk management. The primary objectives of this literature review methodology were multifold. The review offered an all-encompassing grasp of the present research landscape averting redundancy (Kannelønning & Katsikas, 2023). It includes an analysis of published data, discussing the strategies used to manage cybersecurity risks internally and externally. The review presents the publications' information, linking summaries, and synthesis to ascertain their contributions to the subject matter. The review highlights the connections between the various publications, providing insights into cybersecurity and risk management advancements.

7.1. Revitalizing leadership in the cybersecurity landscape

Given by Doan (2019), numerous organizations face challenges integrating cybersecurity as a proactive element within their strategy, day-to-day operations, and overall corporate culture. Human factors play a pivotal role in cultivating cybersecurity leaders who can integrate security seamlessly into corporate culture (Doan, 2019). This deficiency often arises from the perception of cybersecurity as a behind-the-scenes function, compounded by the fact that many cybersecurity leaders need more capacity to wield strategic influence. According to Doan, influential cyber leaders should possess the ability to infuse security seamlessly into all aspects of the company's operations, swiftly respond to emerging threats, and exert influence among their senior leadership peers. Consequently, businesses must focus on recruiting and nurturing security executives with the requisite skill set to accomplish these objectives (Doan, 2019).

7.2. Fairness and cybersecurity leader

Fairness, an essential attribute in leadership (Meyer, 2023), plays a pivotal role in determining whether leaders can earn the trust of their subordinates, peers, or other associates (Zenger & Folkman, 2019). According to Zenger & Folkman, people around leaders might experience a range of anxieties when the leaders act unfairly, actions indicating that something has been done in a biased, prejudiced, or unjust manner, not adhering to principles of equity or impartiality, whether on purpose or accidentally. Meyer (2023) speaks to three types of fairness that are documented in the fairness model; see Figure no.1.



Figure no. 1: Fairness Model
(Source: Meyer, 2023)

Organizations that strive for fairness in their leadership actions, policies, and procedures are more likely to gain the trust and support of their employees, customers, and stakeholders, essential in promoting a culture of cybersecurity awareness (Guo et al., 2020). Embracing fairness represents the path to wielding influence in leadership, or in other words, achieving effective leadership. Conversely, fear induces compliance in people (Meyer, 2023). Also, effective leadership plays a crucial role in ensuring that cybersecurity is given the necessary attention and resources, which is vital in mitigating cybersecurity risks (Chen & Lin, 2022). Moreover, employees who are knowledgeable regarding cybersecurity risks can help identify and report potential threats, enhancing the organization's overall security posture (Jones, 2021, 2020; Kim et al., 2021). While fairness and cybersecurity leadership have positive aspects, there are also critiques. For instance, organizations prioritizing fairness in their cybersecurity policies may avoid alienating their employees, customers, and stakeholders, leading to a lack of trust and support (Guo et al., 2020). Similarly, ineffective leadership or a lack of leadership commitment to cybersecurity can result in a lack of resources and support for cybersecurity initiatives (Chen & Lin, 2022). Finally, employees with limited knowledge of cybersecurity risks can become an unwitting insider threat, inadvertently compromising the organization's security (Kim et al., 2021).

7.3. Consistency and cybersecurity leader

In order to be a consistent leader, one must uphold the same norms, beliefs, and ideals even when doing so is challenging or controversial. Consistent leaders put forth effort, are punctual, establish objectives for themselves and their teams, and plan meticulously (Behrendt et al., 2017; Sorek et al., 2018; Van Wart et al., 2017). There must be positive consistency of statements and behavior to prevent dysfunction and the need to focus on correction (Harmon, 2018). Consistency does not refer to doing the same thing every time; consistency includes adaptability (Coleman, 2017). Also, leaders can attain a strategic stance by melding steadfastness with adaptability and upholding an organization's mission at the utmost level of excellence while demonstrating flexibility when circumstances warrant it (Coleman, 2017). On the other hand, a lack of consistency, for example, in cybersecurity protocols, can result in vulnerabilities and make an organization more susceptible to attacks (Kim & Solomon, 2020). Coleman (2017) speaks to consistency, agility, and the appropriate mix; see Figure no. 2.



Figure no. 2: Agile and Consistency Image
(Source: Coleman, 2017)

Consistent security practices can also lead to clarity among employees, making it less challenging to enforce policies and procedures (NIST, 2020). Effective leadership is essential in creating an organization's cybersecurity culture (Carpenter, 2021). Unfortunately, the lack of cybersecurity leadership is a common problem in many organizations, with only 26% having a designated Chief Information Security Officer (CISO) position (ISACA, 2021). This void can lead to a lack of prioritization of cybersecurity, resulting in increased risk of cyber threats.

Organizations grapple with integrating cybersecurity as a dynamic and proactive component of their strategy, day-to-day operations, and cultural fabric. A prevailing perception exists that cybersecurity belongs solely in the realm of technology rather than being an integral part of the overall business strategy (Nobles, 2018). Next, the need for more essential skills among most cyber executives is needed to ensure their ability to exert a strategic influence (Doan, 2019). Change is the key, considering that the average tenure of a cyber leader is a mere 18 months. Consistency is connected to EI as it involves the ability to recognize, understand, manage, and influence emotions. One's emotional responses and behavior can indicate EI.

7.4. Emotional intelligence and cybersecurity leader

Emotional intelligence (EI) is an essential skill for effective leadership, and it plays a crucial role in managing cybersecurity risks. EI enables leaders to understand their employees' emotional state better and respond appropriately, thereby improving communication and collaboration in the workplace (Huang et al., 2020). Leaders with high EI are more capable of effectively managing conflicts and addressing cybersecurity risks. Moreover, knowledge of cybersecurity risks is crucial for effective leadership. Leaders with a deeper understanding of the technical aspects of cybersecurity risks can make better-informed decisions and implement effective risk management strategies (Weber et al., 2020). Leaders who are knowledgeable in cybersecurity risks can also educate their employees on best practices to mitigate risks.

However, the lack of emotional intelligence and knowledge of cybersecurity risks among leaders can lead to negative consequences. For instance, leaders who lack emotional intelligence may have difficulty understanding the

emotions and motivations of their employees, which can result in conflicts and mistrust (Xiao et al., 2021). Leaders who need to be more knowledgeable about cybersecurity risks may make better decisions, which can result in security breaches and other cybersecurity incidents (Xiao et al., 2021).

To sum up, emotional intelligence and knowledge of cybersecurity risks are essential skills for effective leadership. The integration of these skills can help leaders make informed decisions and better manage cybersecurity risks. However, lacking these skills can lead to negative consequences, emphasizing the need for leaders to prioritize and develop these skills.

7.5. Fear in cybersecurity leadership

Fear in cybersecurity leadership refers to using fear-based tactics or approaches to motivate employees or stakeholders to adhere to security policies and practices (Meyer, 2023). While fear can have short-term benefits, such as immediate compliance and heightened awareness, it also carries significant drawbacks (Meyer, 2023). False benefits of fear are (a.) instantaneous compliance with security measures and (b.) intensified awareness of cybersecurity risks and the significance of security. On the other hand, using fear as a motivational tool in cybersecurity leadership carries drawbacks. Meyer (2023) offer that fear can negatively impact employees, generating anxiety and stress while fostering a hostile work environment that detrimentally impacts morale and mental well-being. Fear tends to yield short-term compliance rather than fostering a genuine, long-term commitment to cybersecurity practices. This emotion stifles creativity and innovative thinking, hindering the organization's development of proactive cybersecurity strategies. Also, fear may breed resentment and resistance among employees, ultimately eroding trust and collaboration within the workforce, which is counterproductive to building a resilient cybersecurity culture Meyer (2023).

7.6. Education and training and the cybersecurity leader

However, many organizations struggle with cybersecurity education and training, with only 45% of organizations having a formal security awareness training program (ISACA, 2021). This lack of knowledge can result in employees inadvertently causing security breaches through actions such as clicking on phishing emails or using weak passwords (Kim & Solomon, 2020). The positive aspect of having a formal security awareness training program is that it can significantly reduce the risk of security breaches by educating employees about potential threats and how to avoid them (Burrell, 2021; Triplett, 2022).

However, the negative aspect is that only 45% of organizations have such a program, leaving most employees potentially unaware of how their actions could inadvertently cause security breaches, such as clicking on phishing emails or using weak passwords (Hart, 2019).

7.7. Gaps in the literature review

The literature review offered positive information on cybersecurity leadership; however, there are gaps. A literature review gap denotes an unexamined facet or aspect within a specific field of study, signifying an area that has not received thorough exploration or comprehensive research (Raes et al, 2020). These gaps in existing knowledge signify missing pieces or disconnects that require further scrutiny and investigation. Identifying these gaps is pivotal in the research process, as it sheds light on areas demanding fresh insights and directs researchers toward topics that remain uncharted or inadequately examined, offering valuable guidance for future research endeavors (Lu et al., 2020).

- **Understanding Human Behavior**: Despite the emphasis on recognizing the significance of human behavior in influencing leadership effectiveness, there is a notable dearth of in-depth studies that

thoroughly investigate the intricacies of human behavior within the realm of cybersecurity leadership. Understanding the nuances of human behavior in cybersecurity leadership is crucial because it enables organizations to develop tailored strategies that address human factors, ultimately enhancing cybersecurity practices, reducing vulnerabilities, and mitigating risks effectively.

- **Emotional Intelligence (EI):** While emotional intelligence (EI) is acknowledged for its potential to foster cognitive absorption, which in turn drives innovative work behavior and enhances innovation efficiency, there is a notable gap in empirical research regarding the specific role of EI in the context of cybersecurity leadership. Understanding the role of EI in cybersecurity leadership is essential for developing effective leadership strategies that address human factors and emotional aspects, ultimately bolstering an organization's resilience against cyber threats and promoting a cyber-secure environment.
- **Leadership Education:** The article advocates for a transformation in leadership education, urging a shift towards a comprehensive and immersive examination of essential leadership qualities. Nevertheless, existing literature frequently confines this comprehension to a singular cultural or methodological perspective. This shift is vital to prepare leaders who can navigate diverse contexts, fostering adaptability and effectiveness in a globalized and multifaceted leadership landscape.
- **Human Factors in Cyber Threats:** There is a pressing requirement for leaders to grasp the human components contributing to cyber threats. Nevertheless, the majority of research concentrates on the technical dimensions of cyber threats, often neglecting the crucial human factors. Understanding human factors is paramount because they play a significant role in the success or failure of cybersecurity strategies, making it essential for leaders to address the human element in threat mitigation.
- **Leadership Principles:** Leadership Principles in Cybersecurity: The evidence indicates that cybersecurity leaders benefit from a holistic grasp of leadership principles and active involvement in associated theories to stimulate innovative thinking. Yet, there is a dearth of accessible frameworks or models for leaders to implement these principles effectively. Practical frameworks are essential as they provide actionable guidance for leaders, facilitating the application of leadership principles in cybersecurity contexts, and enhancing cyber resilience and innovation.

8. Future research

Future research suggestions serve as signposts guiding new studies to explore uncharted territories or delve deeper into existing topics. In this domain, it is crucial to further investigate and elaborate on the complex interplay between human factors, leadership attributes, and the efficacy of cybersecurity measures.

Cross-Cultural Analysis: Comparative studies should explore how leadership qualities, such as fairness and emotional intelligence, manifest in different cultural contexts and impact cybersecurity practices and outcomes.

Longitudinal Studies: Long-term studies can provide insights into the sustained effects of leadership qualities on cybersecurity resilience, employee engagement, and organizational success.

Leadership Development: Research should focus on the most effective strategies for developing leadership qualities, particularly emotional intelligence, within cybersecurity leaders and how these developments impact organizational cybersecurity.

Behavioral Interventions: Exploring the efficacy of behavioral interventions and training programs to mitigate human-related cybersecurity risks and enhance leadership qualities.

Quantitative Assessments: One crucial avenue involves the development of quantitative assessment tools designed to measure leadership qualities, human factors, and their influence on cybersecurity. These tools aim to facilitate more robust and standardized research in this field.

Understanding the dynamics between human elements, leadership qualities, and cybersecurity is pivotal in a rapidly evolving digital landscape. Future research endeavors are key to further unraveling this intricate relationship and providing actionable insights for leaders and organizations striving to thrive in a cyber society.

9. Conclusions

In the ever-evolving digital age, the interplay between human factors and critical leadership traits has become a pivotal aspect of leadership in cybersecurity. This symbiotic relationship is not merely of academic interest but is intrinsically tied to the fabric of our interconnected, technology-driven society. Understanding how human behavior and emotions intersect with technology is essential for safeguarding the security and integrity of the digital infrastructure that underpins our modern world. Human factors encompass the subtle yet pivotal elements that dictate how individuals interact with information systems and how seemingly innocuous actions can inadvertently lead to profound security risks. The cybersecurity landscape is fraught with vulnerabilities stemming from human behaviors, making it imperative for organizations and their leaders to comprehend these dynamics. Moreover, within leadership, three qualities emerge as keystones of success in navigating the complexities of a cyber society: fairness, consistency, and emotional intelligence. These traits serve as moral compasses and are strategic necessities in leadership within a hyper-connected society. Fairness fosters trust and predictability, enhancing innovative work behavior and enabling an agile response to complex cyber threats. Consistency, balancing steadfastness with adaptability, empowers leaders to navigate the rapidly changing digital landscape effectively. Emotional intelligence equips leaders with the skills to navigate the intricacies of human emotions in a hyper-connected world. In conclusion, this paper highlights the critical importance of effective leadership in cybersecurity and the broader digital landscape. It underscores the need for leaders to cultivate the necessary traits and knowledge to navigate the complex challenges of a technology-driven world.

REFERENCES

Behrendt, P., Matz, S., & Göritz, A.S. (2017). An integrative model of leadership behavior. *The Leadership Quarterly, Vol. 28, Issue* 1, 229-244. Available at: https://doi.org/10.1016/j.leaqua.2016.08.002.

Brooks, C. (2023, March 5). Cybersecurity trends & statistics for 2023; What you need to know. *Forbes*. Available at: https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=45f0a5ae19db.

Burrell, D.N. (2021). Cybersecurity leadership from a talent management organizational development lens. [Unpublished Exegesis]. Capitol Technology University.

Burton, S.L. (2022). Cybersecurity leadership from a Telemedicine/Telehealth knowledge and organizational development examination (Order No. 29066056). *ProQuest Central; ProQuest Dissertations & Theses Global. (2662752457).* Available at: https://www.proquest.com/dissertations-theses/cybersecurity-leadership-telemedicine-telehealth/docview/2662752457/se-2.

Caza, A., & Posner, B.Z. (2019). How and when does grit influence leaders' behavior? *Leadership & Organization Development Journal, Vol. 40, Issue 1*, 124-134. Available at: doi:http://dx.doi.org/10.1108/LODJ-06-2018-0209.

Chen, Y.-H., & Lin, Y.-T. (2022). The effect of transformational leadership on cybersecurity behavior: Exploring the mediating role of psychological empowerment. *Journal of Business Research*, 138, 259-268. Available at: https://doi.org/10.1016/j.jbusres.2021.07.019.

Chieh-Peng, L., Her-Ting Huang, & Tse, Y.H. (2020). The effects of responsible leadership and knowledge sharing on job performance among knowledge workers. *Personnel Review,* DOI: 10.1108/PR-12-2018-0527.

Coleman, J. (2017). The best strategic leaders balance agility and consistency. *Harvard Business Review*. Available at: https://hbr.org/2017/01/the-best-strategic-leaders-balance-agility-and-consistency.

Cybersecurity & Infrastructure Security Agency. (n.d.). *Defining insider threats*. Available at: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats.

Dearden, T.E., & Parti, K. (2021). Cybercrime, Differential Association, and Self-Control: Knowledge Transmission through Online Social Learning. *American Journal of Crime Justice, Vol. 46,* 935–955. Available at: https://doi.org/10.1007/s12103-021-09655-4.

Development Dimensions International. (2020). *Global Leadership Forecast 2021*. Available at: https://www.ddiworld.com/glf2021.

Doan, M. (2019). Companies need to rethink what cybersecurity leadership is. *Harvard Business Review*. Available at: https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is.

Gallup. (2020). *State of the Global Workplace*. Available at: https://www.gallup.com/workplace/285674/state-global-workplace-2020.aspx.

Gaskell, A. (2021). Cyberchology: how the human factor affects cybersecurity. *Cybernews*. Available at: https://cybernews.com/editorial/cyberchology-how-the-human-factor-affects-cybersecurity/.

Guo, X., Zhu, L., Deng, S., & Lai, K.K. (2020). Examining the effects of procedural justice and information sharing on employees' information security policy compliance: Insights from China. *Computers & Security, Vol. 89*. Available at: https://doi.org/10.1016/j.cose.2019.101662.

Harmon, C. S. (2018). Inside a Strategic Plan for a Dysfunctional Senior Leadership Team. *Nurse Leader, Vol. 16, Issue 2*, 142-146. Available at: https://doi.org/10.1016/j.mnl.2017.11.005.

Hart, D.V. (2019). Factors influencing the adoption of cybersecurity situational awareness programs. *ISACA Journal*. Available at: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/factors-influencing-the-adoption-of-cybersecurity-situational-awareness-programs.

Harvard Business Review. (2021). *The State of Emotional Intelligence: 2021*. Available at: https://hbr.org/2021/01/the-state-of-emotional-intelligence-2021.

Harvard Business Review Analytic Services. (2021). *The cyber security agenda: Moving from awareness to action*. Available at: https://www.mcafee.com/enterprise/content/dam/mcafee/enterprise/en-us/assets/misc/hbr-cyber-security-agenda.pdf.

Healthcare Cybersecurity Coordination Center. (2021). *2020: A Retrospective Look at Healthcare Cybersecurity. Report #: 202102181030*. Available at: https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf.

Heathcare Information Management Systems Society. (HIMSS). (2021a). *Cybersecurity in healthcare*. Available at: https://www.himss.org/resources/cybersecurity-healthcare.

Huang, X., Wei, Y., Zhu, X., & Chen, Z. (2020). The relationship between emotional intelligence and cybersecurity behavior intention: a moderated mediation model. *Computers & Security*, *Vol. 92*, 101693.

ISACA. (2021). *State of Cybersecurity 2021 Part 1: Cybersecurity and Risk Management*. Available at: https://www.isaca.org/resources/state-of-cybersecurity-2021-part-1.

Jones, L.A. (2021). A content analysis review of literature to create a useable framework for reputation risk management. *Handbook of Research on Multidisciplinary Perspectives on Managerial and Leadership Psychology*, 91-133. DOI: 10.4018/978-1-7998-3811-1.ch006.

Jones, L.A. (2020). Reputation risk and potential profitability: Best practices to predict and mitigate risk through amalgamated factors (Doctoral dissertation). *Dissertations & Theses Global*. (2466047018).

Kannelønning, K. & Katsikas, S.K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information and Computer Security*. Available at: https://doi.org/10.1108/ICS-08-2022-0139.

Kim, S.J., Lim, S.W., & Park, S.H. (2021). The impact of security knowledge and attitudes on cyber security behaviors. *Information & Management, Vol. 58 Issue* 1. Available at: https://doi.org/10.1016/j.im.2020.103374.

Kim, Y. & Solomon, M.G. (2020). A comparative analysis of cyber security threats and vulnerabilities in healthcare and finance. *Journal of Information Privacy and Security, Vol. 16, Issue* 4, 155-173. Available at: https://doi.org/10.1080/15536548.2020.1831532.

Kunzmann, H. (2019). *A human factors view of organizational change: Shifting mindset from success and failure to resilience engineering* (Doctoral dissertation, University of Portsmouth).

Lim, A. (2023). An executive view of key cybersecurity trends and challenges in 2023. *ISACA*. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023.

Lloyd, C. (2018). Literature reviews. *Harvard University*. Available at: https://socthesis.fas.harvard.edu/files/socseniorthesis/files/pres-litreview.pdf.

Lu, V.N., Wirtz, J., Kunz, W.H., Paluch, S., Gruber, T., Martins, A., & Patterson, P.G. (2020). Service robots, customers and service employees: what can we learn from the academic literature and where are the gaps? *Journal of Service Theory and Practice, Vol. 30, Issue* 3, 361-391.

McKinsey & Company. (2020). *The cyber risk landscape is changing rapidly – are you keeping up?* Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-cyber-risk-landscape-is-changing-rapidly-are-you-keeping-up#.

Meyer, R. (2023). Leadership fairness model. *Tilburg, University*. Available at: https://www.tias.edu/en/item/leadership-fairness-model.

National Institute of Standards and Technology (NIST). (2020). *Cybersecurity Framework*. Available at: https://www.nist.gov/cyberframework.

Nobles, C. (2023). Human Factors in Cybersecurity: Academia's Missed Opportunity. *MWAIS 2023 Proceedings*. Available at: https://aisel.aisnet.org/mwais2023/8.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica – Journal of Business and Public Administration, Vol. 9, Issue 3,* 71-88. Available at: https://doi.org/10.2478/hjbpa-2018-0024.

Ponemon Institute. (2021). *Cost of a data breach report 2020*. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

Purdue University. (2023). Writing a Literature Review. Available at: https://owl.purdue.edu/owl/research_and_citation/conducting_research/writing_a_literature_review.html.

Saunders, L., & Wong, M.A. (2020). Learning theories: Understanding how people learn. In *Instruction in Libraries and Information Centers*. Windsor & Downs Press.

Raes, A., Detienne, L., Windey, I., & Depaepe, F. (2020). A systematic literature review on synchronous hybrid learning: gaps identified. *Learning Environments Research*, Vol. 23, 269-290.

Sehgal, S. (2023, July 25). Why emotional intelligence is crucial for effective leadership. *Forbes*. Available at: https://www.forbes.com/sites/forbesbusinesscouncil/2023/07/25/why-emotional-intelligence-is-crucial-for-effective-leadership/?sh=7d26ede44786.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, Vol. 104*, 333-339. Available at: https://doi.org/10.1016/j.jbusres.2019.07.039.

Society for Human Resource Management. (2020). *Employee Job Satisfaction and Engagement: The Road to Economic Recovery*. Available at: https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Documents/2020-Employee-Job-Satisfaction-and-Engagement-Report.pdf.

Sorek, A.Y., Haglin, K., & Geva, N. (2018). In capable hands: An experimental study of the effects of competence and consistency on leadership approval. *Political Behavior, Vol. 40, Issue 3*, 659-679. Available at: https://doi.org/10.1007/s11109-017-9417-5.

The White House. (2023, March). *FACT SHEET: Biden-Harris Administration announces national cybersecurity strategy.* Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy, Vol. 2, Issue 29,* 573-586. Available at: https://doi.org/10.3390/jcp2030029.

Van Wart, M., Roman, A., Wang, X., & Liu, C. (2017). Operationalizing the definition of e-leadership: Identifying the elements of e-leadership. *International Review of Administrative Sciences*. Available at: https://doi.org/10.1177/0020852316681446.

Weber, R.H., Hummel, A., & Wulf, J. (2020). A typology of leadership in cybersecurity: A qualitative empirical investigation. *Journal of Business Research, Vol. 113*, 69-80.

World Economic Forum. (2019). *The global risks report 2019*. Available at: https://www.weforum.org/reports/the-global-risks-report-2019.

Xiao, B., Liao, Y., Jia, R., & Liu, C. (2021). The effect of leader emotional intelligence on employee cybersecurity behavior: A moderated mediation model. *Computers & Security*, *Vol. 108*, 102248.

Xiao, Y., & Watson, M. (2017). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*. Available at: https://doi.org/10.1177/0739456X17723971.

Zenger, J. & Folkman, J. (2019). Emotional intelligence: The 3 elements of trust. *Harvard Business Review.* Available at: https://hbr.org/2019/02/the-3-elements-of-trust?registration=success.