sciendo

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

THE INTERSECTIONALITY OF OFFENSIVE CYBERSECURITY AND HUMAN FACTORS: A POSITION PAPER

Calvin NOBLES
Cnobles1@iit.edu

ILLINOIS INSTITUTE OF TECHNOLOGY, CHICAGO, IL USA

Ian MCANDREW
irmcandrew@captechu.edu

CAPITOL TECHNOLOGY UNIVERSITY, LAUREL, MD USA

ABSTRACT:

This position paper delves into the complex interplay between proactive cyber defense mechanisms and inherent human susceptibilities. The researchers posit that as cyber systems advance in technical robustness, malicious entities progressively exploit human psychological tendencies and behavioral inconsistencies to circumvent security measures. These exploitations are not merely opportunistic but are strategic, leveraging a profound comprehension of human cognitive biases to undermine security infrastructures. The researchers argue for broadening the intellectual horizon in this domain, underscoring the imperative for a multidisciplinary methodology that amalgamates the empirical acumen of psychology, sociology, and computer science. The article asserts that the fortification of cyber defenses is contingent upon the comprehensive integration of human vulnerability assessments within cybersecurity frameworks. This position paper calls for an augmentation of scholarly research at the nexus of offensive cybersecurity and human factors, formulating defense mechanisms centered around the human element and promulgating inclusive cybersecurity policies that harmonize human and technological considerations.

KEYWORDS:

Cybersecurity, human factors, human weaknesses, offensive cybersecurity, psychology

1. Introduction

One of the most significant challenges in cybersecurity is reducing human weaknesses that result in data breaches, cyber-attacks, and ransomware attacks (Evans et al., 2016; Moustafa et al., 2021; Nobles, 2018; Nobles, 2019; Nobles et al., 2022; Nobles, 2022). Human errors are a critical vulnerability in cybersecurity and are exploited by malicious threat actors to gain access to networks and infrastructure (Jeong et al., 2019; Nobles, 2022). Undeniably, relying solely on algorithms, systems, and processes is insufficient to ensure the security of digital systems, considering the alarming rise in cybersecurity incidents reported worldwide (Jeong et al., 2019). The reliance on technology in cybersecurity is not without pros and cons. One of the negative aspects of technology reliance is the failure to explore initiatives to improve human performance in cybersecurity (Nobles, 2022).

DOI: 10.2478/bsaft-2023-0022
© 2023 Calvin Nobles et al. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

Recognizing that the human element in cybersecurity is equally susceptible to risks as the technical aspects have prompted a shift in research focus towards comprehending the diverse human factors influencing cybersecurity (Jeong et al., 2019; Moustafa et al., 2021; Nobles, 2018). Through recent technological advancements, cybercriminals can execute sophisticated cyber-attacks (offensively) by targeting human weaknesses and the psychological frailties of end-users (Aldawood & Skinner, 2018). The focus on human factors in cybersecurity fails to keep pace with technological advancements, creating a significant attack vector for cybercriminals.

Cybercriminals' strategies have evolved to evade traditional defenses and remain undetected within systems for extended periods, spanning months or even years (Montasari et al., 2018). While cybercriminals and adversarial nation-states, which are malicious threat actors, exploit weaknesses in hardware and software, such as the Logj4 vulnerability (Hiesgen et al., 2022), through social engineering practices, more cyber-attacks directly target humans (Aldawood & Skinner, 2018). The human attack vector is becoming a common attack path for offensive cybersecurity operations conducted by nation-states and malicious threat actors. On the contrary, organizations are not proactively addressing human limitations and weaknesses gained from offensive security (red teaming) assessments.

In today's interconnected world, the effectiveness of cybersecurity measures depends not only on technological advancements but also on understanding and addressing the human behaviors, motivations, and vulnerabilities contributing to cyber threats. It is no longer enough to rely solely on firewalls, encryption, and other technical solutions. Human actions, such as falling victim to phishing scams, sharing sensitive information inadvertently, or neglecting security best practices, can significantly impact the overall security posture of organizations and individuals.

Many nation-states, nefarious organizations, and individuals are amassing offensive cybersecurity capabilities. At the nexus of building offensive cybersecurity weaponry is projecting it toward a particular target. In many cases, the target is end-users through social engineering attacks. Approximately 98% of cyber threats incorporate elements of social engineering, underscoring the importance of human factors in digital security (Coatesworth, 2023). While the human dimension is acknowledged as pivotal in cybersecurity, many educational and training programs must comprehensively address the psychological facets integral to robust cyber defenses (Taylor-Jackson et al., 2020). The lack of scientific robustness regarding the human element in cybersecurity increases the success of offensive cybersecurity practices. The intersectionality between offensive cybersecurity and human fallibility is a critical weakness in research and the availability of practical solutions to mitigate the increasing sophistication of attacks. It is essential to call attention to the relational aspects of offensive cybersecurity and human weaknesses as cybersecurity incidents increase through various social engineering attacks. Strengthening cybersecurity by integrating psychologists and human factors practitioners into cybersecurity operations is a significant challenge.

Cybersecurity in many organizations typically revolves around defensive measures. Nevertheless, threat actors actively employ aggressive tactics, capitalizing on technology and human vulnerabilities. While offensive cybersecurity is not novel, the escalating focus on targeting humans underscores an urgent need to fortify the human component. One pressing challenge in cybersecurity is the need for more viable solutions tackling human psychological susceptibilities (Coatesworth, 2023), often leaving end-users as prime targets. While many organizations emphasize technological integrations to bolster cybersecurity defenses, efforts toward reinforcing the human aspects

lag behind. This imbalance in defense strategies renders humans a lucrative target for adversarial cyber endeavors. Cyber antagonists wield a distinct advantage, masterfully designing deceptive stratagems targeting humans that frequently eclipse the defensive countermeasures of organizations.

This position paper aims to illustrate the problematic and understudied intersectionality between human weaknesses and offensive cybersecurity. The inferences within aim to increase discourse around the intersectionality of human weaknesses, psychological limitations, and offensive cybersecurity. This position paper systematically proceeds from the Introduction to the following sections: (a) background, (b) explanations of the definitions, (c) offensive cybersecurity, (d) the intersection of offensive cybersecurity and human weaknesses, (e) the need for psychology-based professionals, (f) recommendations, and (g) conclusion.

2. Background

Research on human factors (a scientific discipline) in cybersecurity continues to evolve and expand. However, one of the challenges is applying human factors as a scientific discipline in the cybersecurity domain. In the present-day digital landscape, organizations prioritize technology over human factors (Nobles, 2018) even as the intersectionality of offensive cybersecurity and human factors become evident. Humans as an attack vector highlight the problematic issues of safeguarding end-users in cybersecurity due to scarce and disjointed research exploring the human element – one of the chief issues is the lack of empirical research leading to practical solutions. The number of research articles regarding human factors in cybersecurity is increasing; however, most published research centers on human weaknesses and limitations and poor security practices rather than human factors as a scientific discipline. Dul et al. (2012) point out the underexplored nature of human factors, citing four key reasons:

1. The need for more appreciation for the value of human factors engineering among stakeholders involved in artifact design and management, leading to limited demand for HFE expertise.
2. Lack of high-quality human factors solutions or narrow application scopes in industries with significant human factors demands, resulting in suboptimal outcomes.
3. The relatively smaller size of the human factors field compared to more established disciplines like engineering and psychology leads to its overshadowing and diminished recognition.
4. Human factors' broad and multidisciplinary nature can lead to confusion and unclear communication due to the field's diversity of topics, perspectives, and practices.

The advancement of human factors as a discipline and profession continues to provide a scientific approach to solving problems associated with humans in their desired work environment. At issue is the need for more empirical and scholarly work highlighting the nexus between human factors weaknesses and offensive cybersecurity, as Dul indicated in 2012, which still stands true today. Robinson (2023) notes a need for more data to illustrate the invaluable contribution of human factors engineering in cybersecurity. A knowledge gap exists around human factors engineering in cybersecurity (Nobles, 2022a). This knowledge perpetuates weaknesses and vulnerabilities in cybersecurity programs through humans as an attack vector.

Maathuis and Chockalingam (2022) undertook research highlighting the importance of establishing criteria for digital security behavior. Digital security behavior refers to an individual's actions within a digital system, aligned with their organization's agreed-upon norms, procedures, and values in a specific digital or organizational context (Maathuis & Chockalingam, 2022). Digital security behavior could provide insight into exploring the factors that distract from responsible

digital security behavior that proliferates cyber-attacks through exploiting human weaknesses.

Robinson (2023) argues that leveraging human factors security engineering in cybersecurity is essential for reducing the risk associated with the human element, such as burnout, fatigue, cognition, workload, technology resiliency, and software design. Robinson articulates human factor security engineering as a new role in cybersecurity because the domain suffers from a profession that focuses exclusively on the human element. Robins emphasizes the importance of integrating human factors principles in cybersecurity to strengthen and accelerate the maturity of cybersecurity.

Research on the intersectionality of offensive cybersecurity and human weaknesses and limitations remains scarce; hence, the significance of this article highlights offensive cybersecurity techniques and tactics deployed on human weaknesses. At this time, to the author's knowledge, no existing literature addresses the intersectionality of offensive cybersecurity and human weaknesses. As nation-states and threat actors amass offensive cybersecurity capabilities, the mounting targeting of humans in cybersecurity is a significant concern.

3. Working through the definitions – the human factor versus human factors

The modern field of Human Factors and Ergonomics (HFE) gained prominence during World War II due to the increasing cognitive demands on pilots from advanced aircraft systems (Rogers & McGlynn, 2018). Traditional methods like selective training proved inadequate, leading to an integration of scientific management principles focused on designing systems to human capabilities (Rogers & McGlynn, 2018). This era notably broadened the scope of HFE to include cognitive ergonomics and its existing focus on physical ergonomics (Rogers & McGlynn, 2018). Initiated in the 1940s through a collaborative effort between psychologists and engineers, Human Factors Engineering (HFE) was established to scrutinize the complex interplay at the human-machine interface (Guastello, 2023). The aim was to comprehensively understand and optimize this interaction for enhanced performance and safety (Guastello, 2023). Human factors engineering optimizes the interaction between people and systems by accounting for human strengths and limitations (PSN, 2019; Rogers & McGlynn, 2018). It assesses task components, physical and mental demands, team dynamics, and environmental conditions to improve safety, effectiveness, and ease of use (PSN, 2019).

The discipline aims to minimize error risk in complex environments by designing systems aligned with real-world human capabilities and constraints (PSN, 2019). Ergonomics and human factors are used interchangeably. As a scientific discipline, human factors in cybersecurity is a crucial area that needs to be understood and recognized by cybersecurity professionals (Nobles, 2022a). However, there is a significant dilemma surrounding the definition of human factors in this context. The first definition focuses on the negative aspects of human behavior in cybersecurity, commonly accepted as the working definition (Nobles, 2022a). On the other hand, the second definition pertains to designing systems and environments to optimize human behavior and performance (Nobles, 2022a). The latter explanation is grounded in the science of human factors engineering. Cybersecurity professionals have a knowledge gap that impedes the integration of human factors as a scientific discipline and profession.

The lack of human factors professionals employed in cybersecurity further contributes to the knowledge gap and the slow adoption of human factors as a scientific discipline in this field (Nobles, 2019). Scholarly articles on human factors in cybersecurity primarily address the negative

aspects of human behavior, conditions, or actions that lead to security breaches or incidents (Jeong et al., 2019; Mohammad et al., 2022; Rahman et al., 2021). Recognizing the conventional definition of human factors in scholarly literature is crucial, yet this often falls short of capturing the discipline's scientific aspects and potential impact on cybersecurity.

Bridging this gap is imperative to develop comprehensive scientific and working definitions of human factors that can inform cybersecurity research and practice (Nobles, 2022a). This would enable a deeper understanding of how human factors contribute to data breaches and cyber-attacks and facilitate the design of practical solutions to mitigate these risks. By expanding the definition of human factors to encompass not only the negative aspects but also the optimization of human behavior and performance, cybersecurity professionals can develop a more holistic approach to addressing human weaknesses and high-friction areas for end-users.

Furthermore, the working definition of human factors has not effectively influenced existing cybersecurity practices, such as improving system designs and the working environment to optimize human behavior and performance. Poor decision-making, security fatigue, burnout, and human-automation interaction continue to plague cybersecurity (Nobles, 2022). Therefore, embracing the broader perspective of human factors as a science, discipline, and profession, cybersecurity professionals can leverage scientific and engineering practices to enhance our understanding of the human element. This, in turn, can lead to developing effective strategies and solutions to mitigate human weaknesses and improve overall cybersecurity posture.

Recognizing and understanding human factors in cybersecurity is crucial for addressing the complex interplay between human behavior, systems, and cybersecurity outcomes. By expanding the definition of human factors to encompass both the negative aspects and the optimization of human behavior and performance, cybersecurity professionals can unlock the full potential of this scientific discipline. Developing comprehensive definitions of human factors will facilitate the integration of human-centric approaches into cybersecurity research and practice, enabling the design of more robust systems and mitigating risks associated with human factors.

4. Offensive cybersecurity

Offensive cybersecurity operations within the U.S. Department of Defense (DoD) community are defined as missions planned to project military effects in cyberspace to support combatant commanders and achieve national security objectives (Joint Publication 3-12, 2018). These operations involve executing cyber activities outside the protected "blue cyberspace" areas, as classified by the Joint Chiefs of Staff (Joint Publication 3-12, 2018). As defined by Zurowski et al. (2022), offensive cybersecurity operations encompass planned activities that target and impact the confidentiality, integrity, and availability of information, ultimately attacking digital assets. Similarly, Smeets (2018) describes offensive cybersecurity operations as deliberate computer-based activities that disrupt, deny, degrade, or destroy the digital infrastructure of a specific target. In the classification proposed by Uren et al. (2018), offensive cyber operations involve manipulating, preventing, interrupting, damaging, or destroying targeted computers, information systems, or networks.

Most view offensive cybersecurity as actions to deny, degrade, destroy, and disrupt an adversary's digital infrastructure. State-affiliated hackers and advanced persistent threat (APT) groups are notable practitioners of offensive cybersecurity tactics (Kim et al., 2021). The landscape of cyber threat actors encompasses diverse

entities, including individual hackers, cyber terrorists, hacktivists, cybercriminals, and state-sponsored hackers (Kim et al., 2021). State-sponsored hackers and organized cybercrime groups leverage APTs, employing multiple offensive cybersecurity approaches (Kim et al., 2021). The growing sophistication of offensive cybersecurity tactics used on end-users is a direct ploy on human weaknesses and psychological limitations.

The recent ascendancy of artificial intelligence (AI) in cybersecurity enables malicious threat actors to produce powerful offensive cybersecurity capabilities that circumvent traditional cyber defenses. Artificial intelligence-driven offensive tactics empower cyber adversaries to outsmart and outmaneuver human defenses, leveraging the advantages of speed and scalability while evading rule-based detection (MIT & DarkTrace, 2021). With the increasing utilization of AI by cybercriminals and threat actors, offensive cybersecurity techniques have become widespread. Traditional security defenses, relying on human intelligence, struggle to keep pace with and outsmart AI-driven offensive cybersecurity in scope and speed. Consequently, the importance of defensive AI is underscored. While significant attention has been devoted to exploring the influence of AI on offensive cybersecurity, further research and literature are necessary to initiate a broader discussion on the implications of leveraging AI to capitalize on human limitations and weaknesses.

Integrating AI into cybersecurity creates new and sophisticated avenues for cybercriminals to exploit vulnerabilities, mainly through adversarial machine learning attacks (Fritsch et al., 2023; Wirkuttis & Klein, 2017). These attacks involve various techniques, such as adversarial inputs, poisoning training data, and model extraction (Kamoun et al., 2020; Yamin et al., 2021). Adversarial inputs are crafted to manipulate models into producing outcomes based on deceitful inputs, evading detection while poisoning training data involves contaminating the data used for algorithm learning, thereby diminishing detection capabilities (Tetaly & Kulkarni, 2022; Yamin et al., 2021). Model extraction attacks focus on reconstructing detection models or recovering training data through black-box examination, allowing attackers to understand how to evade detection capabilities (Fritsch et al., 2023; Kamoun et al., 2020; Tetaly & Kulkarni, 2022; Yamin et al., 2021). While AI has the potential to enhance information system security, it also introduces new risks, making cyber defense more vulnerable to sophisticated attacks (Fritsch et al., 2023; Kamoun et al., 2020; Tetaly & Kulkarni, 2022; Yamin et al., 2021).

Today's cyber security landscape faces increasing threats from various sources, resulting in unprecedented challenges. These attacks are characterized by their speed, diversity, and frequency (Godin, 2017). Notably, the motives behind these attacks are evolving, with a greater emphasis on political and economic motivations (Godin, 2017; Jahankhani et al., 2014). Critical infrastructures like industrial control systems are particularly vulnerable to cyberattacks (Montasari et al., 2018). Consequently, it is crucial to prioritize identifying, assessing, and protecting assets and resources from harm (Montasari et al., 2018). The proliferation of new attack techniques, including zero-day exploits and advanced persistent threats, presents network security with daunting "easy-to-attack and hard-to-defend" challenges (Montasari et al., 2018). Humans are the largest vulnerability to cybersecurity defenses, given that people are fallible to tactics employed by malicious threat actors.

5. The intersectionality of offensive cybersecurity and human weaknesses

As technological systems are progressively enhanced from a cybersecurity viewpoint, cyber threat actors

are pivoting to target human vulnerabilities (Joinson & van Steen, 2018). The increased focus on the human element results in more social engineering attacks. Coatesworth (2022) notes that the complexity of human beings goes hand in hand with their vulnerability to social engineering. Humans' decision-making processes are shaped by a myriad of psychological elements and inherent biases coupled with the trusting nature of people (Coatesworth, 2022). In cybersecurity, threat actors manipulate human biases to prompt risky behavior, such as clicking suspicious links or sharing sensitive website information (Coatesworth, 2022). Social engineering continues as a favorable attack method for threat actors, consequently indicating that exploiting human weaknesses proliferates humans as an attack vector.

Per Verizon's 2022 Data Breach Investigations Report (DBIR), human factors, including phishing and credential theft, contribute to 82 % of data breaches (Verizon, 2023). The Federal Bureau of Investigations noted that phishing, vishing, and pharming are the most prevailing threats in the U.S., as indicated by a 34 % increase from 2020 to 2021 (FBI, 2021). Social engineering attacks capitalize on deceiving end-users, especially as such attacks are difficult to decipher. The nexus between offensive cybersecurity and human weaknesses is a growing phenomenon that organizations struggle to address, serving as an advantageous attack vector for threat actors.

5.1. Humans-as-an-attack vector

Humans as an attack vector are not new in social engineering attacks, as Janczewski and Fu (2010) noted in an earlier study. Janczewski and Fu highlighted that social engineering attacks predominantly focus on people and technology vulnerabilities, as depicted in Figure no. 1. It is important to note that threat actors' social engineering techniques, tactics, and procedures conversely advance as cybersecurity matures. The details of Figure no. 1 continue to hold significance with the advancement of technology and people being the target of many social engineering attacks. The increased sophistication of today's security technology, while not without technology-induced vulnerabilities, makes people a viable option over technology.

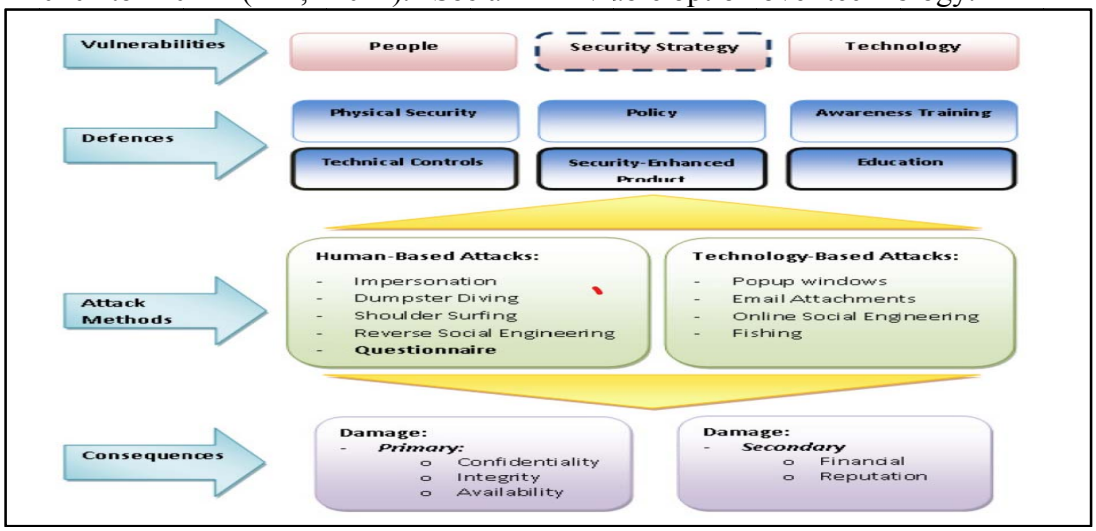

Figure no. 1: The Revised Conceptual Model of the Major Aspects of Social Engineering-Based Attacks
(Source: Janczewski & Fu, 2010)

Coatesworth's (2023) suppositions on social engineering attacks corroborate Janczewski and Fu's findings of people being a central attack vector, especially in social engineering attacks. Coatesworth contends that the complexities of human psychology mean not falling prey to social engineering from one dimension alone.

A multitude of psychological intricacies and biases shape our decisions (Coatesworth, 2023). Central to this susceptibility is cognitive bias, which takes various forms, such as confirmation, hindsight, self-serving, anchoring, and availability biases (Coatesworth, 2023). When coupled with heuristics, these biases can guide us towards less-than-optimal choices, heightening our vulnerability to social engineering machinations (Coatesworth, 2023). Coatesworth mentions the work of Robert Cialdini's book, *"Influence: The Psychology Persuasion",* which outlined the following seven critical pillars for understanding social engineering*:* (a) reciprocity, (b) commitment/consistency, (c) consensus/ social proof, (d) authority, (e) liking, and (f) scarcity and (g) unity was added a late addition. Cybercriminals capitalized on end-users' personal biases to execute successful social engineering attacks (Coatesworth, 2023). Key elements of social engineering are researching targets and establishing a relationship throughout the social engineering lifecycle to execute the attack. A significant challenge for the cybersecurity industry is implementing the psychology of social engineering academics into operational practices.

A reputable vendor classifies attack vectors as the tactics and methods malicious threat actors use to gain unauthorized access to networks to launch subsequent attacks (Cybriant, n.d.). Cybercriminals manipulate and deceive humans to take an active role in executing illicit attacks such as social engineering attacks – thus using humans as an attack vector. Cyber attackers manipulate the minds of computer system users using various nefarious tactics to trick users into divulging information like passwords and spreading misinformation to gain unauthorized access to networks or computer systems (Moustafa et al., 2021). As depicted in Figure no. 2, Aldabbas and Tuefel (2016) illustrate how end-user actions, unintentional or intentional, result in humans being recognized as a threat. Both categories of human behavior, in Figure no. 2, benefit threat actors in achieving their desired illicit effects.

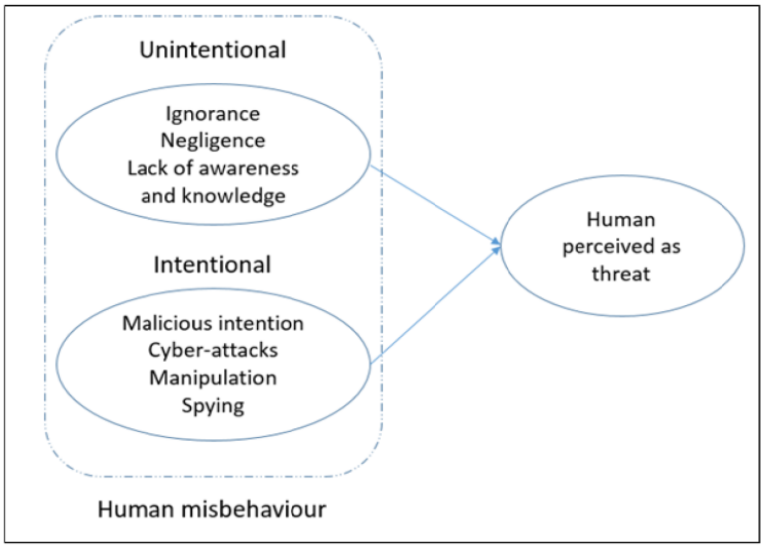

Figure no. 2: Reasons to Perceive Humans as a Threat
(Source: Aldabbas & Teufel, 2016)

Malicious threat actors are increasingly targeting people as a vector to gain access to networks and infrastructure because it is easier and less risky than trying to outmaneuver the technology (Pratt, 2023). Threat actors are aware of humans' psychological weaknesses and cognitive susceptibility (Pratt, 2023), as

indicated by the uptick in social engineering attacks and cognitive hacks. Nobles (2022) argues that the lack of human factors and psychology professionals in cybersecurity perpetuates the growing trend of humans as an attack vector.

Malicious threat actors continue to leverage cognitive hacking as a means to subdue end-users. It is important to note that cognitive hacking is not new (Cybenko et al., 2002). According to Cybenko et al. (2002), cognitive hacking involves manipulating users' perceptions to deceive them into performing certain actions, thereby facilitating cognitive attacks. Unfortunately, cybercriminals and hackers persistently exploit the psychological limitations and vulnerabilities of end-users, primarily due to organizations' inadequate implementation of risk management measures to counter cognitive attacks (Bone, 2017).

A recent AIG (n.d.) report highlights that the human factor extends beyond mere errors and encompasses the influence of security cultures and the exploitation of human behavior and goodwill (AIG, n.d.). Organizations can identify and mitigate areas of human fallibility by gaining deeper insights into workplace dynamics and recognizing how malicious actors leverage inherent human traits (AIG, n.d.). This understanding illustrates end-user weaknesses regardless of cybersecurity awareness and the need for proactive measures to address vulnerabilities to subdue humans as an attack vector.

Human errors in cybersecurity are prevalent as the design of systems, security processes, and technologies are secondary considerations (Maalem Lahcen et al., 2020). Coffey (2017) argues that existing literature highlights the lack of focus on human errors; an increasing number of reports emphasize human errors as contributing to many security incidents and breaches. The paucity of literature on error management in cybersecurity is concerning, given the sustained problem of human errors in information security. Compared to other socio-technical domains, the cybersecurity industry is slow to accept the significance of leveraging error management (Maalem Lahcen et al., 2020). Figure no. 3 depicts a conceptual framework for mitigating human errors. While Figure no. 3 appears simple, mitigating human errors is challenging and can disrupt existing processes and procedures. One critique of Figure no. 3 is the need to depict a human error taxonomy to mitigate the failures and incidents and a feedback loop to illustrate informing business decision-makers of the contributory factors of the failures and incidents.

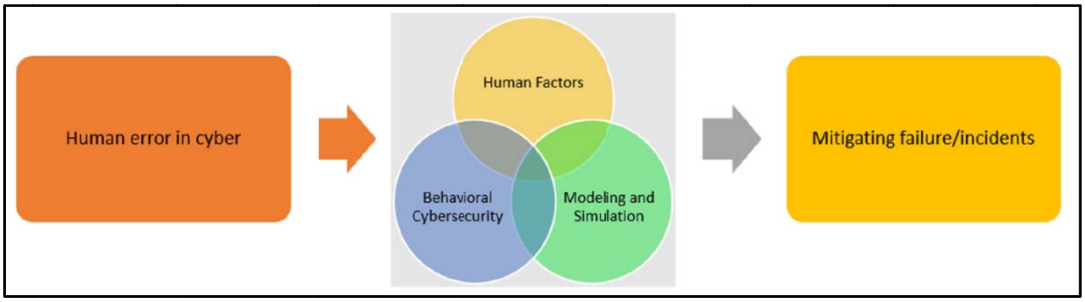

Figure no. 3: Mitigating Human Error Concept Using Proposed Framework
(Source: Maalem Lahcen et al., 2020)

In fairness, it is impossible to eradicate all human errors; however, organizations must leverage human factors principles to reduce human fallibility. Other domains have reduced risks by deliberately targeting human errors by accumulating practical knowledge and design initiatives (Coffey, 2017; Sharit, 2012). There is much

debate about what constitutes human error inasmuch as one researcher prefers using the term "erroneous actions" rather than human errors (Sharit, 2012). As cybersecurity advances along with technological innovations, understanding the science behind human errors or erroneous actions is essential to preventing end-users from becoming attack vectors.

As nation-states and malicious threat actors continue to engage in offensive cybersecurity, the human as an attack vector becomes a critical element. Verizon's Data Breach Investigations Report (2023) findings highlight human weaknesses in cybersecurity breaches. According to the report, 74 % of all breaches involve human involvement, whether through errors, privilege misuse, use of stolen credentials, or social engineering techniques. These statistics underscore the critical importance of addressing human factors in cybersecurity strategies and the need for comprehensive measures to mitigate human-related risks. Using humans as an attack vector is a sustained approach that threat actors leverage because organizations struggle to mitigate h high-friction areas around the human element, thus making it a prime opportunity for offensive cybersecurity operations.

A recent report noted that corporate executives face sophisticated social engineering attacks given the senior leaders' access to sensitive information (Jones, 2023). Cybercriminals are changing tactics to target corporate executives at their residences because most of their personal accounts are not protected by the corporation (Jones, 2023). Social engineering attacks, malware infections, and targeted attacks on their home networks pose significant concerns among the various risks (Jones, 2023). The FBI reported that phishing, a form of social engineering, is one of the leading causes of cyber-attacks (Barton, 2023). The paucity of visible psychological interplay in cybersecurity operations allows threat actors to gain strategic and tactical advantages to outwit end-users. The normalization of offensive cybersecurity operations highlights the need for psychological to reduce humans as the attack vector.

Extensive psychological research has unequivocally demonstrated the multifaceted and unpredictable nature of human behavior and decision-making processes (Benson et al., 2019). This understanding highlights the complexity inherent in human actions and choices, emphasizing the need for comprehensive and nuanced approaches to address cybersecurity effectively. By considering the intricate interplay between human factors and cybersecurity, organizations must develop strategies that account for the diverse range of human behaviors and motivations to counter the increasing onset of offensive cybersecurity tactics.

5.2. Attacking human psychology

Wang et al. (2020) underline that social engineering leverages human vulnerability, not mind control, to breach security. It targets the human factor – often an organization's employees – as the weakest security link instead of attacking technical safeguards like firewalls and authentication systems (Wang et al., 2020). According to researchers, the actions of cyber adversaries are influenced by psychological factors like motivation, group dynamics, and social identity (Taylor-Jackson et al., 2020). Intentional and unintentional insider threats are linked to various psychological aspects, such as cognitive load, mental well-being, trust, and interpersonal relationships (Taylor-Jackson et al., 2020). Integrating psychology into cyber security education will enhance practitioners' abilities to effectively tackle cyber security challenges (Taylor-Jackson et al., 2020). A significant challenge is convincing business decision-makers of the importance of integrating psychology-based professionals into cybersecurity teams.

Cybersecurity incidents consist of

behavioral actions influenced by various psychological factors (Taylor-Jackson et al., 2020). Cyber adversaries often exploit and manipulate the psychological processes of their targets, such as through phishing emails. This illustrates that humans are the weakest link in cybersecurity (Nobles, 2022). Nevertheless, despite recognizing the importance of the human factor, cyber security education and training programs often fail to fully incorporate the essential psychological aspects into their approach (Taylor-Jackson et al., 2020). Despite the wealth of relevant research literature in psychology, which delves into areas such as understanding motivation, predicting future actions, designing human-centric policies and interfaces, and fostering behavioral and organizational change, the incorporation of these insights into the field of cyber security remains insufficient (Taylor-Jackson et al., 2020). A growing concern is the expanding use of offensive cybersecurity tactics by malicious threat actors and end-users lacking an in-depth understanding of the psychological manipulations used against them.

The realm of end-user risks in cybersecurity involves various factors, including the natural inclination to be helpful (AIG, n.d.). Cybercrime, in many ways, mirrors traditional crimes like extortion, blackmail, and fraud, albeit on a larger scale (AIG, n.d.). From a psychological standpoint, engaging in compassionate actions triggers the brain's reward system, reinforcing altruistic behavior (AIG, n.d.). The mental strain experienced by cybersecurity specialists, resulting from the necessity to comprehend novel technologies and associated security protocols, leads to job burnout and fatigue from decision-making (Robinson, 2023). By thoroughly understanding the factors contributing to these issues, we can enhance the security staff's well-being and the systems' users (Robinson, 2023).

Simplifying security procedures with a user-centric focus, grounded in understanding human behavior, can help mitigate risks tied to social engineering and prevalent phishing attacks (Robinson, 2023). This approach would alleviate burnout and improve retention within the cybersecurity profession (Robinson, 2023). However, it is not solely about human error; companies must also consider human behavioral aspects alongside technological defenses. While training and awareness efforts have improved, people still fall victim to phishing attacks, especially as these malicious emails become increasingly convincing. Certain behaviors, like clicking on links, can become automated and challenging to break, particularly when users feel rewarded by gaining access to the desired content (AIG, n.d.). Psychological factors and procedural memory contribute to user noncompliance with cybersecurity best practices (AIG, n.d.).

Social dynamics play a significant role in cybersecurity incidents. People tend to align their thoughts and behaviors with associated social groups, including workplace and cybercriminal groups (Benson et al., 2019). Emotions can spread within these groups, influencing individuals even if they were not directly involved in the initial incident (Benson et al., 2019). Hacktivists may conduct attacks as a protest driven by negative feelings toward their targets (Benson et al., 2019). Within organizations, employees' responses to cybersecurity threats can be influenced by the experiences of targeted colleagues (Benson et al., 2019). Group discussions following an attack are a natural response, as humans seek solidarity in times of threat (Benson et al., 2019). Groups often make riskier decisions than individuals, as observed in both attackers and targets (Benson et al., 2019).

It is commonplace to underestimate how much people are influenced by others, leading to biases that complicate predicting human behavior (Benson et al., 2019). Understanding how social processes shape actions in cybersecurity incidents enhances threat prediction and response strategies (Benson et al., 2019). Trust and

interdependence are crucial in organizations, but misplaced trust or diffusion of responsibility can hinder appropriate actions (Benson et al., 2019). Cybercriminal groups rely on trust, and betrayal can have severe consequences (Benson et al., 2019). Exploring group dynamics, trust, and social identity is essential for managing cybersecurity in socio-technical systems. The social dynamics of psychology are essential, especially as cybercriminals continue to hone their offensive cybersecurity tactics to capitalize on the psychological weaknesses of end-users.

Cyberpsychologists and enterprise cybersecurity practitioners emphasize the importance of a deeper understanding of human-technology interactions to enhance cybersecurity effectiveness (Pratt, 2023). By comprehending how individuals engage with technology, organizations can develop strategies to strengthen their cybersecurity posture and mitigate potential risks (Pratt, 2023). Leveraging the science of psychology in cybersecurity allows professionals to gain insights into the areas where their security programs may be lacking and understand the reasons behind them (Pratt, 2023). Recognizing that security must be designed with people in mind emphasizes the importance of ensuring security measures work effectively for individuals (Pratt, 2023). By incorporating a human-centered approach, cybersecurity professionals can create robust security programs that align with the needs and behaviors of people, thereby enhancing overall cybersecurity effectiveness.

6. The need for psychology-based professionals in cybersecurity

According to Contreras (2022), the presence of psychologists working in the tech space providing psychological science in product development remains dearth even though technological innovations are known to drive behavioral change. Technology influences human behavior, emotion, and reasoning, while most innovations are engineered and built by technologists without expertise in psychological science (Contreras, 2022). The design of tech products and security are critical elements of human factors engineering in cybersecurity (Robinson, 2023); consequently, the absence of psychology-based and human factors professionals in the tech domain contributes to human vulnerabilities and weaknesses exploited through offensive cybersecurity. Other sectors, such as aviation, healthcare, and industrial safety, benefit significantly from human factors and psychological sciences, but cybersecurity continues to lag behind other social-technical domains.

In the past, technology firms were more inclined towards enterprise applications, hardware, and tech-savvy professionals, creating less demand for industrial psychologists. Instead, these companies heavily favored computer scientists (Contreras, 2022). This trend persists, with Google employees exemplifying it. A significant proportion studied computer or computational sciences (29%), while less than 2% studied psychology (Contreras, 2022).The shortage of psychology professionals in the tech sector is a common practice. Consequently, the technology industry has often overlooked the potential contributions of psychology, possibly due to its underrepresentation within tech leadership (Contreras, 2022). This suggests an underutilization of psychological insights in the tech sector.

At its essence, cybersecurity should pivot around human elements, commonly termed as ‘soft components’ or ‘shadow risks’ (Stein, 2018). Comprehending the human factor is pivotal for mitigating inadvertent errors and intentional malicious activities (Stein, 2018). Stein emphasizes the importance of establishing human factor programs and asserts that business decision-makers often place more emphasis on

technological considerations rather than the human psychosocial dimensions (Stein, 2018). Stein provides extensive details about efforts to support organizations and executive leaders in identifying risks associated with insider threats. This highlights psychologists' critical role in offering scientific and analytical support to strategic efforts to understand the boundary between humans and technology, thus preventing unintended consequences (Stein, 2018). As organizations pursue advanced intelligent technologies, psychologists become instrumental in counterbalancing human abilities and comprehension with innovations like artificial intelligence, ensuring optimal decision-making and outcomes (Stein, 2018).

Wiederhold (2014) underscored the following potential applications of psychological expertise:

1. Comprehending user behavior in the context of evaluating risks and rewards.
2. Recognizing and interpreting deviant behaviors of malicious actors and consequently developing technological tools to mitigate psychological manipulation.
3. Acting as consultants to policymakers in creating laws related to cybercrime.
4. Collaborating with labs, media, and social networks to enlighten the public about the various psychological tactics employed by cybercriminals.
5. Examining the psychological impact and experiences of cybercrime victims.

The integration of psychological science and human factors engineering in product development in the tech space is impeded by technologists oblivious to the (a) Dunning-Kruger effect, (b) folk psychology, and (c) illusion of explanatory depth (Contreras, 2022; Nobles, 2022a). Though technology firms employ user researchers to study consumer behavior, they often independently rediscover insights already present in over a century's worth of academic psychology (Contreras, 2022). Technology companies may overlook established findings without psychologists informing this research, leading to potentially redundant explorations (Contreras, 2022).

A standard practice in the cyber domain is to rely extensively on technology – creating an overreliance on technology (Nobles, 2022a). While technology is necessary for cybersecurity due to the tumultuous threat environment, according to researchers, the constant integration of new technology can result in human performance degradation (Wilson et al., 2022). This is an area where psychologists can assist with examining the adverse impact of what Wilson et al. call the technology-induced cycle. An existing gap is the lack of practical solutions to mitigate human weaknesses and limitations when using technologies to combat or outmaneuver offensive cybersecurity tactics imposed by malicious threat actors.

These suppositions underscore the significance and practicality of incorporating psychology-based professions in cybersecurity. By integrating psychological insights and expertise, organizations can enhance their understanding of human behavior, motivations, and decision-making processes, strengthening their cybersecurity posture. Psychology-based approaches can provide valuable insights into the human aspects of cybersecurity, such as insider threats, social engineering, and user awareness and training. This interdisciplinary collaboration between psychology and cybersecurity helps bridge the gap between technical and human factors, leading to more effective strategies and solutions in combating cyber threats.

Psychologists bring unique perspectives and skill sets, enabling the contribution to developing comprehensive cybersecurity programs and initiatives. Their expertise can inform the design and implementation of human-centric security measures, ensuring that cybersecurity solutions align with human cognitive capabilities, limitations, and behaviors. Moreover, psychologists can contribute to

developing training programs, policies, and procedures that promote security awareness and behavior change among individuals and organizations. Collaboration between cybersecurity professionals and psychologists enables the development of comprehensive strategies that account for both technological and human dimensions, ultimately enhancing the resilience of digital systems and protecting sensitive information.

7. Recommendations for mitigating human weaknesses

The current deficit in human factors knowledge within cybersecurity has led to underestimating human factors practitioners as pivotal participants. This significant oversight hinders organizations from harnessing the potential of human factors (Wilson et al., 2020). Consequently, enterprises face enduring threats and growing vulnerabilities in cybersecurity, accompanied by escalating human performance issues. Elements such as stress, security fatigue, and burnout hamper employees' effectiveness in bolstering cybersecurity. Technological dependency culminates in technical and complexity debt, undermining human performance and perpetuating an incessant cycle of cybersecurity events (Wilson et al., 2020).

One benefit of human factors engineering is eradicating risk. Human factors engineering has existed for over 80 years, but its implementation in cybersecurity remains underappreciated due to a knowledge gap. Even with the continuous leveraging of technical solutions in cybersecurity, the human element remains a predominantly inattentive area. Business decision-makers can significantly improve cybersecurity operations by integrating human factors engineering as a core engineering discipline in cybersecurity, similar to what other socio-technical domains (such as medicine, aviation, maritime, and nuclear power) are doing.

Companies designing and developing Cybersecurity products should incorporate Human factor principles at the early stages of their product development. This will increase the usability of the products in the context of a more complex human-work interactive environment and reduce the probability of organizations and individuals falling victim to offensive cyber-attacks. All organizations should realize that despite using state-of-the-art cybersecurity technologies, they are at risk because humans are vulnerable. Therefore, all security-related policies and procedures (and the implementation of cybersecurity technologies) should incorporate human factor engineering. Policies and procedures should be developed with a sound understanding of all stakeholders' psychological biases and weaknesses. Less complex, user-friendly security protocols are more likely to be used effectively. Training and education programs on cybersecurity for employees and other stakeholders should address human factors and how threat actors exploit human psychological weaknesses.

We present the following suggestions for integrating human factors engineering to augment human performance in cybersecurity.

1. Engage with Human Factors Professionals: Business leaders should collaborate with human factors experts to tackle the primary obstacles hindering human performance in cybersecurity. These professionals can offer valuable insights into the implications of rapid technological advancements and their impact on employees (Hollnagel, 2016), particularly in relation to the escalating cybersecurity field. Addressing the human factor challenge presented by the growing demand for accelerated, enhanced, and affordable technological innovation (Hollnagel, 2016) requires the expertise of these professionals.

2. Integrate Human Factors and Psychology-based Professionals into cybersecurity operations. Numerous challenges involve human psychology and human behavior in cybersecurity

(Coatesworth2023; Nobles, 2018), indicating a need for human factors and psychology-based professionals to work in cybersecurity.

3. Develop a Human Factors Program: For organizations with extensive and intricate cybersecurity systems, it is advisable to establish a Cybersecurity Human Factors Program. Such a program could enhance critical elements, such as cybersecurity awareness and training, mitigating security fatigue among cybersecurity professionals and non-technical staff (Nobles, 2019). Human factors programs have demonstrated their effectiveness in diverse sectors, including aviation, healthcare, nuclear power, and industrial safety (Nobles, 2019), and their focus should extend to cybersecurity.

4. Implement human error taxonomies to explore and discover the contributory aspects to prevent such errors. The science behind error management is extensive and has existed since the 1980s (Sharit, 2012). Using an error taxonomy can assist cybersecurity business decision-makers in understanding the types of errors occurring and their contributing factors. Since human errors are considerable in cybersecurity (Nobles, 2022), organizations must proactively reduce and understand errors.

5. Advocate for Human-Centered Cybersecurity: As cybersecurity becomes increasingly complex, understanding and managing the system becomes more challenging. A human-centered approach to cybersecurity is crucial to prioritizing people in system development. This approach, widely used in human-computer interaction, considers human factors in the design of human interfaces in computing (Boy, 2017). Evaluating cybersecurity task analysis from a human-centered perspective could yield valuable insights, such as distinguishing between critical and routine tasks.

6. Research Initiatives on Offensive Cybersecurity and the Human Element: Research initiatives at the intersection of offensive cybersecurity and the human element are vital in improving our defenses. They should include understanding the human vulnerabilities to cyber threats, exploring the various tactics employed by cybercriminals, developing countermeasures based on empirical findings, understanding policy and legislative implications, and adopting an interdisciplinary approach incorporating fields like computer science, psychology, sociology, and law. These initiatives aim to enhance resilience against cyber threats, ultimately fostering a safer digital landscape.

7. Increasing Academic Programs Focused on Offensive Cybersecurity and Humans: To better respond to the escalating cybercrime threats, it is crucial to increase the academic focus on offensive cybersecurity and the human element. The prevalence of cyber threats necessitates education and training programs that equip students with a deep understanding of offensive tactics and the human vulnerabilities that are exploited. The development of such academic programs will foster a new generation of cybersecurity professionals who are not only adept at technical defense but also attuned to the psychological and sociological aspects of cyber threats. These programs should also incorporate ethical considerations and the legal implications of offensive cybersecurity. By doing so, they will produce well-rounded graduates capable of designing and implementing holistic cybersecurity strategies that consider this critical field's technological and human dimensions. An increased academic focus on this intersection can significantly advance our defense against cyber threats.

8. Conclusion

In this position paper, the authors comprehensively highlighted the interplay between offensive cybersecurity and human vulnerability, underscoring a pivotal aspect of the contemporary digital landscape. The

authors contend that as technical security measures become increasingly robust, cyber attackers focus on exploiting human frailties. The human element in cybersecurity, often susceptible to cognitive biases and manipulations, has emerged as a central component in understanding the evolving nature of cyber threats.

The multifaceted nature of human behavior, replete with inherent psychological biases, provides a fertile ground for cybercriminals to distort perceptions and provoke hazardous activities, such as clicking on suspicious links or divulging sensitive information. Verizon's 2022 DBIR shows that the human factor contributes significantly to data breaches, with figures as high as 82 % underlining its magnitude.

As we move forward, the insights underscore the need for an integrated approach to cybersecurity that combines technical measures with a deep understanding of human psychology. Educating users about potential risks and biases and implementing robust security cultures within organizations is fundamental. This human-centered perspective will be pivotal in crafting proactive defenses and building a resilient digital ecosystem. This area of research holds vast potential for further exploration and can provide invaluable insights into creating more holistic and effective cybersecurity strategies.

REFERENCES

Aldabbas, M., & Teufel, B. (2016). Human aspects of smart technologies' security: the role of human failure. *Journal of Electronic Science and Technology*, *14(4)*, 311-318.

Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering,* 62-68. IEEE.

American International Group (AIG). (n.d.). *Human cyber risk: The first line of defence*. Available at: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/ cyber-human-factor.pdf.

Andersson, I., Bjursell, L., & Palm, I. (2023). *Hack the Human: A qualitative research study exploring the human factor and social engineering awareness in cybersecurity and risk management among Swedish organizations*.

Barton, T. (2023, April 20). *The human attack vector: Social engineering*. Available at: https://www.nextdlp.com/resources/blog/human-attack-vector-social-engineering.

Benson, V., McAlaney, J., & Frumkin, L.A. (2019). Emerging threats for the human element and countermeasures in the current cyber security landscape. In *Cyber Law, Privacy, and Security: Concepts, methodologies, tools, and applications,* 1264-1269. IGI Global.

Boy, G.A. (2017). Human-centered design of complex systems: An experience-based approach. *Design Science*, *3*.

Bone, J. (2017). *Cognitive Hack: The New Battleground in Cybersecurity... the Human Mind*. CRC Press.

Contreras, J.M. (2022, March 22). Why tech products should be designed alongside psychologists. Available at: https://thedecisionlab.com/insights/technology/why-tech-products-should-be-designed-alongside-psychologists.

Coatesworth, B. (2023). The psychology of social engineering. *Cyber Security: A Peer-Reviewed Journal*, *6(3*), 261-274.

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,* 85-88.

Cybenko, G., Giani, A., & Thompson, P. (2002). Cognitive hacking: A battle for the mind. *Computer*, *35(8*), 50-56.

Cybriant. (n.d.). Understanding cybersecurity attack vectors and protecting your data. Available at: https://cybriant.com/understanding-cybersecurity-attack-vectors.

Evans, M., Maglaras, L.A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(*17*), 4667-4679.

Federal Bureau of Investigations (FBI). (2021). *Federal Bureau of Investigation: Internet Crime Report 2021*. Available at: https://www.ic3.gov/.

Fritsch, L., Jaber, A., & Yazidi, A. (2022, May). An overview of artificial intelligence used in malware. In *Symposium of the Norwegian AI Society*, 41-51. Cham: Springer International Publishing.

Guastello, S.J. (2023). *Human factors engineering and ergonomics: A systems approach*. CRC Press.

Godin, A. (2017). Using COIN Doctrine to improve cyber security policies. Available at: https://www.sans.org/white-papers/37557/.

Hiesgen, R., Nawrocki, M., Schmidt, T.C., & Wählisch, M. (2022). The race to the vulnerable: Measuring the log4j shell incident. *arXiv preprint arXiv:2205.02544*.

Hollnagel, E. (2016). The nitty-gritty of human factors. *Human factors and ergonomics in practice: Improving system performance and human well-being in the real world*, 45-64.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In *Cyber crime and cyber terrorism investigator's handbook,* 149-164. Syngress.

Janczewski, L.J., & Fu, L. (2010, October). Social engineering-based attacks: Model and New Zealand perspective. In *Proceedings of the International Multiconference on ComputerScience and Information Technology,* 847-853. IEEE.

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC),* 338-345. IEEE.

Joinson, A., & van Steen, T. (2018). Human aspects of cyber security: Behaviour or culture change? *Cyber Security: A Peer-Reviewed Journal*, *1*(*4*), 351-360.

Jones, D. (2023, June 05). Cybercriminals target C-suite, family members with sophisticated attacks. Available at: https://www.cybersecuritydive.com/news/cybercriminals-target-c-suite/652052/.

Kamoun, F., Iqbal, F., Esseghir, M.A., & Baker, T. (2020, October). AI and machine learning: A mixed blessing for cybersecurity. In *2020 International Symposium on Networks, Computers and Communications (ISNCC),* 1-7. IEEE.

Kim, K., Alfouzan, F.A., & Kim, H. (2021). Cyber-attack scoring model based on the offensive cybersecurity framework. *Applied Sciences*, *11*(*16*), 7738.

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(*1*), 1-18.

Maathuis, C., & Chockalingam, S. (2022, June). Responsible digital security behaviour: Definition and assessment model. In *European Conference on Cyber Warfare and Security, Vol. 21, No. 1.*

MIT and DarkTrace. (2021, April 8). Preparing for AI-enabled cyberattacks. MIT Technology Review Insights. *Technologyreview.com*. Available at: https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/.

Mohammad, T., Hussin, N.A.M., & Husin, M.H. (2022). Online safety awareness and human factors: An application of the theory of human ecology, *Technology in Society*, *68*, 101823.

Montasari, R., Hosseinian-Far, A., & Hill, R. (2018). Policies, innovative self-adaptive techniques and understanding psychology of cybersecurity to counter adversarial attacks in network and cyber environments. *Cyber criminology*, 71-93.

Mortazavi-Alavi, R. (2016). *A risk-driven investment model for analysing human factors in information security* (Doctoral dissertation, University of East London).

Moustafa, A.A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, 561011.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(*3*), 71-88.

Nobles, C. (2019). Establishing human factors programs to mitigate blind spots in cybersecurity. *MWAIS 2019 Proceedings*, *22*.

Nobles, C., Robinson, N., & Cunningham, M.(2022, September). Straightfrom the human factors professionals' mouths: The Need to Teach Human Factors in Cybersecurity. In *Proceedings of the 23rd Annual Conference on Information Technology Education,* 157-158.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(*1*), 49-72.

Nobles, C. (2022a, March) The Dunning-Kruger Effect around human factors in cybersecurity, *Top Cyber News Magazine*. Avaialble at: https://www.linkedin.com/company/topcybernews/.

Patient Safety Network (PSN). (2019, September 07). Human factors engineering. Available at: https://psnet.ahrq.gov/primer/human-factors-engineering#.

Pratt, M.K. (2023, July 04). Why cyberpsychology is such an important part of effective cybersecurity. Available at: https://www.csoonline.com/article/643967/why-cyberpsychology-is-such-an-important-part-of-effective-cybersecurity.html.

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021, June). Human factors in cybersecurity: A scoping review, In *The 12th International Conference on Advances in Information Technology,* 1-11.

Robinson, N. (2023). Human factors security engineering: the future of cybersecurity teams. *EDPACS*, 1-17.

Rogers, W.A., & McGlynn, S.A. (2018). Human factors and ergonomics: History, scope, and potential. In *Human Factors and Ergonomics for the Gulf Cooperation Council,* 1-20. CRC Press.

Sharit, J. (2012). Human error and human reliability analysis. *Handbook of human factors and ergonomics*, 734-800.

Smeets, M. (2018). The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*, *12(3*), 90-113.

Stein, A. (2018, June 22). Few minutes with Alexander Stein. *CISO Mag.com*. Available at: https://www.cisomag.com/few-minutes-with-alexander-stein/.

Taylor-Jackson, J., McAlaney, J., Foster, J.L., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating psychology into cyber security education: a pedagogical approach. In *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24,* 207-217. Springer International Publishing.

Tetaly, M. & Kulkarni, P. (2022, October). Artificial intelligence in cyber security – A threat or a solution. In *AIP Conference Proceedings* 2519, p. 030036.

Uren, T., Hogeveen, B., and Hanson, F. (2018, July 04). Defining offensive cyber capabilities. *Australian Strategic Policy Institute*. Available at: https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication (J.P.) 3-12. Washington, DC: CJCS, 8 June 2018.

Verizon. (2023). *Data breach investigations report*. Available at: https://www.verizon.com/ business/resources/reports/dbir/2023/master-guide/.

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access, 8*, 85094-85115. Available at: https://doi.org/10.1109/access.2020.2992807.

Wiederhold, B.K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, *17*(*3*), 131-132.

Wilson, S., Hamilton, & Stallbaum, S. (2020, May 26). The unaddressed gap in cybersecurity: Human performance. *MIT Sloan Management Review*. Available at: https://sloanreview.mit.edu/article/the-unaddressed-gap-in-cybersecurity-human-performance/.

Wirkuttis, N. & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, *1*(*1*), 103-119.

Yamin, M.M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, *57*, 102722.

Zurowski, S., Lord, G., & Baggili, I. (2022, August). A quantitative analysis of offensive cyber operations (OCO) automation tools. In *Proceedings of the 17th International Conference on Availability, Reliability and Security,* 1-11.