HOLISTICA Vol 9, Issue 3, 2018, pp. 71-88 DOI:10. 2478/hjbpa-2018-0024

Botching Human Factors in Cybersecurity in Business Organizations

Calvin NOBLES,
Cybersecurity Policy Fellow, New America Think Tank, Washington, DC, USA
University of Maryland University College, Adelphi, MD, USA
Calvin.nobles@faculty.umuc.edu

Abstract

Human factors remained unexplored and underappreciated in information security. The mounting cyber-attacks, data breaches, and ransomware attacks are a result of human-enabled errors, in fact, 95% of all cyber incidents are human-enabled. Research indicates that existing information security plans do not account for human factors in risk management or auditing. Corporate executives, managers, and cybersecurity professionals rely extensively on technology to avert cybersecurity incidents. Managers fallaciously believe that technology is the key to improving security defenses even though research indicates that new technologies create unintended consequences; nonetheless, technological induced errors are human-enabled. Managers' current perspective on the human factors problem information security is too narrow in scope and more than a training problem. The management of complex cybersecurity operations accompanied by mounting human factor challenges exceeds the expertise of most information security professionals; yet, managers are reluctant to seek the expertise of human factors specialists, cognitive scientists, and behavioral analysts to implement effective strategies and objectives to reduce human-enabled error in information security.

Keywords: Information Security, Cybersecurity, Human Factors, Technological Determinism, Human-centered Cybersecurity, Human-enabled Errors, Technology.

JEL Classification: M1, L32.

1. Introduction

Business organizations continue to invest extensively in technologies to prevent sophisticated cyber threats on prized possessions to maintain business as usual. Even with the latest technological capabilities, malicious cyber actors can gain access to businesses' most critical networks, systems, and data. A 2015 report indicates that Wells Fargo, Bank of America, Citibank, and J. P. Morgan Chase invested 1.5 billion dollars in mitigating emerging and persistent cyber threats (Morgan, 2016). Humans are notably the weakest link in security and risk

management (Alavi, Islam, & Mouratidis, 2016; Proctor & Chen, 2015) because organizations struggle to understand and mitigate behavioral-based risk in information security. Human factors are the study of human interaction with information systems, networks, and practices in an information security environment (Nobles, 2015). Organizations leverage information systems to gain the competitive and strategic advantage to pursue business objectives; consequently, as the complexity of information systems and technologies increase humans become more susceptible to mistakes (Alavi, Islam, & Mouratidis, 2016). The cybersecurity threat landscape is continually evolving, and businesses are quickly adapting, primarily by leveraging technologies to counter cyber threats (Neely, 2017). The investment ratio in technologies to people is vastly disproportionate and problematic as most organizations associate human factors issues as a training issue. Metalidou et al. (2014) lament that businesses pursue technological solutions to resolve behavioral-based risk rather than addressing the issue from a human factors perspective, which highlights the disregard for understanding human decision-making and end-users' interaction with information systems.

One study indicates that humans (86%) are the most prominent security weakness followed by technology (63%) (Metalidou, 2014). It is common knowledge that human-enabled errors account for more than 80% of all cyber-attacks, data breaches, and ransomware attacks (Soltanmohammadi, Asadi, & Ithnin, 2013). The U.S. and U.K. national-level cybersecurity policies listed human-related errors in cybersecurity as a significant degradation to national security (Dykstra, 2016). Nonetheless, most organizations have failed to implement programs to address human factors in cybersecurity (Alavi, Islam, & Mouratidis, 2016). Technology alone will not eliminate human error in cybersecurity. On a daily basis, organizations encounter a barrage of cybersecurity threats indicating the compelling disposition to reduce human errors and stop enabling the efforts of malicious cyber actors (Wirth, 2017). The purpose of this paper highlights the complexity of managing human factors in information security.

2. Cybersecurity Threat Landscape

According to a Symantec Report, in 2016, 401 million pieces of malware traversed the internet in which 89% were new variants of malicious software (Wirth, 2017). The Symantec report revealed that newly installed internet of things devices are scanned by hackers within two minutes after installation, highlighting the swift notification of network changes (Wirth, 2017) and continuous network scanning searching for vulnerabilities. Malicious actors use

spear phishing and malware as threat vectors to capitalize on human error to gain access to networks and critical data. The cybersecurity threat landscape is continually evolving as malicious cyber actors pursue new vectors to target and capitalize on newly discovered or known vulnerabilities (Wirth, 2017). The top industries targeted by cybercriminals are (1) healthcare, (2) manufacturing, (3) financial services, (4) government, and (5) transportation (Morgan, 2015). These industries are targeted for sensitive information primarily in the healthcare and financial services sectors. Researchers are forecasting the global cost of cybercrime in 2019 to reach over 2 trillion dollars (Morgan, 2016).

Cybercriminals persistently take advantage of hyperconnected systems, technology-induced vulnerabilities, human-enabled errors, and underprepared organizations. The most prominent cyber threats in the past 12 months are (a) phishing, (b) spyware, (c) ransomware, and (d) Trojans (Keely, 2017). Malware-less threats are emerging as the weapon of choice for malicious cyber actors seeking to compromise credentials (Keely, 2017). The top three threat vectors are (a) email links and attachments, (b) web-based download, and (c) application vulnerability (Keely, 2017). Of the three threat vectors, the most complicated is application vulnerability because organizations have countless applications with unaccounted for vulnerabilities (Keely, 2017). In 2017, 75% of data breaches were executed by external malicious actors while internal actors conducted 25% of the breaches, and organized criminal entities conducted 51% of breaches and state-sponsored activity accounted for 18% of breaches (Verizon, 2017). Malicious cyber actors use the following tactics (Verizon, 2017):

-81% of breaches resulted from weak or stolen passwords
-62% of breaches stemmed from hacking
-51% of breaches involved malware
-43%of breaches were social engineering attacks

Research indicates that web attacks decreased in 2016; however, 229,000 web attacks occur daily in which 76% of scanned websites contained vulnerabilities, and 9% had critical security weaknesses (Wirth, 2017). Cybercriminals use rootkit exploits as the primary attack vector to conduct malicious cyber operations accounting for 60% of the attacks in 2016; however, researchers noticed a sharp decrease in rootkits as cybercriminals migrated to different techniques such as social engineering, malware, physical theft, and ransom attacks (Wirth, 2017).

Research revealed that 80-90% of security breaches are due to human-enabled errors in the U.S. and U.K. (Maglaras, He, Janicke, & Evans, 2016) which these two countries account for over 90% of reported data breaches (Wirth, 2017). The evolving changes and threats in the cyber landscape are progressing; consequently, requiring organizations to develop holistic and dynamic information security strategies to eradicate and mitigate threats and vulnerabilities (Alavi, Islam, & Mouratidis, 2016). Even with the influx of technological capabilities coupled with operational, administrative, and technical countermeasures; there is a continuity of failure to address human factors concerns in information security, which enables the proliferation of data breaches, ransom attacks, and social engineering attacks at unprecedented levels.

3. Human Factors

Schultz (2005) has stated the significance of the shortage of experts and information security research on human factors and human error. Schultz (2005) has outlined the importance of understanding how the work environment and work culture influence the development or non-development of knowledgeable employees that engage in productive and proper security-oriented behaviors. According to Schultz (2005), human behavior has often been an overlooked focus in information security research and organizational business strategy. As a result, the growth security breaches driven by human factors will continue to create disparaging organizational results, causing bankrupt reputations, enormous customer dissatisfaction, business losses, and significant governmental sanctions (Buckhead, 2014; Van- Zadelhoff, 2016).

Kraemer and Carayon (2007) classified a human factor error as, “Any action leading to an undesired result” (p. 77). Often, employees are tricked by an outsider into engaging in problematic behavior and may not mean to cause an adverse event for the organization (Van- Zadelhoff, 2016). An employee’s action and decision making when engaging in work duties are intended to help advance the goals of the organization, instead of purposely engaging in actions or behaviors that would harm the organization. The result is often human error or mistakes in human decision making that create information security problems (Van-Zedlhoff, 2016).

Van-Zedlhoff, (2016) stressed that human errors or human factors as one of the highest areas of organizational vulnerability. Solutions for information protection should consider human error and flawed decision making as one of the most significant aspects of information security (Schultz, 2005). An organization’s business strategy should encompass creating an effective

information security-oriented organization (Van-Zedlhoff, 2016). This means creating policies that perpetuate a culture where employees are reluctant to circumvent information security controls to complete tasks (Albrechtsen, 2007). This security of enlightened culture is one where employees will purposefully increase their knowledge and concern for in the importance of information security in a manner where they will understand that this is an aspect of everyone's job not just those with information technology job titles and duties (Buckhead, 2014). Many of the studies that pertain to end-user behavior imply that humans make uninformed information security decisions (Van-Zedlhoff, 2016). For example, users base decisions on personal values because of a lack of training and threat perception, or the organization's poor security culture (Van-Zedlhoff, 2016).

An increasing concern for information security is human factors because human error is the leading contributor to (a) data breaches, (b) ransomware attacks, and (c) cyber-attacks (Kraemer Carayon, 2007; Wirth, 2017). Even with the deployment of automated countermeasures, malicious actors gain access to targeted systems by exploiting human error through (a) spear phishing, (b) social engineering, (c) malware, (d) noncompliance, (e) poor policies, and (f) technology-induced vulnerabilities. Given the number of human-enabled errors in cyber operation proves that technology alone will not eradicate human-induced mistakes. Researchers and practitioners postulate that the impact of malicious cyber activity targeting humans remains underexplored in existing research (Mancuso, Strang, Funke, & Finomore, 2014). Mancuso et al. (2014) acknowledge that the existing research gap in human performance and behavior in cybersecurity require urgent attention from human factors practitioners and psychology-based experts.

Moreover, researchers emphasize that understanding human behavior in cybersecurity is a complex problem (National Security Agency, 2015). An egregious oversight in cybersecurity is the absence of cognitive scientists and human factor experts to conduct assessments on human performance and behavior in an active environment (National Security Agency, 2015). The observation of human performance and behavior by cognitive and human factor experts can provide practical insight on automation and information overload, technological deterministic thinking, procedural alignment, operational tempo, and the impact of technology on the workforce (Nobles, 2015). With the ascendancy of technology in cybersecurity, cognitive scientists and human factor experts are pivotal in conducting performance and human factors assessments to predispose (a) systemic weaknesses, (b) vulnerabilities, (c) critical phases of cybersecurity operations, and (d) cognitive overload (Hadlington, 2017; Pfleeger

& Caputo, 2012). Human factors initiatives can be solidified through organizational culture by implementing practices and processes to increase awareness of human performance and decision-making (Hadlington, 2017).

Researchers indicate that 50% of the cyber-attacks in 2014 were due to human error illustrating a 31% increase from 2013 (Evans, Maglaras, Ho, & Janicke, 2015). The increasing complexity of the cybersecurity environments is resulting in security fatigue, alert anxiety, (Masters, 2017; Stanton, Theofanos, Prettyman, & Furman, 2016) and operational fatigue. These phenomena ascend from the increasing number of incidents and vulnerabilities that easily overwhelm cybersecurity operators (Wirth, 2017). The number of system vulnerabilities remains challenging; Masters (2017) alluded that each system could have as many as ten vulnerabilities. A collapse in alertness is indicative of cognitive and information overload leading to a degradation in human performance.

Businesses rely on information systems and technology to yield profits; yet, most companies struggle with integrating human factors into the organizational culture (Hadlington, 2017). Not only are human factors a concern for protecting crown jewels, critical information, intellectual property, and networks. Researchers give prominence to the unbalanced focus of organizations leveraging automated technologies with little to no thought on the impacts on information security (Vieane, 2016). It is imperative for organizations to develop strategic human factors objectives in the organization's information strategy. The U.S. and U.K. both address human-related errors in cybersecurity in national-level policies (Dykstra, 2016). Nonetheless, most organizations failed to implement programs to address human factors (National Science and Technology Council (NSTC), 2016). A noticeable change in information security are efforts to reduce human-enabled errors by including psychologists, cognitive scientists, behavioral analysts, and human factors experts to analyze and evaluate the behavior of end-users in cyber operations (Pfleeger & Caputo, 2012). Pfleeger and Caputo (2012) acknowledge the importance of accounting for human behavior when designing computer systems and technologies and the criticality of behavioral science in ameliorating cybersecurity effectiveness.

Researchers and human factors experts vehemently emphasize that technology alone will not ameliorate information security (Pfleeger & Caputo, 2012; Safa et al., 2015). Therefore, organizations need to leverage behavioral specialists to examine cybersecurity operations from cognitive and bias viewpoints as well as other behavioral factors to develop an amalgamated approach to address capitalized on technology, processes, and procedural to maximize security (Pfleeger & Caputo, 2012; Safa et al., 2015). The community discussion between cybersecurity professional and behavioral scientists as

recommended by Pfleeger and Caputo (2012) is a progressive effort to start developing a common understanding between the two disciplines. The inclusion of human factors experts, cognitive scientists, and behavioral analysts in the cybersecurity domain could potentially benefit the cybersecurity analogous to improvements in the aviation and nuclear power.

4. Theoretical Alignment

4.1 Theory of Planned Behavior

Ajzen (1991) framed the seminal theory of planned behavior (TPB), which is one of the most frequently used theoretical frameworks for explaining many of the human factors that influence behavioral actions. The TPB focuses on theoretical constructs reflecting an individual's motivational and cognitive factors as significant prognosticators of behavioral action or inaction (Ajzen, 1991). The theory of planned behavior assumes the most proximal determinant of the response is an intention to perform a behavior, which, in turn, is strongly affected by attitude and subjective norm toward behavior and perceived behavioral control over the performance of behavior (Ajzen, 1991). The TPB has significant application to this study and exploration of the nature of employee behaviors, human factors, and organizational business strategy around cybersecurity and information security.

Considering cybersecurity from the context of TPB, employee attitudes towards a behavior is significantly influenced by individual dogmas about results of the performance of the conduct (behavioral beliefs). If employees believe that the expected consequence of performing a behavior is positive, that employee will have an encouraging attitude about engaging in that behavior (Ajzen, 1991). That means if proper and effective information security behavior is taught, highly acknowledged, and heavily rewarded, then employees will feel more positive about promoting and engaging in the appropriate behaviors (Ajzen, 1991). On the contrary, if employees have limited knowledge, no vested interest, and are frustrated in a way strongly that creates a convincing belief that performing a behavior is negative, the employees will have an adverse attitude towards a behavior (Ajzen, 1991).

4.2 Change Management

Dhillon's (2001) study on organizations makes a compelling case that human factors and organizational culture can be changed and positively influenced. Dhillon study outlined the importance of employee engagement as a

useful tool for change management. Dhillon (2001) outlined the importance of creating collaborative organizational cultures that focus on ways to leverage the intellectual capital of everyone, which aligns with the socio-technical system model in that the work system and work culture. Dhillion's (2001) research outlines the importance of the entire work system, including the organizational culture and human factors as it relates to the active engagement of cybersecurity management.

Change management is the process of organizing, directing, and executing change within an organization by establishing objectives and metrics to complete the transformation (Benvenuti, 2011). Change at an organizational level is a difficult undertaking because personnel often resist change due to the apprehension of the future or the unknown (Benvenuti, 2011). Change is a strategic objective for organizations to withstand continuous evolution; however, resistance to change is a significant phenomenon (Georgalis, Samaratunge, Kimberley, & Lu, 2015) that can be disruptive and counterproductive. For human factors to be recognized as a credible science requires cybersecurity leaders must undergo a cultural and philosophical change (Hadlington, 2017). A part of the fundamental change involves accepting psychology as a vital element of cybersecurity (Hadlington, 2017). Cybersecurity and information security consist of many technical specialties creating barriers for psychologists, behavioral analysts, cognitive scientists, and human factors specialists (Pfleeger & Caputo, 2012).

Leveraging change management is necessary to remove obstacles and allow cybersecurity professionals to appreciate the value that behavioral specialists and analysts can contribute to reducing human-enabled errors in cyber and information security (Pfleeger & Caputo, 2012). Evaluating the utilization of behavioral analysts and specialists in the aviation, safety, and nuclear power fields can change the perspective of how psychology is regarded in cybersecurity (Lee, Park, & Jang, 2011). Without the expertise of psychology-based professionals, human-enabled errors will continue to wreak havoc on organizations Pfleeger & Caputo, 2012). It is imperative to change the philosophical viewpoint on human error by welcoming and integrating psychology professionals into cyber because the one constant in cyber is humans remain the weakest link (Hadlington, 2012). The information security culture can affect the behavior of end-users within the organization and should be developed to motivate users' actions to meet information security requirements (Albrechtsen & Hovden, 2010; Buckhead, 2014). Alfawaz et al. (2010) conducted a study on information security culture and created a compliance framework, which requires a tremendous amount of employee engagement.

Information security culture is reliant on senior management, priorities, actions, and attitudes (Albrechtsen & Hovden, 2010; Buckhead, 2014). A study by Buckhead (2014) outlined the importance of creating an organizational culture where employees feel a sense of personal ownership regarding the mitigation of information security risk.

4.3 Technological determinism

Technological determinism is a theory grounded on constant creation and integration of new technologies to simplify processes and ameliorates the quality of human life and work procedures with no concern for societal, cultural, or organizational implications (Nobles, 2015). Clegg and Bailey (2007) state that technological determinism is centered on technology impacting humans by revolutionizing societal, organizational, and economic progression. Technological deterministic thinking can have a significant influence on an organization's behavior and acceptance to leverage emerging technologies (NSTC, 2016). Some scholars argue that technology is incapable of influencing humans instead it transforms society (Clegg and Bailey, 2007). The aviation domain leverages advanced technologies to reduce the cognitive demand of pilots through the use of automated avionics and auto-pilot capabilities designed for easy manipulation by pilots. Advanced technologies influenced the aviation community by contributing to the reduction of aviation incidents and accidents (Nobles, 2015).

The cybersecurity domain profoundly demonstrates technological deterministic behavior by continuously integrating emerging technologies as a measure to mitigate advanced persistent threats (Nobles, 2015; NSTC, 2016). A common practice by organizations is investing extensively in cybersecurity technologies to counterpoise the shortage of trained information security professionals and to defend against constant cybersecurity threats (Cobb, 2016; NSTC, 2016). Businesses overreliance on cybersecurity technology has resulted in organizational and cultural fallacies; consequently, shifting the defense of critical networks, systems, and data on technology which minimizes the role information security professionals (Alavi, Islam, & Mouratidis, 2016; NSTC, 2016).

Human-enabled errors in cybersecurity have not decreased with the integration of new technology (Alavi, Islam, & Mouratidis, 2016; NSTC, 2016). There is a shortage of research on human-enabled errors and technology integration in cybersecurity. The underappreciation of human factors in cybersecurity illustrates a gap between theoretical research and organizational practices regarding information security NSTC, 2016). Cybersecurity operations

are growing increasingly sophisticated analogous to aviation and nuclear power operations. Both the aviation and nuclear power industries capitalize on the scientific underpinnings of human factors by holistically assessing the effect of technology, operations, procedures and tasks, decision-making, and the environment on information security professionals (Lee, Park, & Jang, 2011). Human factors assessment can be used by organizations to determine the problematic areas for technical and non-technical employees (Aoyama, Naruoka, Koshijima, & Watanabe, 2015; Hadlington, 2017). Technological deterministic thinking impedes businesses from valuing human factors and increases dependency on technology (Nobles, 2015) to support cybersecurity objectives (Hadlington, 2017).

4.4 Human-centered Cybersecurity

At this time there is a scarcity of scientific research on human-centered cybersecurity framework, which formed from the human-centered design theory. However, a cybersecurity company is focusing on behavioral-related risk in information security through a new paradigm known as human-centered cybersecurity (Bureau, 2018; ForcePoint, 2018). The human-centered cybersecurity framework is places humans at the center of cybersecurity and information security practices, design aspects, and technology integration as an effort to reduce behavioral-centric risks by accounting for psychologic efforts (Bureau, 2018; ForcePoint, 2018). School, researchers, and practitioners are engaging in discourse and designing research projects to further explore human-centered cybersecurity as a theory (Bureau, 2018). Researchers and practitioners are working to elevate human-centered cybersecurity as a standard approach to information security and cybersecurity (Bureau, 2018).

According to ForcePoint (2018), human-centered cybersecurity provides the basis for gaining an in-depth understanding of human behavioral and the reasons humans make specific decisions when interacting with computer systems. Placing humans at the center is a distinctive approach because organizations prefer to put increased emphasis on technology, which has led to an underappreciation of behavioral and cognitive sciences in information security and cybersecurity (ForcePoint, 2018). The proliferation of human-centered cybersecurity requires the inclusion of human factors experts, behavioral analysts, and cognitive specialists into the information security and cyber domain (ForcePoint, 2018). The human-centered cybersecurity approach shifts the centric viewpoint from technology to humans, which will transform existing organizational practices (ForcePoint, 2018).

5. Human Derailments in Information Security

Numerous factors have derailed information security (Hadlington, 2017); consequently increasing risks and threats to organizations (Bureau, 2018). Human factors initiatives and efforts are prioritized against competing requirements and given that organizational leaders do not understand or value human factors as science (Hadlington, 2017). The underappreciation of human factors impedes researchers and practitioners from defining the scope of human behavior when interacting with an information system (Hadlington, 2017). Another significant factor that propagates human errors in cybersecurity is the shortage of information security professionals (Cobb, 2016). By 2019 researchers are forecasting a deficient of cybersecurity professionals by more than 1 million cybersecurity jobs (Cobb, 2016), which will prevent organizations from achieving optimum levels of preparedness to counter malicious activities. Nefarious cyber activities continue to increase each year; therefore, information security professionals face increased operational tempo, stress, fatigue, and burnout due to personnel shortages (Wirth, 2017). The increasing complexity of information security requirements coupled with the continuous integration of technology, regulatory demands, emerging and persistent threats, and the disproportionate reliance on technology negatively affects information security practices and degrades organizations ability reach an optimal level because the science involving human factors is an afterthought (Pfleeger & Caputo, 2012).

The derailment of human factors in cybersecurity is propagated by threat actors targeting end-users' weaknesses in the human-machine teaming (Sawyer & Hancock, 2017). For example, as humans leverage computing capabilities and systems, analogous to any partnering situation, one partner will have stronger performance tendencies than the other (Sawyer & Hancock, 2017). In the case of the human-machine teaming, Sawyer and Hancock (2017) postulate that prevalence paradox effects diminish human performance as a result of overreliance, mistrust, complacency, and misuse. These prevalence paradoxes increase vulnerabilities in cybersecurity, primarily due to human factors.

6. The Urgency for an Organizational Platform

Executive leaders must mandate platforms, in the form of committees, programs, councils, or working groups to address human-enabled error in information security practices and cybersecurity operations. Leveraging platforms to work with human factors specialists, cognitive scientists, and psychologists are vital to understanding operational complexity, organizational

weaknesses, critical phases of security, and reckless attitudes by humans. In the aviation domain, researchers identified hazardous attitudes that contributed to aviation incidents and accidents. Information security and cybersecurity professionals should employ best practices from other industries to mitigate behavioral-based errors that result in cyber-attacks, ransomware attacks or data breaches. Researchers advocate for information security and cybersecurity professionals to leverage the findings of existing human factors studies to cultivate operational practices to minimized human-enabled errors (Vieane, 2016).

The information security domain evolvement outpaces researchers' ability to develop a comprehensive understanding of human interaction with information systems. A 2015 report by IBM highlights that human factor accounts for 95% of cybersecurity incidents as a result of inconsiderate work practices, ignorance, poor software patching, use of malicious software codes, unsecured network connections, and inadequate communication surrounding sensitive information (Gyunka & Christiana, 2017). Research and practitioners deem the study of human behavior in information security as a critical area because humans are labeled as the most vulnerable link in cybersecurity (Gyunka & Christiana, 2017). Even though organizations are leveraging technology in cybersecurity at an unprecedented rate, failure to address human factors nullifies the ability to capitalize on the technological advances (Gyunka & Christiana, 2017). Gyunka and Christiana (2017) argue that threat actors target the vulnerabilities of human factors because it is less complicated than exploiting technologies. The dynamic nature of the cyber threat landscape is onerous because organizations are unable to produce engineering solutions to counter to threat actors' ability to generate emerging threats and technologies (Klimoski, 2016).

Paul and Dykstra (2016) assert that cybersecurity and the paths of social and behavioral science remain undervalued and underexplored, which is indicative of the number of human-related errors in cybersecurity. Another complexing issue is the difficulty in assessing and measuring fatigue, frustration, and cognitive exertion in cybersecurity, which might result in technical mistakes and increased risk (Paul & Dykstra, 2017). The dearth of scientific research on leveraging applicable platforms to address human factors in cybersecurity further perpetuates the dependency on technology. Private and public entities need to work collaboratively to develop platforms and assessment capabilities to identify human factor shortfalls in information security and cybersecurity operations (NSTC, 2015).

Coffey (2017) argues that existing cybersecurity training and awareness is restrictive in scope because training programs fail to modify end-users' behavior. For organizations to influence the behavior of end-users, require fostering an environment that transforms the organizational climate to active learning to perpetuate ameliorating the culture (Coffey, 2017).

The Department of Defense (DOD) Cybersecurity Culture Compliance Initiative (DC3I) exists as an institutional platform to promote a culture to advance human factors by focusing on inadequate authorities, architectures, and capabilities (Department of Defense, 2015). The DC3I is a significant concept that applies to private organizations as well. Unfortunately, the targeted organizational changes by DC3I have been inconsequential due to the lack of appreciation for organizational change (Department of Defense, 2015). The DoD like many private organizations aims to reduce human error in cybersecurity by overly investing in technology (Department of Defense, 2015). Without a doubt, this practice is pernicious because organizations are disproportionately investing in technology and disregarding the underlying behavioral and cognitive issues.

7. Recommendations and Conclusion

Safety science research can help with understanding why information system users do not comply with information security controls (Young & Leveson, 2013). A study by Lawton (1998) focused on rule violations and the motivations given by violators. This study determined that, in most cases, the violations occurred unintentionally because workers were committed to completing the task (Lawton, 1998). Time pressure, workload, and using a "quicker way of working" were among some of the human factor issues that influence the engagement in risky actions by employees in organizations (Young & Leveson, 2013; Buckhead, 2014; Lawton 1998).

Without a doubt, human factor is a scientific field that is underutilized and undervalued in information security and cybersecurity (NSTC, 2016). Human involvement in information security is too invaluable for organizational leaders to continue to ignore the significance of psychology-based specialists to analyze the human behavior in information security (National Security Agency, 2015). The lack of research on human behavior in cyber and information security further acerbates the misunderstanding of human decision-making while operating an information system. The cybersecurity threat landscape expands every day as malicious actors develop sophisticated techniques to conduct nefarious activities.

Technological deterministic thinking influences the constant invest in technologies; yet, human errors remains a primary contributor to data breaches, cyber-attacks, and ransomware attacks (Hadlington, 2017). Many security professionals are unfamiliar with the science of human factors and equate human error to a training and awareness issue which is a misconception (National Security Agency, 2015). Therefore, the following recommendations are necessary to optimize human performance in information security (Clark, 2015; Georgalis et al., 2015; Lee, Park, & Jang, 2011; Paustenbach, 2015):

a) Seek the expertise of human factors specialists and behavioral analysts

b) Mandate an executive-led committee to address human factors in information security

c) Conduct a risk assessment solely based on human factors

d) Integrate human factors objectives into the information security strategy

e) Make humans centric to the foundation of information security and cybersecurity practices

f) Leverage human factors lessons learned from the aviation, nuclear power, and safety industries

g) Design training and awareness programs to include gamification

h) Train personnel on human factors

i) Develop metrics to capture the changes after implementing human factors objectives

j) Sponsor human factors research projects with universities and colleges

k) Integrate human factors course material into information security certification program

l) Advocate for colleges and universities to develop and teach human factors courses

This analysis indicated that human factors in information security continue to be plagued by widespread and systemic issues (Georgalis et al., 2015; NSTC, 2015). The mismanagement of human factors by organizations increases risks and the susceptibility to malicious cyber activities (Georgalis et al., 2015). The above-listed recommendations provide organizations with the basis to explore deeper into human behavior to reduce behavior-related risk. There is a litany of problems surrounding human factors in information security that requires extensive change management to eradicate preventable human errors (Georgalis et al., 2015). Information security professionals must have a profound comprehension and appreciation for human factors analogous to leaders in other industries to stop the perpetuation of information security shortfalls by equating human-enabled errors as a training and technology problem, when in

fact, it is the mismanagement of human factors. Taking aggressive and strategic actions in exploring behavior-based risks accompanied by comprehensive and scientific assessments can yield data to highlight the significant infractions that result in human error.

References

[1] A Eurocontrol FAA Action Plan 15 White Paper. (2015 December). A human performance standard or excellence.

[2] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50, 179-211.

[3] Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information & Computer Security*, *24*(2), 205-227.

[4] Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29, 432-445.

[5] Alfawaz, S., Nelson, K. & Mohannak, K. (2010). Information security culture: A behavior compliance conceptual framework. Eighth Australasian Information Security Conference, Brisbane, Australia.

[6] Aoyama, T., Naruoka, H., Koshijima, I., & Watanabe, K. (2015). How management goes wrong?–The human factor lessons learned from a cyber incident handling exercise. *Procedia Manufacturing*, *3*, 1082-1087.

[7] Benvenuti, S. (2011). Making a case for Change Management Theory to support IS/IT curriculum innovation. *Issues in Informing Science and Information Technology*, *8*(unknown), 093-109.

[8] Blair, T. (2017). *Investigating the cybersecurity skills gap* (Order No. 10623377). Available from ProQuest Dissertations & Theses Global. (1989786177). Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1989786177?accountid=27203

[9] Bureau, S. (2018). Human-centered cybersecurity: A new approach to securing networks. Research at RIT. Rochester Institute of Technology Research Report , Fall/Winter 2017-2018.

[10] Burkhead, R. L. (2014). *A phenomenological study of information security incidents experienced by information security professionals providing corporate information security incident management* (Order No. 3682325). Available from ProQuest Dissertations & Theses Global. (1657429053). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1657429053?accountid=35812

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

[12] Clegg, S., & Bailey, J. R. (Eds.). (2007). *International Encyclopedia of Organization Studies*. Sage Publications.

[13] Cobb, S. (2016). Mind this Gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis.

[14] Coffey, J. W. (2017). Ameliorating sources of human error in cybersecurity: technological and human-centered approaches. In *The 8th International Multi-Conference on Complexity, Informatics, and Cybernetics, Pensacola* (pp. 85-88).

[15] Department of Defense (DoD) Cybersecurity Cultural Compliance Initiative (DC3I). (2015, September).

[16] Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. Computers & Security, 20(2), 165-172.

[17] Dykstra, J. (2017). Cyber Issues Related to Social and Behavioral Sciences for National Security.

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

[19] ForcePoint Security Labs. (2018). 2018 Security Predictions. Retrieved February 23, 2018 from https://www.forcepoint.com/sites/default/files/resources/files/report_2018_security_predictions_en.pdf

[20] Georgalis, J., Samaratunge, R., Kimberley, N., & Lu, Y. (2015). Change process characteristics and resistance to organisational change: The role of employee perceptions of justice. *Australian Journal of Management*, *40*(1), 89-113.

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

[22] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346.

[23] Klimoski, R. (2016). Critical success factors for cybersecurity leaders: Not just technical competence. *People and Strategy*, *39*(1), 14.

[24] Kraemer, S. & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. Applied Ergonomics, 38(2007), 143-154.

[25] Kraemer, S., Carayon, P. & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28, 509-520.

[26] Lawton, R. (1998). Not working to rule: Understanding procedural violations at work. Safety Science, 28(2), 77-95.

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

[28] Maglaras, L., He, Y., Janicke, H., & Evans, M. (2016). Human Behaviour as an aspect of Cyber Security Assurance.

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

[30] Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). The human factor in cybersecurity: Robust & intelligent defense. In *Cyber Warfare* (pp. 173-206). Springer International Publishing.

[31] Masters, G. (2017 June 09). Crying wolf: Combatting cybersecurity alert fatigue. SC Media. Retrieved from https://www.scmagazine.com/crying-wolf-combatting-cybersecurity-alert-fatigue/article/667677/

[32] McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2015). Human performance factors in cyber security forensic analysis. *Procedia Manufacturing*, *3*, 5301-5307.

[33] Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G.

[34] (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.

[35] Morgan, S. (2016, May 13). Top 5 industries at risk of cyber-attacks. Forbes.com. Retrieved on February 17, 2018, from https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#1edfc762715e

[36] National Security Agency (2015). Science of Security (SoS) Initiative Annual Report 2015. Retrieved from http://cps-vo.org/sos/annualreport2015

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

[38] Neely, L. (2017). 2017 Threat Landscape Survey: Users on the front line. Sans Institute. Retrieved on February 17, 2018, from https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

[39] Nobles, C. (2015). *Exploring pilots' experiences of integrating technologically advanced aircraft within general aviation: A case study* (Order No. 3682948).

Available from ProQuest Central; ProQuest Dissertations & Theses Global. (1658234326). Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1658234326?accountid=27203

[40] Paustenbach, D. J. (Ed.). (2015). *Human and Ecological Risk Assessment: Theory and Practice (Wiley Classics Library)*. John Wiley & Sons.

[41] Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

[42] Ponemon Institute. (2017, June). 2017 Cost of Data Breach Study.

[43] Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Human factors*, *57*(5), 721-727.

[44] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

[45] Sawyer, B. D., & Hancock, P. A. (2018). Hacking the Human: The Prevalence Paradox in Cybersecurity. *Human factors*, *60*(5), 597-609.

[46] Schultz, E. (2005). The human factor in security. Computers & Security, 24, 425-426.

[47] Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal of Contemporary Research in Business*, *5*(7), 329-354.

[48] Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. *IT Professional*, *18*(5), 26-32.

[49] Van- Zadelhoff, Marc (2016, September). The Biggest Cybersecurity Threats Are Inside Your Company. Harvard Business Review.

[50] Verizon 2017 Data Breach Investigations Report 10th Edition. (2017). Retrieved on February 18, 2018, from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017

[51] Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., & Wickens, C. (2016, September). Addressing Human Factors Gaps in Cyber Defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 60, No. 1, pp. 770-773). Sage CA: Los Angeles, CA: SAGE Publications.

[52] Young, W. & Leveson, N. (2013). Systems thinking for safety and security. Proceedings of the 29th Annual Computer Security Applications Conference. New Orleans, Lousiana, USA.