Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2019 Proceedings | Midwest (MWAIS)

5-21-2019

Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity

Calvin Nobles
University of the Cumberlands, Calvin.nobles@outlook.com

Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity

Calvin Nobles, PhD
Cybersecurity Policy Fellow, New America Think Tank
University of the Cumberlands
Calvin.nobles@outlook.com

ABSTRACT

Most business organizations lack a human factors program and remain inattentive to human-centric issues and human-related problems that are leading to cybersecurity incidents, significant financial losses, reputational damage, and lost production. Other industries such as aviation, nuclear power, healthcare, and industrial safety leverage human factors problems as platforms to reduce human errors. The underappreciation and under-exploration of human factors in cybersecurity threatens the existence of every business. Cybersecurity operations are becoming increasingly abstruse and technologically sophisticated resulting in heightened opportunities for human errors. A human factors program can provide the foundation to address and mitigate human-centric issues, properly train the workforce, and integrate psychology-based professionals as stakeholders to remediate human factors-based problems.

Keywords: Cybersecurity, Cognition, Fatigue, Human Factors, Human-centered Design, Information Security

INTRODUCTION

Business organizations are plagued continuously by human errors in cybersecurity resulting in data breaches, cyber-attacks, and long-term reputational damages; consequently, leading to diminished profits (Nobles, 2018). Most organizations are diligently leveraging best practices and cybersecurity technologies to mitigate the relentless barrage of cyber threats and vulnerabilities (Nobles, 2018). Cybersecurity threat actors have the strategic advantage and wreak havoc on businesses at will (Carter, 2017). Malicious threat actors' gain the strategic advantage by capitalizing on human weaknesses and vulnerabilities. The contributing factors of human vulnerabilities in cybersecurity are (a) disproportionate investments in humans compared to technologies, (b) poor cybersecurity and awareness training, (c) the underappreciation of human factor engineering, (d) the use of technologies to enforce end-user behavior, (e) lack of a security culture, and (f) the absence of human factors programs (Nobles, 2018). Other industries with advanced sociotechnical environments and operations such as aviation, nuclear power, medicine, and industrial safety have successfully leveraged human factors programs as a platform to address problems that perpetuate human-enabled errors (Nobles, 2018). The absence of human factors programs creates an enormous blind spot for organizations even though most businesses are taking aggressive actions to mitigate cybersecurity threats. Failure to implement a human factors program prevent organizations from determining the causal factors leading to human errors or decisions lapses. The dearth of platforms to address human factor issues at an organizational level propagates the use of ad-hoc practices in cybersecurity. The purpose of this practitioner-based critical analysis is to highlight the necessity of human factors programs in cybersecurity.

PRACTICAL RELEVANCE

The sections below analytically highlight the need for business organizations to implement human factors programs to reduce human errors in cybersecurity. Human factor priorities are competing against a litany of other requirements and given that security and technology leaders struggle to understand the value of human factors (Nobles, 2018) it prevents businesses from investing in human factor initiatives. A shortage of cybersecurity professionals forces security and technology executives to rely extensively on technologies to combat the endless onslaught of threats; thus, creating a disproportionate relationship between humans and technology (Nobles 2018). There is no empirical research on integrating human factors program in cybersecurity, which further impedes the creation of human-centric approaches in cybersecurity.

DISCUSSION / IMPLICATIONS

THE DEARTH OF PSYCHOLOGY-BASED PROFESSIONALS IN CYBERSECURITY

Currently, there is a shortage of psychology-based professionals working and supporting cybersecurity operations. Human factors is a scientific field about the interaction of humans with computers and information systems to optimize human behavior, performance, and cognition (Nobles, 2018). Taylor et al. (2017) postulated that most of the psychology research focuses on averting and mitigating efforts in the post-attack phase. However, social psychology can uniquely provide insight into how technology influences attitudes, perspectives, behavior, and cognition (Taylor et al., 2017). Researchers emphasized that the utilization of psychology in cybersecurity remains unsupported by empirical research (Taylor et al., 2017) even though psychologists, behavior analysts, and cognitive scientists actively support human factors programs in other domains. Psychology in cybersecurity is useful in (a) establishing evaluation and assessment methods, (b) to understand social engineering both from an attacker and victim perspectives, (c) the social behavior and interaction between end-users and systems while (d) cognitive psychology can provide insight into the risk associated with sociotechnical systems (Taylor et al., 2018). A practical disconnect of psychology in cybersecurity is the scarcity of psychology-based professionals supporting cybersecurity operations.

The research gap between human performance and behavior in cybersecurity requires the immediate attention of human factors practitioners and psychology-based experts (Mancuso et al., 2014; Nobles, 2018). An egregious oversight in cybersecurity is the absence of cognitive scientists and human factor experts to conduct assessments on human performance and behavior in cyberspace (National Security Agency, 2015). By integrating psychology-based professionals and human factors practitioners in cybersecurity operations can result in the profound understanding of (a) systemic human weaknesses, (b) cognitive overload, (c) misuse of automation and technologies, (d) task and cognitive alignment, (e) identify critical phases of cybersecurity operations, and (f) information inundation (Nobles, 2018). Even though cybersecurity operations are primarily dependent on technology, psychology-based professionals are imperative for optimizing cybersecurity professionals' performance, cognition, and effectively transitioning between automated and manual tasks and functions (Pfleeger & Caputo, 2012; Nobles, 2018). Including psychology-based professionals and human factors practitioners in cybersecurity can reduce human-enabled errors, preventing costly security incidents, and increase profits through optimized human performance.

TECHNOLOGICALLY DEPENDENT

The cybersecurity environment is dynamically and hyperactively coercing businesses to become reliant on technologies due to a shortage of cybersecurity talent (Nobles, 2018) and the absence of human factor programs. Organizations are leveraging technological capabilities to offset the shortage of cyber professionals and the unpredictable cyber threat landscape because cybersecurity threat actors are employing sophisticated tactics to gain access to sensitive data (Nobles, 2018). Corporate organizations implement the latest technologies to combat cybersecurity threats and vulnerabilities; however, failure to address human factor issues lessens the effectiveness of technologies because humans are prone to mistakes (Gyunka & Christiana, 2017) even while using up-to-date technologies. Even with the integration of new technology, human-enabled errors remain a constant vulnerability, emphasizing that technology fails to reduce human-enabled errors (Alavi, Islam, & Mouratidis, 2016; NSTC, 2016). Technology integration in cybersecurity occurs in a silo rather than from an end-user centric approach, which ensures technology is counterbalanced and aligned with human-centric practices, policies, and sociotechnical systems. Metalidou et al. (2014) contended that technology is erroneously perceived as the definitive solution to information security problems without any consideration for human involvement. Taking a human-centric approach in cybersecurity aligns technology integration, training, and the mitigation of problems areas to optimize human behavior and performance.

Cybersecurity technologies and information systems are part of a larger sociotechnical ecosystem or system of systems that require pragmatic manipulation especially with the continuous integration of new technical capabilities. When using human factors principles, system design is a critical element of the system of systems ecosystem, which incorporates the training techniques and development, programs resulting in the creation of training aids and devices (Holstein & Chapanis, 2018). Holstein and Chapanis (2018) claimed that balancing human-machine interaction requires practical consideration of people, training, and operating practices to achieve safe, systematic, and proficient operations. Given the complexity of humans, tool design, and operational environments mandate a formal and methodical approach to address human factors (Holstein & Chapanis, 2018), especially in cybersecurity. Hence, the need for a human factors program to formalize organizational practices involving human-machine and human-centric techniques. From personal observation and experiences, the interplay between cyber operations, cybersecurity operators, end-users (non-technical), technology, procedures, and policies are often negated from a human factors perspective. Researchers argue that the integration of technology needs to be supported by scientific practices rather than using logic, intuition, and practicality to avoid human and technology mismatches (Holstein & Chapanis,

2018). The point is not to be technology averse but to incorporate longstanding scientific practices to ensure humans remain the central factor in a technologically intense environment.

SECURITY FATIGUE

Implementing a human factors program in cybersecurity can result in improved and proprietary cybersecurity awareness and training to prevent security fatigue. Researchers recently coined an emerging phenomenon in cybersecurity as security fatigue. A recent study noted that cybersecurity personnel suffers from inundation due to the continuous security changes in cybersecurity such as changing passwords, updating antivirus software, policy and security controls, and combatting cyber threats (Stanton, Theofanos, Prettyman, & Furman, 2016). The study highlights that once a worker experiences security fatigue, desensitization sets in and the employee no longer complies with the security policies and changes (Stanton, Theofanos, Prettyman, & Furman, 2016). A fundamental factor of security fatigue is cognitive overload (Stanton, Theofanos, Prettyman, & Furman, 2016). From a cybersecurity viewpoint, organizations have not invested extensively in determining the rational demand for cyber professionals; hence, the need to leverage human factors engineering in cybersecurity. The pressure placed on cyber professionals leads to less than optimal security practices because the cybersecurity domain lacks a scientific process to evaluate cognitive overload. Another phenomenon that a recent study noted was decision fatigue (Stanton, Theofanos, Prettyman, & Furman, 2016) because cybersecurity professionals work in demanding environments due to constant attempts by malicious actors, changes, and the complexity of technology. Placing increasing demands on cybersecurity personnel leads to security fatigue or decision fatigue (Stanton, Theofanos, Prettyman, & Furman, 2016), which signifies that the operational capacity is exceeding the cognitive abilities of cyber professionals.

HUMAN-CENTERED DESIGN

Human factors in cybersecurity are necessary to reduce human-enabled errors (Nobles, 2018) and to increase the scope of operational requirements by developing human-centered and socio-organizational initiatives (Mancuso et al., 2014). By using human-centered designs, human factors practitioners could potentially expose the objectives that cybersecurity professionals do not account for mounting cognitive workload, emotional changes, and modified mental models (Mancuso et al., 2014). A new paradigm in the human-centric model is human-centered cybersecurity (Bureau, 2018; ForcePoint, 2018). The current practices consist of technology at the center of cybersecurity operations in which the human-centered cybersecurity challenges the existing paradigm due to an underappreciation and under-exploration of behavioral and cognitive sciences in cybersecurity (Forcepoint, 2018; Nobles, 2018). The human-centered cybersecurity model position humans as the central element of cybersecurity and information security procedures, frameworks, designs, and the integration of technology as an effort to reduced human-enabled errors (Nobles, 2018). Researchers are advocating for the use of human-centered cybersecurity as a standardized approach to information security and cybersecurity (Bureau, 2018; Nobles, 2018). A prominent vendor stated that human-centered cybersecurity enhances the foundation for obtaining an in-depth comprehension of human behavior and the rationality of human decision-making when interacting with an information system (Forcepoint, 2018). Human-centered cybersecurity is necessary for cybersecurity as a mechanism to reduce human error and improve business operations.

EDUCATING CYBERSECURITY PROFESSIONALS ON HUMAN FACTORS

Cybersecurity professionals are woefully undertrained on human factors due to a dearth of empirical research. Researchers assert that most cybersecurity training and awareness programs are ineffective in modifying end-users' behavior (Coffey, 2017). Another factor that is adversely impacting the cybersecurity domain on human factors is the scarcity of psychology-based professionals, human factor practitioners, and cognitive scientists involved in business organizations cyber operations (Clark, 2015; Georgalis et al., 2015; Lee, Park, & Jang, 2011; Paustenbach, 2015). Nobles (2018) stressed that equating human error to a training and awareness issue is a fallacy. Mansur (2018) advocates that people are not the weakest link in cybersecurity; the problem is organizations failed to provide meaningful training and support to cybersecurity professionals. Properly educating cybersecurity professionals on human factors is imperative to optimize human performance. Professional associations and organizations should include learning objectives for human factors in certification training manuals.

HUMAN FACTORS ASSESSMENTS IN CYBERSECURITY

A significant mistake in cybersecurity is the marginalization of cognitive scientists and human factor experts; thus, resulting in the lack of assessments on human performance and behavior in active cyber environments (National Security Agency, 2015).

Scientific work on human performance and behavior by cognitive and human factor experts can provide practical insight on (a) automation and information overload, (b) technological deterministic thinking, (c) procedural alignment, (d) operational tempo, and (e) the impact of technology on the workforce (Nobles, 2016). 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). The omission of human factor assessments in businesses equates to organizations not holistically understanding human behavior and techniques to reduce errors while optimizing performance.

BENEFITS OF HUMAN FACTORS PROGRAMS

Federal agencies like the Nuclear Regulatory Commission, Federal Drug Administration, Federal Aviation Administration, and the National Aeronautics and Space Administration benefit from established human factors programs. Business organizations should seriously contemplate developing and implementing a human factors program given the number of cybersecurity incidents caused by human-enabled errors. A human factors program can serve as an organizational platform to address human-centric issues in cybersecurity and develop formalized processes for ensuring human-centered cybersecurity practices are achieved. A possible objective for a human factors program is to ensure all employees undergo annual human factors training as well as for organizations to complete an annual human factors assessment. Within the human factors program, organizations can create an executive-led human factors board or council to oversee enterprise human factor issues. Another area that a human factors board can assist with is optimizing the functions and tasks that require automation to prevent the misuse of automation and to determine the cognitive demands required for each task. Identifying dangerous attitudes in cybersecurity is necessary to enable organizations to take preemptive measures analogous to the dangerous attitudes in aviation. It is important for technology and security leaders to quantify and qualify the complexity of cybersecurity operations to enable psychology-based professionals to investigate and remediate problematic areas. The ultimate goal of a human factors program is to mitigate misalignments between people, technology, and processes to reduce error and cybersecurity incidents that result in substantial financial losses.

PRACTITIONER TAKEAWAYS

Below is a list of practitioner takeaways from this research:

1. Business organizations can benefit from human factors programs
2. Most business organizations lack the residential expertise to solve human factor-based issues in cybersecurity without the inclusion of psychology-based professionals in cybersecurity
3. Partner with psychology-based professionals, cognitive scientists, and human factor experts
4. Human-enabled errors in cybersecurity are costly and mostly avoidable
5. Security fatigue is a real phenomenon that most organizations failed to remediate
6. Cybersecurity and technology professionals require human factors training
7. Without conducting human factor assessments, organizations' information security risk assessments are inconclusive

Conclusion

Without a human factors program, business organizations are failing to mitigate a significant blind spot that results in human errors and subsequently cybersecurity incidents. Cybersecurity attacks are mounting and intensifying; consequently, making most organizations vulnerable from a human factors viewpoint especially as cyber threat actors increasingly target human weaknesses and limitations (Nobles, 2018). Even though organizations are investing substantially in cybersecurity technologies and services, most will experience a cybersecurity incident due to the inattentiveness to human factors. Research indicates that humans are the weakest link and a critical vulnerability within cybersecurity; yet, most organizations fail to provide adequate human factors training so in truth this is an organizational induced vulnerability. Thus, making organizations the weakest link instead of humans because business decision-makers are responsible for ensuring the organization is adequately trained. The cybersecurity threat landscape is too hyperactive and perilous for businesses to continue to turn a blind eye to human factors in cybersecurity.

REFERENCES

1. 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.
2. Carter, W.A. (2017). Forces shaping the cyber threat landscape for financial institutions. *SWIFT Institute Working Paper No. 2016-004*, October 2, 2017. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Cyber_Threat_Landscape%20_Carter.pdf
3. Clark, A. (2013). Whatever next? Predictive brains, situated agents, and the future of cognitive science. *Behavioral and brain sciences*, *36*(3), 181-204.
4. 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).
5. 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
6. 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/
7. 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.
8. Hasib, M. (2018). Cybersecurity as People Powered Perpetual Innovation. In *Information Technology-New Generations* (pp. 7-10). Springer, Cham.
9. Holstein, W.K. & Chapanis, A. (2018, May 11). Human factors engineering. Encyclopedia Britannica. Encyclopedia Britannica, Inc. Retrieved from https://www.britannica.com/topic/human-factors-engineering
10. 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.
11. 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.
12. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.
13. National Security Agency (2015). Science of Security (SoS) Initiative Annual Report 2015. Retrieved from http://cps-vo.org/sos/annualreport2015
14. 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
15. Nobles, C. (2016). Cyber Threats in Civil Aviation. *Security Solutions for Hyperconnectivity and the Internet of Things*, 272.
16. Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88. doi: 10.2478/hjbpa-2018-0024
17. Paustenbach, D. J. (Ed.). (2015). *Human and Ecological Risk Assessment: Theory and Practice (Wiley Classics Library)*. John Wiley & Sons.
18. Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

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

20. Taylor, J., McAlaney, J., Hodge, S., Thackray, H., Richardson, C., James, S., & Dale, J. (2017, April). Teaching psychological principles to cybersecurity students. In *2017 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1782-1789). IEEE.