Summary To " Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity"

Author: Calvin Nobles PhD, University of the Cumberlands

By : Erwin Firdhani

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.

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

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).

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)

. 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). There is no empirical research on integrating human factors program in cybersecurity, which further impedes the creation of human-centric approaches in cybersecurity.

THE DEARTH OF PSYCHOLOGY-BASED PROFESSIONALS IN CYBERSECURITY

Currently, there is a shortage of psychology-based professionals working and supporting cybersecurity operations. Human factorsis a scientific field about the interaction of humans with computers and information systemsto 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)

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).

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)

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)

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)

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)

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 psychologybased 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). 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).

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 PROGRAM

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.

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.

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).

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.