2023

# Human Factors in Cybersecurity: Academia's Missed Opportunity

Calvin Nobles

# Human Factors in Cybersecurity: Academia's Missed Opportunity

**Calvin Nobles**
Illinois Institute of Technology
cnobles1@iit.edu

## ABSTRACT

With human errors and behavior being significant contributors to data breaches and cyber-attacks, it is critical to integrate human factors principles into cybersecurity education. The lack of emphasis on human factors in cybersecurity curricula has resulted in a significant gap in understanding and addressing the role of human behavior in cybersecurity. This paper highlights the need for colleges and universities to offer courses in human factors principles in cybersecurity to educate the future workforce. The article discusses the importance of understanding human factors in designing secure systems and the benefits of integrating human factors into cybersecurity research and practice. The paper addresses the challenges institutions face in developing and teaching human factors courses in cybersecurity, including the need for more faculty members with relevant expertise and credentials. This research argues that teaching human factors in cybersecurity is essential to prevent data breaches and cyber-attacks caused by human errors and behavior.

### Keywords

Cybersecurity, Human Behavior, Human Factors, Information Security, Information Technology

## INTRODUCTION

A report by the Ponemon Institute (2019) indicated that 49% of data breaches result from human errors and system glitches. Security and technology executives indicated that cloud misconfigurations are human errors that hinder security compliance (Coker, 2020). Nobles (2018, 2019, 2022a, and 2022b) emphasized the importance of leveraging human factors in cybersecurity to better understand the human element in digitized environments, impeded by a lack of appreciation and under-exploration from the academic community. Given the persistent issues with human errors, poor cybersecurity behavior, and organizations' inability to understand the human element in cyberspace, the academic community could be the nexus to increase the appreciation for human factors by integrating such classes into cybersecurity.

First, it is essential to note that human factors engineering is a scientific discipline that has existed for more than 80 years (Nobles, 2022b) that evolved from experimental psychology research in military aviation. Existing literature defines human factors as the scientific discipline based on understanding and improving human interactions with systems (IEA, 2000)—which some practitioners call human factors engineering. Second, companies note employees as the weakest link in cybersecurity, compounded by a skewed reliance on technological solutions, as 70-80 percent of cyber-attacks result from human-induced errors (Blau, Alhadeff, Stern, Stinson, & Wright, 2017; Meshkat, Miller, Hillsgrove, & King, 2020). A recurring misconception in practice is leveraging technology solutions to prevent human limitations and weaknesses in cybersecurity (Meshkat et al., 2020; Schneier, 2000). Cyber-attacks' ascendancy results from malicious cyber threat actors capitalizing on human errors and psychological weaknesses (Blau et al., 2017). Nobles (2022a) contends that the challenges associated with the human element in cybersecurity are a significant blind spot because technology does not correct human behavior and human performance.

## BACKGROUND

No study to date has examined the importance of developing and teaching human factors courses in cybersecurity. While there are studies on human-computer interaction (HCI); however, it is vastly different from a human factors course, and their variances should be respected. Furthermore, existing literature on cybersecurity curricula lacks guidance on what should be included in the education and training (Jones, Namin, & Armstrong, 2018). Here lies the problem! Human factors as a scientific discipline fail to garner support from government, academic, and industry stakeholders, hence the lack of human factors courses in cybersecurity curricula.

Beach's (2014) study of 129 colleges and universities offering cybersecurity programs found that 2% mandated a human factors course for graduation, 36% offered human factors courses as an elective, and 62% did not. The analysis included human-computer interaction courses as part of human factors curricula. The HCI specialization evolved from human factors, providing a truncated curriculum focusing primarily on digital interfaces. Despite being an 80-year-old scientific discipline, human factors remain under-utilized in cybersecurity, with a significant gap in understanding its value (Nobles, 2019; 2022a; 2022b). Human errors and behavior contribute to 70-80% of data breaches, highlighting the need to better understand human factors in cybersecurity (Blau et al., 2017; Meshkat et al., 2020). The effect of more institutions not teaching human factors courses remains unclear. This preliminary study aims to explore the number of institutions teaching undergraduate and graduate-level human factors courses. This study will support subsequent research inquiries regarding human factors curricula in cybersecurity.

### The Human Factor versus Human Factors

The knowledge gap in cybersecurity concerning human factors as a scientific discipline is evident, hence the unfamiliarity of human factors engineering and its significance in cybersecurity (Nobles, 2022c). Nobles (2022b) asserts that understanding human factors is crucial, yet many cybersecurity professionals remain unaware of its scientific nature. Two conflicting definitions exist: (a) the working definition of human factors focuses on negative human behavior (Nobles, 2022b), while the scientific definition (human factors engineering) emphasizes designing systems to optimize human performance, fit, and behavioral outcomes (Nobles, 2022b). The scarcity of human factors professionals in cybersecurity exacerbates the knowledge gap (Nobles, 2019). Scholarly articles often address adverse security outcomes related to human factors (Jeong, Mihelcic, Oliver, & Rudolph, 2019; Mohammad, Hussin, & Husin, 2022; Rahman, Rohan, Pal, & Kanthamanon, 2021), but the current working definition fails to capture the benefits of human factors as a scientific discipline. Developing comprehensive scientific and working definitions (Ladner, 2019) could improve understanding and inform solutions to mitigate risks, ultimately enhancing cybersecurity practices. The purpose of discussing the different definitions highlights that human factor engineering is a scientific discipline with foundational significance and historical proof of addressing reducing high friction areas associated with the human element.

### Human Factors Course Curriculum

There is a paucity of scholarly research on developing and teaching human factors in cybersecurity. The study of human factors focuses on improving the fit between end-users and systems to optimize human behavior and performance. For cybersecurity, human factors courses should focus on the human element in a digitized environment to safeguard critical data. According to Glavin and Maran (2003), a human factors curriculum should integrate consist of the following topics: (a) task management, (b) situational awareness, (c) decision-making, (d) teamwork, and (e) information processing. Traditional human factors courses include topics such as (a) anthropometry, (b) perception, (c) cognition, (d) human performance, and (e) design (D'Souza, 2017). I teach courses in human factors in cybersecurity that include the following areas listed above and the following topics: (a) history of human factors, (b) human error, (c) fatigue, (d) sociotechnical systems, (e) cyberpsychology, (f) cybersecurity threat landscape, (g) human factors analysis and classification system, (h) human capability, (i) cognitive hacking, (j) cybersecurity awareness, (k) technology integration and implications, (l) design thinking in human factors and (m) human performance issues—to teach a complete immersion in human factors. To offer human factors in cybersecurity courses, faculty members with relevant expertise and credentials are crucial. However, colleges and universities may face challenges in finding faculty members with both cybersecurity and human factors expertise, which could contribute to the lack of such courses in cybersecurity curricula.

## METHODS

This research is the preliminary study of multiple inquiries about human factors in cybersecurity. In order to identify how many CAE institutions require or offer a course in human factors within a cybersecurity curriculum is critical for exploring the gap. With the number of human errors resulting in cyber-attacks and security incidents, the criticalness of human factors education is necessary. The objective was to determine the number of CAE-accredited institutions that offered a human factors course in cybersecurity using the CAO website that listed approved and accredited schools by the National Security Agency.

Due to the unavailability of most human factors course syllabi online, this project relied on course titles and descriptions to identify relevant courses. Human-computer interaction courses were excluded due to being different from human factors courses. The primary criteria for inclusion were courses that emphasized the human element in cybersecurity.

The analysis will take place in the following steps.

1. Using the CAE community website: https://www.caecommunity.org/cae-map
2. Select institutions that offer cybersecurity programs
3. Use the CAE-provided link for the institution or google via the Internet to locate the school's graduate cybersecurity program
4. Review the cybersecurity curricula to determine if human factors is a required course or
5. The institution offers a human factors course
6. If not, go on to the next school
7. If yes, annotate the name of the course and the course description
8. Analyze the course description to determine if human factors principles will be explored in the course

## FINDINGS

The research team collected data using the CAE-accredited institutions with cybersecurity programs listed on the CAE community website. The researchers annotated each university from the CAE website that offered a cybersecurity program and institutions that offered a human factors course in cybersecurity. Table 1 lists the graduate-level schools, and Table 2 lists the undergraduate institutions.

| NAME OF INSTITUTION | NAME OF COURSE | REQUIRED | ELECTIVE | PROGRAM |
|---|---|---|---|---|
| Augusta University | AIST 6353 - Human Factors in Information Security | | X | ISM |
| Arizona State University | IFT 598 - Human Factors in Cybersecurity | | X | IT |
| Bay Path University | CBY 635 - Human and Organization Aspects of Cybersecurity | X | | Cyber |
| Baylor University | ISEC 5310 - Cyber Security Human Factors: Ethics, Integrity, Practices, Policies, And Procedures | | X | IS - Concentration in Cyber |
| Bellevue University | CYBR 520 – Human Aspects of Cybersecurity | X | | Cyber |
| City University of Seattle | ISEC 510 - Human and Organization Security | X | | Cyber |
| Columbus State University | CPSC 6136 - Human Aspects of Cybersecurity | X | | Cyber |
| Illinois Institute of Technology | ITMS 534 – Human Factors in Cybersecurity | | X | IT / Cyber |

| | | | | |
|---|---|---|---|---|
| Norfolk State University | CYS 688 - Human Aspects in Cybersecurity | X | | Cyber |
| Norwich University | GI 532 – Human Factors and Risk Management | X | | Information Security and Assurance |
| Penn State University | IST 577 – Human Factors of Security and Privacy | | X | Information Science |
| UNLV | CSEC 704 – Human Factors in Cybersecurity | X | | Cyber |
| University Of North Dakota | PSYC 522 - Human Factors in Cyber Security | | X (Cybersecurity Analyst Track) | Cyber |
| University Of Washington - Bothell | CSS 518 - Human Factors in Cybersecurity | | X | Cyber |
| University of Wisconsin (University System) | CYB 705 – Sociological Aspects of Cybersecurity | X | | Cyber |

**Table 1: List of CAE Accredited Institutions with a Human Factors Course (Graduate)**

The researcher determined that 224 institutions offered graduate-level cybersecurity programs. Of the 224 institutions examined, 15 offered a human factors course in cybersecurity. I reviewed the programs and examined the course descriptions to determine if the class met the criteria for this analytical effort. Below is a table of each university and the name of the class. From the Tables, one can observe the different naming nomenclature of the courses. Table 1 shows that 15 out of 224 (14.9%) CAE institutions with graduate-level cybersecurity programs offer a human factor in cybersecurity courses. I reviewed and analyzed 224 CAE institutions with cybersecurity graduate programs and reviewed the course names and descriptions to verify the human factors classes. Eight out of the 15 (53%) institutions listed in Table 1 offer a human factors course as a required class, and seven out of 15 (47%) offer the course as an elective. Table 2 displays the undergraduate results. Out of 391 undergraduate institutions (CAE accredited), six schools (1.53%) offered a human factors course in cybersecurity, in which five out of the six schools indicated the human factors course was mandatory. The analysis indicated that the human factors courses were part of the cybersecurity, information security, information technology, information security and assurance, and information science programs. Institutions took various approaches to establish their cybersecurity curriculum, as indicated by the different programs in which the classes were aligned. The study omits the courses incorporating human factors as a subtopic, such as general MIS courses with a week dedicated to information security human factors, resulting in a limitation.

| NAME OF INSTITUTION | NAME OF COURSE | REQUIRED | ELECTIVE | PROGRAM |
|---|---|---|---|---|
| Bowie State University | CTEC 440 Human Factors | X | | Computer Technology |
| Gwinnett Technical College | HITC 1050 Usability and Human Factors | X | | Health Info Tech |
| Illinois State University | IT 467 Human Factors in Info Systems | X | | Information Tech |
| University Of California, Irvine | ICS 4 Human Factors for The Web | | X | Informatics |
| University Of Detroit, Mercy | CIS 3350 Intro to Human Factors in Security | X | | Computer & Info Sys |
| U.S. Navy Academy | SY 304 Huma Factors in Cyber Operations | X | | Cyber Operations |

**Table 2: List of CAE Accredited Institutions with a Human Factors Course (Undergraduate)**

## CONCLUSION

The lack of human factors in cybersecurity curricula is a significant concern for academia, which impedes addressing human factors problems in industry. Colleges and universities must bridge this gap by offering human factors courses in cybersecurity to educate the future workforce and provide continuing education for cybersecurity professionals. Understanding the barriers that prevent institutions from embracing human factors in cybersecurity is critical, as human errors and poor behavior continue to cause significant damage to organizations, governments, and academia. By addressing this gap and educating on human factors, we can equip future cybersecurity professionals to aid in preventing data breaches and cyber-attacks caused by human errors and poor decision-making.

In future research, the researcher will engage with instructors who effectively teach human factors in cybersecurity to address human error mitigation. Collaborative efforts among institutions could facilitate the development of pedagogical frameworks, thereby benefiting universities lacking expertise in both cybersecurity and human factors.

## REFERENCES

1. Beach, S. K. (2014) Usable cybersecurity: Human factors in cybersecurity education curricula, *National. Cybersecurity Institute Journal*, *1*(1), 5-15.
2. Blau, A., Alhadeff, A., Stern, M., Stinson, S., & Wright, J. (2017) Deep thought a cybersecurity story, *Ideas42© 2017*.
3. Coker, J. (2020, July 23) Cloud misconfiguration a major compliance risk, say ITdecision-makers, https://www.infosecurity-magazine.com/news/cloudmisconfigurations-compliance/.
4. D'Souza, C. (2017) Topics in inclusive design for the graduate human factors engineering curriculum, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, (1), 403–406, https://doi.org/10.1177/1541931213601583.
5. Glavin, R. J., & Maran, N. J. (2003) Integrating human factors into the medical curriculum, *Medical Education*, *37*, 59-64.
6. International Ergonomics Association (IEA). (2000) Definition of human factors. http//www.iea.cc/whats/.
7. 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)* (pp. 338-345). IEEE.
8. Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018) The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals, *ACM Transactions on Computing Education (TOCE)*, *18*(3), 1-12.
9. Meshkat, L., Miller, R. L., Hillsgrove, C., & King, J. (2020, January) Behavior modeling for Cybersecurity, *In 2020 Annual Reliability and Maintainability Symposium (RAMS)*1-7, IEEE.
10. 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.
11. Nobles, C. (2022a) Investigation cloud computing misconfiguration errors using the human factors analysis and classification system, *Scientific Bulletin*, (1) 53, 59-66, doi:10.2478/bsaft-2022-0007.
12. Nobles, C. (2022b, March) The Dunning-Kruger Effect around human factors in cybersecurity, *Top Cyber News Magazine*. https://www.linkedin.com/company/topcybernews/.
13. Nobles, C. (2022c) Stress, burnout, and security fatigue in cybersecurity: A human factors problem, *HOLISTICA–Journal of Business and Public Administration*, *13*(1), 49-72.
14. Nobles, C. (2019) Establishing human factors programs to mitigate blind spots in cybersecurity, *MWAIS 2019 Proceedings*, *22*.
15. Nobles, C. (2018) Botching human factors in cybersecurity in business organizations, *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88.
16. Ponemon Institute. (2019) Cost of a data breach report; IBM Security: North Traverse City, MI, USA, 2019.
17. 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* (pp. 1-11).
18. Schneier, B. (2000) Semantic attacks: The third wave of network attack, *Crypto-Gram Newsletter*, *14*.