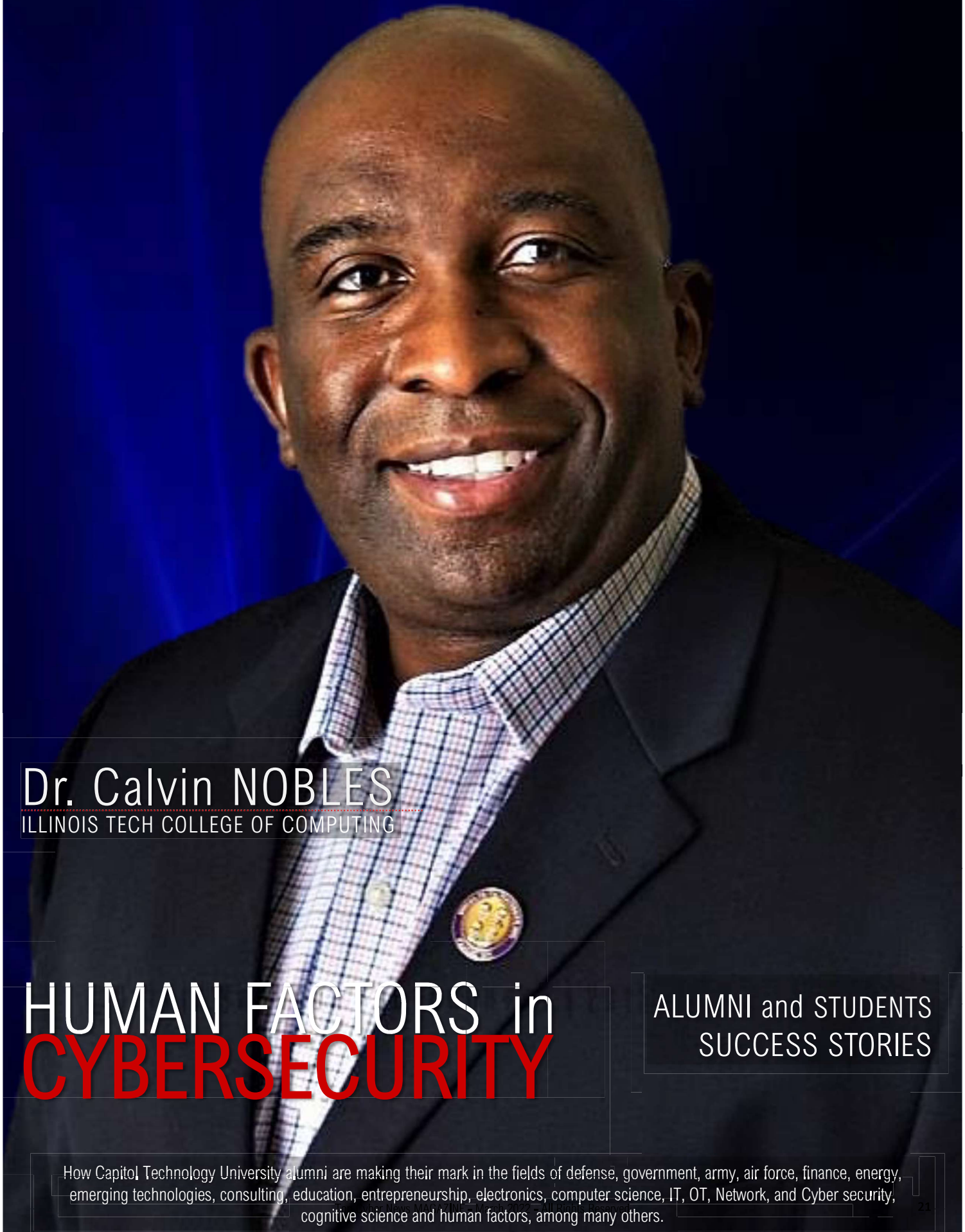
#myCapTechU

Capitol Technology University, the USA



Dr. Calvin NOBLES

ILLINOIS TECH COLLEGE OF COMPUTING

HUMAN FACTORS in CYBERSECURITY

ALUMNI and STUDENTS SUCCESS STORIES

How Capitol Technology University alumni are making their mark in the fields of defense, government, army, air force, finance, energy, emerging technologies, consulting, education, entrepreneurship, electronics, computer science, IT, OT, Network, and Cyber security, cognitive science and human factors, among many others.

The Dunning-Kruger Effect Around Human Factors in Cybersecurity

Author: Dr. Calvin NOBLES

Many organizations continue to struggle with cybersecurity, especially as the cybersecurity threat landscape evolves and threatens the current postures implemented by most businesses.

A recent article titled ***The Unaddressed Gap in Cybersecurity: Human Performance*** in the *MIT Sloan Management Review* highlights that organizations are prone to implement technology as a mechanism to combat cybersecurity threats and vulnerabilities without realizing the implications on human performance.

Organizations universally practice leveraging technology to level up against emerging and sustained threats in cybersecurity. The abovementioned article illustrates how a technology-led cycle makes organizations more vulnerable to cybersecurity threats.

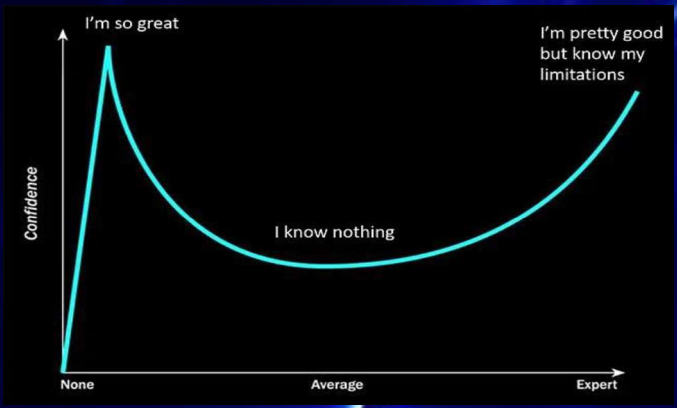
"A steady diet of technologies to mitigate threats is problematic in that the human element is an afterthought and often forgotten." The human factors field has existed for 80 years and uses scientific methods to improve system designs, yet it is noticeably missing in cybersecurity operations.

The purpose of human factors is to engineer systems, technologies, and processes that account for human capacity and limitations to optimize human performance within an environment-in other words, designing systems to maximize human performance, which indirectly reduce errors or other high friction areas that degrade performance and functionality.

"Human factors as a scientific discipline are practiced in aviation, medicine, space operations, nuclear power, and mining operations. These domains use human factors methods to improve system designs, reduce errors, and risk while optimizing operations."

"Cybersecurity is a sociotechnical system analogous to the aforementioned fields, but cyber decision-makers undervalue human factors (scientific discipline), a significant blind spot in cybersecurity."

It is important to note that the "human factor" is often misconstrued. Most articles or publishing reference the working definition of human factors. The working definition is any human-related factor that pertains to human errors, poor security behavior, noncompliance, or any negative connotation regarding humans making mistakes in cybersecurity.



The scientific definition, as noted above, relates to using scientific methods to enhance human performance through effective system designs. The working definition overshadows the scientific definition and meaning of human factors. Unfortunately, this impedes the acceptance of human factors as a scientific field in cybersecurity. Most articles addressing human factors in cybersecurity refer to the working definition. As the human element continues to emerge as an area of concern, the conversation is shifting towards human factors as an engineering discipline to increase the focus on the human aspects in cybersecurity.

From engaging in discourse with senior technology and security executives, it is apparent that most are naive that human factors engineering is a scientific discipline leveraged by other sociotechnical domains to ameliorate human performance in complex systems. Without a doubt, cyber business decision-makers are busier than ever, and this has increased the Dunning-Kruger effect associated with human factors in cybersecurity.

The Dunning-Kruger concept pertains to possessing a low level of knowledge on a particular subject (in this case, human factors) in which an individual overextends his competency resulting in errors.

The Dunning-Kruger effect is a cognitive bias, whereas people with a low level of knowledge overestimate their competency regarding a particular topic. The Dunning-Kruger effect, in this case, applies to cybersecurity decision-makers' low-level understanding of human factors as a scientific discipline. Poor security behavior remains a high-friction point in cybersecurity, yet most organizations fail to adopt human factors methods based on a scientific approach.

Human behavior and human performance issues in cybersecurity cannot be remediated through technology; consequently, it requires the integration of human factors practitioners into cybersecurity operations to conduct analyses and assessments to develop practical solutions for high-friction areas. Security and technology executives must acknowledge their lack of competence with human factors and proactively partner with human factors professionals. A salient goal of human factors initiatives is to reduce organizational risk.

Many cybersecurity professionals are unaware that "human factors" is an engineering discipline like software engineering, network engineering, and cybersecurity engineering. However, most pretend to be subject matter experts on the topic based on the working definition - this is the Dunning-Kruger effect in full effect. **The proliferation of the Dunning-Kruger effect in cybersecurity is risky and costly due to errors and mistakes concealed by incompetence.**

In fairness, it is impossible for security and technology executives to be all-knowing in cybersecurity; however, these cyber decision-makers must be cognizant of blind spots and the intersectionality of multidiscipline areas - such as human factors engineering.

"Security and technology executives lack an appreciation and respect for the human factors discipline, which enables the Dunning-Kruger effect."

Given the complexity of human-related issues in cybersecurity, this persistent fallacy relies on technology to mitigate human behavior. It is apparent by the absence of human factors engineers in cybersecurity. Psychology professionals and human factors practitioners are essential areas of expertise needed in cybersecurity to counter cybercriminals' use of psychology. Most organizations' current organic cybersecurity talent pool lacks the training and expertise to develop strategies and initiatives to address the human factors issues. The heightened attention on social engineering, cognitive attacks, and human errors in cybersecurity are relegated to technical solutions - a clear sign of the Dunning-Kruger effect.

"Believing that technology is an effective and permanent solution to a human behavior problem is a fallacy."

Human factors engineering is a developing discipline for cybersecurity as cyber evolves across many domains and grows into a sociotechnical system. Security and technology executives are under immense pressure to advance their organizations while maximizing security. Therefore, the easier path for increasing cybersecurity is leveraging technology; consequently, security and technology executives are unaware of the adverse implications of a technology-led cycle, such as human performance degradation. Accounting for the human element in cybersecurity operations takes an assertive approach. The Dunning-Kruger effect prevents cybersecurity decision-makers from effectively addressing human factors in cybersecurity. At issue is that human factors engineers are not viewed as essential staff for cybersecurity, which is further compounded by cybersecurity professionals' failed attempts to address human factors problems through policies, technologies, and security awareness.

The benefits of human factors initiatives include:

- Improved usability and acceptance
- Increased safety
- Reduced lifecycle cost and risk
- Reduced risk

"A flourishing cyber-attack vector is cognitive hacking, resulting from cybercriminals and malicious hackers capitalizing on the psychological vulnerabilities of end-users."

James Bone, the author of *Cognitive Hacking: The New Battleground in Cybersecurity—The Human Mind*, points out that employees are underprepared to counter cognitive attacks. In this book, the author explores haking as a sustained industry and practice and the engineering aspects behind cognitive hacking. Most organizations attempt to mitigate cognitive hacking and social engineering through security awareness. Unfortunately, security awareness is insufficient and lacks the robustness and reinforcement to achieve the intended outcome. A human factors engineer can assist organizations with designing more effective systems, training, processes, and initiatives to enhance human performance in cybersecurity.

The cybersecurity domain is not the first to experience human behavior and performance issues. However, the reluctance of cybersecurity leaders to expand our optics to explore such problems in other sociotechnical systems and domain propagates the Dunning-Kruger effect. In the past decades, researchers have written extensively to address the human factors problems in cybersecurity. Cybersecurity decision-makers are aware of human behavior issues, and it remains a lower-tier priority. Humans are one of the most significant vulnerabilities in cybersecurity, and organizations predominantly pursue technical solutions to resolve human behavior - in which the technology-led cycle leads to complexity debt and human performance degradation.

The human factors problems plague cybersecurity, and the reluctance to engage human factors engineers proliferates the Dunning-Kruger effect.

People, processes, and technology are the universally accepted pillars of cybersecurity. Technology is necessary for cybersecurity, but it cannot be the only solution or the dominant pillar. Because technology is the preferred method of solving cybersecurity problems, technical solutions are applied in most situations even when it is not appropriate - human performance problems arise from the technology-led cycle; thus, making organizations more vulnerable. At this point, we cannot remove the human element from cybersecurity because people are involved in most aspects of cybersecurity (software engineering, network engineering, incident response, policymaking, artificial intelligence implementation, governance, digital forensics, etc.).

The people, processes, and technology approach demand a proper balance regarding the human element to reduce cybersecurity risks and vulnerabilities.

There is optimism for eradicating the Dunning-Kruger effect on human factors in cybersecurity.

First, cyber decision-makers need to recognize the knowledge gap and partner with human factors practitioners, similar to teaming with cybersecurity consultants.

Second, academia, industry, and governments should elevate the importance of human factors in cybersecurity given the increasing complexity and advanced technologies (AI, ML, and intelligent devices). This includes human factors educational programs that highlight the importance of addressing the human element in sociotechnical systems—cybersecurity.

Third, colleges and universities need to develop a human factors specialization in cybersecurity, information security, and information technology.

Fourth, cybersecurity and information technology certifications should include sections on human factors because, as of today, certification programs omit training objectives on the human element.

Furthermore, ***"human factors practitioners and researchers are responsible for spearheading efforts to inform cyber decision-makers and government agencies on the importance of human factors in cybersecurity."***

Additionally, ***"human factors researchers are responsible for research to develop practical solutions for human-related problems in cybersecurity. Human factors experts need to pursue every possible platform to educate on the importance of human factors as a scientific and engineering discipline in cybersecurity."***

Dr. Calvin NOBLES, the USA

Dr. Calvin Nobles is a native of Mount Vernon, Georgia, a globally recognized human factors engineering and cybersecurity. He currently serves as Department Chair and Associate Professor for Information Technology and Management at the Illinois Institute of Technology.

Calvin began his distinguished career in the U.S. Navy. He served as a senior advisor on signals intelligence, cryptology, cybersecurity, and cyberspace operations on multiple military staffs and various assignments. Additionally, he worked in national security supporting various military campaigns and deployed on several occasions to support national and maritime operations throughout his military career. Upon retiring from the U.S. Navy in 2017, he embarked on a corporate career in the financial services industry as a cybersecurity and information security subject matter expert. Calvin continues to advise senior executives on cybersecurity, risk management, and human factors engineering in cybersecurity. Many recognize him as a thought leader for his expertise in human factors.

Among his multiple graduate degrees in STEM and business administration, including a Ph.D. in Human Factors. He speaks and writes prolifically on advancing human factors engineering and its importance in cybersecurity. As a researcher, he focuses on human performance and behavior in cybersecurity and technology implementation to reduce organizational risk. Calvin currently serves as a Cybersecurity Fellow at Harvard's Belfer Center and previously served as a Cybersecurity Policy Fellow at the New America Think Tank in Washington, DC. He is a frequent visitor on various social media platforms discussing reducing cybersecurity risk through the human element.