Ensuring Accessibility when Implementing the CIA Triad

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

April 23, 2025

Assignment

For this assignment, you will produce a paper-length analysis of the social meaning and impact of cybersecurity-related technical systems. It'll be easier than it sounds. You'll produce a rough draft of most the paper by combining two of the journal entry assignments you've already completed. After that, you'll edit and revise so that it reads smoothly and then add a final section with a concluding analysis. In the end, you'll have a 1200+ word paper that draws from and draws together work that you've done throughout the course.

Analytical Paper - DETAILED INSTRUCTIONS

Ensuring Accessibility when Implementing the CIA Triad

This paper contends that cybersecurity policies must enhance CIA Triad accessibility to address the digital divide for older adults and people with disabilities, leveraging Human Factors Cybersecurity Engineers' (HFCEs) human-centered design (HCD) for equitable system access (Lochstampfor, 2025). This analysis builds on prior coursework examining HFCEs' role in inclusive design, adapted to focus on CIA Triad implementation. The CIA Triad—Confidentiality, Integrity, and Availability—underpins cybersecurity. However, mechanisms like multi-factor authentication (MFA) often exclude marginalized users due to complex interfaces (Messer, 2023). Through the Responsible Cyber-Infrastructure Development lens, I propose policies mandating accessible designs, such as biometric MFA and text-to-speech, drawing on social science principles to foster trust. This analysis examines accessibility challenges, HFCE solutions using information and communication technologies (ICTs) and assistive technologies (AT), societal impacts, and unresolved issues. The following section outlines the ethical and political framework guiding this analysis, introducing the Responsible Cyber-Infrastructure Development lens and emphasizing policy changes for inclusive cybersecurity.

Responsible Cyber-Infrastructure Development

Responsible Cyber-Infrastructure Development demands ethical and political policy changes to ensure cybersecurity systems serve all users equitably. Jonas (1973) argues that technology's societal impacts require policies integrating morality into design to promote fairness (p. 42). In cybersecurity, this means making the CIA Triad's principles—Confidentiality (restricting data access), Integrity (maintaining data accuracy), and Availability (ensuring system access)—accessible to older adults and people with disabilities who face digital exclusion from inaccessible systems (Renaud & Coles-Kemp, 2022, p. 2).

Current CIA Triad implementations prioritize security and usability over accessibility, creating barriers. For example, using CAPTCHAs or SMS tokens, MFA for Confidentiality challenges older adults with cognitive decline or visually impaired users (Ellefsen & Chen, 2022, p. 205). Interfaces for verifying Integrity or accessing systems (Availability) exclude users reliant on AT (Renaud & Coles-Kemp, 2022, p. 5). Policies must mandate accessible solutions, like biometric authentication and text/voice-to-speech, aligned with Web Content Accessibility Guidelines (WCAG) 2.1, which require high-contrast visuals, keyboard navigation, audio descriptions for videos, and adjustable time limits for tasks (Renaud & Coles-Kemp, 2022, p. 4). To help mandate inclusive digital services, governments could establish accessibility task forces, fund HFCE training, and offer tax incentives that mirror the EU's Web Accessibility Directive and Canada's Accessible Canada Act. Industry collaboration with organizations like the World Wide Web Consortium can standardize solutions, ensuring platforms like telehealth portals are usable in a "digital-first" society, fostering trust and equity (Renaud & Coles-Kemp, 2022, p. 2; Ali et al., 2024, p. 8). Thus, in the following section, we will examine accessibility challenges and HFCE solutions.

Evidence and Analysis

Accessibility Challenges in CIA Triad and AAA Framework

The CIA Triad, supported by the AAA Framework (Identification, Authentication, Authorization, Accounting), is cybersecurity's cornerstone. However, its mechanisms often exclude marginalized users, worsening digital exclusion. First, Confidentiality relies on protocols and procedures such as MFA, combining passwords, biometrics, or tokens (Nieles et al., 2017, pp. 22, 44–45). However, older adults struggle with CAPTCHAs or complex passwords due to cognitive or visual impairments (Ellefsen & Chen, 2022, p. 205). For example, complex login protocols hinder visually impaired users from accessing government service portals or online messaging apps, essential ICTs for civic and social engagement (Renaud & Coles-Kemp, 2022, p. 3). These barriers heighten vulnerability to cybercrimes like phishing, vishing (voice-based scams), or smishing (SMS-based scams), which exploit trust and cause psychological distress, such as anxiety over identity theft, discouraging digital engagement (Ellefsen & Chen, 2022, p. 206).

Second, data Integrity requires user verification through tools like hashing and digital signatures; however, inaccessible interfaces challenge motor-impaired tablet users (Renaud & Coles-Kemp, 2022, p. 5). Third, Availability ensures system access through redundancy (Nieles et al., 2017, pp. 24–25). However, it is irrelevant if interfaces lack accessible controls, like voice activation for telehealth tools (Wu et al., 2015, p. 194). Lastly, the AAA Framework exacerbates this: Authentication's CAPTCHAs exclude visually impaired users; Authorization's Role-Based Access Control assumes interface interaction; Identification's document requirements hinder access to digital IDs; and Accounting needs accessible logs (Nieles et al., 2017, pp. 41–45, 47–49; Renaud & Coles-Kemp, 2022, p. 3). Therefore, these barriers necessitate HCD solutions.

HFCE Solutions Using ICTs and Assistive Technologies

To help eliminate accessibility barriers, HFCEs apply HCD and social science principles—self-efficacy, human-computer interaction, risk perception—to design accessible CIA Triad implementations, using ICTs and AT to empower marginalized users. Older adults use ICTs like smartphones, email, social media, video conferencing (e.g., Zoom), and online portals but fear cybercrimes and cyber victim precipitation (e.g., phishing, identity theft) (Wu et al., 2015, p. 194; Ellefsen & Chen, 2022, p. 206). HFCEs provide training to improve self-efficacy, enabling MFA use. Wu et al. (2015) found that educational programs help improve the comfort of older adults when they handle ICTs, promoting confident use of platforms like telehealth (p. 196). For example, tailored workshops teach older adults to use biometric MFA on smartphones or navigate telehealth apps with voice controls. Simplifying secure access while reducing their reliance on caregivers for assistance is a boon for society and their local communities.

AT enhances accessibility by supporting diverse user needs. Text-to-speech interfaces enable visually impaired users to access online portals, ensuring Availability (Renaud & Coles-Kemp, 2022, p. 5). Voice recognition systems streamline MFA for motor-impaired users, bolstering Confidentiality (Renaud & Coles-Kemp, 2022, p. 3). Health monitoring devices, automated medication reminders, and emergency alert systems maintain secure data Integrity, addressing privacy concerns (Ellefsen & Chen, 2022, p. 206). Memory-enhancing applications support cognitive-impaired users, facilitating secure system interaction (Wu et al., 2015, p. 193). Home automation tools, like secure door entry systems, foster independent living (Wu et al., 2015, p. 193). Lastly, HFCEs use threat modeling and focus groups to design intuitive systems, identifying gaps like SMS-based MFA struggles for hearing-impaired users (Renaud & Coles-Kemp, 2022, p. 3).

Modern Security Education, Training, and Awareness (SETA) programs support accessibility in society. Ali et al. (2024) recommend gamification, such as mock phishing exercises on platforms like GoCyberSafe.org or Cyber-Seniors, to train older adults (p. 9). For example, a simulation might teach users to spot phishing emails on tablets, using leaderboards, badges, and role-playing scenarios to reward progress or guide biometric MFA setup on Android devices. Tailored modules for hearing-impaired users incorporate visual cues and sign language videos, ensuring inclusivity. Such training minimizes human errors, which are responsible for about 95% of security breaches, enabling confident navigation of digital platforms (Nobles, 2018, p. 82).

Societal Impacts

Accessible CIA Triad implementations benefit society. Older adults build confidence with ICTs, enhancing social engagement via social media or Zoom platforms and fostering stronger community connections (Wu et al., 2015, p. 196). People with disabilities access healthcare and finance via AT, such as hearing aids, promoting equity and digital literacy and reducing healthcare disparities through telehealth access (Renaud & Coles-Kemp, 2022, p. 3). SETA programs lower cybercrime risks, enhancing workforce inclusion by enabling secure online training (Ali et al., 2024, p. 7). Critics argue that accessibility increases costs or vulnerabilities (e.g., biometric breaches), fearing threat actors will exploit decentralized and fragmented systems. However, evidence suggests that enhanced accessibility may produce long-term benefits, such as reduced cybercrime and greater digital participation, potentially offsetting initial implementation costs (Ali et al., 2024, p. 7; Renaud & Coles-Kemp, 2022, p. 3). Lastly, HFCE threat modeling mitigates risks, enhancing security by reducing errors and supporting mental health through reduced digital stress (Ali et al., 2024, p. 7; Nobles, 2018, p. 82).

Final Analysis & Remarks

In summary, policies enforcing CIA Triad accessibility, guided by HFCEs' HCD and SETA, address the digital divide, enabling older adults and people with disabilities to securely and confidently engage with ICTs and AT (Lochstampfor, 2025). Evidence from Wu et al. (2015), Renaud and Coles-Kemp (2022), and Ali et al. (2024) shows that biometric MFA, screen readers, and gamified training enhance Confidentiality, Integrity, and Availability, fostering trust. For example, an older adult using a smartwatch with accessible interfaces monitors health confidently.

Critics highlight costs, biometric risks, or system fragmentation. HFCE-driven solutions balance accessibility and security, minimizing errors (Ali et al., 2024, p. 7). However, Jonas's (1973) Short Arm of Predictive Knowledge suggests uncertainty about AI-driven AT vulnerabilities, like data breaches or quantum threat resilience, requiring vigilance (p. 39). Unfortunately, challenges continue to this day in funding equitable access and unifying global accessibility standards across diverse cultural and economic contexts, risking inequity if policies lag. Therefore, to help reduce digital exclusion and ensure an equitable digital society for all users worldwide, leaders and countries must prioritize accessibility within their cyber infrastructures.

References

Ali, A., Overboe, C., Mailewa, A. B., & Chen, Y. (2024, April). The human factor in cybersecurity: Understanding psychology, training efficacy, and error reduction strategies. *In Proceedings of the 2024 Conference on Cybersecurity (pp. 1–14). ResearchGate.* https://www.researchgate.net/publication/380156139

Ellefsen, J., & Chen, W. (2022). Privacy and data security in everyday online services for older adults. *In Proceedings of the 10th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion (DSAI 2022)* (pp. 204–208). Association for Computing Machinery. https://doi.org/10.1145/3563137.3563149

Jonas, H. (1973). Technology and responsibility: Reflections on the new tasks of ethics. *Social Research, 40(1)*, 31–54. http://www.jstor.org/stable/40970125

Lochstampfor, C. (2025). Human Factors: A CISO's Response to Human Error & Threats. *Unpublished manuscript, Department of Cybersecurity, Old Dominion University*. https://sites.wp.odu.edu/locky/it-cyse-200t-2/

Lochstampfor, C. (2025). Human factors cybersecurity engineering: Inclusive design through social science. *Unpublished manuscript, Department of Cybersecurity, Old Dominion University*. https://sites.wp.odu.edu/locky/cyse-201s-cybersecurity-social-science/

Lochstampfor, C. (2025). The CIA Triad & the AAA Framework. *Unpublished manuscript, Department of Cybersecurity, Old Dominion University*. https://sites.wp.odu.edu/locky/it-cyse-200t-2/

Messer, P. (2023, November 1). *The CIA Triad - CompTIA Security+ SY0-701 - 1.2 [Video]. YouTube.* https://www.youtube.com/watch?v=SBcDGb9l6yo

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security *(NIST Special Publication 800-12 Revision 1). National Institute of Standards and Technology*. https://csrc.nist.gov/pubs/sp/800/12/r1/final

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA, 9(3)*, 71–88. https://doi.org/10.2478/hjbpa-2018-0026

Renaud, K., & Coles-Kemp, L. (2022). Accessible and inclusive cyber security: A nuanced and complex challenge. *SN Computer Science, 3(5),* Article 346. https://doi.org/10.1007/s42979-022-01239-1

Wu, Y.-H., Damnée, S., Kerhervé, H., Ware, C., & Rigaud, A.-S. (2015). Bridging the digital divide in older adults: A study from an initiative to inform older adults about new technologies. *Clinical Interventions in Aging, 10, 193–201.* https://doi.org/10.2147/CIA.S72399