Digital Security Challenges in the Disciplines of Arts, Humanities, and Social Sciences

By

Dr Joel Kelechi Ezirim
Trinity Theological College Umuahia

Abstract

Security challenges in the disciplines of arts, humanities, and social sciences may not immediately seem as apparent as in fields like technology or defense, but they are increasingly relevant. These challenges can be broadly categorized into digital, physical, intellectual, and ethical dimensions; each impacting the ways research, teaching, and cultural preservation are approached in these fields. In this paper the researcher decides to focus on the digital security. The researcher was informed based on what is currently happening in the field of arts, humanities and social sciences. In the field of humanities today, digital security issues are becoming increasingly prominent due to the widespread use of digital technologies for research, communication, and cultural preservation. The paper adopts the qualitative sociological approach. This paper, therefore aims at describing what digital security is all about and its security challenges in the disciplines of arts, humanities and social sciences. The study discovers that, although Digital security measures protect personal, financial, and sensitive data from unauthorized access, theft, or leaks as the advantages and thus providing a deeper and fuller protection to the fields, yet it has some key challenges which include: Data Sensitivity and Privacy, Copyright and Intellectual Property, Cyber security Awareness and Skill Gaps, Open Access and Data Sharing, Interdisciplinary Collaboration and Ethical Considerations. The study therefore recommends among other things that for an effective and hitch free Digital security, attention must be given to these challenges and ways of overcoming them.

Key Words: Arts, Challenges, Digital Security, Disciplines, Humanities, and Social Sciences

Introduction

The arts, humanities, and social sciences are interconnected fields that collectively study human creativity, culture, behavior, and societal structures. They explore the richness of human experience, often focusing on qualitative aspects of life and addressing questions about meaning, value, and relationships. As a body of knowledge together, these fields form a comprehensive framework for understanding and improving the human condition. This body of knowledge is dynamic, integrating perspectives to address complex global issues, and remains essential for fostering empathy, critical thinking, and informed citizenship. Security challenges in the disciplines of arts, humanities, and social sciences may not immediately

seem as apparent as in fields like technology or defense, but they are increasingly relevant. These challenges can be broadly categorized into digital, physical, intellectual, and ethical dimensions; each impacting the ways research, teaching, and cultural preservation are approached in these fields. In this paper the researcher decides to focus on the digital security. This is because in the field of humanities today, digital security issues are becoming increasingly prominent due to the widespread use of digital technologies for research, communication, and cultural preservation. Digital security is the protection of digital assets from unauthorized access to sensitive information.[1] This paper attempts to describe and critically examine the challenges of digital security in the fields of arts, humanities and social sciences. The paper started with the concept of Digital security, different types of digital security to the fields were identified, described and critically examined, exposing the challenges in the field of arts, humanities and social sciences.

Concept of Digital Security

Digital security is the protection of digital assets from unauthorized access to sensitive information.[2] It is also known as information security, is the practicing of protecting digital information from unauthorized access, use, disclosure, disruption, modification, or distruction.[3] It is also regarded as cyber security by some scholars notwithstanding the fact that there are notable differences between the two. Digital security refers to the practices, tools, and measures used to protect electronic devices, networks, and data from unauthorized access, attacks, theft, or damage. It encompasses a wide range of techniques such as encryption, authentication, firewalls, antivirus software, and secure coding practices to safeguard personal, academic, business, and governmental information. According to Simplilearn, Digital security is the collective term that describes the resources employed to protect your online identity, data, and other assets. These tools include web services, antivirus software, Smartphone SIM cards, biometrics, and secured personal devices. According to him, it is the process used to protect your online identity[4]. Uwadia and Friday[5] posits that digital security can be understood as the protection of information systems from theft, damage, or unauthorized access, ensuring the integrity, confidentiality, and availability of digital data. This includes measures to safeguard against cyber threats like hacking, identity theft, and malware attacks**.** Digital security aims to maintain the confidentiality, integrity, and availability of data, ensuring that only authorized users can access sensitive information and systems. It covers various domains like cybersecurity, information security, and online privacy protection**.**

Boyd researches social media, privacy, and the ways young people interact with technology. She emphasizes that digital security in social networks is not just about protecting information but also about protecting people's social relationships and reputation in digital contexts[6]. Lessig while dealing on cyber law argues that "code is law" in the digital age, meaning that the architecture of digital systems shapes what is possible, permissible, and secure. His work suggests that legal frameworks need to account for how digital code influences individual rights and freedoms, highlighting the need for laws that ensure digital security and privacy[7].

Nevertheless, Crawford examines the ethical implications of artificial intelligence and data, noting that AI can amplify existing power structures and biases. She argues that digital security must address data sovereignty and the impact of big data on marginalized communities, who are often most vulnerable to surveillance[8]. Contributing on digital security Dourish focuses on how people interact with digital technologies in different cultural contexts. He argues that security and privacy policies should consider cultural and social factors, as perceptions of privacy vary across societies and impact how digital systems should be designed and implemented[9].

Eubanks in her work explores how automated systems and data-driven policies affect marginalized communities. She argues that digital security must address systemic inequalities, as surveillance disproportionately affects low-income communities, potentially leading to discrimination and privacy erosion[10]. Angwin is a journalist who has extensively covered digital surveillance, often focusing on how government and corporate practices affect personal privacy. She highlights the need for transparency and accountability in digital security practices, particularly when they involve the collection and analysis of personal data.[11]

Morozov coming from the angle of Sociology, Political Science, Technology Criticism was critical of the way technology companies use digital security as a pretext for invasive surveillance. He argues that cybersecurity is often shaped by corporate interests and highlights the risks of digital monopolies controlling sensitive.[12]

Some Key Digital Security Challenges in the Fields of Arts, Humanities and Social sciences

Each of the following factors forms part of an evolving framework that scholars, researchers, and practitioners use to address the dynamic challenges of digital security.

Digital security poses unique challenges to the disciplines of arts, humanities, and social sciences due to the nature of the data, research practices, and modes of collaboration common in these fields. The following are some of the major security challenges in these fields.

1. **Data Sensitivity and Privacy**

Researchers in these disciplines often work with sensitive data, such as personal interviews, ethnographic fieldwork, or cultural artifacts, which require careful handling to protect privacy and confidentiality. Implementing and maintaining digital security systems can be expensive. Therefore, inadequate security measures due to high costs of maintenance can lead to data breaches, threatening the trust between researchers and participants.

2. **Copyright and Intellectual Property**

Arts and humanities researchers often deal with creative works (music, literature, art) and social sciences handle large datasets. Ensuring that digital versions of these materials are protected against unauthorized access, copying, or distribution is essential. Digital piracy and copyright infringement are ongoing threats.

3. **Cyber security Awareness and Skill Gaps**

Scholars in these fields may not have extensive technical training in cybersecurity, making them more vulnerable to phishing, malware, or other forms of cyberattacks. Limited awareness or training in safe digital practices can leave academic projects, archives, and communications at risk. The care-free life of some people in Nigeria, their ignorant of regular security breach and negligence of information has left our worthwhile information or gadget into the hand of cybercriminal.[13] Some people leave their gadget anywhere later to find out that somebody has made away with it and such exposing information into wrong hands that can use it for something evil. Unfortunately, too many users don't deploy the privacy settings on the device. Moreover, advanced digital security systems require highly skilled professionals for setup, monitoring, and management, which can be difficult to find and costly to hire.

4. **Open Access and Data Sharing**

The growing push for open access to research findings and data presents both an opportunity and a security challenge. While openness fosters collaboration, it also requires careful balancing to prevent the exposure of sensitive materials or intellectual property.

5. **Digital Preservation and Integrity**

Long-term preservation of digital works (such as digital art, oral history archives, or social media analysis) faces risks from data corruption, format obsolescence, or even intentional

tampering. Ensuring the integrity and authenticity of these works over time requires robust security frameworks.

6. **Interdisciplinary Collaboration**

Increasing collaboration across disciplines, including partnerships with tech developers or data scientists, introduces the challenge of sharing data securely. In interdisciplinary projects, participants from non-technical fields may not fully understand the vulnerabilities involved, leading to potential breaches.

7. **Surveillance and Censorship**

Researchers in social sciences and humanities often engage with politically sensitive topics. Digital security lapses can make them vulnerable to state surveillance, censorship, or harassment, particularly in authoritarian regimes or environments hostile to certain research topics.

8. **Ethical Considerations**

The ethics of data collection, especially in digital ethnography or social media research, involves navigating the boundaries of privacy, consent, and data security. The potential for large-scale surveillance or data scraping raises ethical dilemmas about participant rights and security.

In short, the challenge is to create secure systems and practices while maintaining the open, collaborative, and creative spirit that defines these disciplines.

Some Major Factors that can be used to Address the Dynamic Challenges of Digital Security.

Digital security encompasses a range of factors that scholars from various fields highlight as essential to protecting information, systems, and individuals in the digital landscape. Here are some of the major factors identified:

1. Confidentiality, Integrity, and Availability (CIA Triad)

Confidentiality: Ensuring data is accessible only to those with authorization.

Integrity: Ensuring data is accurate and has not been tampered with.

Availability: Ensuring data and systems are accessible to authorized users when needed.

Scholars in information security widely use the CIA triad as a foundation for discussing and implementing security measures.

2. **Authentication and Access Control**

Authentication: Verifying the identity of users and systems (e.g., passwords, biometrics, multi-factor authentication).

Access Control: Managing who has permission to access or modify data

Scholars like David Ferraiolo and D. Richard Kuhn emphasize role-based access control as a critical factor in maintaining security within organizations.[14] The use of flimsy/trivial or stress-free to predict passwords are not good for security purpose. However, passwords are going to continue to be the first point of validation for a long time. Trivial password is like no password, any password that resolves around the name of the owner, name of organization or acronym of organization can easily be predicted by hacker or people. It can then become an issue of what password should be used for security bearing in mind that owner of password always want what they can remember. The owner of system should think of what cannot easily be predicted regardless of how it will be recall by the individual.[15]

3. **Encryption and Data Protection**

Encryption is key for protecting sensitive information both at rest and in transit.

Cryptography experts like Bruce Schneier[16] highlight encryption as essential for maintaining privacy and ensuring data security. This challenge, highlighted by researchers, is balancing the utility of data with privacy protection. While organizations collect data to drive insights and improve services, ensuring that sensitive data remains private is critical. Privacy-enhancing technologies (PETs), like differential privacy and homomorphic encryption, are areas scholars are actively exploring to balance data utility with privacy.

4. **Risk Management**

This involves identifying, assessing, and mitigating potential risks, including technical vulnerabilities and human errors. Scholars in cyber security, such as NIST researchers, emphasize a risk-based approach to prioritize resources and address potential threats. The following measures should be adopted to curb such risks:

(i)Always shut down computer: Computer should be shut down when not in use or on your way out of the computer room otherwise exposes the computer to malicious attack which may cause bandit to carry away computer thereby exposing the information into a wrong hands. This can also make hackers to use undue privilege to attack the system.[17]

(ii) Negligence to adopt security progams: This negligence is recorded mostly when security measures are neglected by owners or key players in these fields due undue consciousness to cybercrimes. This paper stands to say that every internet user should be aware of the challenges pose by hackers and give possible solutions to cyber insecurity in Nigeria. It could be none of the aforementioned issue but wickedness of people. People can overlook setting

security measures.[17] They get familiar with the society that they neglect security measures. Some of them will end up crying heard I know later.

(iii)Social media: The social media contains the good and bad. Engaging the social media while doing serious academic work exposes your information of hacker or intruder unknown to you. Social media is a hotspot embedded with malwares and vices that may affect academic material.[19]

5. **User Education and Awareness**

Human error is a major factor in security incidents, so user education is essential.

Researchers like Angela Sasse have shown that user training and awareness can reduce security incidents, as people are often the weakest link.[20]

6. **Incident Response and Recovery**

This involves preparing for, detecting, responding to, and recovering from security incidents.

Scholars in cyber security frameworks like the NIST Cybersecurity Framework emphasize structured incident response to minimize damage.

7. **Legal and Regulatory Compliance**

Compliance with regulations like GDPR, HIPAA, and PCI-DSS is essential to avoid legal consequences and protect user data.

Legal scholars and researchers focus on regulatory compliance as critical in the context of protecting data rights and reducing fields and organizational risks.

8. **Privacy Protection**

Privacy extends beyond security to include data collection and usage transparency.

Experts like Daniel J. Solove highlight the importance of privacy-preserving practices, including data minimization and anonymization.[21]

9. **Emerging Threats and Technological Advances**

Staying ahead of emerging threats such as AI-driven attacks, ransomware, and quantum computing is vital. Researchers in fields like artificial intelligence and quantum cryptography study how advances can improve security but also present new risks.

10. **Collaboration and Information Sharing**

Cooperation between organizations, governments, and industries helps in sharing threat intelligence. Scholars argue that threat intelligence sharing helps improve the collective response to security threats on a global scale.

Conclusion

In conclusion, digital security in the fields of arts, humanities, and social sciences presents unique challenges due to the increasing reliance on technology for research, communication, and dissemination of knowledge. These fields often handle sensitive data, including cultural heritage, personal narratives, and societal trends, making them vulnerable to cyber threats such as data breaches, intellectual property theft, and digital misinformation. Addressing these challenges requires tailored strategies that balance accessibility and security, fostering awareness and equipping researchers with the necessary tools and best practices. Collaborative efforts between technologists and scholars are essential to safeguard digital assets while promoting innovation and trust in these disciplines.

Endnotes

1. Sailpoint-https//www.sailpoint.com.digital
2. Sailpoint-https//www.sailpoint.com.digital
3. EC-Council, University-eccu.edu/blog/technology.
4. https://www.simplilearn.com/authors/simplilearn.
5. Uwadia Francis & Eti, I. Friday (2018) "Cyber Security in Nigeria: Issues, Challenges and Way Forward," International Research Journal of Advanced Engineering and Science, Volume 3, Issue 2, pp. 351-354,
6. Boyd, D. (2011). Protecting Sensitive Information: The Virtue of Self-Restraint. *Homeland Security Affairs*, *7*(1)
7. Lessig Lawrence(1999), Code and other laws of Cyberspace ,America: Basic Books,10 E. 53rd Street, New York, NY 10022-5299.
8. Bird, S., Barocas, S., Crawford, K., Diaz, F., & Wallach, H. (2016). Exploring or exploiting? Social and ethical implications of autonomous experimentation in AI. In *Workshop on Fairness, Accountability, and Transparency in Machine Learning*.

9. Dourish Dourish, P. (2001). *Where the action is: The foundations of embodied interaction* (Vol. 210). MIT Press.

10. Eubanks, V. (2012). *Digital dead end: Fighting for social justice in the information age*. MIt Press.

11. Angwin, J. (2017). Digital security for Journalists. In *Journalism After Snowden: The Future of the Free Press in the Surveillance State* (pp. 114-129). Columbia University Press.

12. Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*.

PublicAffairs.

13. Mead, D. (2023). Creating disinformation: Archiving fake links on the Wayback Machine viewed through the lens of routine activity theory. *First Monday*.

14. David Ferraiolo and D. Richard Kuhn(1997) Role Based Access Control https://www.researchgate.net/publication/2792237_Role-Based_Access_Control

15 Montoro and Massimiliano(2009) Q&A: Cain and Abel, the password Recovery tool https://www.helpnetsecurity.com/2009/07/07/qa-cain-abel-the-password-recovery-tool/

16 Schneier, B. (2019). *We have root: Even more advice from Schneier on security*. John Wiley & Sons.

17. Friess, P. (2016). *Digitising the industry-internet of things connecting the physical, digital and virtual worlds*.River Publishers.

18. Ed Gelbstein (2013). Gelbstein, E. (2013). Quantifying information risk and security. *ISACA Journal*, *4*.

19. Jim Finkle (2014). Finkle, J. (2014). Exclusive: FBI warns healthcare sector vulnerable to cyber attacks. *Reuters, April*.

20. Sasse, M. A. (2005). Usability and trust in information systems. Edward Elgar.

21. Solove, D. J. (2010). *Understanding privacy*. Harvard University press.