# IMPEDANCE OF UPHOLDING CYBERSECURITY ETHICS IN A DATA DRIVEN PROFESSION

**Godslight Thomas SESE**
Department of Cybersecurity, Faculty of Science
Federal University Otuoke, Bayelsa State, Nigeria
https://orchid.org/0009-0004-3497-063
sesegodslight@yahoo.com
+2348069659313

## Abstract

*Nigeria's rapidly growing digital economy is increasingly reliant on data-driven professions. In an era characterized by rapid digital transformation and pervasive data utilization, professionals engaged in data-driven fields face significant risks and ethical challenges. Cybersecurity ethics, a subset of professional ethics related to safeguarding information and ensuring privacy within the cyberspace, has become paramount. This paper is geared to identify the impedance of upholding cybersecurity ethics and recommend sustainable solutions to enable state and non-sate actors in data driven profession, uphold cybersecurity ethics. This paper explores the foundational principles of cybersecurity ethics, the importance of ethical conduct in data-driven professions, challenges faced by practitioners, and strategies for fostering an ethical cybersecurity culture. Qualitative research method was employed, interviews and group discussion was also done to complement the secondary data sources. Findings reveal that impedance of upholding cybersecurity ethics include inadequate cybersecurity infrastructure, skills gape, evolving cybercrime dynamics, poor enlightenment, clash of interest by state and non-state actors, no generally accepted cybersecurity ethical framework in data driven profession, no constitutionally approved regulatory body for cybersecurity ethical practice and conducts amongst others. Recommendations include rapid investment in cybersecurity infrastructure, emphasizing the responsibility of the Nigerian government and professionals to prioritize privacy, integrity, and trust. This paper advocates for a comprehensive ethical framework and continuous education to uphold cybersecurity ethics in the evolving digital landscape.*

***Keywords*:** Impedance, Cybersecurity, Ethics, Data

## Introduction

The proliferation of digital data has revolutionized how organizations operate, making cybersecurity a critical concern. Data-driven professions are at the forefront of this transformation. However, the immense power of data also introduces significant ethical dilemmas, such as privacy violations, data misuse, and breaches of trust. Upholding Cybersecurity ethics is essential to safeguard stakeholders' interests, maintain professional integrity, and promote societal trust in digital systems. In today's digital era, Nigeria has experienced exponential growth in data generation and utilization across various sectors, including finance, healthcare, agriculture, arts and culture, entertainment, education, sports, commerce, telecommunications, and government. This surge underscores the importance of cybersecurity which implies principles that guide responsible behavior when handling data. Upholding cybersecurity ethics is crucial to safeguarding sensitive information, maintaining public trust, and ensuring compliance with legal frameworks. To this end, upholding cybersecurity ethics requires finding a near perfect balance between security and privacy while acknowledging the concrete impacts of security decisions. (Shewale, 2025).

In today's world where data fuels decisions, innovations, and connections, cybersecurity has emerged as a pivotal area of concern. As organizations increasingly rely on data-driven strategies, ensuring ethical practice of cybersecurity is paramount. The ethical landscape of cybersecurity not only encompasses adherence to legal requirements but also involves maintaining trust, privacy, transparency, accessibility and integrity in handling data. This article explores the critical aspects of upholding cybersecurity ethics in a data driven profession driven. Thus, the role of cybersecurity professionals has become more crucial than ever as the ethical responsibilities of those safeguarding this information are paramount. (Von Solms & Van, 2013)

The cybersecurity landscape is constantly evolving, driven by technological advancements and the increasing sophistication of cyber threats. Data has become a central component of cybersecurity, enabling professionals to analyze patterns, identify anomalies, and predict potential attacks. Data-driven security practices such as Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), and Threat Intelligence Systems, rely heavily on the collection, processing, and analysis of vast datasets. However, the increasing reliance on data raises significant ethical considerations, particularly concerning privacy, bias, and accountability. (Flechais & Chalhoub, 2023).

Cybersecurity professionals working in data-driven environments face complex ethical dilemmas. They must balance the need to protect systems and data with the rights and interests of individuals and organizations. The potential for misuse of data, the risk of bias, and the lack of transparency in data-driven security practices can undermine trust and create unintended consequences. This paper aims to provide a comprehensive overview of the ethical challenges facing professionals in

data-driven profession and to propose a framework for promoting ethical conduct and responsible innovation.

**Why Ethics Matter in Data-Driven Profession**

In today's progressive digital transformation as a result of technological advancement, below are reasons why ethics matter in data-driven profession

1. Data fuels decisions in both defenses and offensive research (misuse can tantamount to irreversible damages to both state and non state actors).

2. Ethical lapses erode trust, accountability and integrity which might lead to legal arbitration. (Jaisan, T. 2025).

3. Cybersecurity professionals should ensure both human and systems safety within data-driven professions.

**The Significance of Cybersecurity Ethics**

Cybersecurity ethics encompass the moral obligations and responsibilities of professionals who manage information systems. These ethics enables the mitigation of computer crime in relations to information insecurity such as data breaches, identity theft, unauthorized access and insider threats amongst others. In Nigeria, where cybercrime is on the rise, strict adherence to ethical procedures cannot be overemphasized. Cybersecurity ethics serve as a moral compass for professionals working with sensitive information in data-driven professions. Given the sensitive nature of personal and institutional data, ethical practices prevent malicious activities like unauthorized access, data breaches, and identity theft (Flechais & Chalhoub, 2023).Thus, strict compliance to ethical procedures and processes is crucial to mitigate threats and compromise. Thus, below are ways to ensure a safe data-driven ecosystem,

i. **Builds Trust and Reputation**

Trust is an abstract currency as unethical practices can lead to data breaches that compromise sensitive information which might tantamount to reputation damage. Thus, cybersecurity ethics ensure integrity and confidentiality of sensitive data for both state and non-state actors. (Brown & Treviño 2006).

ii. **Privacy and Compliance**

Data-driven professions handle vast amounts of individual and corporate data. Ethical cybersecurity practices ensure compliance with the Nigeria Data Protection Act (NDPA) of 2023 and other legal frameworks that guide the handling of data and information.

iii. **Security Breaches and Their Implications**

Cybersecurity professionals must understand the dynamics of cybercrime, develop mitigation plan and manage risks associated with security breaches.

**Cybersecurity Core Ethical Principles**

According to the European Agency for Cybersecurity (2023), cybersecurity core ethical principles are anchored on the following

- **Confidentiality**

Protecting sensitive data from unauthorized access is paramount. Ethical practices ensure that confidentiality is maintained through robust encryption, steganographic and access control measures

- **Integrity**

Ethical cybersecurity practices demand honesty and transparency, ensuring that data integrity is never compromised. Maintaining the accuracy and trustworthiness of data is essential. Ethical practices include preventing unauthorized modifications and ensuring data is not altered maliciously or negligently.

- **Availability**

Ensuring that data and systems are accessible to only authorized users when needed, without disruption, aligns with ethical best practices.

- **Privacy**

Respecting individuals' rights to control their personal data involves implementing privacy-preserving measures and adhering to relevant legal frameworks such as theNigeria Data Protection Act 2023 (NDPA).

- **Accountability and Transparency**

Professionals should be accountable for actions that affect data security. This involves maintaining logs, documenting decisions, and being ready to answer for their actions.

Cybersecurity professionals should act responsibly and be transparent about security practices, vulnerabilities, and incidents. This fosters trust and accountability.

- **Non-Maleficence** This principle involves not inflicting harm. In cybersecurity, this translates to taking proactive measures to prevent data theft, loss, or corruption.

**Ethical Frameworks Guiding Cybersecurity Practices**:

1. **Code of Ethics:** Professional organizations like the Computer Professionals Registration Council of Nigeria (CPN), Nigeria Computer Society (NCS), Practical Artificial Intelligence Development Foundation (PAIDF) etc, provide codes of ethics for computing professionals. These codes emphasize integrity, confidentiality, and responsible use of technology.

2. **Legal Data Protection Policy:** The Nigeria Data Protection Act (NDPA) outlines principles for data processing, including lawfulness, fairness, transparency, and data minimization.

**Impedance in Upholding Cybersecurity Ethics**

Nigeria faces several cybersecurity challenges that impact data-driven professions. In the cause of this research, the following impedance was uncovered.

- **Evolving Cyber Threats:** As technology keeps advancing, cyber threats become more sophisticated. Hence, been ahead requires continuous learning and adaptation while maintaining ethical standards.

- **Resource Constraints:** State and non-state actors struggle with the resources needed to implement robust cybersecurity defenses due to its huge financial implications. Therefore, making it difficult to comply or maintain ethical standards.

- **Ethical Dilemmas:** Ethical dilemma is one of the impedance against upholding cybersecurity ethics due to unclear and ununified ethical standards. For instance, the conflict between user privacy, access rights and national security.

- **Conflicting Interests**: The major intent of every business owner is to maximize profit and remain in business. Hence, business plan conflict with ethical standards, such as prioritizing profit over privacy.

- **Rapid Technological Change:** Evolving threats and innovative tools require continuous reassessment and evaluation of cybersecurity ethical and legal framework.

- **Limited Oversight:** Lack of standardized ethical frameworks across organizations can lead to inconsistent practices. Thus, similar organizations should have same standard for the sake of compliance, periodic monitoring and evaluations.

- **Power Dynamics:** Superiority in knowledge base and enable unethical behavior or exploitation.
- **Skills Gap:** There exist huge gapes of skilled cybercrime and cybersecurity professionals in Nigeria, hindering effective defense against cyber threats. Thus, engaging unprofessionals, who do not have in-depth knowledge of cybercrime and cybersecurity neither the rules of engagement.
- **Lack of Awareness:** Insufficient awareness among employees about cybersecurity risks and best practices increases vulnerability.
- **The Dynamics of Cybercrime:** Nigeria is a hub for cybercrimes such as phishing, identity theft, financial fraud amongst others. According to Godslight, T. S. (2025), Nigeria is ranked the highest in the world in scams having 52.17% followed by USA with 22.72% in 2025.

**Godslight T. S 7 Pillars of Cybersecurity Etiquette in Data-Driven Professions**

The Godslight T. S. 7 pillars of cybersecurity etiquette is formulated to help both state and non-state actors to be abreast and equipped with the fundamental principles of upholding cybersecurity ethics in data driven professions in Nigeria.

- Critically develop and implement a dynamic and sustainable crystal cybersecurity ethical framework in line with the Nigeria Data Protection Act (NDPA) of 2023.
- Design a security and privacy framework to periodically review cyber risks.
- Quarterly implement or carryout cybersecurity Data Impact Assessments (DIA) to identify vulnerabilities.
- Design and implement a Role-based Access Control mechanism.
- Design and implement an ethical role-based access disclosure policy for all parties.
- Constitute an ethical regulatory and monitoring board or committee to evaluate implementation and compliance level.
- Sustainable training and retraining of employees on current trends in cybercrime and cybersecurity with respect to professional code of conduct.

## Conclusion

As our world becomes increasingly data-dependent, upholding cybersecurity ethics is more crucial than ever. It requires a balanced approach that integrates technical solutions with ethical considerations. Organizations and cybersecurity professionals must collaborate to foster environments where ethical standards are not just met but exceeded. By doing so, they safeguard not only data and systems but also the trust and social contracts businesses rely on. More so cybersecurity ethics in a data-driven profession is vital to safeguarding not only digital assets but also societal trust and individual rights. As technology evolves, so too must the ethical standards guiding cybersecurity practices, ensuring they adapt to new challenges and uphold the core principles of responsibility, fairness, and respect. By adhering to established codes, fostering awareness, and cultivating a culture of ethics. Finally, upholding cybersecurity ethics is essential for building a resilient and trustworthy data-driven ecosystem in Nigeria. Addressing the existing challenges requires a multi-faceted approach involving education, awareness, legal compliance, ethical leadership, government interventions, partnerships and collaborations. By integrating ethical frameworks into cybersecurity practices, Nigeria can mitigate risks, protect data, and foster responsible innovation.

## Suggestions

To ensure a sustainable downplay of impedance of upholding cybersecurity ethics in data driven profession in Nigeria, both state and non state actors must ensure to:

1. **Implement Continuous Training and Education**

Regular training sessions on the latest ethical standards and understand the dynamic nature of cybercrime to enable professionals stay informed and prepared.

2. **Establishment of a Unified Policy**

Organizations should have well-defined cybersecurity and ethical policies that guide professional conduct and decision-making.

3. **Imbibe a Culture of Ethics**

Encouraging a workplace culture that prioritizes ethics can influence positive behavior among employees.

4. **Incident Response Planning**

Having a clear, ethical incident response plan ensures that breaches are handled promptly and transparently.

5. **Collaboration and partnership**

The Nigerian government, cybercrime and cybersecurity professionals and non-state actors must ensure sustainable collaboration and partnership to achieve professional conduct in data driven professions

6. **Legal and Regulatory Compliance**

Ensure compliance with the NDPA of 2023 and other relevant laws. Implement robust data protection policies and procedures.

7. **Ethical Leadership** Promote ethical leadership within organizations to foster a culture of integrity and accountability.

8. **Independent Audits**

Conduct regular independent audits to assess cybersecurity practices and identify areas for improvement.

## References

Brown, M. E., & Treviño, L. K. (2006). Ethical leadership: A Review and Future Directions. *The Leadership Quarterly 17(6), 595-616.* https://doi.org/10.1016/j.leaqua.2006.10.004

European Agency for Cybersecurity (2023). *Multilayer Framework for Good Cybersecurity Practices for AI.* https://www.enisa.europa.eu

Godslight T. S, (2025). Cybercrime: A Threat to National Security in Nigeria. *International Journal of Basic Science and Technology. July, Volume 11, Number 2, Pages 197 – 203* **https://doi.org/10.5281/zenodo.16729087**

Jaisan, T. (2025). Legal and Ethical Challenges in the Digital Age: Data Privacy, AI, and Cybersecurity. *Journal of the International Academy for Case Studies, 31*(S1), 1-3. https://www.abacademies.org

Shewale V. (2025) The Ethics of Cybersecurity: Balancing Security and Privacy in the Digital Age. *European Journal of Computer Science and Information Technology*,13(15),11-20.

https://doi.org/10.37745/ejcsit.2013/vol13n151120

Von Solms, B., & Van Niekerk, J. (2013). "From Information Security to Cybersecurity". *Computers & Security, 38, 97 – 102*. https://doi.org/10.1016/j.cose.2013.04.004

Flechais I, Chalhoub G. (2023). Practical Cybersecurity Ethics: *Mapping CyBOK to Ethical Concerns.* https://doi.org/10.1145/3633500.3633505