Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P); 2583-7907 (E)
Vol.13 No.2, 2024, pp.61-66

www.crijournals.org
DOI: https://doi.org/10.70112/ajcst-2024.13.2.4289

Evaluating the Ethical Frameworks of Information Security Professionals: A Comparative Analysis

Ohwo Onome Blaise[1*], Izang Aaron[2], Udosen Alfred[3] and Afolarin Amusa[4]
[1&4]Department of Computer Science, [2]Department of Information Technology, [3]Department of Software Engineering, Babcock University, Ogun State, Nigeria
E-mail: izanga@babcock.edu.ng, udosena@babcock.edu.ng, amusaa@babcock.edu.ng
Corresponding Author: ohwoo@babcock.edu.ng
(Received 20 September 2024; Revised 18 October 2024, Accepted 11 November 2024; Available online 14 November 2024)

***Abstract* - Information Technology (IT) networks have become a cornerstone of business communication, evolving alongside the Internet, which now facilitates the interconnection of independent IT infrastructures. This interconnectedness has increased the risks of information disclosure and privacy violations, presenting ethical challenges for information security professionals. This study aims to evaluate the ethical codes of four major information security professional organizations in computing sciences to identify critical ethical considerations for these professionals and highlight areas for potential improvement. The study analyzes the ethical frameworks and guidelines provided by these organizations, examining their alignment with the multidimensional aspects of security, including technical, organizational, legal, social, and ecological factors. The analysis reveals that information security extends beyond technical measures, encompassing broader organizational and societal dimensions. Ethical concerns cannot be effectively addressed without engaging all stakeholders. While existing codes of ethics and security policies are valuable, they require updates to address the evolving challenges of the information society. For effective information security, professional codes of ethics must integrate comprehensive stakeholder considerations and adapt to meet the growing demands of a connected digital world. Enhancing these ethical frameworks is crucial for fostering trust and resilience in the information society.**
Keywords: **Information Security, Ethical Codes, Privacy Violations, Stakeholder Engagement, Information Society**

I. INTRODUCTION

Over the years, Information Technology (IT) networks have become an integral part of business communication infrastructure, with most components operating independently. In recent times, the Internet has evolved into a dynamic marketplace, enabling businesses to share information by connecting these independent IT infrastructures to the global network. With the world becoming increasingly interconnected, numerous methods for exploiting the Internet to cause damage, obtain valuable information, and promote disruption have significantly increased. These actions are perpetrated by crackers, hackers, dissatisfied individuals, rivals, and terrorists [1].

Security is a broad topic that encompasses a multitude of threats and challenges. In simple terms, security involves the protection of information and assets from unauthorized access. Security issues are often caused deliberately by malicious individuals seeking to gain an advantage or cause harm. Examples include unauthorized access to email, hacking to steal information, and the leakage of sensitive data [2]. Information security covers all aspects of protecting the confidentiality, integrity, and availability of information within a network. It involves safeguarding a network from both external and internal threats.

Ethics refers to the moral principles that guide a person's behavior or the conduct of an action. Computer ethics focuses on how professionals in computing sciences make decisions regarding professional and social conduct. As information technology introduces new ethical dilemmas for stakeholders, it also creates opportunities for significant social change. This duality means that information technology can foster social progress while also facilitating crimes and threatening cherished societal values [2].

The widespread use of the Internet and information technologies has raised new and often complex security and ethical issues. These challenges include establishing responsibility, setting security standards for network excellence, and preserving the integrity and values essential in an information society. Organizations must confront these problems and determine effective ways to address them.

A. Statement of the Study

Information Technology (IT) plays a central role in various organizations and communities, offering numerous commercial and societal benefits. However, it also poses certain negative impacts on society, particularly in areas related to ethics, which can be categorized into issues of privacy, access rights, and destructive actions. These issues significantly influence public reactions to technological change.

IT enables the sharing of information on a large scale from any location and at any time. However, this capability increases the potential for information disclosure and privacy violations. Consequently, with the growing popularity of e-commerce and social networking, information security has swiftly become a higher priority. In the context of

information security ethics, damaging actions refer to undesirable consequences, such as the loss or damage of information, or unintended ecological and social impacts.

Without appropriate information security policies and strategies, operations and network connections via the Internet remain insecure. It is the duty of all stakeholders to ensure the privacy and integrity of information. Precautions must be taken to maintain data accuracy and protect it from illegal access or unintended disclosure. Additionally, stakeholders should be educated on the benefits of implementing appropriate security practices [3].

B. Research Objectives

The aim of this paper is to highlight essential considerations regarding ethics for information security professionals and to identify areas for improvement. The specific objectives of the study are as follows:

1. Evaluate the moral responsibility of the information security profession;
2. Analyze the codes of ethics of four different information security organizations in computing sciences, highlight key considerations, and identify areas for potential improvement.

C. Significance of the Study

This study aims to help stakeholders critically examine their actions, choices, and decisions, considering how these impact others. Additionally, it will assist stakeholders in identifying what is truly beneficial and determining the appropriate steps to achieve it.

II. MATERIALS AND METHODS

A. A Biblical Worldview of Information Security

Information security is an increasingly critical issue that requires serious consideration. With the pervasive use of information technology in businesses, there has been a rise in information security-related crimes involving privacy and safety. Modern smartphones are highly powerful, enabling connections to various businesses, banks, offices, churches, and educational institutions via the Internet. While individuals seek the convenience of real-time access to their data, this also introduces risks, such as criminals gaining access to the same resources.

Information security professionals use their skills to protect systems and data rather than committing crimes. Psalm 19:7-10 states, “The Law of the LORD is perfect” and that “The judgments of the LORD are true and righteous altogether.” The increasing prevalence of cyberattacks demonstrates what can occur when individuals lacking a Christian worldview acquire certain professional or technical skills. Therefore, individuals with strong Christian ethics are needed to use their abilities for a greater purpose, embodying the exhortation in 1 Corinthians 10:31: “Whatever you do, do it all for the glory of God.”

Individuals who follow the teachings of Jesus, such as “Do to others as you would have them do to you” (Luke 6:31) and “Love your neighbor as yourself” (Mark 12:31), are less likely to misuse their skills for personal gain. Trust in an individual’s moral and ethical foundation is crucial when considering information security from a position of trust. A foundation rooted in strong Christian doctrine reflects in an individual’s actions, fostering trust and assurance in their ethical performance.

One of God’s commandments, “Thou shall not steal,” underscores this perspective. Consequently, Christian information security professionals not only refrain from stealing but actively prevent attacks by protecting information systems. They identify and correct vulnerabilities before they can be exploited. However, in some cases, the distinction between performing an authorized job and carrying out an attack lies solely in the permission granted to hack the information system [4].

B. The Moral Standing of Information Security

Information security involves maintaining the security goals of confidentiality, integrity, and availability. This raises the question: what ethical issues does information security present? To address this, it is necessary to explore the relationship between information security and ethics.

Information security breaches can carry significant economic costs. The loss or corruption of valuable data may lead to economic losses, while any form of data loss is also likely to cause mental or emotional distress. In extreme cases, breaches may even result in life-threatening consequences, such as injury or death [5]. Breaches of confidentiality can lead to additional problems and rights violations, including the infringement of intellectual property rights, copyrights, and privacy rights. Similarly, breaches of availability can encroach upon freedoms, such as the right to information and free speech.

Although information security procedures are designed to prevent damage and protect rights, they can sometimes cause harm or infringe upon rights. For instance, while security procedures safeguard information and system resources, they may also inadvertently prevent stakeholders from accessing information or services. Additionally, these procedures can exhibit bias by incorrectly excluding certain categories of users or privileging others.

C. Who are Professionals?

M. C. Loui [6] defined professionals as members of a distinguished professional organization possessing expert knowledge and skills acquired through academic and practical experience. These individuals contribute to the advancement of knowledge through systematic research.

Professionals aim to serve clients and address their needs while considering the welfare of both the clients and the community. Since clients may lack the expertise to fully evaluate the quality of services, other professionals can assess the services' quality. This evaluation process often leads to ethical conflicts among organizations, professionals, and clients [7].

D. Moral Responsibilities of Information Security Professionals

The responsibility of an information security (IS) professional involves maintaining the security of systems and information, thereby safeguarding the confidentiality, integrity, availability, and security of all information and its system features. These responsibilities carry moral implications, as activities performed by information security professionals may not only secure but also potentially violate individuals' moral rights.

Codes of ethics for computer and information security professionals address moral responsibilities partially but rarely in detail. For instance, the Information Systems Security Association (ISSA) [8] ethical code of conduct encourages its members to "perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles." However, it provides little to no specification of what these ethical principles are or their application in specific situations.

Therefore, ethical codes alone are evidently insufficient for information security professionals to fully understand and navigate the moral complexities of their work. There is a need for education in information security ethics to assist professionals in understanding the rights and moral standards at stake, identifying ethical questions and issues, and balancing diverse moral standards when resolving ethical dilemmas [5].

E. Application of Ethical Practices in Information Security

1. *Password Policy:* This involves securing system access using a set of words known only to the authorized individual. Passwords may consist of numbers, alphabets, or alphanumeric combinations. The strength of a password depends on its format and length. However, passwords are vulnerable to social engineering attacks.
2. *Authentication:* This is the process of verifying a person's identity. The identification provided must match the records in a database of approved individuals, either on a local operating system or an authentication server. Authentication mechanisms are susceptible to man-in-the-middle attacks.
3. *Cryptography:* This refers to the science of securing communications - whether written, voice, or in other formats - by scrambling the information using mathematical methods. Cryptography provides a means of validation and authentication for the communicating parties. However, it is important to note that cryptography alone cannot solve all problems related to information protection. It does not ensure availability, leaving systems vulnerable to denial-of-service (DoS) attacks.
4. *Intrusion Detection:* Intrusion detection systems (IDS) monitor network packets for malicious activities or policy violations, which are then reported or centrally logged using a security information system. However, the effectiveness of IDS can be significantly limited by noise, which can obscure malicious activities.
5. *Firewall:* A firewall is a system designed to monitor incoming and outgoing network traffic and prevent unauthorized access to or from a private network. Firewalls can be implemented as hardware, software, or a combination of both. Despite their utility, firewalls are susceptible to IP spoofing attacks.

F. Challenges of Ethical Practices in Information Security

Failure to employ best ethical practices can expose the network environment to several challenges, including but not limited to [9].

1. *Harms to Privacy:* With the massive amounts of sensitive data generated today, poor security practices can expose individuals' personal lives and property to the public.
2. *Harms to Property:* Assets can be attacked directly (e.g., intrusion) or indirectly (e.g., extortion) through data privacy violations, embezzlement of electronic funds, theft of valuable intellectual property, social engineering, or remote destruction of digital or physical property.
3. *Security Resource Allocation:* The high cost of security significantly influences security practices. Security measures require considerable resources, including time, money, and expertise.
4. *Transparency and Disclosure:* Transparency in general practices impacts individual welfare. Due to the risk management nature of security and its significant implications, there is an inherent ethical responsibility to disclose known risks to enable informed decision-making.
5. *Security Roles, Duties, and Interests:* Security practices involve multiple roles and interests, making ethical responsibilities ambiguous. Determining to whom the greatest ethical duty is owed and what responsibilities should take precedence can be challenging.

III. LITERATURE REVIEW

S. Wurster [10] specifically examined the code of ethics and privacy standards, introducing privacy from a new perspective - an interaction between standards and modernization in the fields of information security and critical infrastructures. A survey focusing primarily on German and European viewpoints was conducted. Based on the survey, recommendations were proposed for a new privacy standard to promote the endorsement of emerging security solutions.

S. O. Ogunlere *et al.,* [7] analyzed the code of ethical conduct of four major professional organizations in computing and engineering sciences, discussing their roles in professionalization policies, ethical standards, and practical methods. The study aimed to increase fundamental awareness of ethics among computing professionals and to highlight areas of ethical challenges.

The role of ethics in information security was explored by T. Aşuroğlu *et al.,* [11]. The study introduced rules, standards, and concepts in information security, presenting ethical dilemmas and various perspectives. By emphasizing the importance of ethics in information security, several pieces of literature were reviewed. Additionally, tools and strategies to make codes of ethical conduct effective in organizations and communities were presented.

R. Nagahawatta *et al.,* [12] conducted an extensive literature review on the rise of cyberattacks targeting Small and Medium Enterprises (SMEs) in the context of Internet and innovative technologies. The study found that unethical behavior within SMEs made them more vulnerable to cyberattacks. Furthermore, ethical dilemmas and potential solutions were discussed, concluding with a call for future research on ethical issues in SMEs.

The digital revolution has transformed various sectors, including higher education, by enabling widespread information exchange and collaboration. However, it has also introduced risks such as cyberattacks and malicious software (e.g., viruses and spyware), which threaten educational processes, infrastructure, and stakeholders, including students, teachers, and administrators. To address these challenges, K. A. Y. Yaseen [13] suggested that higher education institutions should raise awareness, provide cybersecurity training, and implement robust cybersecurity policies. The study explored the significance of cybersecurity in higher education and outlined strategies for students, faculty, and staff to enhance cybersecurity across institutions.

E-learning, a key outcome of the information revolution, has revolutionized education through platforms and applications supporting distance learning. While offering flexibility and efficiency, this digital shift has exposed the education sector to significant cybersecurity risks, including denial-of-service (DoS) attacks, ransomware, and phishing, making it one of the most targeted sectors. K. A. Y. Yaseen [14] analyzed these threats using the Kaspersky DDoS Intelligence System, part of Kaspersky DDoS Protection, and proposed effective strategies to protect the digital infrastructure of educational institutions.

IV. METHODOLOGY

To achieve the objectives outlined in this research, the moral responsibilities of Information Security professionals will be discussed. Additionally, a comparison will be conducted on the codes of ethics of four Information Security Professional Organizations. The professional organizations considered are

1. The Information Systems Security Association (ISSA)
2. The Australian Information Security Association (AISA)
3. The Information Systems Audit and Control Association (ISACA)
4. The Association of Information Security Professionals (AiSP)

V. RESULTS

Ethics encompasses the study of actions that should be taken by a responsible individual, the values adopted by an honorable individual, and the character of a virtuous individual [6]. According to S. O. Ogunlere [7], ethical considerations are crucial for stakeholders involved in information security decision-making. Consequently, national and international information technology organizations have endorsed codes of ethics and incorporated these codes into their constitutions. Among these organizations are:

A. Information Systems Security Association (ISSA)

The Information Systems Security Association (ISSA) promotes practices that ensure the security of information resources. The following ethical codes have been established [8].

1. Professionals should perform in compliance with all relevant laws and adhere to the highest ethical standards in all activities and duties.
2. Commonly accepted information security best practices and current standards should be promoted.
3. Suitable confidentiality of proprietary or sensitive information handled during professional activities must be maintained.
4. Diligence and honesty should guide all professional responsibilities.
5. Activities that create a conflict of interest or harm the reputation of employers, the information security profession, or the Association should be avoided.
6. Professionals must not deliberately harm or challenge the professional standing or training of colleagues, clients, or employers.

B. Australian Information Security Association (AISA)

The Australian Information Security Association (AISA) requires its members to adhere to the standards outlined in their Code of Ethics to develop a highly respected, valued, and recognized Information Security profession [15].

1. Maintain honesty in all representations, including knowledge, goods, services, skills, and capabilities.
2. Abide by all applicable laws.
3. Conduct professional activities with competence and diligence.
4. Preserve the confidentiality of all sensitive and proprietary documents and information handled, and adhere to AISA's privacy policy and standards.

5. Stay updated on educational requirements needed to fulfill professional roles and support others in enhancing their knowledge and capabilities.
6. Uphold integrity and the highest ethical standards. Avoid disseminating false or misleading information with the intent to harm the organization, its members, or the security community. Treat all individuals with respect.

C. Information Systems Audit and Control Association (ISACA)

The Information Systems Audit and Control Association (ISACA) developed the following ethical codes to guide the professional and personal behavior of its members and certificate holders [16].

1. Support and encourage the application and adherence to appropriate standards and procedures to ensure effective control and management of an organization's information systems and technology, including audit, control, security, and risk management.
2. Perform duties in accordance with professional standards, with objectivity, due diligence, and professional care.
3. Serve stakeholders' interests legally while maintaining high ethical standards without compromising the integrity of the profession or the Association.
4. Maintain the privacy and confidentiality of information obtained during professional duties unless required otherwise by legal authority. Such information must not be used for personal gain or shared with unauthorized parties.
5. Accept only those duties that can reasonably be completed with the requisite skills, knowledge, and competence.
6. Do not withhold the results of work performed if such withholding may hinder the presentation of those results.
7. Promote the education of stakeholders to enhance their understanding, control, and management of an organization's information systems and technology, including audit, control, security, and risk management.

D. Association of Information Security Professionals (AiSP)

The Association of Information Security Professionals (AiSP) requires its members to adhere to the following ethical codes [17].

1. Take reasonable actions to prevent unlawful activities.
2. Prevent harm to employers, personnel, property, public interest, and relevant national interests while performing duties.
3. Report any actions or events believed to violate relevant laws, legal requirements, or regulatory standards to the appropriate authorities.
4. Report issues that may significantly impact the organization's information security to the relevant authorities.
5. Respect the confidentiality of information obtained during the course of duty and refrain from disclosing it without explicit authorization.
6. Adhere to the principles of professional care.

VI. DISCUSSION

Ethics is a vital component in securing networks from security threats and vulnerabilities. Ethical investigations of security issues within network environments can assist information security professionals and security communities in identifying and resolving ethical dilemmas and developing ethical procedures and strategies for the use of information technology. To achieve the security goals of confidentiality, integrity, and availability of information, various organizations invest significantly in technological and human resources to create robust security measures.

Organizations also implement codes of ethics that summarize the core values, standards, and expected behaviors of their members. These codes outline the objectives expected from their members and guide professional conduct. Different codes of ethical conduct in information security, along with various models, aim to achieve better information security. This underscores that information security transcends the technical domain; it also encompasses organizational, legal, social, and ecological levels. Therefore, ethics cannot be addressed without considering all stakeholders, including information security professionals, organizations, and communities. Codes of ethical conduct should be developed collaboratively by individuals from diverse fields to effectively contribute to securing information.

With the growing security threats stemming from the widespread adoption of the Internet and information technology, improving existing codes of ethics for information security professionals is essential. Since there is no universal code of security ethics, it is imperative to encourage the development of clear guidelines, strategies, and best practices for information security ethics, tailored to specific activities and challenges.

S. Vallor [9] highlighted several general rules and guidelines for ethics in information security practices, including but not limited to

1. *Keep Security Ethics in the Spotlight:* Ethics is a pervasive aspect of information security practice with significant social power. Ethical considerations are continuously relevant when striving to secure information technology and its operations.
2. *Consider Human Lives and Interests Behind the Systems:* Security often involves sensitive aspects of human lives, such as reputations, opportunities, property, freedoms, physical and psychological well-being, and social connections.
3. *Establish Chains of Ethical Obligation and Liability:* To avoid diffusion of responsibility, clear chains of

accountability should be established and communicated to all parties involved as early as possible.

4. *Promote Values of Transparency, Self-sufficiency, and Honesty:* Hiding security risks behind legal, technical, or public relations jargon undermines users' efforts to enhance their security and erodes public trust. Transparent communication is a better long-term approach.
5. *Design for Privacy and Security:* This includes procedural, social, and administrative designs that align with privacy and security objectives.
6. *Make Ethical Reflection and Practice Standards Prevalent, Iterative, and Rewarding:* Ethical reflection and practices should be accepted as essential, continuous, and integral to every security context, supported by active measures from both practitioners and governments.
7. *Advocate for Ethical Security Practice Models:* Attention should be given to exemplary models of ethical practice. Becoming an exemplary model allows professionals to guide others and collaborate to improve standards.
8. *Encourage Training and Awareness:* Promoting training and awareness ensures all stakeholders understand security policies and commit to best practices, enhancing ethical and security behavior.

VII. CONCLUSION

Information technology, information networks, and the Internet inevitably give rise to a wide range of social, political, and ethical problems. Many of these issues become evident as most activities increasingly rely on the Internet. Key ethical concerns in the use of information technology through the Internet include data privacy, access rights, and harmful actions. Technical approaches such as cryptography, Secure Socket Layer (SSL), digital IDs, and firewalls have been proposed to address these challenges. However, existing codes of ethics for information security professionals and security policies integrated into current practices require improvements to meet the evolving needs of the information security community. Guidelines and strategies must be implemented to ensure that information is used socially and ethically, benefiting future advancements and applications. Moreover, a wide range of ethical dilemmas urgently demands the attention of governments, businesses, institutions, and individuals worldwide.

REFERENCES

[1] A. D. Smith, "E-security issues and policy development in an information-sharing and networked environment," *New Information Perspectives*, vol. 56, pp. 272-285, 2004.

[2] D. K. Tiwary, "Security and ethical issues in IT: An organization's perspective," *International Journal of Enterprise Computing and Business Systems*, vol. 1, no. 2, pp. 1-13, 2011.

[3] H. Gunarto, "Ethical issues in cyberspace and IT society," Ritsumeikan Asia Pacific University, pp. 1-8, 2003.

[4] G. T. Gowing, "Cybersecurity from a Christian worldview," 2020. [Online]. Available: https://www.letu.edu/academics/arts-and-sciences/story-cybersecurity-glyn-gowing.html. [Accessed: Nov. 25, 2024].

[5] P. Brey, "Ethical aspects of information security and privacy," in *Security, Privacy, and Trust in Modern Data Management*, Berlin Heidelberg: Springer, 2007, pp. 21-36.

[6] M. C. Loui and K. W. Miller, "Ethics and professional responsibility in computing," University of Illinois, Springfield, 2008.

[7] S. O. Ogunlere and A. O. Adebayo, "Ethical issues in computing sciences," *International Research Journal of Engineering and Technology (IRJET)*, pp. 10-16, 2015.

[8] ISSA, "ISSA code of ethics," Information Systems Security Association, 2005.

[9] S. Vallor and W. J. Rewak, "An introduction to cybersecurity ethics," Santa Clara University, pp. 1-65, 2018.

[10] S. Wurster, "Ethics and privacy issues of critical infrastructure protection - Risks and possible solutions through standardization," *DE Gruyter*, vol. 37, no. 3, pp. 205-210, 2014.

[11] T. Aşuroğlu and C. Gemci, "Role of ethics in information security," in *International Conference on Advanced Technology & Sciences*, Konya, Turkey, 2016.

[12] R. Nagahawatta, M. Warren, and W. Yeoh, "Ethical issues relating to cyber security in Australian SMEs," Deakin University, pp. 71-76, 2020.

[13] K. A. Y. Yaseen, "Importance of cyber security in the higher education sector," *Asian Journal of Computer Science and Technology*, vol. 11, no. 2, pp. 20-24, 2022.

[14] K. A. Y. Yaseen, "Digital education: The cybersecurity challenges in the online classroom (2019-2020)," *Asian Journal of Computer Science and Technology*, vol. 11, no. 2, pp. 33-38, 2022.

[15] AISA, "Code of ethics and conference behaviour rules," Australian Information Security Association, pp. 1-2, 2018.

[16] ISACA, "Code of professional ethics," Information Systems Audit and Control Association, 2021.

[17] AiSP, "Association of Information Security Professionals code of conduct," 2021.