MIS303 Professional Ethics

Riley

7/10/22

**Introduction**

Information security guards against potential risks to the confidentiality, integrity, and availability of information assets. Information security cannot be provided solely by technical safeguards. Operational, ethical, social, and legal considerations must be made in addition to technological ones to create a strong and effective information security system. Better and more reliable security may be attained with the aid of ethics. Codes of ethics are meant to provide recommendations for the specific standard of acceptable conduct in a professional setting. This essay evaluates the importance of a code of ethics in information security including basic principles in law, and ethics.

**Body**

Businesses rely on people, technology, and procedures. Even if we have the best security and information technologies available, these systems are still operated by people (Wildauer and da Silva, 2013). They must act morally and ethically since if they don't, the information system will be subjected to vulnerabilities. Strong information security depends heavily on people. So, ethics steps into action to save the data. Information security is ensured by those who behave ethically in the field of information systems.

**Hacking & Ethics**

Computer security is primarily concerned with safeguarding valuable data and computer assets against breaches and illegal access. Hackers are users of computers who obtain illegal access to a system and, in doing so, divulge information to other users or hackers. White hat hackers or hackers who identify themselves as the such claim that their acts have no negative effects on the community. Instead, they assert that they support the creation of a better security system. Hackers have created a code of ethics. They recommend that when hacking, hackers adhere to a code of ethics.

**Privacy & Ethics**

Although there is no exact definition of privacy, it primarily relates to the "right to be left alone" (Stahl, 2007). Privacy doesn't just pertain to private details. Additionally, it has to do with our houses, personal items, acts, and even human relationships. Many privacy-related sectors, such as monitoring, healthcare confidentiality, internet freedom, and workplace privacy, raise ethical questions (Brey, 2007).

With regard to private data, confidentiality is not the sole concern. The management of that data is a major challenge as well. consequences start to appear that go beyond the exposure of previously secret information to the possible abuse of data (for example, to influence election outcomes) or might if materials are handled poorly, hurt the quality, authenticity, and broader implications of those data.

The effectiveness of ethical guidelines in a community is crucial for information security. Giving people a set of ethical guidelines to follow and raising their understanding of ethics would undoubtedly improve the security layer in enterprises. There are two techniques to offer more effective and reliable information security: creating a code of ethics or behaviour and giving people pieces of training so they may learn about security and ethics Many communities and organisations now create codes of conduct for their members to abide by (Aşuroğlu and Gemci, n.d). Without the creation of these rules, there would be holes in information security since laws couldn't cover all of them, whereas ethics could. A small amount of foresight will imply that effective security will increase a company's reputation and customer trust in that organisation.

All contributors in an information system, comprising network engineers, programmers, clients, and security professionals, are subject to the same code of ethics. Organization should develop their codes of conduct in place of using universal codes of ethics. To ensure that security standards are fully adhered to, awareness training must teach everyone in a company how to act ethically and securely (Muller, 2020).

Information security ethical problems can't only be delegated to intellectuals or professionals since the core nature of work as information security specialists necessarily inform it. For instance, some academics are working on methods that provide privacy-preserving training and prediction procedures for machine learning-based systems. The mechanics of vulnerability rediscovery also require ongoing investigation, as (Blaze, 2017) noted.

**Conclusion**

In both the world of cyber technology and our daily life, ethics are crucial. Laws are unable to fill the gaps left by ethics in a system of information. This essay has examined the value of ethical considerations in information security. Examining various ethical stances in literature demonstrates how an ethical layer may be added to a security layer to show conclusively that ethics complete information security. Finally, strategies for making ethical laws successful in a community are provided. Several research under consideration revealed that codes of conduct and awareness training are successful in this way.

**References**

Aşuroğlu, T., & Gemci, C. Role of Ethics in Information Security. In International conference of advanced technology & sciences (pp. 141-144)

Blaze, M. (2017). When Should the Government Disclose ‘Stockpiled’Vul-vulnerabilities? Exhausted Search blog, 10.

Brey, P. (2007). Ethical aspects of information security and privacy. Security, privacy, and trust in modern data management, 21-36.

Muller, S. R. (2020). A Perspective On the intersection of information security policies and IA awareness, factoring in end-user behavior. Annals of Computer Science and Information Systems, 24.

Stahl, B. C. (2007). Privacy and security as ideology. IEEE Technology and Society Magazine, 26(1), 35-45.

Wildauer, E. W., & da Silva, F. P. H. (2013, June). Ethical, social, privacy, security, and moral issues in an e-society. In 2013 8th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE