Chapter 10
Digital Ecosystem Security Issues for Organizations and Governments:
Digital Ethics and Privacy

Heru Susanto
The Indonesian Institute of Sciences, Indonesia and Brunei University of Technology, Indonesia

Leu Fang Yie
Computer Science Department, Tunghai University, Taiwan

Desi Setiana
Universiti Brunei Darussalam, Brunei

Yani Asih
The Indonesian Institute of Sciences, Indonesia

Ambar Yoganingrum
The Indonesian Institute of Sciences, Indonesia

Slamet Riyanto
https://orcid.org/0000-0001-6367-5150
The Indonesian Institute of Sciences, Indonesia

Fadly Akbar Saputra
The Indonesia Institute of Sciences, Indonesia

ABSTRACT

The growth of the digital ecosystem has given a sense that the rise of security implementations must be considered by every organization including governments in terms of adopting the best digital ethical approaches and awareness on the importance of ensuring privacy. Increased use of the internet has also

DOI: 10.4018/978-1-7998-4570-6.ch010

increased matters of cyber threats and unethical behaviors. Therefore, implementation of digital ethics has become crucial to prevent or minimize the impacts of cybercrime, and so, securing sensitive information from unauthorized access has become extremely important. This study analyses and describes the future trends regarding security in digital ethics and privacy within the digital ecosystem. The results point to a relative correlation between the government and business sector and the types of attacks and that digital ethics and privacy makes up the core elements of security. Implementing cautionary steps are also necessary to prevent from any form of cyber-attack.

INTRODUCTION

We are living in the age of digital ecosystem, where information and knowledge is becoming increasingly important. There is no denying the fact that information and knowledge are important assets that need to be protected from unauthorized users (such as hackers, phishers, social engineers, viruses and worms) that threaten governments and organizations of all types. The rapid advancement of digital ecosystem and the growing dependence of government organizations (as well as the commercial sector) on digital ecosystems, continue to intensify concerns on information security and privacy. Although, most digital ecosystems are designed to have a considerable amount of strength in order to sustain and assist organizations in protecting information from security threats, they are not completely immune from the threats from unauthorized users.

Government organizations are paying increased attention to protecting information relating to their business processes, as the impact of information security breaches today have a much more serious and tangible effect. Information security needs to be considered as a business enabler that becomes an integral part of business processes. The assurance of information security may also help to raise trust of the users in any organization, including the government sector. Besides, it should be understood that security of information brings many advantages to organizations e.g. improved efficiency due to the exploitation of new technologies, and increased trust from partners and users. The important driver for information security adoption is to demonstrate to partners and customers that the organization has identified and measured their security risks, implemented a security policy and controls that will mitigate or at least minimize these risks; also to protect assets in order to support the achievement of business process objectives (Susanto & Almunawar, 2015; 2016; 2016a; 2018).

In the following sub-sections, we define and discuss the importance of, and implications of security, ethics and privacy within organizations and for connected governments.

Security

Security refers to keeping anything of perceived value away from any harm that might risk its health. In case of connectivity between technological objects, appropriate security gives protection, where safety guidelines are practiced to ensure the prevention of any danger that may affect the technological vulnerabilities. Lack of security presents threats from various kinds of cyber-attacks within an individual's technological usage, as well as organizational use. There are many varieties of hackers, viz: white hat, black hat, grey hat, green hat, blue hat, red hat, and script kiddies. Whether they are nation sponsored hacktivists or whistleblower hackers, they are all mostly of white hat, black hat and grey hat varieties.