Chapter 48
Understanding the Information Security Landscape in South Africa:
Implications for Strategic Collaboration and Policy Development

Blessing M. Maumbe
West Virginia University, USA

Vesper Owei
Cape Peninsula University of Technology, Republic of South Africa

ABSTRACT

Information security risks are a major threat to South Africa's bid to build a broad-based information society. The integration of information security in e-government is no longer an option, but an imperative given the resulting "information overload" and the need to filter "good" from "bad" information. Unless South Africa integrates information security in its e-government development policy and practices, the acclaimed benefits of e-government will not be realized. The moral hazard problems arising from bad information behavior such as human manipulation, withholding information, unauthorized access, and violation of individual privacy and confidentiality heightens the need to combat info-security risks and vulnerabilities. South Africa's readiness to deal with the information security risks has come under scrutiny. The information security infrastructure in South Africa is also not clearly understood. This chapter examines South Africa's information security landscape and describes how institutional and agency coordination could help improve information security in e-government.

1. INTRODUCTION

South Africa, just like the rest of the world, is facing pressing challenges in the area of information security. As the country moves towards building an "information society" the threats from information security are also rising. The information security risks have been heightened by the growing use of e-government and e-banking as service delivery platforms (Bakari, et al, 2006). Such developments

DOI: 10.4018/978-1-4666-8111-8.ch048

also entail an "information overload" to certain categories of users, and therefore a need to filter "good" from "bad" information. Some factors that contribute to bad information behavior are human manipulation, unauthorized access, violation of individual privacy and confidentiality, money laundering and terrorism. Recurring information systems failure also affects the integrity of the information supply chain. The information and communication technology (ICT)-induced rapid changes in information production, processing, and dissemination suggest the need to develop a sound information security "landscape" or "architecture" and simultaneously integrate information security, especially in e-government development policies and practices.

Little is being done to promote information security in Africa (Bakari, et. al., 2006). Traditional methods of protecting information such as authentication and authorization have become obsolete globally. As new security systems are being probed, an intensive debate is raging on the rationale for newly introduced information security legislation. For instance, others argue that the September 11th 2001 event has affected citizen privacy, freedom of expression and information access. As a result, concentration of focus on national and global security has led to greater control over access, secrecy over transparency, national security bias over civil liberties and surveillance over anonymity (Caidi and Ross, 2005). Further, the authors argue that the new legislation introduced has affected "what the public can know about the government not just what the government can know about the public," which is an infringement of civil society's information rights.

It is not clear to what extent the South African information security landscape is prepared to deal with the information security risks poised by the information age and the modernization of public service delivery on the e-service format. The extensive information security infrastructure in South Africa is not clearly understood by many. There is need for researchers to scrutinize the information security landscape, and examine whether or not the Government of South Africa (GSA) has aligned itself with other global agencies to combat information security threats and vulnerabilities.

The paper argues that the systematic inclusion of security in e-government projects is no longer an option, but an imperative. Information security helps to deliver information values such as accuracy, reliability, rapidity, timeliness, privacy and relevancy. Without assurances that information provision and access are secure, the aforementioned value propositions are easily eroded. E-government and its acclaimed benefits of efficiency, accountability, effectiveness, flexibility, transparency and trust among others, can also be compromised if information security is poorly handled.

South Africa is endowed with several state agencies, institutions, businesses, research institutes and various other strategic partners that could play a prominent role in arresting information security threats. But working in isolation, such organs will remain necessary but insufficient in combating information security threats. The fact that the global risk of information security seems to be growing unabated despite a proliferation of legislation globally, and renewed commitments to provide information security protocols justifies the need to probe and or transform the security landscape and enhance coordination with global partners.

Although this paper does not seek to determine the appropriate level of information security that policy makers should aim for, it seeks to examine the information security landscape and how its organization can best provide solutions that could help build secure information security landscape in South Africa. Global trends demonstrate a shift from mere information access and provision, to e-value creation which can only be guaranteed by a "state of the art information security landscape." The importance of increased coordination and collaboration in dealing with information security threats in a global information age is also highlighted.