Chapter 14
Information Security Management: A South African Public Sector Perspective

Harold Patrick
University of KwaZulu-Natal, South Africa

Brett van Niekerk
University of KwaZulu-Natal, South Africa

Ziska Fields
University of KwaZulu-Natal, South Africa

ABSTRACT
The frequency and sophistication of cyberthreats and attacks are increasing globally. All organizations including governments are at risk as more devices are connected to a growing network coverage. There is no doubt that the new technologies in the Fourth Industrial Revolution bring numerous opportunities for smarter and efficient ways of doing business. However, these new processes, technology, and people interacting increases the cyber-risks. Cyber-risks cause a threat to the reputation, operations, data, and assets of the organization. A holistic information security management plan is needed that will transform the organization’s approach to mitigate the cyber-risks, protect its infrastructure, devices, and data. This approach will inevitably improve information technology governance and better accountability to the public.

INTRODUCTION
South African Government departments are not sharing information security incidents, and they are not communicating threat information and breaches within their various sections in the department and amongst other Provincial or National departments. In the United States of America (US), four out of 10 security incidents and breaches go undetected (Deltek Solutions, 2014, p. 4). Although increased reliance on the Internet offers numerous benefits and advantages, it also offers countless opportunities for...
Information Security Management

criminals to exploit South Africa’s cybersecurity vulnerabilities. Tamarkin (2014) notes that cyber-crime is on the rise and thus has become a very significant concern in South Africa (SA) (p. 1). South Africa should consider the following: (1) Defining roles and responsibilities for government departments, (2) Collaborating with and other government departments and sharing of security incidents and threat data (Tamarkin, 2014, p. 1).

If the government have the political will, resources and skills, their challenges to digital transformation would be better improved. The government would effect and shift a better security position in the Fourth Industrial Revolution. Embedding information security management would lead to the deployment of new technologies, which would lead to improve accountability in government and lead to improved service delivery to its citizens. This is a necessity to grow the digital maturity of the government departments. This chapter will present the global perspective of information security initiatives and the current information security management landscape in government. South African laws about information security will be discussed. Finally, solutions for managing the information security management in the Fourth Industrial Revolution will be discussed.

BACKGROUND

Cyber-attacks are an international and local reality, therefore, it is essential that management accept that threat actors are moving towards espionage, crime and intentional disruptions of their networks and systems. Management and government leaders must acknowledge this reality and institute measures to curb threats and attacks (Ross, 2014, p. 4). As new technology is introduced universally, timely, and easy access to government networks and services will be essential to ensure good quality and complete information. Technology in the digital age will continue to drive organisations, creating information security concerns for management and the designated information technology staff (TraceSecurity, 2012, p. 1). Government departments are under excessive strain to protect their networks and systems from cyber-threats a result of new modernizing technology to render better services to the public (Govloop, 2014, p. 10). An insider or external threat or attack can disrupt government services and critical infrastructure operations. Therefore, government departments need to be resilient against these potential threats and attacks. Also, government departments are already part of the interconnected world of technologies and other organisations and will continue to be vulnerable to threats and attacks by cyber-criminals (Ixia, 2014, p. 4).

Information Security will continue to be an organisation and global problem that will involve different elements, including people, government and organisations. Government departments’ efforts to deliver faster, transparent and better services will be hampered by the intricacy of information security, lack of information security capacity skills among the workforce will inevitably place enormous burdens on their networks and systems (Australian Signals Directorate, 2014, p. iii), thus creating new opportunities for adversaries. Optimizing the existing Information technology infrastructure and implementing new information technology developments and applications, (e.g. online services) have become a critical intervention in successfully managing the demands and pressure on the government to ensure quicker connectivity to organisations’ own networks and systems as well as those of other organisations. Government’s failure to implement new technologies and system applications can severely compromise delivery of government services (EMC Corporation, 2014, p. 10). It is vital that designated Chief Information Officers and infrastructure architects create and maintain a suitable infrastructure that will achieve the
Related Content

Security-Efficient Identity Management Using Service Provisioning (Markup Language)
www.igi-global.com/chapter/security-efficient-identity-management-using/20674?camid=4v1a

Metamorphic malware detection using opcode frequency rate and decision tree
www.igi-global.com/article/metamorphic-malware-detection-using-opcode-frequency-rate-and-decision-tree/160775?camid=4v1a

Advances in Security and Privacy in Wireless Sensor Networks
www.igi-global.com/chapter/advances-security-privacy-wireless-sensor/49504?camid=4v1a

Realized Applications of Positioning Technologies in Defense Intelligence
www.igi-global.com/chapter/realized-applications-positioning-technologies-defense/23204?camid=4v1a