Chapter 13
Government's Dynamic Approach to Addressing Challenges of Cybersecurity in South Africa

Thokozani Ian Nzimakwe
University of KwaZulu-Natal, South Africa

ABSTRACT

Cybersecurity is the practice of making the networks that constitute cyber space secure against intrusions. The aim is to maintain the confidentiality, the availability and integrity of information, by detecting interferences. Traditionally, cybersecurity has focused on preventing intrusions and monitoring ports. The evolving threat landscape, however, calls for a more dynamic approach. It is increasingly clear that total cybersecurity is impossible, unless government develops a cyber-security strategy. The aim of this chapter is to discuss government's dynamic approach to addressing challenges of cybersecurity. The chapter looks at the co-ordination of cyber-security activities so as to have a coordinated approach to cyber-crime. This chapter also highlights the idea of protecting sensitive data for the public good. It is generally accepted that technology has become indispensable in modern society. Government's cybersecurity presents a unique challenge simply because of the volume of threats that agencies working for government face on a daily basis.

INTRODUCTION

Information and Communications Technologies (ICTs) are indispensable in modern society. The interconnectivity of computer networks contributes significantly to economic growth, education, citizens' participation in social media and many other aspects. This new electronic environment is commonly known as cyber space. The dependence of the daily functioning of society on information communication technology solutions has led to a concomitant need for the development of adequate security measures. This is because the danger that cybersecurity threats pose is real. The numerous cyber-attacks launched in

DOI: 10.4018/978-1-5225-4763-1.ch013

recent years against advanced information societies aimed at undermining the functioning of public and private sector information systems have placed the abuse of cyber space high on the list of international and also local security threats. Given the seriousness of cyber threats and of the interests at stake, it is therefore imperative that the comprehensive use of information communication technology solutions be supported by a high level of security measures and be embedded in a broad and sophisticated cyber-security culture. This chapter discusses the concepts of cyberspace and cyber security, the influence of information-related technology, initiatives in relation to preventing cybersecurity, an understanding of the threat of cybercrimes, the closing of the cyber skills gap and understanding the government's approach in addressing cybersecurity challenges. The chapter also discusses cyber-security awareness and an education framework for South Africa that could assist in creating a cyber-secure culture in South Africa as one of the many users of the internet. The chapter further discusses the link between cybersecurity and the Fourth Industrial Revolution. Finally, the chapter proposes solutions and future research directions in terms of cyber threats.

BACKGROUND

Cybersecurity is complex and multi-faceted. There are current means to create cyber security awareness designed to make an impact. The fragmented and uncoordinated nature thereof, has, however, the potential to create its own dynamics for the Fourth Industrial Revolution. The increase in mobile use (mobile phones with web connectivity) is, unfortunately, opening the door for cyber criminals to exploit mobile users with little or no cyber-safety knowledge. Reliance on information systems (IS) has increased and now places government operations at higher security risk. Nowadays, the cyber threat is one of the newest and most challenging threats to security, being able to jeopardise not only the safety of a state entity, but also the functioning of international organisations and economic and financial companies (Dinicu, 2014).

Cyberattacks involving ransomware, in which criminals use malicious software to encrypt a user's data and then extort money to unencrypt it, increased 50% in 2016, according to a report from Verizon (Kahn, 2017). Despite technology and electronic devices and media being used more regularly in easing everyday activities, these technological advances are also used in sophisticated criminal activities. The current information age comes with an aggressive technological growth to which there is no foreseeable end. One of the challenges associated with the technological revolution is that cyberspace is full of complex and dynamic technological innovations that outwit any lagging administrative and legal system.

According to Kortjan and Von Solms (2014), the Internet is becoming increasingly interwoven in the daily lives of many more individuals, organisations and nations. It has, to a large extent, had a positive effect on the way people communicate. It has also introduced new avenues for business, and it has offered nations an opportunity to govern online. However, although cyberspace offers an endless list of services and opportunities, it is also accompanied by many risks, of which many Internet users are not aware. As such, various countries have developed and implemented cyber-security awareness and education measures to counter the perceived ignorance of the Internet users. There is a view that people are currently living in an age where the use of the Internet has become second nature to millions of people (Kortjan and Von Solms, 2014).