Chapter 41
Developing Cybersecurity Resilience in the Provincial Government

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 approach that the organization uses to manage its cyber-risk to its workforce, information, systems, and networks is paramount to ensure sustainability and continuity in the Fourth Industrial Revolution. Improving cyber-resiliency in the organization reduces the chance of future threats and attacks and builds better capability. Cyber resilience involves continuous operations, good governance, and diligence supported by the right security strategy of a computer security incident response team (CSIRT) that can protect government operations and control cyber-risks. CSIRT can build better resiliency at the decentralized provincial government level, and contribute to cyber awareness amongst the workforce, public, and other government departments. A CSIRT can further contribute to resilience to the organization by analyzing the threats and attacks, developing countermeasures for the future in protecting its systems and networks from threat actors.

INTRODUCTION

Government services are the backbone to service delivery and social upliftment (Education, health and energy). Minimal disruptions in this infrastructure are crucial to ensure reliable information, resilience and secure services and networks (Hoffman, 2015, p. 2). An organisation can reorganize its efforts and save costs by prioritizing irregular and suspicious cybersecurity events, thereby allowing cybersecurity

DOI: 10.4018/978-1-5225-8897-9.ch041

response persons to focus on the actual security threat or breach (Symantec, 2017, p.1). Government departments need to build resilience capabilities to ensure that they can improve on cybersecurity preparedness and response capabilities. Data (such as cybersecurity statistics and intelligence) provides the department with reliable information that can be used improve to decision-making (Hoffman, 2015, p.2) and thereby reducing the impact of disruption of government services. The government department can monitor cybersecurity incidents which it is aware of before the impact of the attack or breach increases. This speedy response allows the provincial department to isolate the cybersecurity incident so the government networks are not maliciously further targeted. With the introduction of the Fourth Industrial Revolution, government needs a radical shift to better design and build technologies that will meet their technological progress or economic productivity. Strong government leadership is needed to improve government capabilities and proactively manage cyber-risks.

In the Fourth Industrial Revolution, imminent encounters between organisations and countries will be fought through the cyberspace environment (Cole, 2017, p. 1). Organisations, government and threat actors would use the target network and systems to deliver cyber incidents like social engineering, malware, spear phishing and denial of service to disrupt the organisation or government operations and services. This chapter will discuss cyber resilience, South African government initiatives, cybersecurity incident management mainly on CSIRT as a resilient approach to managing cybersecurity risks in the Fourth Industrial Revolution.

BACKGROUND

South African Government Structure and Spheres

There are three spheres in the South African government namely: (1) National, (2) Provincial; and (3) Local government. National government (National departments') mandate are developing for policies and developing national standards, norms, and regulations. Provincial government (Provincial departments) are responsible for provincial planning, health, school education, and social grants (Department of Public Service and Administration, 2003, pp. 15 & 17). Provincial departments do not receive any monies for services rendered therefore they are dependent on National department for revenue. Hence, they receive the largest budget allocation from National Department (Department of Public Service and Administration, 2003, p. 30). Local government (Municipalities) functions are to care for providing municipal roads, local amenities, electricity, water, housing and local amenities (Parks and gardens)

Cyber-Resilience

Cyber-resilience is the ability of the organisation to prepare, withstand and recover from a cybersecurity incident, threat and attack (Department of Homeland Security, 2017, p. 1). Cyber resilience provides a strategic direction for the management of cybersecurity incidents, which includes: (1) Recognizing, (2) Managing (which can include business continuity, disaster recovery and CSIRT); and (3) Responding to the threat or adversary. The CSIRT as a main approach to management of cybersecurity incidents will be discussed later and will provide the incident response. The importance of cyber-resilience in government is to develop and support a cybersecurity culture and build a solid base to deal with cyber-risks (The