Chapter 12
A Need for Cyber Security Creativity

Harold Patrick
University of KwaZulu-Natal, South Africa

Ziska Fields
University of KwaZulu-Natal, South Africa

ABSTRACT

Information technology is rapidly increasing and evolving all the time in pursuit for better solutions and products for the digitized world. Technology advancement and greater connectivity has moved organizations to better economic markets for sustainability. Together with better technology and greater connectivity, cybercrime is swiftly growing on par with these developments. This chapter focuses on the cyber security landscape and threats faced by organizations. The growth and sophistication of cybercrime is stressed. Cyber security creative approaches security risk assessment, cloud collaboration and data analytics are provided. This chapter ends with propositions that security creative approaches should be used as a method of managing cybercrime and ensuring that the organization's sustainability and governance are improved.

INTRODUCTION

With the rise of the technology and digitization labelled the Fourth Industrial Revolution (World Economic Forum, 2014, p. 8) internet connectivity between countries and amongst organizations have altered the way of doing business and drives new possibilities of economic gain (Negroponte, Palmisano & Segal, 2013, p. 10). The width spread and rapid growth of the internet technology has increased better speed access to networks (NATO Cooperative Cyber Defence Centre of Excellence, 2012, p. 5) and offers better service. However, these innovations and complexity have also given rise to cybercrime actors. At the same time attacks have increased in number. It is now a priority for organizations to address cybercrime. Cybercrime requires new measures that can be costly for the organization to implement (Holtfreter & Meyers, 2015, pp. 55-61).

DOI: 10.4018/978-1-5225-5634-3.ch012

Many organizations have experienced major vulnerabilities and many prominent organizations suffered security breaches (Hardekopf, 2015, p. 1). For example, a million customers' credit and debit cards were affected and hackers stole 53 million customers' email addresses from a Home Depot store and 76 million households and seven million businesses were affected when hackers stole customers' names and email addresses from JP Morgan (Verizon, 2015, p. 1).

Traditional approaches to managing security breaches is proving to be less effective as the growth of security breaches are growing in volume, variation and velocity (Bhatti & Sami, 2015, p. 1). There are constant media headlines about new security incidents and attacks, identity theft and data breaches (Crosby, 2015, p. 1). Organizations are being bombarded with cyber-attacks and penetration threats, network intrusions and politically motivated attacks (Polancich, 2015, p. 1). Cybercrime is no more a uniqueness it has become a global reality and features in the daily operations of organizations (Symantec, 2016, p. 1).

On-going advances in the sophistication of technology, while ground breaking, bring with them a multitude of security challenges (Rogerwilco, 2015, p. 1). There is no doubt that cybercrime incidents are difficult (Zio, 2016, p. 137) and complex to manage. A new proactive approach to mitigate cyber security vulnerability and risks is needed. It is imperative that organizations understand these vulnerabilities and risks so a resilient approach is proposed (Amann & James, 2015, p. 1). Organizations will not know the type and severity of a cyber-attack until it has been a target by cybercriminals. Organizations suffer huge financial losses due to the cyber-attacks (Khan & Estay, 2015, p. 7) and some organizations may not even recover from the attacks.

Geographical location of organizations, their complex systems with increased connectivity amongst their different business operation and other organizations make cyber security efforts very challenging (Bertino, 2016, p. 13). The challenges for organizations are to demonstrate that they can adequately protect (Accenture, 2015, p. 1) and safeguard their systems and networks from new cyber security breaches thereby create a better investor confidence. Organizations must demonstrate the leadership and confidence needed to better protect the organizations systems and networks from security breaches and ensure resilience in managing these fatalities (EY, 2013, p. 2). In addition organizations must rethink their approach to meet the demands or the digitalized world (Negroponte et al., 2013, p. 4).

BACKGROUND

Importance of Cyber Security

The cyberspace ecosystem is rapidly getting bigger as a larger number of users of internet and emails increase (Jardine, 2015, p. 3). Organizations are now more globally connected in pursuit of greater sustainable economic opportunities together with this the cyber landscape is increased (Levesque, Walsh & Whyte, 2015, p. 28). Organizations need to adapt (Levesque et al., 2015, p. 32) and remain relevant to protect their systems and networks. Organizations process and store confidential information on computers and communicate across different computer networks. Continuing protection of sensitive information because of the volume and complexity is needed (University of Maryland University College, 2016, p. 1). Better security protects the organization's assets and information, maintains organization communication and ensures continuation of productivity (CISCO, 2010, p. 1).