Chapter 16
Communication, Technology, and Cyber Crime in Sub-Saharan Africa

Dustin Bessette
National Graduate School of Quality Management, USA

Jane A. LeClair
National Cybersecurity Institute at Excelsior College, USA

Randall E. Sylvertooth
National Cybersecurity Institute at Excelsior College, USA

Sharon L. Burton
Florida Institute of Technology, USA

ABSTRACT

As a region that is rapidly developing its technology base, Sub-Saharan Africa is experiencing many of the issues associated with the benefits of cyber technology as well as its many negative sides. This paper discusses mobile and internet technologies currently being utilized in Sub-Saharan Africa as well as some of the major cybersecurity concerns threatening networks in the region that are associated with the new economic growth on the African continent. Such topics will include a viable increased awareness of news, historical events, and recent gatherings of information on this main topic.

INTRODUCTION

The field of cybercrime has hit the mainstream of the economic world by storm. Cybercrime has overwhelmingly been a high risk for communication devices in developing countries, such as those in Sub-Saharan African. Cybercrime has even surpassed illegal drug trafficking as a major criminal offense in many developed countries. So what does this mean for the under-developed countries? Development and keen protection must be at its highest level based on circumstances and internal process changes. In other words, developing countries need to invest in order to protect themselves based on underlying illegal activities such as cyber-attacks from internet sources. This chapter will identify the history of cybercrime in Sub-Saharan African countries, specify cyber themes, show national security awareness
and reasons for government regulation, and provide solutions and recommendations for successful developing countries. This chapter will also assist with correlating the national security awareness towards a global enterprise of cybercrimes in other Sub-Saharan African countries.

BACKGROUND

One of the fastest growing economies in the world today can be found on the continent of Africa, particularly in Sub-Saharan Africa. In the last five years, Africa has seen its mobile, internet, and technology industry explode with the introduction of undersea fiber optic cables and international companies providing internet and mobile service to the various countries and their civilian populations. Macharia (2014) notes that, “Africa’s growth in mobile and internet access has been rising faster over the last decade than any other region of the world” (p. 18). While there has been rapid economic growth on the continent, it still remains plagued with decades of civil war, government corruption, poverty, disease, and terrorism. The recent activities of Boko Haram and the Ebola epidemic are clear indicators that negative forces continue to be alive and well in Africa. Despite these issues, the economic improvement in Sub-Saharan Africa has been met with cautious excitement from the civilian population who have great hopes of gaining economic success and prosperity (Nwabueze, 2014).

There has been a growing demand for internet service and mobile technology in Sub-Saharan Africa. In the past decade across the region, Macharia (2014) writes, “…mobile phone penetration has grown from 1% in 2000 to 54% in 2012” (p.18). This rapid expansion, however, is providing cyber criminals an increased opportunity to make money from unsuspecting individuals utilizing the Internet in both the business and private sectors. On the cybercrime issue in Nigeria, Ndubueze, Mazindu, Emmanuel, & Okoye write: “Cyber crime has become a serious problem in Nigeria, culminating in the listing of Nigeria as third on the roll of the top ten cyber crime hot spots in the world by a 2009 Internet Crime Report” (2013, p. 225). Kshetri (2010) observes that a similar problem exists in the growing Internet areas of Kenya and notes that “Kenya experienced about 800 bot attacks per day in July 2009, which is projected to increase to 50,000 per day after the fiber connectivity goes live” (p. 1063).

Goodman, (2010) writes that the problem of cyber crime may actually be continent wide and notes:

As the use and utility of mobile phones in Africa continues to rise, so too will security vulnerabilities. Unless properly addressed, security vulnerabilities endemic to the use of the information and communications technologies (ICTs) will be magnified by a number of factors unique to Africa, possibly leading to a tsunami of information insecurity across the continent. (p. 24)

The increase in Sub-Saharan African cybercrime is a result of poor resources from local law enforcement and government security services to combat the threat. The void created by inadequate government infrastructure presents a lucrative operating environment for global cyber criminals looking for less risky endeavors than in their home nations. In addition to a permissive environment, much of the cybercrime occurring in the region can also be attributed to a lack of understanding from the business and civilian populations on how to best protect their private and business information from cyber theft.

Individuals and businesses are unwittingly purchasing or downloading pirated software infected with malware to their mobile devices and computers resulting in the theft of funds from banks or businesses. Businesses have not introduced needed technology such as sound firewalls and encryption nor have they