CYBERCRIME: A STUDY INTO THE NATURE, IMPACT AND POTENTIAL SOLUTIONS TO CYBERCRIME ON E-COMMERCE BUSINESSES IN KENYA:

Case Study Loopah Experience

Victor Khaemba Wanyama

BBM/113/00772

The Management Research Project submitted in partial fulfillment of the requirements for the award of the Degree of Bachelors in Business Management, School of Business, Mount Kenya University.

September, 2015

ABSTRACT

The advent of information technology in this day and age has brought about somewhat of a tectonic and revolutionary shift in how we do things. It has been of profound importance all across different sectors such as in the E-Commerce sector and the standard business processes in a business. With this good brought about by the meteoric rise of information technology use, it has also brought with it a myriad of challenges and consequences. In particular, the spread of the use of information technology has led to the prevalence of cybercrime in the E-Commerce sector. According to Shinder (2002), cybercrime is defined as any criminal offenses committed using the internet or another computer network as a component of the crime. Cybercrimes are offences that are committed against individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet and mobile phones.

Cybercrime has had a profound impact to all sectors of the economy and the E-Commerce sector is one that has had to grapple with a diverse range of cases on cybercrime, such as Denial of Service Attacks, identity theft, spoofing, hacking, phishing and spamming. The motivation to do this study is to qualitatively investigate the nature and extent to which Kenyan E-Commerce businesses are impacted by cybercrime and what are the possible solutions to this problem and also to provide further insight into the landscape of cybercrime of which very little has been done in regards to the understanding of business, the public and the government on what cybercrime entails and what it means for the future for our nation, hence with this information we can now be able to come up with a variety of means of protecting ourselves and our information from cybercriminals.

This paper seeks to scrutinize deeply the nature and the different types of cybercrime that pose a threat to the Kenyan E-Commerce sector, the persons or groups involved in cybercrime, in addition to their motives to carry out such acts and lastly to identify solutions to the threat posed by cybercrime in the Kenyan E-Commerce sector, in order to combat this issue and prevent further attacks from cybercriminals in the future. This study tackled the issue of cybercrime from an investigative and theoretical point of reference. An online review of books, articles, reports, and an analysis of media reporting of crimes. A structured questionnaire with government officials, cyber security experts and victims from all across different sectors was conducted.

Keywords: Cybercrime, E-Commerce sector, Cybercriminal