ABSTRACT

This study is informed by very little empirical research in the field of cybercrime and specifically in the context of South African banks. The study bridges this gap in knowledge by analyzing the cybercrime phenomenon from the perspective of a South African bank. It also provides a sound basis for conducting future studies using a different perspective. In order to achieve this, an interpretive research approach was adopted using a case study in one of the biggest banks in South Africa where cybercrime is currently a topical issue and one that is receiving attention from senior management. Cohen and Felson (1979) Routine Activity Theory was used as a theoretical lens to formulate a conceptual framework which informed the data collection, analysis and synthesis of cybercrime in the selected bank. Primary data was obtained via semi-structured interviews. Secondary data was also obtained which allowed for data triangulation. From the perspective of a South African bank, the study concluded that weak security and access controls, poor awareness and user education, prevalent use of the internet, low conviction rates and perceived material gain are the major factors that lead to cybercriminal activity. In order to curb the ever increasing rate of cybercrime, South African banking institutions should consider implementing stronger security and access controls to safeguard customer information, increase user awareness and education, implement effective systems and processes and actively participate in industry wide focus groups. The transnational nature of cybercrime places an onus on all banks in South Africa and other countries to collaborate and define a joint effort to combat the increasing exposure to cybercriminal activity. The use of the Routine Activity Theory provided an avenue to study the cybercrime phenomenon through a different theoretical lens and aided a holistic understanding of the trends and the behavioral attributes contributing to cybercriminal activity that can help South African banks model practical solutions to proactively combat the splurge of cybercrime.

Keywords: *Cybercrime, internet, crime, computer networks, Routine Activity Theory, South African banks.*