**Cybercrime: an emerging threat to the banking sector**

**MS21908606- R M M M Rathnayake**

Faculty of Computing, Sri Lanka Institute of Information Technology

New Kandy Rd, Malabe 10115, Sri Lanka

[malkarathnayake@gmail.com](mailto:malkarathnayake@gmail.com)

FINCSIRT Sri Lanka  
(Financial Sector Computer Security Incident Response Team)  
Level 18, Bank of Ceylon Head Office,  
"BOC Square", No. 01, Bank of Ceylon Mw,  
Colombo, 00100, SRI LANKA

*Abstract-*The purpose of this study is to gain more insight into the impact of cybercrime incidents in the banking sector. This study investigates the significant contribution of information security awareness on the relationship of cybercrimes and organizational performance.

**Introduction**

Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Most of the earliest victims and villains of cybercrime were Americans because of the early and widespread use of computers and the Internet in the United States. By the 21st century, however, barely anywhere in the world remained a hamlet that had not been touched by cybercrime of one kind or another.

**Defining Cybercrime**

New technology generate new criminal opportunities. What makes cybercrime different from conventional criminal activity? The use of digital computers is clearly one difference, but technology alone is insufficient for any differentiation that may occur between different areas of criminal activity. Criminals do not require a machine to conduct fraud, child porn trafficking, Intellectual property, stealing an identity or violating the privacy of others. Before the 'cyber' prefix became ubiquitous, all those activities occurred. In addition to some novel illegal activities, cybercrime, particularly involving the Internet, represents an extension of established criminal behavior.

Cybercrime is an assault on data concerning people, companies, or governments. While the attacks do not take place on a physical entity, they do take place on a simulated private or corporate body, a collection of intelligence characteristics that characterize the Internet as individuals and entities. In other words, our virtual identities are crucial elements of daily life in the modern age: we are a bundle of numbers and identifiers in various government and corporate-owned electronic databases. The centrality of networked computers in our lives is demonstrated by cybercrime, as well as the fragility of otherwise strong evidence such as human identity.