Volume 1(2), June 2014 ,pp 33-39
Available online at http://www.ijtcse.com
ISSN 2349-1582

Survey of Cyber Security Frameworks

Alice Nambiro Wechuli

(Department of Computer Science, Masinde Muliro University of Science and Technology, Kenya

alicenambiro@yahoo.com)

Geoffrey Muchiri Muketha

(Department of Information Technology, Meru University of Science and Technology, Kenya

gimuchiri@gmail.com)

Nahason Matoke

(Department of Computer Science, Masinde Muliro University of Science and Technology, Kenya

nahason@gmail.com)

Abstract: In a digital world, the national economy and welfare have grown critically dependent on the cyber infrastructure due to the capabilities and opportunities the Internet provides. This leaves organizations open to various forms of malicious attack by cybercriminals which has overwhelmed some current methodologies used for tracking cyber attacks and vulnerabilities. This paper presents a review of literature on cyber security status, challenges to cyber security, and existing cyber security frameworks. Findings indicate that though efforts are in place to bring about effective assessment of cyber security, there is no single accepted framework to offer a lasting solution to the cyber security assessment challenge.

Key Words: Cyber Security, Internet, Vulnerability, Threat, Cyber Attack, Cyber crime

1. Introduction

The way of carrying out business in the world today is changing rapidly with new technologies taking the center stage. Both government and the private sector are increasingly adopting the emerging technologies to modernize their service delivery. According to the US President's Information Technology Advisory Committee [1], innovations in ICT have created a whole new industry through the ubiquitous interconnectedness first exhibited by the Internet. This revolution of interconnectivity has brought with it an increased potential of opportunities, including risk and uncertainties, especially for those cyber criminals who can now cause harm with catastrophic impact from remote locations, while equipped with only a computer and the knowledge needed to identify and exploit vulnerabilities [1]. As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all.

Throughout the world, governments, defense industries, and companies in finance, power, and telecommunications are increasingly targeted by overlapping surges of cyber attacks from criminals and nation-states seeking economic or military advantage [2]. The number of attacks is now so large and their sophistication so great, that many organizations are having trouble determining which new threats and