Chapter 18
Policy Perspectives and Strategy for Communication Data and Network Security Projects and Tools:
Issues and Challenges in India

Inderjeet Singh Sodhi
University of Dodoma, Tanzania

ABSTRACT

This chapter highlights the constant increase in the number of attacks on computer network systems, which has pushed governments, researchers, and experts to devise better security policies and strategies. However, the rapid growth of systems, components, and services offered has increased the difficulty of administering them. In many organizations in developed and developing countries, more emphasis is being given on use of Automatic Computing for proper network security. The chapter clarifies how various projects and tools could be relevant for network security. The chapter provides insights about what steps have been taken for network security in a developing country like India. It looks into various strategies adopted for communication data and network security in India. It emphasizes that, with increasing demand for basic/citizen services over the Internet, it has become important to protect data and ensure efficient backup and data recovery. The chapter proposes a need for better and effective policy and strategy for communication data and network security to make the government citizen-oriented in developing countries.

DOI: 10.4018/978-1-4666-5146-3.ch018

INTRODUCTION

Information technology has become important method for government functioning, law & order, etc. In this 21st Century, the internet has become the largest public data network, showing, enabling, facilitating, and helping communications in public/ private sectors and for personal use. The volume of data moving over the internet is expanding exponentially everyday. With increasing demand for basic services through IT, it has become important to protect data and ensure efficient backup and data recovery.

In the 1990s, the entire planet is organized around telecommunicated networks of computers at the heart of information systems and communication processes. The entire realm of human activity depends on the power of information, in a sequence of technological innovation that accelerates its pace by month (Manuel Catells, 1999). Over 2 billion people are now connected to the Internet, and this number is set to increase significantly with the advance of the Internet of Things[1] in which a wide range of networks, devices, appliances and objects are to be connected (WEF, 2012).

The world today has become increasingly interconnected, dynamic and complex. It is ever more decentralized and driven by bottom-up innovation and where self-organizing produces unexpected side effects (WEF, Technology, 2012). In this 21st Century, the explosion of the internet, e-governance, e-commerce, e-business, computer networks, if not adequately secured, are increasingly vulnerable to damaging attacks to the whole or par of that system. Viruses, human error, vindictive employees, hackers, etc. all represent threats to networks and the security related to it.

In most of the institutions/organizations based on computer and related aspects, information or network is tampered, stolen or threatened to unauthorized access which occurs because of ignorance of the security mechanisms and effective network policies and the lack of awareness to the user. It is widely acknowledged that the security of the information and the information technology cannot be entrusted to any single system, be it any government agency/body or any private sector or technology alone.

Security in computer networks is an area that consists of protecting data during transit against its unexpected changes, unauthorized access and unavailability (Teles, Mendes and Abdelouahab, 2011). Network security is the ability to maintain the integrity of a system or network, its data and its immediate environment (KOLO and DAUDA, 2008). With the advent of internet, information technology, security of information technology, hardware, software, related equipments and tools became a complex issue which led to development of computer security, information security, network security, cyber security, etc.