SYNOPSIS

Title: CYBER SECURITY ISSUES IN INDIA

ABSTRACT

Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is cybercrimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

INTRODUCTION

‘Over the years, Information Technology has transformed the global economy and connected people and markets in ways beyond imagination. With the Information Technology gaining the centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. An increasing proportion of the world’s population is migrating to cyberspace to communicate, enjoy, learn, and conduct commerce. It has also created new vulnerabilities and opportunities for disruption.

The cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain and the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities. As such, cyber security threats pose one of the most serious economic and national security challenges.

Cyberspace is such a term, which is not yet completely defined and also has no geographical limitation. It is a term associated with application of the Internet worldwide. It is also called as a virtual space as physical existence of cyberspace is not detectable at all. Cyberspace is “the total interconnectedness of human beings through computers and telecommunication without regard to physical geography.”

Information through computers is transferred in the form of Ones (1) and Zeros (0), which do not inherently carry any separate information along with them for authentication. For authentication purposes, additional information needs to be carried with cyberspace transactions for identity purposes.

Providing extra information in digital communication introduces the possibility for identity theft. Because nothing prevents the transmission of false identity information, or the

Duplication of another’s identity information. The seriousness of this problem is highlighted when you consider that future technologies will allow extremely important identifiers, such as a retinal scan or a fingerprint, to be represented digitally. These biometrics characteristics are protected in real space because they are embedded in the physical body of the person. This is lost in cyberspace. Thus, cyberspace needs a system that allows individuals to verify their identities to others without revealing to them the digital representation of their identities.

DEFINITION

Cyber Security is “the security of information and its communicating channels as applied to computing devices such as computers and smart phones, as well as computer networks such as private and public networks, including the Internet as a whole.”

The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters.

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses.

It has proved a challenge for governments all around the world. The task is made difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators. The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialized has seen the use of cyberspace expand dramatically in its brief existence. From its initial avatar as a N/W created by academics for the use of the military, it has now become a global communications platform for socio-economic issues as well as for commercial and social purposes.

The increasing centrality of cyberspace to human existence is exemplified by facts and figures brought out recently by the International Telecommunications Union (ITU), according to which,

- The number of Internet users has doubled between 2005 and 2010 and surpasses 2 billion.
- Users are connecting through a range of devices from the personal computer (PC) to the mobile phone, and using the Internet for a variety of purposes from communication to e-commerce, to data storage for several services.

The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown apace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by politico-military-national security actors at one end and economic-civil society actors at the other.

Objectives of the research:-

1. To find out the attitude of people towards adoption of cyber security in India.

2. To understand the Cyber security threats (challenges) faced by the Indian banks.

3. To offer suitable suggestions in handling cyber issues in banking sector.

SCOPE OF THE STUDY:

To understand the awareness among the public regarding cyber security issues in India. The study is restricted to the 50 respondents who are randomly selected with in the twin cities of Hyderabad and Secunderabad.

METHODOLOGY:

Sources of data collection:

- Primary data
- Secondary data

PRIMARY DATA:

The main source of primary data is questionnaire consisting of simple questions prepared and distributed to respondents for collection of data on awareness in public regarding web search engines.

SECONDARY DATA:

The main source of secondary data includes Books, Magazines, Newspapers, Articles and Journals and websites.

SAMPLE SIZE:

For the present study, 50 respondents were selected at random.

LIMITATIONS OF THE STUDY

- The study is conducted in Hyderabad and Secunderabad only.
- The study is restricted to the users of web search engine only.
- Time perspective is also one of the elements in limiting the scope of this study.

CHAPTERISATION

Detailed/final Project Report will include the following chapters

CHAPTER –I

- Introduction
- Significance of the study
- Need of the study
- Objective and scope of study
- Methodology
- Limitations
- Scope

(Details of methodology used in studying and collecting the data and issue will be described)

CHAPTER –II

- Literature review
- Theoretical study

CHAPTER –III

- Industry & company profile

CHAPTER –IV

Analysis of the topic & Interpretation

(Descriptive work on the topic, this chapter will include analysis and interpretation of data tabulation and categorization)

CHAPTER –V

- Recommendation

- Bibliography
- Appendix

BIBLIOGRAPHY

- www.google.com
- www.wikipedia.com
- www.insightsonindia.com/2017/10/19/insights-editorial-safe-cyberspace

www.visionias.in