view Vol. 45(3), New Delhi: Bar Council of India Trust, p. 166

4 Ibid, p. 167

5 Sharma Vakul, (2018), Information Technology Law and Practice (pp. 170-171). New Delhi: Universal Law Publishing

6 United Nations General Assembly Resolution A/RES/51/162, adopted on 30th January, 1997, Retrieved March 10, 2021 from http://www.un.org/documents/ga/res/51/ares51-162.htm

7 Sharma Vakul, (2018), Information Technology Law and Practice (p. 113). New Delhi: Universal Law Publishing

❑❑❑

07

COMMERCE MANAGEMENT AND CYBERSECURITY

Dr. Sharad Ranganath Darandale
Associate Professor and Head,
Department of Commerce,
MES's. Arts, Commerce & Science College
Sonai, Tal:- Newasa, Dist:- Ahmednagar

****

ABSTRACT

Cyber security is a big challenge before economic and trade economy. E-Commerce security any nations is a part of the information security from work and is specifically applied to the components that affect e-commerce that includes computer security. Data security and other wider realms of the information security framework,Commerce Management security has its own particular security and is one of the highest visible security components that affect the end through their daily payment interaction with business.

Keywords: -Cyber security, Commerce, Management, E- Commerce,Security threats, Security issues.

Introduction:-

Cyber security is a topic of working inCommercial Management. Apart from this, no country can do secure trade with other countries. The foundation of success in the digital world is having the proper cyber security measures in place to protect consumers, employees and the business itself from constant security threats. Cyber security is woven into the very fabric of business operations and has special impact on the e-commerce sector. Today, privacy and security are a major concern for electronic technologies.

Management commerce shares security

concerns with other technologies in the field. Privacy concerns have been found, revealing a lack of trust is a variety of contexts, including commerce, electronic health records, e-recruitment technology and social networking and this has directly influenced users (Shankar Sen-2003). Web e-commerce applications that handle payments (online banking, using debit cards, credit cards, electronic transaction and others) have more compliance issue,at increased risk from being targeted than other websites and there aregreater consequence if there is data loss or alteration. Privacy has become a major concern for consumers with the rise of identity theft and impersonation and any concern for consumers must be treated as a major concern for e-commerce providers (Carr, I-2003).

Threats of cyber security:-

From identify theft and fraud to corporate hacking attacks;cyber security has never more important for e-commerce sites, large or smaller ones. An attacker over whelms a server with bogus traffic, causing the website or application hosted there to slow down or become unavailable. It is found in recent survey that 60% of respondents saying they are worried about DDoSattacks and 39% admitting it is likely their organization has been targeted.Beware by watching youtube video, anyone can learn to send DDoS attacks (Dr. Subhash Chandra-2001).

E-Commerce;-

E-commerce is the buying and selling of goods and services or the transmitting of funds or data, over an electronic network, primarily the internet. The terms e-commerce and e-business are often used interchangeably.The terms e-tail is also sometimes used in thereference to transactional process for online shopping. Recent years have exponentially witnessed the growth of e-commerce. The growth of e-commerce as a business technology is the result of such internet driven initiative. It has created a universal platform for buying and selling goods services and driving important business process inside the organization (Dr.Farooq Ahmad 1992).

Cyber Attacks and Security for Commerce Management:-

In the world,like the wolf's eyes that always preys on the hen's pen, ahackers eyes always scurries to steal your online stores data. Hackers are ripping off credit card information, personal identity credentials and even sensitive organization data from online databases. The internet is not a safe place to hoardyour data anymore. For e-commerce business, the risk is even grave (C.S.V.Murthy-2002).

The most common cyber security threats include scammers impersonality a business, the sending of fraudulent emails and viruses and malware. Cyber attacks can impact business finances reputation, operations, valuation and staff. As cyber attacks are more likely to occur.It is important to understand the short-term and long-term effect cyber attacks could have on your business (Prasad.R.S-2004).

Importance of cyber security:-

Cyber security is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiableinformation (PII), protected health information (PHI),personalinformation, intellectual property data, and governmental and industry information systems. Protect your business against cyber security threats and make the most of online opportunities. No business with an online presence is immune to a cyber-attack, and the financial, physical and legal implications of an attack on any business can be absolutely devastating (Pandoy Ashish -2006).

Data Leak protection:-

It is the most personal threat to cyber security is data leaks, which can be extremely damaging to both an individual business.All business hold a range of data, from customer insight to employee data which often contents sensitive information.Which can easily be put at risk if business does not take a number of steps to protect cyber security management can