REVIEW OF LITERATURE

The alarming rate of increasing cyber crime has started attracting attention not only of security authorities but also of technologists and sociologists so as to find out a solid solution for this rapidly increasing menace. Almost all the technologically advanced nations of the world have begun to formulate cyber legislation and laws to combat cyber crimes. But these laws have proved ineffective so far for the white-collar criminals which remain physically away from the place of crime.

The latest report released by Internet Crime Complaint Centre of the United States illustrates India ranks fifth among countries reporting the maximum number of cyber crimes. The US report analyzing internet crime in 2008 compiled by experts from FBI, Internet Crime Complaint Centre (ICCC) and other agencies shows the number of complaints from victims shot up by almost a third since 2007 with the total touching 275,284 cases in which about USD 265 million were lost globally. Although cyber criminal activity remained low in India, compared with other emerging economies, the report says that "there has been a leap in cyber crime in recent years". Reported cases of cases of spam, hacking and fraud have multiplied 50-fold from 2004 to 2007, it claims. India is fast emerging, as a major hub of cyber crime as recession is driving computer literate criminals to electronic scams, claimed a study conducted by researchers at the University of Brighton. Titled 'Crime Online: Cyber Crime and Illegal Innovation', the study states that cyber crime in India, China, Russia and Brazil is a cause of "particular concern" and that there has been a "leap in cyber crime" in India in recent years, partly fuelled by the large number of
call centres. "Russia, China and Brazil are world leaders in cyber crime, with groups and individuals in India powering up to compete. However, companies in Europe and the US are increasingly moving IT functions and software development tasks to India, Brazil, Russia and Eastern Europe in a bid to draw on their good IT skills and lower wages", says Prof. Howard Rush who led the study.

Although cyber criminal activity remained low in India compared with other emerging economies, the report says that there has been a leap in cyber crime recent years". Reported cases of cases of spam, hacking and fraud have multiplied 50-fold from 2004 to 2007, it claims. "The report ranked India in 2008 as the fourteenth country in the world hosting phasing websites. Additionally, the booming of call centre's in India has generated a niche for cyber criminal activity in harvesting data" the report maintained.

The report also says that cyber crime is a global industry but the combination of poor economic opportunities and high skills is driving many developing regions to surface as major players: n cyber crime.

According to ‘Crime in India 2006’ report prepared by National Crime Records Bureau 155 cases were reported in 2005 while Madhya Pradesh registered the largest number of cyber crimes (131) in 2006 followed by Andhra Pradesh (116). The largest state of Uttar Pradesh, which had four cyber cases and 153 cases were registered under IPC Sections in Gujarat in 2005.

The Economic Offences Wing (EOW), Crime Branch, Delhi Police, unearthed a major phishing scam involving fake e-mails and websites of UTI Bank. An analysis of the accounts of the four arrested Nigerian Nationals Indicated financial transactions of over Rs. 1 crore in an eight month period till December 2006. This indicates the estimated amounts involved. Investigations revealed that the scam is multi-layered with pan India international characteristics.
Granville Williams, R. Nagpal, Pawan Duggal and so many other authors have extensive work on cyber crime to highlight the basics of Computer crime. According to Sundari Nanda, Superintendent of Police, CBI, “Most of the times the victim do not complain, may be because they are aware of the extent of the crime committed against them, or as in the case of business houses, they don’t want to confess their system is not secure”. As the research shows, computer crime poses a real threat. Those who believe otherwise simply have not been awakened by the massive losses and setbacks experienced by companies worldwide. Money and intellectual property have been stolen, corporate operations impeded, and jobs lost as a result of computer crime. Similarly, information systems in government and business alike have been compromised. The economic impact of computer crime is staggering. Cyber crime is rapidly evolving from the domain of misguided corner, or halfway around the world.

Erhabor (2008) cyber crimes are described as one of the fastest growing criminal activities on the planet. He reiterated the fact that it covers a large range of illegal activity including financial scams, computer hacking, downloading of pornographic images from the internet, virus attacks, stalking and creating websites that promote hatred. In recent time, young students in the tertiary engage in forgery of all kinds ranging from false admission paper to school fees receipts, certificates racketeering and examination malpractice that is, accessing useful information during examinations through the handset and other electronic devices.

Waziri (2009) spoke about the horrendous level of corruption as being a threat to Vision: 2020. Cyber crime is one of these corruptions that may shut the door of progress against the nation. This was why Aluko (2004) gave 17 ways of stopping financial corruption in Nigeria. One of these crimes according to him has to do with cyber crimes.

Jaeseung Hong, Jongwung Kim, Jeonghun Cho School of Electrical
Engineering and Computer Science, Kyungpook National University. 1370, Sangyuk-dong, Buk-gu, Daegu, Korea (2010) in their research paper titled “The Trend of the Security Research for the Insider Cyber Threat” unfold an insider security which has been one of the biggest issues in the network security. By surveying and analyzing an issue of previous studies, an effective approach is suggested for future research. Approximately 90 per cent of the information leakage incidents are recently being performed by internal workers. It is coming as a more serious problem than outsider attacks. The information leakage incident makes an organization or a company not only loses information but also gives a hard blow to the image. To prevent economic loss and damage to the image in advance, we need various research and development for effective solution.

They have aptly pointed out that “Until recently, the cyber security considers just external attacks for protecting inside resource. Firewall, IDS/IPS, VPN and antivirus are used as a protection device for the system and the network from Cracking, viruses or worm. However, such as the core technology leakage, customer information leakage or embezzlement is frequently performed by most of the insiders at companies and financial institutions. According to the Small Business Administration in Korea, 90 per cent of the information leakage incidents are made by internal staff. Because the damage is getting serious with the information leakage incident, insider security study has become one of the big issues in the network security.

Internal workers have access rights to various inside resources for their own business. They have a lot of knowledge about system of an organization. Therefore, they know where resource or information they want is and how to access them. If they want, they can avoid security system to obtain the desired resource and information. It is possible to give serious damage to an organization, if these insiders have a
M. O. Asokhia (2010) conducted a research study with the objective of enhancing national development and growth through combating cyber crimes/internet fraud. National development and growth hinge on the people having the right perspective towards others, organizations, industry and government. The absence of this is an automatic threat to the economy and invariably to the growth and development of any nation. The young adults’ perception should be guided to enhance growth, through having respect for other people’s information and materials. In order to find out if cyber crimes exists among young adults in Edo State, Nigeria, a comparative study of young adults’ perception of cyber crime in two Local Government Areas of Edo State namely: Esan (Central and West) was conducted. The study was guided by three hypotheses. Random samples of 200 subjects were selected from the four centres used for the study where 50 subjects were also selected. The research design was a comparative one. A questionnaire titled: “CSYAPCCS” (Comparative Study of Young Adults Perception of Cyber Crimes Scale) was used to gather information from the respondents. The data collected was analyzed using the t-test to find out if differences existed.

In view of the aforesaid facts, it is clear that though the magnitude of the cyber and cyber related crimes are increasing fast, but studies are too limited on this serious issue. As such, the present research as is believed will to some extent fill the existing gap in the literature.

**Noteworthy contribution in the field of proposed research**

The rapid incidence of cyber crimes has become a field of immediate attention and big industrial houses, multinational organizations, technologists, economists’ sociologists and Government officials - all are very much concerned to curb the graph of cyber crimes. J. Chirillo, J.
Erickson, S. Furnell and D. Gunkel have made very notable contribution in highlighting the cyber crimes.

As per the National Crime Records Bureau statistics, during the year 2005, 179 cases were registered under the IT Act as compared to 68 cases during the 2004, thereby reporting a significant increase of 163.2 per cent in 2005 over 2004. During 2005, a total of 302 cases were registered under IPC Sections as compared to 279 such cases during 2004, thereby reporting an increase of 8.2 per cent in 2005 over 2004. In 2006, 206 complaints were received in comparison with only 58 in 2005, a 255 per cent increase in the total number of complaints received in the Cyber Cell/EOW over the last year. In terms of cases registered and investigated in 2006 (up to December), a total of 17 cases, where the computer was the victim, a tool or a repository of evidence, have been registered in the Cyber Cell/EOW as compared to 12 cases registered in 2005.

While the number of cyber crime instances has been constantly growing over the last few years. The past year and a half, in particular, has seen a rapid spurt in the pace of cyber crime activities. Cyber lawyers, Pawan Duggal, advocate with the Supreme Court of India and Karnika Seth, Partner, Seth Associates, Advocates and Legal Consultants, testify to this, pointing out that they have seen a jump in the number of cyber crime cases that they have been handling in the last one year. One also should remember that the term “Cyber Crime” should be applied to all offences committed with the use of ‘Electronic Documents’. Hence, cyber crimes must grow at the same rate as the use of the Internet, mobile phone, ATM, credit cards or perhaps even faster. “With the little offences came the larger ones involving huge money and one has seen this sudden jump from smaller crimes to financial crimes in the last one year”

According to Captain Raghu Raman, CEO, Mahindra Special Services Group (SSG), the contributing factors are high volume of data
processing, rapid growth and major migration into the online space, especially of financial institutions and their customer transactions. However, actual numbers and quantum of such transactions, continue to get away from the real picture, when we consider the fact that a majority of the cases go unreported. Most victims, especially the corporate, continue to downplay on account of the fear of negative publicity thereby failing to give a correct picture of the cyber crime scene in the country. According to Cyber law expert Vijayshankar, it is difficult to measure the growth of Cyber Crimes by any statistics, the reason being that a majority of cyber crimes don’t get reported.

In assessing cyber crime legislation, policy makers and gender and development advocates must carefully consider the implications for privacy and information security. On the one hand, information and communications technologies (ICT) have created opportunities to combat inequality through movements and communities against issues that were once deemed 'private', such as domestic violence and sex trafficking. On the other hand, ICT exacerbate existing structures of inequality by enabling cyber criminals to access and misuse private information to target vulnerable groups. As ICT blur the lines between personal and public, the nature of the internet and cyber crime- including how they affect human rights and social justice is questioned.