CHAPTER II

REVIEW OF LITERATURE

This chapter includes the review of studies relating to the present research and to the variables examined in the study. The literature is presented according to the key variables of the study such as the profile of victims of cybercrime victimisation, Internet usage cybercrime victimisation, computer knowledge and cybercrime victimisation, the extent and forms of cybercrime victimisation, the impact of cybercrime victimisation, the reporting behaviour of victims and the needs and expectations of victims of cybercrime.

2.1 Profile of Victims of Cybercrime Victimisation

Ample research has been carried out relating to the characteristics of victims of cybercrime, such as age, gender, education, nativity and so on.

Studies on the relationship between the characteristics of victims including age and cybercrime victimisation particularly on sexual victimisation were conducted in U.S. For instance, researchers of University of New Hampshire, U.S. carried out two national level surveys (Youth Internet Safety Surveys – YISS 1 & YISS 2) in the years 2000 and 2004, among respondents with sample sizes of 1,501
and 1,500 respectively, belonging to the age group of 10-17 years, with the objective of tracking the trends in certain sexual victimisation on the Internet over a period of time. These two surveys also examined the prevalence of certain forms of sexual victimisation such as unsolicited sexual solicitations, harassment and unsolicited exposure to pornography among the sample of Internet users. The study in the year 2000 revealed that among Internet users of the stipulated age group (10-17 years), 19 percent had been sexually solicited in the previous 12 months. The authors found that in the U.S., the proportion of youth Internet users who reported sexual solicitations declined between the year 2000 and 2005, due to heightened awareness on Internet behaviour among adolescents. However, the other forms of victimisation such as online harassment and unwanted exposure to pornography also increased. It was also revealed that there are some differences in victimisation based on the subgroup of respondents. For example, the decline in sexual solicitations was found among the white youth and among those living in affluent households (Wolak, Mitchell & Finkelhor, 2006).

A study was carried out on online/offline victimisation among adolescents aged 10–17 years as part of a national survey of children’s exposure to violence between January and May 2008 in U.S. A sample of 2,051 respondents answered the Juvenile Victimisation Questionnaire (JVQ) and Trauma Symptoms checklist for children. The results indicated that the type of online
victimisation experienced was sexual harassment and the online victimisation was strongly related to offline victimisation like being assaulted by peers or sibling, experiencing psychological or emotional abuse. The study also revealed that respondents of the selected age group (10-17 years) who had experienced certain offline victimisation might be at risk for online victimisation (Mitchell, Finkelhor, Wolak, Ybarra & Turner, 2010).

Some studies have also examined the relationship between age and cyber bullying – a form of cybercrime. A study by Juvonen and Gross (2008) was conducted on 1,454 respondents within the age group of 12–17 years in a web-based survey across the U.S., predominantly from California and New York, between August and October 2005. The findings revealed that 72 percent of respondents indicated at least one online incident of bullying, 85 percent of them also experienced bullying in school. The findings have further shown that name-calling or insults through instant messaging was a form of bullying. It also found that the bullying in schools and online bullying led to an increase of social anxiety in the respondents. However, results indicated that 90 percent of respondents did not tell an adult about the experience of being bullied online.

Besides age, the relationship between gender, nativity etc. in cybercrime victimisation was also studied. A national survey, namely, the Health Behaviour of School aged Children (HBSC) was conducted
by the National Institute of Child Health and Human Development in the year 1998 with the objectives of gaining an understanding of the prevalence of bullying in the offline physical space. A nationally representative sample of school going children studying in grade 6–10 from both public and private schools participated in the survey. The study examined the differences of bullying behaviour between different gender, age and nativity etc. With regard to the gender of respondents, bullying behaviour and being bullied was high among males than females. The results have shown that bullying was more prevalent among middle school children than among high school children. With regard to the race, Caucasian children were more frequently found to experience bullying than Hispanic or African-American children. However, no significant difference was found between children from the urban, suburban and rural areas (Nansel et al., 2001 cited in MacDonald & Roberts-Pittman, 2010).

There have also been studies among college and university students on bullying in general and cyber bullying in particular. For example, Chapell et al. (2004) in their initial study explored bullying in the physical space in college by students and teachers. The study was carried out among 1,025 under-graduates in New Jersey, U.S.. Close to 25 percent of the students reported that their fellow students bullied other students occasionally. They also reported that students being bullied very frequently (2.8%), and occasionally (5%). The study revealed that male students bullied their fellow students more
than the female students did. The prediction of student bullying was measured by viewing other students bully or being bullied by both students and teachers.

As an extension of the above mentioned study, along with other authors Hasselman, Kitchin, Lomon, Maclver and Sarullo, Chapell (2006) had examined the problem of bullying among students studying in colleges. They conducted the retrospective study among 119 undergraduate students in New Jersey, U.S. to investigate the continual bullying experience from elementary school to college in the frequency of being bullies, victims and bully-victims in elementary school, high school and college. The results revealed that 72 percent who had experienced bullying in elementary school and high school, in turn, bullied others while in university. Around 54 percent of respondents who had been bullies in their schooling years continued to be bullies in college too. Similarly, nearly 42 percent who had been bully-victims in schools also remained bully-victims in college. The results also show that though age did not deter bullying in the physical space, only a few reported bullying in university compared to the bullying experiences in elementary and high schools. However, this is not true with college and university students with regard to cyber bullying, owing to the fact that the older students own mobile phones and other electronic gadgets. MacDonald and Roberts-Pittman (2010) conducted a study on cyber bullying among 439 college students enrolled at a midsize mid-western university in the U.S. The
results clearly established that 38 percent of the respondents who participated in the study knew someone who had been cyber bullied and 21.9 percent reported having been cyber bullied. The study also examined the inter-relationship between cyber bullying, traditional bullying and demographic variables such as gender, ethnicity and sexual orientation. It was observed that gender significantly and negatively correlated with bullying others, which indicated that men were more likely to bully in the traditional form than others. In the case of cyber bullying, such correlation was not found. Further, no significant correlation between ethnicity and any of the cyber bullying or bullying variables was found. However, sexual orientation was significantly and positively correlated with knowing someone who had been cyber bullied.

Similarly, Walker, Sockman and Koehn (2010) made an attempt to assess the events related to direct and/or indirect cyber bullying experiences by under-graduate students at East Stroudsburg University of Pennsylvania, United States. A total of 131 students, comprising 73 were females and 57 males were chosen as the sample. The results showed that overall, 54 percent respondents knew someone who was cyber bullied. Facebook was mostly the main platform (56%) used to bully and harass others. The study also reported that 71 percent of respondents reported their experience of cyber victimisation to a parent/guardian or to other adults.
Buzzle, Foss and Middleton (2006) based their study on an online survey of 134 students attending under-graduate programmes in the mid-western universities of the U.S. The study determined that 90 percent of the total sample owned personal computers. The study was conducted for over a period of four weeks in the months of March to April, 2005, to assess the relationship between low-self control and two forms of pornography access, such as downloading pornographic images and visiting sexually explicit sites. Keeping low-self control and opportunity as independent variables; and downloading pornographic images and visiting sexually explicit sites as dependent variables, the study used a standard 24-item scale to measure self-control. The scale used six cognitive dimensions of self-control that was proposed by Gottfredson and Hirschi (1990), namely, impulsivity, simple tasks, risk seeking, physical activity, self-centeredness and temper. The dimensions of opportunity that were measured in the study were access, sophistication and monitoring. The study found that ‘being a male’ significantly correlated with the variable, Internet pornographic use. Low-self control was related to both the forms of the Internet pornography use. When opportunity is combined with low-self control, frequency of downloading pornography increases. Risk-seeking and self-centeredness were significantly related to visiting sexually explicit sites.

Yet another study was carried out among students (N=25,000) studying in North American universities on the habit of viewing
pornography. It was found that around 51 percent male students and around 32 percent female students first admitted to viewing pornography before they were 12 or younger. Around 35 percent of students admitted that their first exposure was through the Internet or computer-based access in comparison with the 32 percent from magazines, 13 percent from VHS or DVD, and 18 percent from Cable or pay-per-view. The study also found that around 51 percent male students and around 16 percent female students spent under five hours per week online for sex. 11 percent male students and 1 percent female students spent 5–20 hours a week online for Internet sex. The results projected that 18–22 million male and female sex addicts were living in the U.S. The results further stated that four percent females felt that their sexual activity on the Internet interfered with their family lives (Leahy, 2009). These studies have demonstrated that there is an association between age and experiencing cybercrime victimisation. Such studies have also shown that children, adolescents and youth were the more vulnerable groups to cybercrime victimisation.

Over a period of time, studies on cybercrime victimisation have also attempted to examine the relationship between gender and cybercrime victimisation. Finn (2004) conducted a study on online harassment (cyber stalking) among 339 students at the University of New Hampshire, U.S. in April 2002. The study revealed that 1 in 10 college students at the University was a victim of repeated threats,
insults and harassment via the Internet. The results showed that above 50 percent of respondents received unsolicited pornographic messages or pictures and one in three students received unsolicited pornographic information five or more times in a week. Online harassment mostly occurred through e-mail and/or Instant Messaging. The study found that the extent of online harassment through e-mail differed only with students who were Lesbian, Gay, Bisexual and Transgender (LGBT) (37.5%) than with heterosexual students (13.1%). The results also revealed that only 6.8 percent of respondents reported their bad experiences to anyone. With regard to gender and cyber stalking, interestingly no significant difference was found in this study.

In contrast to the above mentioned study that indicates that there is no relationship between gender and cybercrime victimisation, the study conducted among 290 youth in Chennai by Lavanya and Prasad (2014) found that there existed a relationship between gender and cybercrime victimisation. The authors found that 36.2 percent of male respondents thought cyber bullying occurred frequently, 25 percent thought it occurred occasionally and 38.7 percent thought that it occurred rarely. Only a few of female respondents witnessed cyber bullying occasionally (5.7%) and rarely (10.3%). Around 41 percent female students reported that they had never seen it happening. The results further revealed that more males witnessed cyber bullying than females. The study also revealed that over 80 percent of respondents
were aware of the meaning of cyber bullying and only a few accepted that they resorted to cyber bullying to target their victims, which implied that cyber bullying was a growing trend and a social threat among the youth in Chennai, Tamilnadu.

### 2.2 Internet Usage and Cybercrime Victimisation

Many studies have been carried out among the students community to understand the factors and purposes related to the usage of the Internet in general and to find out the relationship between the Internet use and cybercrime victimisation in particular.

A study was carried out among 502 tertiary students in Sunyani municipality, Ghana on Internet knowledge and purpose of Internet usage. Regarding the purpose on Internet usage, the study revealed that searching for information for academic assignments was the primary purpose to use the Internet. Close to 45 percent of respondents reported that they used the Internet several times a week, while 21.4 percent indicated daily use of the Internet. As far as the duration of usage is concerned, the study showed that 42.3 percent used the Internet for 30 minutes to one hour every day and 33.8 percent used the Internet for 1 to 2 hours every day. The study found that 92.9 percent of respondents reported that they knew how to use the Internet. The study also revealed that students tend to use Internet cafes more frequently than any other means to access the Internet (Brafi & Arthur, 2013).
While this study examined the various reasons students use the Internet, the study by Cheang and Huang (2005) attempted to analyse how using the Internet helps better learning performance and improves job prospects. Their study was carried out among 328 university students aged between 20–22 years in Hong Kong, to explore the use of the Internet in university learning. They used a few analytical tools and models such as Technology Assistance Model that dealt with individual perceptions and attitudes toward certain behaviour such as the use of the Internet. The study also attempted to find out the motivators that stimulate the use of the Internet in learning. Such motivators can be intrinsic (joy and pleasure) or extrinsic (social pressures). The authors found that Internet usage correlated positively with student perceptions of better job prospects. The study revealed that a gap was created by learning within the university and the business needs of organisations, which could very well be filled up by the use of Information Technology, specifically the Internet. The study suggested that higher Internet usage while studying in university could result in better learning performance and job prospects.

Some studies have also attempted to find out the differences in Internet usage among men and women. There is no single pattern of Internet usage among men and women with differences in the purpose of using the Internet. Fortson, Scotti, Chen, Malone and Del Ben (2007) conducted a study among 411 under-graduate students enrolled
in an introductory psychology course at a south-eastern regional university in the U.S. to assess Internet usage, abuse and dependence. The authors used a questionnaire that consisted of questions related to the demographic profile such as gender, race, ethnicity, perceived sociability (sociable, shy, introverted and loner) and social interaction (more face-to-face than on the Internet and more on the Internet rather than face-to-face). The authors also assessed Internet dependence through questions that dealt with being online for longer than intended. The findings revealed that 90 percent of participants used the Internet daily with a majority (68%) of participants using the Internet anywhere between 30 minutes to four hours every day. It was observed that there were differences among men and women in their reasons to use the Internet. Men were significantly more likely to use the Internet to meet new people and to look for salacious material. In addition, the study found that men were significantly more likely to use the Internet to surf the web, read the newspapers, participate in chat groups and bulletin boards and play both single and multi-user games. However, there was no gender difference in using the Internet for academic purposes.

Another study also investigated gender differences in Internet usage. In the U.S., Shade (2004) studied the issue of gender difference in Internet usage. The study found that men were less habitual users of e-mail with 53 percent women using e-mail more often than men. Women used the Internet mostly (65%) to search for information on
health and medicine, which could be attributed to the fact that women as care-givers used the Internet with a purpose to care for their families etc. In contrast, men used the Internet for news and financial information, selling and buying stocks, information on their hobbies, political news and to get sports updates. The study revealed that men used the Internet for non-personal reasons than women who used the Internet for personal reasons.

Some studies have also attempted to establish a relationship between the purpose of Internet usage and victimisation. A study was conducted by Yang et al. (2004) on 936 students in South Korea in the age group of 13–14 years. The study also involved a follow-up of 835 students after two years, when the students were 15–16 years. The parents of the students were also interviewed. The students were administered a questionnaire with items relating to inappropriate sexual exposure, their cyber bullying experiences, peer-victimisation and bullying behaviour. The research measured the psychological impact of the Internet experience. This was tested using inventories like Children’s Depression Inventory, State-Trait Anxiety Inventory for Children, Self-esteem Inventory, Ways of Stress Coping strategies Checklist, Attention Deficit Hyperactivity Disorder Rating Scale, Strengths and Difficulties Questionnaire and socio-demographic characteristics such as gender, family structure, number of friends etc. were also considered. The findings indicated that computer overuse was for academic purposes (8.5%) and to play games (21.8%).
The study revealed that feelings of guilt were associated when the parents disapproved being online. Those who experienced online sexual harassment or who were solicited online when they stayed away from home had strong feelings of vulnerability or potential embarrassment. The study also found that those with higher depression, higher anxiety and passive coping strategies easily became prey to unsolicited sexual exposure. Higher level of anxiety was associated with cyber bullying victimisation. With respect to gender, female students were found to use the Internet for academic purposes while for male students Internet use was more game-oriented. However, the study brought out an important insight, indicating that faster growth and advanced pubertal stages influenced higher computer usage and higher levels of hostility and defiance of parents’ online safety and computer rules. The study also found that male students were most likely to become vulnerable to Internet obscenity and harassment and thereby come up against some form of victimisation.

Fleming, Greentree, Cocotti-Muller, Elias and Morrison (2010) examined the purpose of Internet usage among students. Of the many reasons for using the Internet, 34 percent male students and 36 percent female students used the Internet to look for material/information to do the homework. Other reasons were to talk to friends via Instant Messaging (male 28%, female 37%), to download and/or play games (male 10%, female 3%), to talk to
friends via e-mail (male 6%, female 13%), to download and play their favourite songs and videos (male 6%, female 3%) and to get information about their favourite TV programmes and movies (male 4%, female 2%). The study also revealed that 52 percent males and 26 percent females used the Internet frequently.

Though limited literature is available in this area, studies have attempted to explore the purpose of Internet usage in the Indian context. Sujatha (2011) conducted a study among five colleges in Mangalore city with a sample of 390 under-graduate students to find out the different reasons for students to use the Internet. The results of the study showed that 79.6 percent of respondents used the Internet to obtain course related information; 75.6 percent to prepare for their seminars and assignments; 67.8 percent to communicate with friends and family via e-mail; 47.0 percent to chat with friends and relatives; an almost equal percentage of students used the Internet to watch the news, for social networking, to play online games and to listen to music; and 35.2 percent used it to download software. Overall, students were found to use the Internet primarily for educational purposes.

The time spent on the Internet is considered an important indicator with regard to overuse or excessive use of the Internet (Internet addiction) (Chou, Condron & Belland, 2005). Given the easy accessibility and personal characteristic of the Internet, a time limit
for Internet usage cannot be determined or mandated. This does not mean that overuse is a myth. Late adolescents and young adults contend with strong psychological and developmental problems. Their major focus is to develop a sense of identity coupled with meaningful and intimate relationships. The social network sites like Facebook, Twitter and Whatsapp etc., provide ample opportunities for them to meet fulfill their expectations, which in turn causes them to be easily influenced and further harmed by cyber predators. In this way, the youth possess a unique vulnerability to Internet addiction or pathological use of the Internet among the youth. The following study has explored the relationship among the hours of Internet usage, purpose of Internet usage and cybercrime victimisation.

In a study that used the Longitudinal Internet Studies for the Social Sciences (LISS) and panel administered by CentERdata of Tilburg University, The Netherlands, LISS carried out a study among 6,693 people in February 2010. It was found that the hours spent on the Internet on a weekly basis increased the probability of getting hacked or attacked by a virus online. The forms of cybercrime ranged from experiencing a hacking attack, a virus attack causing data loss, making online purchases but not receiving the item and having money stolen from the bank account. The study used the constructs of Routine activity theory, namely, motivated offender, suitable target and lack of capable guardianship along with self-control as an individual factor in the four different forms of cybercrime. It was
found that an individual with a high monthly income had a higher probability of being victimised predominantly because of unauthorised money transfers from the bank account (26%) and not receiving items that were paid for (45%). The study also found that age correlated with being attacked by a virus online; and the level of education negatively correlated to victimisation in the case of stealing money from a bank account and not receiving items that were paid for. Interestingly, the study indicated that the technical guardianship, namely, the security software did not safeguard Internet users instead gave them a false sense of safety (Angelidakis, 2012).

Yet another study on the overuse of the Internet was conducted among high school students in Taiwan. The study was carried out among 1,289 students (mean age being 17.4) from 11 senior or vocational high schools across Taiwan. The study aimed at exploring the perceptions of the participants on being monitored by their parents, their leisure boredom, their leisure time activities and their Internet addiction behaviour. The four constructs were measured using various standardized tools designed particularly for the purpose, such as Internet Addiction Diagnostic Questionnaire designed by Young (1998) to measure Internet addiction. Interestingly, the results revealed that there were no differences between male and female students with regard to their Internet addiction. Male students were found to be mostly interested in outdoor activities, socialising and using the Internet. The results also showed that age and gender were
not main factors of the Internet addiction of adolescents. However, the time spent on the Internet was the main factor in predicting Internet addiction. The results illustrated that leisure boredom and their involvement in the Internet and social activities increased the probability of Internet overuse. The study concluded that if the perceptions of adolescents on boredom in leisure time and if the activities during the leisure time were properly maintained, Internet addiction could be avoided (Lin, Lin & Wu, 2009).

One of the studies examined the levels of Internet abuse among men and women and the relationship between Internet abuse and the purpose of using the Internet. Gencer and Koc (2012) conducted a study among 1,380 high school students of vocational, general and Anatolian types of schooling, belonging to the age group of 15–18 years in the city of Isparta, Turkey, on Internet abuse among teens and the related usage patterns and demographics. The study took into consideration a perceived socio-economic status such as low, middle and high class and a perceived academic achievement such as poor, average and good performance. The respondents were administered a questionnaire seeking information with regard to their background and their Internet usage. Questions related to whether the respondents used the Internet for information, communication, entertainment and/or business. An Internet Addiction Test (IAT) was also administered to the respondents. The results indicated that respondents with a high level of personal problems were diagnosed as
Internet abusers and 24.3 percent of respondents who showed symptoms of moderate problems were abused on the Internet. The study revealed that male respondents experienced a slightly higher level of Internet abuse than female respondents. The results indicated that a perceived academic achievement had an impact on Internet abuse, that is, perception of poor achievement indicated a higher level of Internet abuse when compared with respondents who had average and good achievement. However, the school type and the perceived socio-economic status were not related to Internet abuse. Another important finding of the study was that respondents who used the Internet every day had a higher level of Internet abuse when compared to those who used the Internet a few times a week or a month. The study revealed that respondents who had access to the Internet at home were more prone to Internet abuse when compared to the respondents who used the Internet from school. Finally, the research indicated that the purpose of Internet usage was significantly related to Internet abuse, which implied that respondents who used the Internet for entertainment and communication were more prone to Internet abuse than those respondents who used the Internet for information.

A few studies have attempted to demonstrate the relationship between regular Internet usage and cybercrime victimisation. Bernat and Godlove (2012) found that individuals who were most susceptible to cyber property crimes and cyber bullying, cyber stalking or cyber
harassment were the ones who regularly used the Internet. They were young and did not know who to turn to for assistance when experiencing such victimisation. However, merely spending time on the Internet does not lead to victimisation but spending time on specific activities can result in ‘problems’ while using the Internet. Using 788 college students at a south-eastern university campus in U.S. as samples and applying the Routine activity theory to account for online victimisation in 2006, Holt and Bossler (2009) attempted to use the framework of Routine activity theory to find out whether loss of data due to virus attacks was linked to online activities and guardianship of respondents. They found that the respondents’ general computer usage and activities such as playing video games, shopping or checking e-mail or visiting chat rooms did not have a significant impact on the likelihood of experiencing online victimisation, but activities such as pirating media or associating with friends who spent much of their time watching pornography increased the risk of losing data by malicious virus attacks.

Similarly, using the constructs of the Routine activity theory, Marcum, Ricketts and Higgins (2010) conducted their study among 744 under-graduate students pursuing 100-level courses at a mid-sized north-eastern university in the U.S. during the academic term of Spring, 2008. The survey questionnaire that was used for the purpose of the study was based on Internet behaviour, activities and experiences during the high school senior and college freshman years.
The study aimed at assessing the differences in online victimisation between gender, using variables that would picture the three constructs of the Routine activity theory, namely, suitable target, a lack of capable guardian and a motivated offender. To measure the exposure to a motivated offender, questions on the duration and the purpose of Internet usage was asked. To measure target suitability, Internet users were asked questions on privacy matters and the type of information provided by them. And to measure the lack of capable guardianship, questions on the place of Internet usage and parents’ monitoring mechanisms were asked. The study evinced that Internet behaviour, which exposed the user to a motivated offender had a higher possibility of being cyber victimised by both genders. The behaviours that increased target suitability offered more opportunities for victimisation. The study concluded three important factors, namely, that those respondents who spent an increased amount of time using the Internet and specific computer-mediated communication were more likely to be victimised despite their gender; protective software did not reduce the likelihood of victimisation; and that male and female Internet users with unrestricted Internet access had a higher possibility of being victimised.

Besides the duration of the time spent on the Internet (How long do you spend your time on the Internet?), the frequency of the Internet use (How often do you spend time on the Internet?) also has an effect on cybercrime victimisation. In a study among 692 university students
in Australia, Fleming et al. (2010) found that the higher frequency Internet users were more exposed to varied unsolicited material on the Internet than the low and moderate Internet users. The study investigated the extent of exposure of teens to inappropriate material, their online behaviour and whether protective software would reduce such exposure. In addition to these objectives, the study also aimed at determining the relationships between age, gender and parental discussions on online safety. The results showed that many young people exposed themselves to pornography (male 92.5% and female 61.3%), violent images (male 76.9% and female 55%), rude comments (male 85.4% and female 69.8%) and sexual comments (male 85.4% and female 62.2%). Moreover, of the frequent Internet users logging onto the Internet at least three times a week, male students (82%) outnumber their female counterparts (66%). Teenaged boys viewed more violent images and pornographic sites than girls. Furthermore, the results revealed that the protective software to block or filter the unsolicited material on the Internet did not make any significant difference in students’ Internet behaviour. However, the study revealed that parental discussions on online safety practices safeguarded students from viewing or being exposed to unsolicited material.

Some authors have examined the impact of technology on young Internet users. Anderson and Rainie (2012) in their study among 1,021 Internet experts and users found out the impact of technology
on teens and the implications for the future. The negative response chosen by 42 percent of respondents indicated that teens lacked face-to-face social skills and depended on unhealthy ways of using the Internet and mobile devices for their daily activities.

A study compared the forms of victimisation experienced both online and offline among 354 college students (mean age = 22) in a southwestern university in the U.S. between September 2007 and April 2008. The questionnaire, consisting of 77 self-reporting items included personal use of social network sites, activities conducted while online and types of victimisation that might have occurred as a result of the use of social network sites. The survey also included 13 questions from the Sexual Experience Survey (SES). The study found that 92 percent of college students used social network sites. The study revealed that sexual harassment occurred more often online than offline; persistent badgering also occurred more often online; verbal harassment happened at similar levels both online and offline; and stalking behaviour was found occurring more frequently offline (10.1%) than online (3.1%). Internet behaviour on social network sites was measured by the level of privacy employed in participants’ profiles such as public (34.9%), semi-private (31.5%) and completely private (33.6%). The study revealed that there was no significant relationship between privacy levels and harassment or receiving unsolicited material. The study also revealed that other behaviours like the number of hours spent online; the number of friends on the
friend list; specific information such as home address did not significantly vary with levels of privacy (Kennedy & Taylor, 2010).

The literature mentioned above shows that studies have been conducted to understand the purpose of Internet usage including gender differences. The relationship between victimisation and the purpose of Internet usage was also established by some studies. Literature has further exhibited other related items such as Internet addiction, duration of Internet usage, Internet behaviour etc. among the youth, especially the student community.

2.3 Computer Knowledge and Cybercrime Victimisation

This section includes the review of the existing literature on the level of computer knowledge of students. Some studies also attempted to examine the relationship between the level of computer knowledge and cybercrime victimisation.

Arch and Cummins (1989) conducted a study among 362 first year college students in Oregon, U.S. on structured and voluntary exposure to computers. The study found that there was a gender difference in computer usage initially but this changed after computer training by way of regular classroom settings, decreasing the gender difference. The study revealed that male students reported higher usage, a more positive attitude and a greater perceived skill in computers both at the beginning and at the end of the term in two types of learning
patterns—the structured introduction of computers in the classrooms and self-learning. The study found following structured classroom programmes for a term, all students used computers at the highest level and showed a positive attitude towards computers and their own computer skills. Where computer knowledge was not part of structured programmes, male students reported lower computer usage and female students reported even lower usage.

In India also, a study on the level of computer knowledge was conducted by Halder and Chaudhuri (2011) among 84 teacher trainee students at the University of Calcutta, West Bengal on their self-efficacy in relation to computer usage. Computer self-efficacy was defined by Compeau and Higgins (1995) as “judgment of one’s capacity to use computer” and as “self assessment regarding one’s computer skills” (p. 189). The study found that respondents were moderately knowledgeable in computers. It was also found that subjects studied in school or college was an important factor in determining computer self-efficacy and that students who pursued computer-related disciplines had higher computer self-efficacy.

There have been very few studies in the past that relate computer knowledge and cybercrime victimisation. A study by Beran and Li (2005) among school children found that even when computers were used in the classroom as an educational teaching tool, nearly two thirds of students were aware of cyber harassment. 25 percent of the
students experienced several instances of harassment, and some even reported using this medium of technology to intentionally harm their peers.

A study done by Umarathab, Rao and Jaishankar (2009) elucidated a similar pattern of cybercrime victimisation for those who had computer knowledge. The study was carried out in Chennai with a sample size of 100 people who had experience in working with computers. The results showed that nearly 29 percent of computer users were victims of cyber stalking, 24 percent were victims of job search sites, 38 percent were victims of home-based job opportunity sites, and 70 percent were victims of virus, malware attacks such as Trojan.

A study was conducted by Mishna, Cook, Gadalla, Daciuk and Solomon (2010) on middle and high school students through a self-reporting questionnaire in Canada. The study showed that respondents did not always possess computer knowledge and online safety practices. The study revealed that 49.5 percent respondents were bullied online, of which, nearly 52 percent revealed that they did not do anything about the bullying as the bully was often thought of as a friend. The results indicated that one-third of the respondents shared their online passwords with their friends; and three-fourth of the respondents were unaware that anything that they uploaded, such as images and texts, continued to exist in cyberspace even if deleted.
The study also indicated that one-fourth of cyber bullying occurred in the presence of cyber witnesses.

2.4 Extent and Forms of Cybercrime Victimisation

The existing literature shows that there are extensive studies to understand the forms and extent of cybercrime victimisation. A few authors have acknowledged the difficulty in estimating the extent of cybercrime victimisation due to factors such as small size samples, self-reporting surveys and so on. The following section includes the review of existing literature on the extent of cybercrime victimisation. Some authors have attempted to explain how the extent of cybercrime victimisation can be estimated. Reyns (2010), in his study on cyber stalking evinced that the extent of cyber stalking is not estimated with standardised methodology and there exists many difficulties in assessing the extent of cybercrime. However, the existing studies only provide only a fundamental idea of the extent of the phenomenon.

The difficulty in estimating the extent of cybercrime victimisation may also be due to the lack of proper and standard definition of the term cybercrime victimisation. Even to define one form of cybercrime victimisation, different authors have used different terms. Kennedy and Taylor (2010) used the term ‘online harassment’ for ‘cyber bullying’ whereas Van Wilsem (2013) used the term ‘cyber stalking’. Although in some cases, they are interchangeably used. However,
when online harassment is used to refer to cyber bullying, items such as posting defamatory remarks or threatening messages are used in the surveys and when the same term is used to refer to cyber stalking, items such as impersonating others or stalking them online is used in the survey. Therefore, the extent of online harassment varies according to the understanding of the definition of the term.

Reyns (2010) mentioned that the lack of statistical analyses, relying on convenience samples, small size samples and self-reporting surveys were some of the reasons that pose challenges in estimating the extent of cybercrime victimisation. For example, the study of Chapell et al. (2006) had only a convenience sample size of 119 under-graduate students. The study of Walker et al. (2010) had a sample of 131 under-graduate students. Similarly, Buzzle et al. (2006) conducted a study among 134 students. Reyns (2010) added that the small size of the sample limited the generalisation of results, because such small numbers would not fully represent the larger population. Statistically, a larger sample is preferable as it is likely to better represent the population and provide a more accurate estimate of observations in the population. There have also been studies with a large sample size, such as YISS I and II with 1,500 and 1,501 samples. A study by Leahy (2009) had a sample size of 25,000.

Some studies have also highlighted the difficulty in sample selection to study the extent of cybercrime victimisation. A few studies (Eg.
Brafi & Arthur (2011) at Sunyani Municipality in Ghana; and Lavanya & Prasad (2014) in Chennai, India) that were conducted in local or small areas may not indicate the extent of cybercrime victimisation at the global level. For example, some researchers have collected samples from a single university or from single department in a university. For example, Kennedy and Taylor (2010) studied online harassment and victimisation of college students through a survey within one department in a university. Such samples do not fully project the extent of cybercrime victimisation. Hence, it is imperative that the studies on cybercrime victimisation not be limited to small geographical boundaries.

Some researchers focussed on a single crime or offence for the purpose of their study (Eg. MacDonald & Roberts-Pitman, 2010 studied cyber bullying), while a few other studies focussed on a mix of crimes or offences (Eg. Van Wilsem, 2013 studied hacking and online harassment) to measure the extent of cybercrime victimisation. The full-scale extent of cybercrime victimisation cannot be fully comprehended in small studies that use just one or two forms of cybercrimes or offences.

Although sample size determination or the types of cybercrime studied are general limitations while estimating the extent of cybercrime victimisation, the research tool used to measure cybercrime victimisation also becomes a limiting factor in the
estimation of the extent of cybercrime victimisation. Buzzle et al. (2006) used 24 items and Kennedy and Taylor (2010) used 77 items in their questionnaire, while some other studies have used only simple and direct questions such as ‘Have you been a victim of cybercrime?’ or ‘Did you know anyone who has experienced cyber bullying in the past 12 months?’.

Some authors (Nansel et al., 2001, as cited in MacDonald & Roberts-Pitmann, 2010) have provided an estimation of the extent of cybercrime victimisation based on official statistics published by the Government. For example, ‘Crime in India’ is an annual, national publication of crime statistics published by the Government of India. This publication is based on police records that often are not the ‘real’ figures due to severe under-reporting and recording of cybercrime. Similarly, some authors (Eg. Mishna et al., 2010) have also estimated the extent of cybercrime victimisation based on a self-reporting questionnaire that mostly is data-biased (Fanfiski, Dutton & Margetts, 2010).

At the global level, Kaspersky Lab and INTERPOL (2014) jointly conducted a study on cybercrime in the world. The report stated that over a period of one year, Kaspersky Lab security products reported 3,408,112 malware attacks on the devices of 1,023,202 users. The report revealed that in the first half of 2014 alone 1,75,442 new and unique Android malicious programmes were created. The report
further stated that from August 2013 to July 2014, 1,020,000 Android users encountered around 3,400,000 attacks. Furthermore, the report found out that Trojan-SMS malware attacks accounted for 57.18 percent of the total attacks and they were frequent in Russia with 59.0 percent followed by Kazakhstan. In India, there were 30,201 attacks in that period. The study also revealed that 59.01 percent attacks were committed to steal money from victims. It was also reported that every second user was indeed attacked by a cyber-criminal.

The Dell Security Annual Threat Report compiled based on various resources collected from around the world by the Dell Global Response Intelligence Defense (GRID) Network, reported that cyber offenders employed new techniques, such as using weak links in victims’ security programmes (Dell, 2015). The report revealed that the development of new malware for Android phones continued to be on the rise. The report further stated that the malware attempts caused damage to government agencies, organisations, corporations and individuals. The attacks have doubled reaching 8.2 billion in 2015.

According to the Internet Security Threat Report of Symantec Corporation (2013), India had 42 million cybercrime victims every year. The report also added that in the previous year 52 percent of victims suffered attacks such as malware, viruses, hacking, spam, fraud and theft. India lost nearly US$ 8 billion in the same year due to cybercrime. The report stated that around 42 percent of the total
financial loss was due to fraud and 82 percent of the total loss was
due to fraud and theft. The report revealed that 7 out of 10 victims
encountered various forms of cybercrime in their lifetime. The report
further stated that there was a 58 percent increase in mobile viruses
that were primarily used to steal e-mail IDs and phone numbers. It
was also mentioned that India topped the list of spam attacks in the
International scenario and ranked second in virus attacks and third in
all other kind of threats.

The report of a study conducted by Associated Chambers and Industry
of India (ASSOCHAM) and Mahindra SSG (2015) stated that the
financial industry in India would be the most affected area by
cybercrime. The report showed that phishing attacks of online
banking accounts or cloning of ATM/Debit cards were the most
commonly occurring offences. Further, the study found 35–40 percent
of people today used their mobile device for banking transactions
thereby, increasing the vulnerability of victims. The report stated that
the maximum number of offenders belonged to the age group of 18–30
years and there was a six-fold increase in the cases related to credit
and debit card fraud. The report stated that 2,277 complaints of online
banking, credit, and debit card fraud were reported. The report also
revealed that a total of 191 Facebook-related complaints of
cybercrime such as morphed pictures, cyber stalking and cyber
bullying; 61 incidents of cheating through mobile devices; 59
incidents of hacking of e-mail IDs; and 55 incidents of abusive, offensive and obscene phone calls and SMSs were reported.

The varied forms of cybercrime victimisation manifest different kinds of cybercrime victims and diverse experiences. Studies on cybercrime victimisation, though few, have focused on the issue either of one unlawful and deviant cyber activity or combining many activities under one crime or many activities of several forms of cybercrime. Hinduja and Patchin (2008) conducted a survey among 1,378 adolescents in the U.S. on the cyber bullying experiences as a victim, offender and witness. The study found that respondents were computer literate and spent an average of 18 hours per week online. The study also found that 36 percent girls and 32 percent boys were victims of cybercrime. Eighteen percent boys and 16 percent girls reported harassing others. The study further stated that respondents were commonly victimised in a chat room or via computer text messages. Statistically, no significant difference was found among boys and girls in their experiences of cyber bullying both as a victim and as an offender.

While attempting to find out the extent of cybercrime victimisation, some authors have also analysed the relationship between variables, such as, gender, race, marital status, employment and age in the light of a few theories. Ngo and Paternoster (2010) at a south-eastern university in the U.S. examined two-theories – Self-control theory
and Routine activity theory – as independent variables. The respondents comprised 295 students (mostly female) who took an online survey. The research measured self-control, based on 24 items and routine activity theory was tested using three constructs, namely, exposure to motivated offenders, target suitability and capable guardianship. The dependent variables were experiences of cybercrime victimisation in the past 12 months, such as encountering a computer virus, receiving unsolicited exposure to pornographic material, being solicited for sex, encountering phishing, experiencing online harassment (by a stranger and a non-stranger) and experiencing online defamation. The study revealed that white respondents when compared to non-white respondents had significantly fewer chances of getting a computer virus (55%); receiving unsolicited pornographic material (67%); and being solicited for sex (62%). The study also showed that race, age and employment significantly related to online defamation and harassment by a stranger. However, gender and marital status were not significantly related to any form of cybercrime. The results revealed that Instant Messaging which fell under the construct of motivated offenders, was significantly related to harassment by a non-stranger. With regard to the element of capable guardianship, the study affirmed that older respondents were less likely to encounter a computer virus and experience online harassment by a stranger when compared to younger respondents. Thus, indicating that older individuals had lower risks of becoming
victims of cybercrime than younger individuals. A relationship between offending and victimisation was also established. Individuals who engaged in virtual offending had a higher risk of receiving unsolicited pornographic material, encountering online defamation and experiencing online harassment, when compared to individuals who did not engage in virtual offending.

Few studies have directly measured the extent of some types of cybercrime victimisation. Van Wilsem (2013) studied in The Netherlands, the generality of cybercrime victimisation keeping the focus on two types, namely, hacking and online harassment (stalking). On an annual basis, his study found that 3.1 percent of the sample was victims of hacking, 2.3 percent were victims of online harassment and 0.5 percent of the total sample was victims of hacking as well as online harassment. The study showed that one out of six hacking victims also experienced online harassment.

There are studies in India that have focused on analysing the regions and services that face high cyber security risks. Pinkerton and Federation of Indian Chambers of Commerce and Industry (FICCI) released India Risk Survey 2014 that comprehensively covered various sectors of economy and geographical areas in India. The report (Pinkerton & FICCI, 2014) showed that western India had the highest risk factor in information and cyber security. The study
brought to light the fact that the financial services in India would run into the highest cyber security risk in the future.

The Ministry of Communication and Information Technology of India published a document detailed the extent and types of cybercrime victimisation. The Indian Computer Emergency Response Team (CERT-In) reported that it had handled over 1,30,000 incidents of cyber abuse in 2014, the numbers increasing from 22,060 in 2012 and 71,780 in 2013. The report further stated that the incidents were mostly spam (85,659), website defacement (25,037), website intrusion and malware propagation (7,286), malicious code (4,307), phishing and network scanning and probing (4,339) (APCERT, 2014). The report is a clear indication that cybercrime victimisation persists in India and is rapidly growing.

McAfee (2013), a global computer software technology company released a survey report, namely, McAfee’s Tween & Technology Report of 2013. The survey was carried out across Indian tweens (children aged 8–12 years) comprising 572 male and 428 female respondents from Mumbai, Kolkatta, Chennai, Bangalore, Hyderabad, Ahmedabad and Delhi. The report stated that 12 year old children had seen nasty comments online (33%) than 8 year olds (16%). One in four had received a nasty comment from his/her friend. The report also revealed that 49 percent told their friends, parents (46%), teacher (20%) or someone in the family (20%). A notable percentage of
children (21) did not do anything about the victimisation. It was also revealed that 36 percent had spoken to someone online whom they did not know in person. It was also noted that 12 year old children (40%) were more likely to chat with strangers online than 8 year old children (25%).

McAfee also conducted the same type of survey (Mohan, 2014) in 2014 among 711 male and 711 female students of aged 8–17 years from various cities in India. The study found that 53 percent met in person, someone whom they had met online and 46 percent stated that they did not mind the risk if it got them more activity on their posts. The report also revealed that 70 percent of online adolescents spent above 5 hours a week on the Internet. Around 52 percent of Indian adolescents accessed their social media accounts while at school. Of them, 57 percent were of the age group of 8-12 and 47 percent were 13-17. Over 50 percent claimed that online risk did not apply to them and they were not concerned with privacy matters etc.

2.5 Impact of Cybercrime Victimisation

Studies on the impact of crime on victims have been conducted world over for several decades. However, the impact of cybercrime on victims has not been extensively studied and hence, a few existing studies were reviewed and have been presented below. It must be noted that the terms cyber harassment and cyber bullying have been interchangeably used by researchers. Both types of cybercrime are
repetitive in nature; use different technology such as mobile devices, e-mail, instant messaging services and websites; and are perpetrated by an individual or a group to cause harm. A study was conducted among 432 Canadian school 7th to 9th grade students to study their experience of cyber harassment and the consequences of such harassment. The study focused on the schools in Calgary, Canada that had a heterogeneous population of students. The results showed that over 50 percent of victims felt angry (57%) and 36 percent felt sad and hurt because of harassment online. It is worthy mentioning that 64 percent of the victims of cyber harassment also experienced other forms of harassment. This expounds a well-known fact that victims of ‘traditional’ harassment very likely become victims of cyber harassment. The intensity of cyber harassment also varied from merely annoying to dangerous, and sometimes life-threatening, to the extent of victims receiving death threats. It was found that the consequences of cyber harassment were manifold, emotions ranging from anger and sadness and blame. The consequences of cyber harassment were not just limited to the feelings of anger, fear, anxiety and sadness it directly impaired the students’ ability to cope with academic goals and expectations. The study further observed that through humiliation, perpetrators tried to impart power and control over their victims. It was also found that despite the harassment, students continued to stay connected online, as withdrawing from groups and chat rooms would mean losing contact with peers. The
Internet, with its immense pool of information and knowledge is an essential educational tool for students. Therefore, creating a positive school environment and inculcating values and ethics in students, cyber harassment could be curbed. The study further recommended for more research as the need of the hour to better understand cyber harassment and its impact (Beran & Li, 2005).

National Crime Prevention Council (2007) in the U.S. conducted an online survey among a nationally representative sample of 824 middle and high school students aged 13–17 years. The survey was conducted over a period of two weeks in February 2006. It attempted to explore the experiences of cyber bullying among teens and their emotional and behavioural responses to those experiences. The survey reported that 96 percent of respondents used e-mail and on an average each one had more than two e-mail addresses. The study observed that 27 percent used the Internet for over an hour a day before they participated in the survey. Though 97 percent used the Internet at home, a significant percentage of the respondents used the Internet either at a friends’ house (42%) or in other places (33%). The study found that teens most commonly went online for Instant Messaging (75%), to read and post messages on blogs (60%) and to log onto chat rooms (23%). The results of the survey also brought to light that about 4 in 10 teens reported having experienced cyber bullying in the previous year. Regarding age, the study found that 15 and 16 year olds mostly experienced cyber bullying and it was prevalent among
females (51%) than males (37%). The emotional and behavioural responses were also examined in the survey. The findings revealed that 56 percent of victims of cybercrime felt angry, 33 percent felt hurt, 32 percent felt embarrassed and 13 percent felt scared. The study also pointed out that females of age 13–15 were more likely to be emotional about their victimisation.

In 2010, a study was carried out by Hay, Meldrum and Mann (2010) to examine the effects of both traditional bullying and cyber bullying. It was conducted among 400 middle and high school adolescents in a south-eastern state in the U.S. through self-report data study. The study examined the effects of traditional bullying, cyber bullying and deviance. The study revealed that traditional bullying and cyber bullying tended to put adolescents under pressure and constraints, which resulted in delinquency, self-harm and suicidal tendencies. However, they both caused different levels of strain among adolescents. The findings of the study explicated that cyber bullying had higher effects than traditional bullying due to strain, with the consequences of suicidal tendencies being higher compared to self-harm and delinquency.

In the same year, a study among school students was conducted in Turkey to assess the relationship between the demographic variables and cyber bullying and also to examine the consequences of cyber bullying. 165 secondary school students of age from 10 to 14 were
chosen as respondents of the study with the aim to assess how the demographic variables such as age and gender are related to cyber bullying experiences of both victim and the bully. It also attempted to find out whether cyber victimisation was related to depressive symptoms. The study used a standard cyber bullying scale, which was deliberated by Erdur-Baker and Kavist (2007) as cited in Baker and Tanrikulu (2010). The study found that both age and gender were not significantly related to cybercrime victimisation. This result implied that school students were victimised irrespective of age and gender. The study also illustrated that victims of cyber bullying were forced to contend with a range of psychological problems. The authors observed that counselling programmes for victims of cybercrime, especially child victims was mandatory and a compelling need to help protect children from the severe consequences that victimisation had on them (Baker & Tanrikulu, 2010).

The financial impact of cybercrime was also studied by some authors. For instance, Feltcher (2007); Tan (2002) as cited in Bernat and Godlove, (2012) found that governments became victims of cybercrime and measures put in place to reduce infiltration in their computing systems. Government institutions were not as frequently and gravely targeted as compared to the general population. Individuals and private financial institutions mostly encountered financial losses due to cybercrime victimisation by way of harassment, bullying and stalking. Financially, cybercrime cost about
£1,000 (i.e. around Rs. 9,700) per household each year in UK and US$ 4,000 (i.e. around Rs. 2,75,000) for an individual per annum in U.S. The study suggested that the financial impact of cybercrime affected an individual than the Government.

2.6 Reporting Behaviour of Victims of Cybercrime

The reporting behaviour of victims has often been researched in the field of victimology. However, the reporting behaviour of victims of cybercrime has not been exclusively studied. The Interdisciplinary Research Centre in Cyber Security at the University of Kent (2014), Canterbury, UK launched a survey in 2014 to explore the prevalence of cybercrime victimisation among the population with a sample of 1,502 individuals of ages 18 to 65+. Eight questions were administered on cybercrime victimisation, cyber security practices and risks that the participants of the survey came up against over the previous 12 months. The survey reported that 68 percent of respondents felt at risk of being a victim of online crime over the period of one year. 91 percent of respondents did not experience a cyber-enabled crime such as fraud, theft, online harassment, stalking and sexual offending. However, the study found that a notable percentage of respondents experienced online fraud and theft (3.9%), cyber harassment (2.9%), cyber stalking (2.3%) and some form of sexual offences (1.7%) in the year prior to the survey. With respect to the impact of online crimes on respondents, 87 percent felt no impact
at all, 5.5 percent of respondents felt emotionally and psychologically disturbed, 4.7 percent experienced a little financial impact and about 3 percent of felt a demeaned. The survey also explored the reporting behaviour of victims that included the person to whom the victimisation was reported and the reason for not reporting it. Surprisingly, nearly 85 percent did not report their victimisation to anyone while only 5 percent of victims reported their financial loss to the financial institutions. The study found that only 2.7 percent victims reported their cybercrime victimisation via an online reporting platform provided by Action Fraud, a national centre for reporting fraud and cybercrime in United Kingdom. When asked about the reasons for not reporting, eight percent of victims felt that it was a wasted effort as it did not result in any recourse for them and five percent were not aware of the modalities of the reporting.

A similar study was conducted by Buhi, Clayton and Surrency (2009) among the women students in the south-eastern colleges of U.S. The results showed that though 50 percent of respondents claimed their victimisation, only four percent approached the police for further assistance. In India, a few studies were carried out to find out the reporting behaviour of cybercrime victims. For example, Afroz and Amin (2014) found that women who were cyber-exploited did not report it to the police for various reasons such as fear of secondary victimisation and incompetency of the police.
2.7 Victims' Needs and Expectations

There is a dearth of studies on the needs and expectations of victims of cybercrime victimisation. However, some significant international scholars and publications have elaborately dealt with the needs and expectations of victims of cybercrime. The European Commission (2015) in its report on Victims’ Rights highlighted the needs and expectations of victims. Every victim develops his/her own coping strategies and the time to readjust to normalcy varies depending on various factors such as their capacity to sustain an emotional injury or hurt, the support and guidance from family/friends, the immediate assistance and reinforcements rendered to them and so on. In general, victims need respectful treatment and recognition within the justice system and more widely by society. They must be protected from intimidation and further harm, given short-term and long-term support and assistance to help them overcome the stress of victimisation, have access to the justice system and ensure they are aware of their legal rights, and understand them to be able to participate in the legal proceedings, and be liable for compensation and restoration either by the offender or by the State.

While drafting the policies and programmes for the victims in Australia, a study by Cook, David and Grant (1999) revealed that support from family and friends as well as support received from victim support agencies and other support groups were important
basic needs for victims of crime. Together with victim service providers, they further detailed a broad course of action that would necessitate a victims’ psychological well-being, emotional healing, physical security, financial recovery and an overall return to a semblance of normalcy. They are: being informed and knowledgeable about the available support services; cooperating with the legal system and providing victim impact statements as required; being open to guidance and support from family/friends, being informed and keeping abreast of police investigation; being able to make some of their own choices and regain control over their lives; accessing a coordinated and streamlined system of victim services; and being treated by family, friends, police, medical practitioners, judiciary and media in a sensitive manner.

The Stockholm Criminology Symposium (2012) held in Stockholm brought together many victimological researchers under one roof. The proceedings of the symposium which was published included the research works of several international scholars and victimologists. Modern day victimologists like van Dijk, agree that the focus of criminological research had shifted from the offender to the victim, from machine to an individual and from using criminal procedures on offenders to justice for the victims of crime. Hence, victims’ needs are important elements in the dispensation of justice by the criminal justice system. Victims’ needs are wide-ranging and depend on the intensity of the crime and the impact on the victims. Hosoi (n.d.) as
cited in The Stockholm Criminology Symposium (2012) conducted a web-survey among victims of various kinds of crimes to ascertain the needs of victims. Victims reported that to be able to get back to normal life, it was important for them to receive appropriate compensation and that the offender was to be given fitting punishment. The study revealed that with cybercrime, there was always an element of recurrence that could likely filtrate into the physical space, hence, victims needed to have access to every possible method of recovery. The survey highlighted that victims of cybercrime needed adequate legal and police support.

Whitty and Buchanan (2012) obtained data through a survey from 2,028 British adults in July 2011. The survey aimed at finding out whether the respondents lost money through online romance scams or if they personally knew someone who had lost money to this online crime. The results showed that 0.7 percent of respondents lost money and 2.3 percent claimed to know someone who had lost money to romance scams. The authors proposed that law enforcement agencies needed to make it easier for victims to report the loss of money from online romance scams and other offences related to online romance/relationships.

The study conducted by Nfuku, Sanga and Mshangi (2014) employed mixed research methods of participant observation, semi-structured interview with selected systems/network administrators and
documentary analysis from existing documents of the Government of Tanzania and FBI. Information relating to victims’ needs and expectations were ordered in three perspectives, namely, legal, strategic and technical in responding to cybercrime and protecting victims. Legal perspectives comprised, creating appropriate and effective cyber laws; an efficient forensic bureau; imposing high penalties for not only cybercrime perpetrators but also for those not reporting incidents; and training to create an awareness among all stakeholders. Strategic perspectives included revising the existing Information and Communication Technology Policy; adopting strong security policies; exercising multi-factor authentication for accessing information; and performing regular information security audits etc. Technical perspectives involved using firewalls; strictly enforcing the password policy; training employees in the use of new technology; and blocking access to exploitive sites and networks etc.

Previous research conducted in different parts of the world including India has approached the problem of cybercrime victimisation from different perspectives. The review of such existing literature presented above has demonstrated that different forms of cybercrime victimisation have been significantly increasing and there is also qualitative change in the forms of cybercrime victimisation. The review has clearly established that most of the research hitherto conducted particularly in India is at the micro level with a small sample size. There is a felt need to undertake an extensive research
with a large sample size and to examine the issue of cybercrime from victimisation point of view. Therefore, the present research was carried out with the aim to fill the gap and enrich the existing literature both in the field of victimology and in the area of cybercrime victimisation.