CHAPTER 2

REVIEW OF LITERATURE

As a post-modern form of offence, cybercrime has been a concern attracting the attention of researchers for some time. A review of earlier studies conducted on this issue has been presented in this chapter. The literature is useful to take stock of the current status of research studies in the area of cybercrime, to identify the gaps and to understand the significance of the present study. As observed by Semmens (2011), a literature review plays a defining role in a research study as it assists the researcher in obtaining an in-depth understanding of the issue at hand. According to Davies, Francis and Jupp (2011), literature review is an evaluative summary of the focal published work in a given field of interest.

This chapter discusses the relevant literature which the researcher reviewed on the different stages of the present research. The literature has been classified under the following heads such as 1. Characteristics of cybercrime victims, 2. Nature and extent of cybercrime victimization, 3. Causes of the victimization, 4. Reporting behaviour of the victims, 5. Attitude towards the police, 6. Impacts of victimization such as financial, social, psychological, academic and career and 7. Victim-offender relationship.

2.1 CHARACTERISTICS OF CYBERCRIME VICTIMS

The researcher acknowledged the importance of retrieving demographic information from the respondents. This section of the chapter outlines the relationship between demographic characteristics of the respondents (sex, age, education, occupation and income) and their cybercrime victimization. According to
Hutton and Haantz (2003), anyone may be a victim in cyber space, but certain demographic groups such as women, youths, newcomers to the Internet and other specific vulnerable groups are more at risk compared to others.

According to the United Nations Broadband Commission Report (2015), women aged 18 to 24 years were at a risk of cybercrime victimization. Women were likely to experience stalking and sexual harassment and other type of harassments. According to the survey report, in Europe, 18 per cent of women (9 million) in the age group of 15 years and above have experienced cybercrime victimization.

Sissing (2013) in her study found that majority of the cybercrime victims were female. The participants were young and belong to the age group of 18 to 25 years. The majority of the victims shared that they were cyber stalked through social networking sites by strangers. Significantly, none of the participants were relatives or ever romantically involved with their cyber stalkers. Fall (2012) also stated that victims were most often females and nine out of ten victims were females. Offenders were males and three-fourths of cyber stalking offenders were males.

Reyns (2010) in her study found various forms of victimization against women. 27.9% of female and 16.1% of male respondents were victims of unwanted contact. 25.2% of females and 12.9% of male respondents were victims of harassment. 18% of female respondents and 7.5% of male respondents had experienced sexual advances. Majority of the respondents belonged to the age group of below 21 years. 44% of the respondents were married and 36.8% were single. Among female respondents, 48.2% of the married women were victimized.

An exploratory study by Paulet (2009) with 302 undergraduate and graduate students found that 13% of students were victims of cyber stalking. Of the
39 victims, 64% were females and 36% were males. Further, the study indicates that there is a relationship between gender and being a victim of cyber stalking. Women were almost twice as likely as men to become a victim of cyber stalking. Of the 39 victims of cyber stalking, 9% males and 91% females feared for their safety during their stalking experience. Also, Sheridan and Grant (2007) in their study with 1,051 stalking victims found that the mean age of the victims as 32.6 years. 86.8% of the victims were females.

Hossain, Hasan, Haque, Ansar and Runa (2009) discussed on various types of cybercrime with the profile of cyber criminals and the victims. According to the study, the potential victims of cybercrimes include desperados and greedy people, gullible, unskilled and inexperienced and unlucky people.

The Baum, Catalano, Rand and Rose (2009) by Bureau of Justice Statistics surveyed 65,270 adults across the US based on a stratified multistage cluster sample. Approximately 14 out of every 1,000 adults in the United States (3.4 million people) are stalked each year (20 per 1,000 females and 7 per 1,000 males). Of the victims who were stalked, 40% are still experiencing unwanted contacts from the perpetrator. According to the survey, cyber stalking affects both men and women. However, women (75%) were disproportionate targets, especially those who are in the age group of 16-35 years, who are stalked by men. Adults aged 18 to 24 years and those who are divorced or separated experience the highest rates of stalking (34 per 1,000 individuals). The survey also reveals that a pattern of decreasing risk for stalking victimization existed for persons residing in households with higher income.

Jaishankar and Sankary (2006) in their article discussed the characteristics of the victims of cyber stalking. The majority of the victims were female. Victims
belong to the age group of 18 – 32 years often involved in a real or imagined romantic or sexual relationship with the offender. According to the author, the victims may be “member of a targeted minority group or special ethnic group, racial and religious minorities, gays and lesbians, cancer or other patients with serious illnesses, adoptive or birth parents, political or special interest group”.

Alexy, Burgess, Baker and Smoyak (2005) explored the Internet usage and the similarities of cyber stalking and stalking victimization experiences of 756 undergraduate and graduate students. Results indicated that 28 of 756 students had been victims of cyber stalking. Cyber stalking victims were likely to be victimized offline also. Overall, women were more likely to have been stalked, but men were more likely to be cyber stalked. The mean age of participants was 20.7 with 54.8% male and 45.2% female.

Spitzberg and Hoobler (2002) in their study analysed various cyber stalking victimization from 235 undergraduate communication students. The focus of the study was the exploration of the relationship between electronic stalking and stalking behaviours. The sample was 55% female and 43% male, with a mean age of 22 years.

Burgess and Baker (2002) in a study on offline and online stalking studied 656 persons. Findings of the study indicated that 11 per cent had been harassed. 61 per cent of the complainants were female in the age group of 17 to 42 years. 55 per cent belonged to the age group of 20 years and below.

LeBlanc, Levesque, Richardson, and Berka (2001) conducted a survey to assess the prevalence of stalking via the use of email and the Internet among the university’s students, faculty and staff. The survey questionnaires were sent to 600
undergraduate students and 142 faculty and staff members. The return rate for students was 28.7% (172 respondents), and faculty and staff was 9.1% (13 respondents). Of the 172 students, 3 males and 21 females (14% of respondents) reported having been stalked; five male students and one female student (4% of respondents) reported having been a stalker. Two students (one male and one female) indicated they had been both victims and stalkers.

According to the Budd and Mattinson (2000), individuals between the age group of 16 and 24 years; single people; students; those living in privately rented accommodation or flat or maisonette and those living in low income of less than 15,000 $ per annum were vulnerable to cyber victimization.

2.2 NATURE AND EXTENT OF CYBERCRIME VICTIMIZATION

This part of the chapter discusses studies and findings related to the nature and extent of cybercrime victimization. The nature of victimization refers to various forms of cybercrime victimization against women such as cyber stalking, cyber harassment, cyber pornography etc. and the extent of victimization refers to the frequency of victimization.

According to the study conducted by Sivakumar (2013) with 600 cyberbullying victims, only 19.8% of the respondents felt that they were victimized by bullying through mobile phones, however, 27.8% of the respondents felt that they were victimized by photos taken using mobile camera. Significant percentage of the respondents felt that they were victimized through email bullying (30.7%), text message (22.3%), social networking sites (13%) and chat room bullying (10.8%). According to the author, Bengaluru (Mean 164.98) tops in cyber bullying victimization followed by Delhi (Mean 149.8) and Chennai (Mean 139.73).
Fall (2012) in her comparative study of traditional stalking and cyber stalking stated that majority of cyber stalking victims have reported that the offender sent exaggerated messages of affection (78%). Approximately three out of four cyber stalking victims indicated having their online behaviour monitored or tracked (76%) or having the offender intrude into their cyber life (70%), such as adding the victim’s friends and family to their friends list and joining similar online groups. Nearly half of the cyber stalking victims (46%) reported experiencing four or more instances of electronic monitoring. 32 per cent of the stalking victims received exaggerated messages of affection or cyber-intrusions on at least 4 different occasions.

Henson (2011) in her study with 516 female respondents found that 47.1% experienced some form of cyber stalking behaviour, 18.6% had an online program hacked and 13.2% had their identity stolen online.

Reyns, Henson and Fisher (2011) studied 974 participants of potential stalking crimes and found 41% were victims of cyber stalking. Of the 41 per cent, 23 per cent were victims of unwanted contact, 20 per cent have experienced harassment and 14 per cent have experienced unwanted sexual advances and 4 per cent have experienced threats of violence.

Mala and Ramdoss (2011), in their study, observed that the women faced different types of cybercrime victimizations such as threatening mails (30%), spam mails and other unwanted mails (30%), obscene mails (18%), obscene pictures (15%) and harassment mails (7%) (N= 27).

Halder and Jaishankar (2010) have found in their study that 60 female respondents of the total 73 respondents were victims of cybercrime. The various
forms of cybercrime victimization as stated by the respondents includes abusive, obscene and dirty messages (85%), repeated mails asking to befriend them (16.7%), threat mails and messages from ex partners and husbands (50%). The other forms of victimization includes sexually teasing remarks in their social networking profiles and email (75%), hacking (48.3%), stalking (40%), phishing attack (43.8%), impersonation (61.7%), cloned profiles (50%), cyber defamation (71.7%), hate messages (41.7%), bullied (33.3%) and morphing (33.3%). Also, 45.5% were targeted for their lifestyle choices, sexuality and feminine ideologies. Similar forms of victimization were discussed by Geetha and Pagutharivu (2010).

Hensler-McGinnis (2008) in her study found that the most frequently experienced pursuit behaviours included needy or demanding messages (68%), threatening messages (50%) and pictures (5%), sexually harassing messages (47%), falsely representing the victim online (46%), spreading of rumours or embarrassing information via online services (33%), obtaining and exposing private information without permission (29%), to harass the recipient online or offline (27%). The other forms of victimization include sending pornographic images or messages (21%), electronic identity theft (16%), posted or distributed pictures online without consent (14%), disabled a computer, cell phone, etc. (7%) and having one’s whereabouts tracked using a Global Positioning System (GPS) device in a cell phone, car, etc. (2%). These findings are similar to the findings of Spitzberg and Hoobler (2002).

Sheridan and Grant (2007) in their study with 1,051 stalking victims found similarities and differences between stalking and cyber stalking. Victims were classified into four groups. The first group, “purely online” (n = 42, 4%) who were stalked online only. The second group, “cross-over” group (n = 51, 4.9%) who were stalked purely online for a minimum of 4 weeks but later experienced offline stalking. The third group, “proximal with online” who were stalked offline
but harassed via the Internet (n = 401, or 38.6%). The final group, “purely offline” who had not been harassed via the Internet at any time (n=545, or 53.5%).

Employing a snowball technique via email with a sample of 169 respondents, Bocij (2003) found that one-third of the respondents were cyber stalked. Majority of the respondents were female (62.5%) and the harassment consisted of threatening or abusive messages through email, Instant Messaging and chat rooms. The posting of false rumors in chat rooms, impersonation of individuals in email messages to friends and encouragement of others to harass or threaten the respondents were other forms of victimization.

2.2.1 Cyber harassment

Cyber Harassment includes blackmailing, threatening, bullying and constant sending of love letters in anonymous names or regular sending of embarrassing mails to one’s mailbox (Jeet, 2012) and even cheating via email. According to Dalla and Geeta (2013), harassment takes place in cyber space due to various reasons such as sexual, racial, religious, etc.

Barak (2005) in his study discussed the similarities between offline and online sexual harassment with respect to the gender harassment, the exhibition of unwanted sexual attention, and sexual coercion in both contexts. According to the researcher, gender harassment includes active verbal sexual harassment (sending offensive sexual messages, gender-humiliating comments and sexual remarks), passive verbal sexual harassment (use of offensive nicknames and online identities), active graphic gender harassment (mail or posting sexual and pornographic content online) and passive graphic gender harassment (picture and movies published on pornographic sites). Unwanted sexual attention is communicating sexual desires or
intentions toward another individual and sexual coercion is forcing the victim into sexual cooperation through online.

Beran and Li (2005) in their study with a total of 432 students from grades 7-9 reported their experiences of cyber harassment, through the use of electronic communications such as email and cell phones. More than two-thirds of students (69%) have heard of incidents of cyber harassment, about one quarter (21%) were victims of harassment several times and a few students (3%) admitted that they had harassed someone.

Finkelhor, Mitchell, and Wolak (2000) found that 6% of 1,501 respondents, between the age group of 10-17 years had been harassed online. The study focused on various forms of online victimization of youth such as sexual solicitation, unwanted exposure to sexual material and online harassment. Threatening behaviour as reported by the respondents include sending of threatening emails messages either to harm the youth or their family and friends, threats to embarrass or humiliate the individual by sending messages about them to other people, threats to post degrading stories or pictures of them on the Internet. Significantly, three fourths (73%) of the youth who reported an online victimization have also reported offline victimization.

Goodson, McCormick and Evans (2001) reported online sexual harassment experiences of 506 undergraduates when searching for sexually explicit materials online. The following were the experiences and responses of the female students during sexually explicit chatting: 12.8% of students were active participants during the discussion and 25.8% were silent observers, 5% of students posted objections to distasteful sexually explicit chat-group conversations.
2.2.2 Cyber Bullying

Peluchette, Karl, Wood and Williams (2015) in their study with 572 respondents examined the impact of risky social networking practices and individual differences in self-disclosure and personality on the likelihood of cyber bullying victimization among young adult Facebook users. Results revealed that posting indiscreet or negative content and number of Facebook friends were all strong predictors of cyber bullying victimization. In addition, most of the personality variables such as conscientiousness, extroversion, agreeableness, emotional stability and self-disclosure were significant predictors of at least some of these risky social networking practices. However, only extroversion and openness were significant predictors of cyber bullying victimization.

The General Social Survey (2009) found that 7% of Internet users aged 18 years and above had been the victims of cyber bullying in their lifetime. The most common form of bullying involved threatening or aggressive emails or instant messages, reported by almost three-quarters (73%) of cyber bullying victims and other forms of victimization includes hateful comments (55%) of the victims.

Li (2007) examined the nature and extent of adolescent’s cyber bullying experiences and other contributing factors for cyber bullying and cyber victimization. In this study, one in three students was cyber victim, one in five students were cyber bully and over half of the students have either experienced or heard about cyber bullying incidents. Culture and engagement in traditional bullying were strong predictors not only for cyber bullying, but also for cyber victimization. Gender also played a significant role, as males compared to their female counterparts, were more likely to be cyber bullies.
Ybarra, Espelage and Mitchell (2007) in their study identified four different groups namely youth with little-to-no involvement (n=1326; 81.7%); perpetrator-victims of Internet harassment (n= 205; 14.3%); victims of both Internet harassment and unwanted sexual solicitation (n= 45; 3.1%); and perpetrator-victims of Internet harassment and unwanted sexual solicitation (n = 12; 0.9%).

The Pew Internet study (2006) found that one-third of online teenagers had been victims of online harassment and thirty-nine per cent of social network users have been cyber-bullied.

Ybarra and Mitchell (2004) in their study found that 19% of Internet users were involved in online aggression, 12% were online aggressors, 4% were targets of online aggression and 3% were aggressor/targets.

2.2.3 Cyber Stalking

The University of Virginia defines stalking as behaviour wherein an individual willfully and repeatedly engages in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, torments, or terrorizes that person (Jeet, 2012). Sometimes, harassment and stalking can occur over the Internet. This is known as cyber stalking. Stalking is a gender specific crime with significantly more female victims and male perpetrators. Typically, the cyber stalker's victim is new on the web and inexperienced with the rules of netiquette and Internet safety. Their main targets are mostly females, children, emotionally weak or unstable, etc.

While cyber bullying and cyber harassment may damage an individual’s reputation or livelihood, cyber stalking is more likely to result in severe and
immediate emotional or physical harm. According to Miller and Morris (2012), the threatening nature of cyber stalking makes it more serious than mere harassment.

Fall (2012) in her study found out the various forms of victimization such as threatening or obscene email, spamming, live chat harassment, leaving improper messages on message boards or in guest books, sending electronic viruses, sending unsolicited emails, tracing another person's computer, Internet activity and identity theft.

Reyns and Englebrecht (2010) in their study found that stalking victims (9%) and cyber stalking victims (10%) were physically attacked. Victims of cyber stalking reported higher incidences of breaking and entering (13 per cent of cyber stalking victims compared to 11 per cent of stalking victims). Victims of cyber stalking were also more likely to report feeling intimidated compared to victims of stalking (15 per cent of cyber stalking compared to 9 per cent of stalking victims) and threatened more often compared to victims of stalking (21 per cent of cyber stalking victims compared to 19 per cent of stalking victims).

Sheridan and Grant (2007) in their study revealed that 40.2% of the victims received unsolicited emails, 6.2% of the respondents had first met their stalker online and 47.5% had been harassed via Internet by the stalker. Further, the study examined whether cyber stalking represents a distinct form of stalking or simply the extension of physical stalking. Overall, the findings indicate the similarities between stalking cases that range from purely online to exclusively offline. The findings of this study are consistent with the study of Barak (2005).

The analysis of a sample of over 1000 stalkers by Mohandie, Meloy, McGwan, and Williams (2006) found that 40% of the communication content
expressed love or desire for a relationship, 37% expressed some form of insult, 8% received unwanted communication and 2% offered help.

Results of the study by Haugaard and Seri (2004) revealed that 8% of the 631 respondents stated that they had perpetrated intrusive contact toward someone, 20% had been the target of intrusive contact and 1% were both the target and the perpetrator of intrusive contact. Female students were more likely to have been targets of intrusive contact.

The stalking behaviour as reported by Budd and Mattinson (2000), includes silent phone calls (45%); physical intimidation (42%); following (39%); touching or grabbing (34%); and waiting outside the victim's home (33%).

2.2.4 Cyber Pornography, Morphing and Cyber Defamation

Cyber pornography is transmitting, storing and receiving sexually explicit pictures of women in cyberspace. In morphing, the original pictures of people were downloaded by the offenders and were altered with pornographic images with malicious intention to defame them. Defamation is an act of portraying someone falsely to deprive their reputation. Cyber pornography is alarming which is evident from the following statistics. According to Sinha and Pendyala (2010), the number of pornographic websites is 4.2 million, which is 12% of total websites. The daily pornographic search engine requests are 68 million (25% of search engine request). 42.7% Internet users view pornography.

According to the NCRB (2014), in India, total cases registered under cybercrimes in the year 2014 was 7,201. Of which, 758 (10.5%) cases were related to publication/transmission of obscene and sexually explicit content and 491 persons have been arrested in connection with cyber pornography.
The Pew Research Center’s Internet and American Life Project (2010) conducted a study, examining data on sending and receiving of sexually nude or semi-nude images by American adolescents and adults. The study found that adults who belonged to the age group of 18 years and above had sent sexually suggestive images (6%) and 15% had received such sexts. The prevalence of sending and receiving sexually suggestive nude or nearly nude photos differed between age groups.

According to the State Crime Record Bureau (2009), in Tamil Nadu, in the year 2007, 70% of the cases (7 cases of the total 10 cases) registered under IT Act 2000 were related to obscene publication/transmission in electronic form, normally known as cyber pornography. 87.5% (7 out of 8) of the persons arrested were under obscene publication/transmission in electronic form. In 2009, 3 persons have been arrested under obscene publication/transmission in electronic form.

According to Sinha (2004), Delhi police investigated large number of cybercrimes, almost half of the cases were reported by women. Almost 40% target innocent victims, whose faces were morphed on pornographic websites or posted on message boards to tarnish their image. In each case, the complainant came to know that her face had been posted on the website after receiving a call on their cell phones, inquiring about a meeting place.

According to Griffiths (2000), 41% of regular female Internet users reported having received unsolicited pornographic materials, being harassed, or stalked on the internet.

According to Halder (n.d), cyber pornography is a threat to the society, especially women and children as their pictures have been downloaded by
unauthorized users for malicious purpose. The edited photo is again uploaded on different websites by creating fake profiles. Stalker employs other communication tools such as email, SMS and chat room to send vulgar and filthy messages. In addition, many also morph photographs of the victims partially or totally nude. Further, the morphed images were used to threaten the victim or victim’s family. In social networking sites, the photos of the users are downloaded from victim’s personal albums for the purposes of pornography or defamation. Later, that image was morphed with pornographic content. Sometimes, content of the message was edited by unauthorized user to send vulgar and obscene message to others known to the victim. In addition, the harasser hacks the profile information and photo to send obscene messages to friends of the owner of the profile as well as a broader audience.

2.2.5 Online frauds

According to Sullivan (2008), online social networking sites are a great threat to Internet users where personal information disclosed can potentially harm individuals even critical legal documents can be procured. The Times of India (2013) reported that stalkers access the victim’s personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim. According to Bowker and Gray (2004), in cyberspace, the victim’s identity can be easily manipulated by the perpetrators to send inflammatory messages to online discussion groups or social networks under the guise of the victim. According to Lipton (2012), the difficulty in verifying the online identity of the perpetrators is the main reason for the increase of crimes of this nature.
Nosko, Wood and Molema (2010) in their study found the association between information disclosed online and identity theft. For the purpose of the study, the personal profiles of 400 users identified from eight Canadian Facebook networks were used. The results of the study indicated that more than 63% of the users disclosed personal information such as birth date, gender, profile pictures, photo albums, tagged photos and general photos of the user as well as their social groups joined and friend’s details. Further, the users revealed education information (college/university attended) and regular update information (status, wall and mini-feed) and playful communications such as acceptance of pokes, messages, gifts and applications.

Halder and Jaishankar (2010) in their study addressed various forms of victimization through emails and social networking websites such as fake profiles (28.3%), phishing and spams mails (2.5%), cloned profiles in social networking profiles or email-id profile or chat room ID profile (41.1%). 60.3% of the respondents have not encountered any victimization because they were irregular in cyber space or they use cyber space only for professional purposes and do not use cyber space to socialize with others.

Paek and Nalla (2015) analyzed data from Korea Crime Victim Survey and the results indicated that the respondents who have received phishing attempts are more likely to be victimized by identity theft. Moreover, education level, routine online activities and fear of identity theft victimization are positively related with identity theft victimization.

McFarlane and Bocij (2003) in their study found that in eight cases the perpetrator impersonated the victim online. Four were impersonated in emails to their family/friends/Usenet groups, three were impersonated on electronic dating
sites or chat rooms, and the last victim’s credit card details were used to purchase goods over the Internet and they were mimicked in Usenet groups.

2.3 CAUSES OF THE VICTIMIZATION

The following section discusses the studies trying to understand the causes of the crimes against women in cyber space. The factors which predict the causes for the victimization are victim-offender relationship, online behaviour of the victim, etc. According to Brewster (2003), rejection by others, relationship breakup and one-sided love affair, jealously, hate and anger were some of the reasons for the victimization. Therefore, the motive can range from personal problem to financial gain which depends on victim-offender relationship. Sometimes, it can be simply for fun and pastime. In some cases, women fall victim unknowingly by giving true profile of themselves in cyber space while chatting, social networking and during discussion in weblogs, industry forums or boards, and commercial websites.

Fall (2012) in her study with 338 stalking and cyber stalking victims reported several causes such as the offender wanted to continue the relationship (30.9%), wanted to date (30.9%), jealous, possessive, insecure, to control (10.7%), retaliation, to scare, angry and upset (2.7%). The offender’s personal characteristics and background were the other reasons for the crime victimization. The offenders committed crime as they were lonely, unhappy with their own life (2.3%), alcoholic or drug abusers (1.1%), to attract the victim (1.9%), victim was alone or vulnerable (1.9%) and emotionally unstable (2.7%).

Some researchers suggest that easy availability of victims’ personal information is one important reason why they were victimized. Some of the more industrious cyber stalkers also collect personal information about their victims.
through the use of hardware devices installed on the victim’s computer to monitor key strokes, which enable the collection of passwords, PIN numbers, email accounts, and other personal information. According to Wilsem (2011) and Wykes (2007), stalkers often take advantage of the personal information stored on network sites, hard drives of personal computers, laptops, and smart phones to learn more about their victims.

Haygunde (2010) observed that most of the cyber-attacks on females were the fallout of one-sided love affairs or break-off in friendship. The cyber-attacks on women are being carried out by their former husbands after divorce. The men defame the victims on the web and also blackmail them.

Baum, Catalano, Rand and Rose (2009) found that the most common reasons victims perceived for the stalking were retaliation, anger, spite (37%), or desire to control the victim (33%). About 1 in 6 victims stated the reason for victimization as the offenders wanting to continue their relationship with the victims. 1 in 10 reported the stalking began while living with the offender. About a tenth of victims did not know why the stalking began.

Halder and Jaishankar (2009) observed that social networking users give away their vital information like residential address, marital status, age, phone numbers, likes and dislikes, etc. Even though many social networking sites provide options for using pseudo names and publication of such information as only “optional”, many first time registrants, including women, float their personal information on the web through these social networking sites without actually knowing the dangerous effect of it. This gives a huge chance for harassers to victimize the targets particularly women. The author further stated that among several factors which push women to become victims on the Social Networking
Sites, the ignorance of the policy guidelines and safety measures stands first. Majority of the women join the Social Networking Sites without checking any of such safety measures. Women are less aware of the privacy policies and safety tips of using networking sites.

Truman (2007) in a study with 983 stalking victims and 700 harassment victims found the following reasons for the victimization. 36.4% of cyber stalking victims and 19.7% harassment victims have stated retaliation/anger/spite as a possible cause for the victimization. To control the victim is another reason stated by 32.5% of cyber stalking victims and 12.8% of harassment victims. Offender initiates the crime to keep the victim in relationship was another reason stated by 15.7% of cyber stalking victims and 7.2% of harassment victims.

Fox (2001) explained that many people volunteer personal information to organizations for the sake of convenience (e.g., banking and retail membership discount cards), thus leaving the Internet “door” open for would-be offenders who keep track of a victim’s routine activities by monitoring their online behaviours. Cyber stalkers may also use spyware software, which is available free over the Internet or for purchase. Thus, it is clear that Information technology paves way for the stalkers with exclusive set of tools to gather information about their victims. In addition, it provides anonymity (Doring, 2000; Citron, 2009) and lets stalker scot free. Therefore, easy availability of information online (Mustain& Tewksbury, 1999) is one of the primary reasons for the increase of cybercrimes against women.

According to Ogilvie (2000), the motivations behind cyber stalking were precipitated by a breakup or relational rejection, and offenders were driven by the desire to either initiate or mend a relationship.
According to Zona, Palarea and Lane (1998), the motives for the crime victimization are to intimidate, control, or seek revenge after rejection, relationship break-up and termination from employment.

A few researchers used the criminological theories to understand the causes of cybercrime victimization. Victim’s lifestyle and routine activity, over exposure, lack of awareness and safety measure in cyber space were some of the factors for online victimization. The relationship between these variables and certain characteristics of the victims prone to the victimization have been discussed by various criminological theories. The two theories which could be applicable to the phenomenon of cybercrime victimization are Lifestyle Exposure Theory and Routine Activity Theory. Various researchers have attempted to apply the lifestyle and routine activity perspectives to explain opportunities for online victimization.

According to Hindelang, Gottfredson and Garofalo (1978) and Cohen and Felson (1979), exposure, proximity to potential offenders, guardianship, and target attractiveness are conducive to creating opportunities for victimization in cyberspace. Besides, individual’s online lifestyle activities such as spending time online, engaging in online deviance may be another predicting factor for the victimization.

Strawhun, Adams and Huss (2013) found that those who spent more time on general Internet forums such as Twitter and Facebook were more likely to encounter problems with other individuals.

A study by Reyns, Henson and Fisher (2011) provided a support for cyber lifestyle-routine activity theory to explain cyber stalking victimization. Online exposure and proximity proved to have the weakest relationships with victimization.
Online target attractiveness and guardianship had moderate effects on cyber stalking. Finally, online deviance had the strongest effect on all forms of victimization. The victim’s past deviant Internet behaviour includes downloading pirated media, contacting someone in a threatening manner, and sending sexual images. Individuals who engaged in deviant online behaviour were found to be 14 times more likely to be victims of cyber stalking. The above finding that participation in online activities increase the risk for cyber victimization is in line with the findings of Holt and Bossler (2009).

Marcum (2009) in a study found the association between the nature of victimization and online exposure, target attractiveness and lack of guardianship. Exposure and lack of guardianship both increased victimization risk for online harassment, while the presence of capable guardianship actually increased risk of receiving unwanted sexual materials.

Contrary to the above researchers, Paullet, Rota and Swan (2009) in a study with 302 students found that there is no correlation between frequent use of the Internet and becoming a victim of cyber stalking. But, students who were victims of cyber stalking were more likely to receive harassment by email, text messaging, and social network sites. The study also reveals that all the respondents used email, majority of them accessed Social Networking Sites (70%), and 60% used instant messaging. It is explicit in author’s conclusion that the victims of cybercrime are more likely to experience re-victimization.

2.4 REPORTING BEHAVIOUR OF THE VICTIMS

The study by Feuer, Bianca, and Psy (2014) with 279 adults, was to examine specific behaviours associated with reporting cyber stalking. The results
indicated that victim-offender relationship, especially stranger, the participant's gender being female, and the combination of the two in addition to the presence of high severity cyber stalking behaviours would increase the likelihood that victims would report. Significant differences were noted in the results that women were more likely to report cyber stalking than men.

Halder and Jaishankar (2015) in their baseline survey among 70 respondents revealed that only 34.3% were willing to report the cases to the police. 61.4% of the respondents stated that they did not want to report to the police because they felt reporting was not necessary (12.8%), or police was worthless in such cases (2.9%). Significantly, 18.6% and 27.1% did not report due to fear of media flash and unwanted harassment to the family members respectively.

Fall (2012) in her study found that cyber stalking victims were less likely to contact the police than traditional stalking victims. The cyber stalking victims felt that they can deal with the problem by altering their accounts, changing passwords or blocking the perpetrator from electronically contacting them.

Mala and Ramdoss (2011) in an empirical study among female students of a university, to find out their attitude towards cybercrimes, found that 32% of the respondents were victims of cybercrimes (N=83). Only 2% of them reported their victimization.

Reyns and Englebrecht (2010) in their comparative study on stalking and cyber stalking explored various factors associated with reporting the victimization to the police such as the seriousness of the offense, victim-offender relationship and the prior record of the offender. Stalking victims (29%) and cyber stalking victims (25%) have contacted the police. Overall, victims of both stalking and cyber stalking
reported similar levels of seriousness. Three indicators of seriousness were positively associated with cyber stalking victim’s decisions to contact the police - intimidation, financial impact and career impact. Study shows that cyberstalking victims whose offender was an intimate partner were significantly more likely to contact the police compared to victims whose offender was a non-intimate, non-stranger (e.g., friend, co-worker). Victims who reported feeling intimidated were over three times more likely to contact the police when compared to victims who did not report feelings of intimidation. The more significant the financial loss, the more likely a victim was to contact the police. Further, victims who lost time at work were over two and a half times more likely to report to the police. Victims who felt afraid were four and a half times more likely to contact the police than victims who did not report being afraid.

Avdi (2010) in a study with 531 undergraduate students found that crime-reporting behaviour varies by the severity and the consequences of crimes. The findings of the study indicated that gender, race, citizen interaction with the police, police behaviour, attitudes towards the police, and fear of criminal retaliation are the most reliable crime-reporting predictors.

A study by Paulet, Rota and Swan (2009) with 39 victims from 302 participants observed the following reporting behaviour among the victims. 5 males (21%) and 19 females (79%) of cyber stalking victims have reported their victimization. Of those who did not report the cyber stalking were 9 males (60%) and 6 females (40%). Women were four times more likely than men to report the cyber stalking experience. A total of 34 students reported the cyber stalking either to law enforcement (3 males and 17 females), their Internet service provider, cell phone provider or web administrator. Of the 34 students who reported the cyber stalking, only 11 victims had received help.
According to the Baum, Catalano, Rand and Rose (2009), the most common reasons for not reporting stalking victimization to the police were that it was a private or personal matter or less serious. About 40% of victims stated that police were contacted once regarding the stalking, while 3% of victims stated that police were contacted in excess of 15 times. Stalking victimization was most often reported to the police by the victim (83%), the victim’s family (26%), friend or neighbor (12%).

Halder and Jaishankar (2008) observed the reasons for not reporting the crime to the police which include fear of being tracked, re-victimization, lack of trust in authorities and widespread victim blaming.

Sheridan and Grant (2007) in their comparison of groups with different degrees of cyber-involvement in stalking, indicated that victims in their purely cyber stalked category were more likely to report that police took them seriously.

The National Crime and Safety Survey (1993) explored various factors for reporting the crime to the police. The decision to report crimes to the police is influenced by factors such as personal characteristics of the victim, perceptions about the seriousness of crime incident, previous crime experiences, victim-offender relationship, the likelihood of compensation for personal harm or property damage or loss and attitudes toward the police and the justice system in general. The findings of the survey are consistent with the findings of Skogan (1984).

### 2.5 Attitude Towards the Police and Outcome of the Case

According to Baum, Catalano, Rand and Rose (2009), the most common police response was to take a report. 17% of the respondents stated that police gave
self-protection advice and 8% of the respondents stated that the police arrested the perpetrator. Nearly 20% of victims stated that the police took no action when contacted. Victims were equally likely to perceive that no action was taken by law enforcement because police did not want to get involved (29%), had no legal authority (18%) or were inefficient or ineffective (16%). About 50% of victims perceived the stalking situation remained the same after contacting the police. Regarding the outcome of the case, a fifth of victims filed charges against the stalking perpetrator. Of those individuals filing charges, 3 out of 10 victims stated the outcome was still pending and the problem is under control, or stay away order was issued to deal with the offender. Victims were equally likely to report being satisfied (46%) or dissatisfied (49%) with the Criminal Justice System’s responses to their stalking incident.

Finch (2001) undertook 40 interviews with victims of stalking and identified the reasons for the victim’s dissatisfaction towards police complaint which includes a dismissive attitude to the conduct, police perceptions that the conduct is a private matter between the parties, a disinclination to intervene, particularly in cases where the stalker is unknown or there is no proof or corroborating evidence of the behaviour and failure to keep the victim informed of progress of the investigation into the complaint.

Sheridan and Davies (2001) in their study with 95 stalking victims found that 33% of respondents felt that the police had been very helpful, with 19% reporting satisfaction with the way their cases had been treated. The study revealed that 41% of the victims expressed dissatisfaction with the way police had dealt with their cases. Nearly half of those who took part in the survey were unhappy with the way police handled their case. One respondent reported being told by the police to ignore it.
2.6 IMPACT OF THE VICTIMIZATION

Impact refers to the effect of the victimization on the individuals. The impact of the victimization can be categorized into financial impact, psychological impact, social impact, academic and career impact. According to Fisher, Cullen, and Turner (2000), the effects of cyber stalking upon an individual may include behavioural, psychological and social aspects.

According to Halder and Jaishankar (2011), India is predominantly a patriarchal and orthodox country and women who are victimized are mostly blamed, online victims being no exception. Stalking is a widespread and chronic problem that can significantly impact a person’s life (Obama, 2011; Sheridan et al., 2003; Spitzberg, 2002). As the offender and the victims are apart in cyber space, chances for physical attacks are very low. Therefore, the effect of cybercrime on women victims will be in a form of mental and emotional stress which range from minor misunderstanding and simple relationship breakup to major problems like suicide.

Reyns and Englebrecht (2010) in their comparative study of cyber stalking and stalking found that 18 per cent of both stalking and cyber stalking victims lost time from work due to their victimization. Approximately one-fifth of victims reported being fearful due to their victimization (22 per cent of stalking victims and 21 per cent of cyber stalking victims).

Hensler-McGinnis (2008) in her study found that certain variables such as nature of the cyber stalking, fear factor related to the victimization, the frequency, duration and intensity of the cyber stalking, the number of intrusive behaviours, the prior relationship with the stalker, the victim’s sex, the pursuer’s sex, and the academic status of the victim may predict severity of impact.
Dickinson (2006) in his study with 168 respondents (92 female and 76 male) found that eleven respondents (13%) felt fear for their safety due to the cyber stalking incidents and 8 (9%) changed daily routine activity. 15 respondents (18%) adopted personal security measures.

Bocij (2003) in his study measured psychological impact of the respondents. The result revealed that majority of the respondents indicated maximum value of ten on a ten-point scale when asked about the level of distress felt as a result of their victimization experiences.

2.6.1 Financial Impact

According to the Baum, Catalano, Rand and Rose (2009), about 3 in 10 of stalking victims had financial expense due to crime victimization. About a tenth of victims spent less than $250, while 13% spent $1,000 or more. About 296,000 stalking victims lost pay from work. Majority of the victims lost income as the result of victimization and 12% of stalking victims took leave because they were afraid of what their stalker might do or to handle court related matters, with some losing pay. Other expenses incurred as a result of the stalking were court fees, damage to property, moving expenses and expenditures related to other lifestyle changes.

A study by Hensler-McGinnis (2008) found that nine per cent (n = 41) of the study participants reported financial loss that they had incurred as a result of their cyber stalking victimization. Participants who experienced financial impact of cyber stalking have reported fairly substantial to extreme losses. The financial impact includes purchase of new cell phone and phone number, purchase of a new computer and software with stronger filters for identity protection. The other financial expense includes theft of money from bank accounts, loss of income due to
lost work time, a lost job, lost property, moving costs and legal costs for filing protection orders. Those participants who experienced financial loss as a result of their cyber stalking victimization also reported more severe victimization and psychological trauma compared to participants who reported no financial loss.

2.6.2 Psychological and Social Impact

According to Sissing (2013), psychological effects as a result of cyber stalking victimization can range from stress, hurt, paranoia and betrayal to anger, fear and in some cases even depression. One of the study participants described her experience as a violation of privacy which left her feeling naked for a while. Other impacts stated by majority of the respondents were sleep disturbances, constant worry and paranoia, poor concentration and the fear of being watched. Most of the research participants have changed their contact details and terminated friendships.

In a study by Fall (2012) revealed that cyber stalking victims were more concerned with damage to their reputation when compared to traditional stalking. 89 per cent of both groups experienced emotional and/or physical effects as a result of being stalked. Sleep disturbances were the most frequently stated impact by both the groups. Cyber stalking victims frequently cited an increase in distrust whereas traditional stalking victims most often mentioned anxiety. Further, the result indicated that traditional stalking victims showed greater signs of intrusion, avoidance and hyper-arousal symptoms than cyber stalking victims. Moreover, victims of both online and offline stalking showed slightly more psychological disturbances than victims contacted through the Internet only.

Henson (2011) observed that female respondents reported higher levels of fear than male respondents when experiencing unwanted contact and unwanted
sexual advances. There was a significant and positive relationship between the number of times the behaviour experienced and the level of fear reported by respondents who experienced unwanted contact, harassment, and threats of violence. It was also found that there was a positive and significant relationship between the identity of the perpetrator and the level of fear reported for incidents of unwanted sexual advances, indicating that respondents reported higher levels of fear of unwanted sexual advances when the perpetrator was a stranger. The study further reveals that women individuals in relationships and light Internet users are significantly more fearful of cyberstalking victimization than men, single individuals and heavy Internet users.

Hensler-McGinnis (2008) observed the significant predictors for cyberstalking victimization that may predict severity of impact. The factors such as count of cyberstalking behaviours experienced and being cyber stalked by a dating/intimate partner were associated with psychological trauma.

Sheridan and Grant (2007) investigated the emotional effects of stalking on four groups of stalking victims. The most important finding in terms of effects on victims was that levels of psychological, social and financial effects did not differ significantly according to degree of cyber involvement. According to the authors, some of the impacts of the cybercrimes against women include 1) Psychological effects such as fear, sadness, anxiety, irritation, anger, suicidal thoughts and attempts, distrust, confusion, depression, weakness, sleep disturbance, loss of appetite, etc. 2) Social effects on victims such as losing touch with friends/family, changing employment/course of study, giving up social activities, low performance at work, relationship break-up, etc. 3) Financial effects such as legal expenses, annual leave used up on stalking-related problems, expense on counseling, shifting of house, etc.
Truman (2007) examined differences among intimate and non-intimate stalking. The findings revealed that overall intimate partner cyber stalking victims experienced greater levels of seriousness and severity of cyber stalking and expressed more fear than non-intimate partner cyber stalking victims.

According to the National Center for Victims of Crime (2004), cyber stalking victims experience abrupt changes in sleep and eating patterns, nightmares, hyper vigilance, anxiety, helplessness and fear for safety.

Bocij (2004) reported that victims of cyber stalking often suffer from “depression, anxiety, guilt, shame, helplessness and post-traumatic stress disorder (PTSD)”. Further, cyber stalking victims may also suffer feelings of loss of control, seclusion, self-blame, hyper vigilance and hyper activity. The victims may also experience relentless feelings of intense fear. Cyber stalking may produce distress and a forceful sense of infringement among victims.

A Handbook for Police and Crown Prosecutors on Criminal Harassment (1999) pointed out that the victims of online harassment and bullying experienced greater extent of trauma compared to victims of stalking. The severity of the psychological impact was due to “24/7 nature of online communication, inability to escape to a safe place, and global access of the information. The sense of humiliation they experienced was often increased due to the public nature of the bullying or harassment”.

According to Hall (1998), victims of stalking frequently experience a variety of physical and psychological effects. For example, psychological effects of stalking victimization often include feelings of paranoia, fear, anxiety, and post-traumatic stress symptoms, while physical symptoms may consist of appetite
disturbances, headaches, asthma attacks, persistent nausea and chronic sleep disturbance. In some cases, victims of cyber stalking are vulnerable to psychiatric disorders and suicidal tendencies.

2.6.3 Impacts on Internet usage, Academic and Career

Sissing (2013) observed that half of the research participants have reduced their involvement in electronic communication due to their cyber stalking victimization. Some of the research participants reported that they are more vigilant and cautious regarding online security when they engage in electronic communication. Some of the research participants prefer to completely disengage themselves from electronic communication.

According to Baum, Catalano, Rand and Rose (2009), about 1 in 8 of the victims lost time from work because of fear for their safety or court related matters. Seven per cent of victims lost time from work for activities such as changing a phone number, moving, or fixing or replacing damaged property. For 1 in 7 of the victims, a day or less was lost from work. More than half of victims lost 5 or more days from work. About 130,000 victims reported that they were asked to leave their jobs because of the victimization.

Hensler-McGinnis (2008) in her study found that 56.2% of the students had impact ranging from a little bit to extreme depending on various factors. The factors contributing to academic/career impact includes offender’s gender, fear of victimization and the frequency of the victimization. Out of 56.2%, approximately 6 to 9% of university students reported major disruptions to their courses of study, including taking incompletes or withdrawing from courses and transferring schools. Further, the victims had limited disclosure of their personal information on the
Internet (74.3%), blocked the electronic accessibility (65.7%), decreased use of Internet, cell phone, etc.

Ybarra, Espelage and Mitchell (2007), in their study found that cyber bullying victims were less able to concentrate at school. Bunking classes and receiving detention and suspensions from school were some of the academic impact on the victims.

According to Beran and Li (2005), students who are bullied only in cyberspace and students bullied both in cyberspace and school, experience difficulties at school such as low marks, poor concentration and absenteeism. Other issues related to cyber bullying and victimization were emotional distress, depression, school problems, substance abuse, delinquency, etc.

Pathe and Mullen (1997) indicated that half of their sample of 100 victims reported a decrease or a cessation of work or school attendance due to incessant telephone calls or other disruptions at the victim’s workplace, or to absenteeism related to court attendances or medical appointments. Over a third of victims altered their workplace, school or career as a direct result of the stalking, and approximately 40% relocated their residence one or more times.

2.7 VICTIM - OFFENDER RELATIONSHIP

The perpetrators of cybercrimes exploit various tools and methods to cause victimization in society. Some of the tools employed by the offenders to contact the victims include email, IM, the Internet, PDAs, cellphones, faxes and pagers.

Carter (2013) in her study found that the participants had access to social media sites compared to those with limited or no access. Participants varied in the
hours per day they access social media sites, months to over three years. Facebook was reported as the most utilized social media site compared with other sites. He also reveals that the highest rate of cyber bullying was found among Facebook users. A significant correlation for the use of Facebook and bullying was reported.

Fall (2012) in her study found that nine out of ten respondents knew their perpetrators. She also stated that over half of the cyber stalking group (53%) consisted of offenders that were current or prior romantic partners, while a little more than a third of the traditional stalking group (38%) were intimately involved with the victim. Overall, the data suggest that cyber stalking offenders were more closely known to their victims, as this group included more romantic partners and friends and fewer strangers as perpetrators than the traditional stalking group. The most common forms of Internet contact for both groups were through social networking sites and email, followed by instant message or other chat forums.

According to Reynolds, Henson, and Fisher (2011), 42% of the students who used online social network sites admitted to being victims of cyber stalking. Other factors increasing the chance of victimization include the frequency of updating one’s account and adding strangers as friends.

According to Wilsem (2011), greater use of technology and online tools for communication including webcams, chat rooms, social media and online dating sites enhance the level of transparency a person has in the digital world and can expose them to vulnerabilities.

According to the Pew Research Center’s Internet and American Life Project (2010), the majority of sexters reported sending sexts to someone with whom they shared a sexual relationship (82%, n = 43). 41% (n = 21) of the sexters had sent
a sext to a friend, and 31% (n = 16) have sexted an acquaintance; only two students reported sending a sext to a professor.

According to Baum, Catalano, Rand and Rose (2009), about a tenth of all victims were stalked by a stranger. Three out of four victims knew their offenders in some capacity. The stalkers were former intimate partners or a friend (21.5%), roommate or neighbor (16.4%). The communication between the victim and the offender was through email (83%) or instant messaging (35%). Electronic monitoring was used to stalk 1 in 13 victims. Global Positioning System (GPS) technology comprised about a tenth of the electronic monitoring of stalking victims.

A study by Paulett, Rota and Swan (2009) showed 13% of the 302 students sample defined themselves as having been previously cyber stalked. The majority of victims in this study knew their stalkers and 24% were former intimate partners, 21% were someone from school, 15% were friends, 9% from work, and 6% were online friends. Most of the victims were harassed through email, text message, and social networking sites. The frequent mode of contact by the stalker was through text messaging (49%).

Buhi, Clayton and Surrency (2009) in their study based on a stratified random sample of 391 college women at a southeastern university found that 2 out of every 5 stalking victims were sent unsolicited emails (45%).

Hensler-McGinnis (2008) in her study with 450 students reported that their cyber stalkers had obtained their information online (N = 131), stalkers got their information from Facebook (57) and MySpace (31). Other sources include Google, chat rooms, AOL, university directory/website and Yahoo (43). The participants reported the relationship with the offender as family members/relatives (0.4%),
friends (9.3%), service provider/customer relationship (1.3%), work colleagues (3.5%), acquaintances (16.4%), and online acquaintances/buddies (11.5%), unknown (10.4%), strangers (22.6%), dating/intimate partners (2.4%) and spouses/committed partners (0.9%).

Sheridan and Grant (2007) found that victims of only cyber stalking were more often stalked by acquaintances or strangers and less often stalked by ex-partners. The nature of cyber stalking and cyberspace environments allow potential offenders to contact or stalk people they did not know well, or did not know at all. Therefore, when a victim is stalked in cyberspace by someone known to them and in particular by an intimate partner, they may consider the occurrence more serious.

Truman (2007) in his study examined differences among stalking types by the victim-offender relationship; intimate partner stalking victims were still more likely than non-intimate partner stalking victims to have experienced a greater stalking severity.

Dickinson (2006) in his study found out the victim-offender relationship. The results clearly indicated that the cyber stalker was not often unknown to the victim. Only 22 respondents (33%) said a stranger was responsible for the incidents they experienced, while 15 (22%) attributed them to a former friend, 7 (10%) to a current friend, 14 (21%) to a classmate, co-worker or acquaintance, 6 (9%) to a former significant other and 3 (5%) to a current significant other. According to Alexy, Burgess, Baker and Smoyak(2005), most of the cyber stalkers were classmates or former intimate partners of the victims.
Patchin and Hinduja (2006) stated that the offenders contacted the victims through emails, cell phones text messages, instant messaging and online chat rooms. Similar results have been reported by Fall (2012).

According to Petrocelli (2005), cyber stalkers use email as the primary means to harass and threaten victims, far more than any other electronic communication device. Unsolicited email is one of the most common forms of harassment which includes hate, obscene or threatening mails. Ogilvie (2000) observed other forms of harassment such as sending the victims viruses or high volumes of electronic junk mail known as spamming. Sometimes, the victim will receive a mail along with a link (phishing mails) as if it was sent from a bank asking for credentials to verify the account. Innocent victims give away details and finally, they come to know the trick played by the offender. Sometimes, offender hack or hijack victim’s email account to impersonate like the victim to demand money from the victims’ contacts stating some urgent reasons. The author also stated that discussion forums are typically a place for Internet users to post opinions and comments on one or more subjects. However, discussion boards can also be a place for cyber stalkers to post harmful, negative personal information about the victim, including the victim’s name, address, phone number, email address, and other private information.

McFarlane and Bocij (2003) in their study found out that the most common method of initial Information and Communication Technology contact by cyber stalkers was email (10 cases), followed by network access at work (six cases) and Web discussion groups, for example, Usenet or bulletin boards (six cases). Other methods of contact included electronic dating sites and chat rooms, (one case each).
According to the National Centre for Victims of Crime (2003), cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, blogs and emails. The availability of free email and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment.

According to Hutton and Haantz (2003), cyber stalkers use the victim’s email address and other personal information to subscribe to or purchase books, magazines, or other Internet services without the victim’s knowledge or consent. As such, revenge and retaliation appear to be the key components of cyber stalking. Cyber stalkers have been known to send the victim’s personal information to websites relating to pornography in a hope that the site will continuously flood the victim with obscene email messages and pop-ups.

Sheridan and Davies (2001) revealed that in 20% of cases the offender was victim’s ex-husband or wife and in 28% of cases the offender was ex-boyfriend or girlfriend. The stalker was a stranger to the victim in 12% of cases. The remaining relationships consisted mainly of work-related acquaintances (7%), neighbours (16%) and clients (8%). Social Networking Sites were used in nearly half of the cases.

LeBlanc, Levesque, Richardson and Berka (2001) found that stalking via email was reported by 14 (57%) of the students and three (13%) of the students believed that their stalkers had obtained their information from email and social networking homepages.

Fisher, Cullen, and Turner (2000, 1999) reported that the majority of stalkers (80%) were known to their victims. Stalkers were boyfriends/ex-boyfriends
(42.5%), classmates (24.5%), acquaintances (10.3%), friends (5.6%), and coworkers (5.6%). Infrequently, stalkers were college professors or teaching assistants. Stalkers communicated to the victim through telephone calls (77.7%) and emails (24.7%) and other offline methods.

According to Reno (1999), the offender was likely to employ anonymous remailers to spoof the email header (email spoofing) in order to misrepresent the origin and to hide the identity of the offender. In this case, Internet service providers, law enforcement, or victims find it difficult to trace the offender.

The review of the previous studies conducted on cybercrimes and related areas helped the researchers to understand the existing knowledge on the area of research. Most studies revealed that like many other violent crimes, women are at the receiving end of cybercrimes. Many researchers asserted that majority of the victims are females and they are young. Majority of the researchers observed that most of the cybercrime victimizations are resulting from cyber harassment, cyber stalking, cyber pornography, cyber defamation and online frauds. The studies trying to understand the causes of cybercrimes are quite lesser compared to the number of studies conducted on other aspects of the study. Some researchers tried to understand the causes of victimization by studying the perception of the victims and found easy availability of victim’s personal information and ignorance and negligence of the victims as important contributing factors for their victimization. Several studies used the criminological theories to understand the motivation for cyber offending such as Routine Activity Theory and Life Style Exposure Theory. The studies attempting to understand the reporting behaviour of the victims found that gender of the offender, attitude towards the police, seriousness of the offence, victim-offender relationship, extent of the impact and certain demographics factors of the victims are some of the major factors affecting the reporting behaviour of
cybercrime victimization. As per the findings of certain studies, majority of the victims were not satisfied with the attitude of the police towards them or the way they dealt with the cases. Even though the cybercrimes are nonviolent in nature, most of the studies point towards the far reaching impact on the life of the affected. The past researchers illustrated that cybercrime victimization had financial, social, psychological, academic and career related impacts on the victims. They pointed out that the perpetrators were acquainted or related to their victims in some cases or the offenders were strangers to them in some cases. The literature on the mode of communication between the victim and the offender suggests that the main means through which the offenders contacted the victims are SMS/MMS, emails, chat rooms or discussion forums, and Social Networking Sites.

The present research is an attempt to study, inter alia, the nature and extent of cybercrime victimization of women in Chennai city of Tamil Nadu, India. The findings of the study will fill the gap in the literature pertaining to cybercrime victimization of women in the Indian context.

The methodology adopted in the present study has been explained in detail in the forthcoming chapter.