CHAPTER 5

SUMMARY AND CONCLUSIONS

5.1 BACKGROUND

Cybercrimes are crimes committed with the help of computers and internet. Cybercrime is a great threat to the society irrespective of age, gender, race, education and financial status as anything to any extent can be done with a click of the mouse. Cybercrimes can hinder the development of country as it cause a huge financial loss. Gone are those days were people used traditional methods for financial transaction. People started using internet to pay bills and to socialize with others in social networking sites. Cyber space has created new avenues for people to have wider communication with large number of people. Further, the development in Information Technology has created opportunity to use the internet to a greater extent. The stalker finds the cyber space as a medium and makes it an easy way to communicate with the potential victims to commit various forms of cybercrimes. Mostly, women are potential victims as they are accustom ed to use communicative tools such as Facebook, Twitter, Blogs, Forums, etc. to socialize with others.

Some of the cybercrimes which are frequently being committed by the perpetrators include sending viruses, spam and phishing mails, email spoofing, email bombing, email hijacking, unauthorized access to other’s system, dumpster diving, identity theft, intellectual property crimes, cyber pornography, cyber defamation, fake profile, morphing, posting abusive comments, online frauds, credit card frauds, banking frauds, denial of service attack and password attacks. Of late, some of the above crimes are being committed against women to harass them. The
The present study has found the various forms of cybercrime victimization of women such as cyber stalking, cyber defamation, cyber harassment, cyber pornography, circulating and posting photos and personal information, morphing, spam and phishing attacks, fake profiles, anonymous calls of obscene nature and vulgar and abusive SMS.

5.2 STATEMENT OF THE PROBLEM

The present study aims to understand the nature and extent of cybercrime victimization against women and its impact on them.

5.3 OBJECTIVES OF THE STUDY

The following are the objectives of the study:

1. To study the demographic characteristics of the women victims of cybercrime in Chennai city.

2. To analyze the nature, extent and causes of the victimization of women.

3. To study the victim – offender relationship.

4. To understand the impact of victimization on women.

5. To study the reporting behaviour of the victims and their attitude towards the police.

5.4 VARIABLES INVESTIGATED

The independent and dependent variables of the present study are given below:
• **Independent variables**

1. Age
2. Marital status
3. Educational qualification
4. Occupation
5. Annual Income
6. Religion
7. Community
8. Type of family
9. Place of stay
10. Online behaviour

• **Dependent variables**

1. Nature of cybercrime victimization
2. Extent of the victimization
3. Causes of the victimization
4. Victim-offender relationship
5. Mode of communication
6. Reporting behaviour
7. Attitude towards the police
8. Impact of the victimization
   a) Financial Impact
   b) Social Impact
c) Academic Impact  
d) Career Impact  
e) Psychological Impact

5.5 METHODOLOGY

The methodology employed in the present research has been presented here.

5.5.1 Research Tools

Two research tools have been used for the present study viz. a semi-structured questionnaire constructed by the present researcher and a General Health Questionnaire (GHQ), a standardized tool developed by David Goldberg (1979).

• Questionnaire

For the purpose of the present study, both closed ended and open ended questions were included in the questionnaire. Thus, a semi-structured questionnaire organized into five parts based on the objectives of the study was constructed by the researcher to collect both quantitative and qualitative data from the respondents. The questionnaire consisted of a total of 50 items.

• General Health Questionnaire

The GHQ was used to measure psychological impact of the victimization on the women victims. The tool is based on four point Likert scale with options ranging from better to much worse. The tool consisted of 28 questions divided into four parts comprising of seven questions each which intend to measure four aspects
such as somatic symptoms, anxiety & insomnia, social dysfunction and severe depression.

### 5.5.2 Study Population

The respondents for the present study were the women victims who had reported their victimization in Cyber Crime Cell, Chennai. For the present study, secondary data of the women victims who had reported their victimization to the police during the period 2009 to 2013 had been collected from Cyber Crime Cell, Chennai. During this period, totally 530 cases had been reported by women victims. Though the researcher wanted to study all the victims, due to several reasons, the researcher was able to study 205 women victims of cybercrime.

### 5.5.3 Analysis of data

The data obtained from 205 respondents have been processed using the Statistical Package for Social Sciences (SPSS version 21.0). Descriptive statistics was employed to obtain the frequencies and percentages. Inferential statistics such as Chi-square, t-test and ANOVA have been used to extract valid information and to draw corresponding conclusions for the variables chosen under this study.

Items in the GHQ 28 have been given the scores 1-2-3-4 using the Likert scale. For each of the four aspects such as somatic symptoms, anxiety & insomnia, social dysfunction and severe depression, individual mean has been calculated to compare which particular aspect of the trauma is more among the respondents.

### 5.6 MAJOR FINDINGS OF THE STUDY

The major findings of the present study have been given here under different sub-heads:
5.6.1 Demographic characteristics of the respondents

- A significant per cent of the respondents belong to the age group of 36 years and above (34%) and 23% of the respondents belong to the age group of 26 to 30 years.

- A majority of the respondents were married (57%), a significant per cent of the respondents were unmarried (31%) and 12% of the respondents comprised of widow, divorce and deserted.

- A significant per cent of the respondents were under graduates (42%) and 36% of the respondents were post graduates.

- A significant percentage of the respondents were employed in private organizations (46%) and 36% of the respondents were unemployed.

- A great majority of the respondents were Hindus (87%) following Christians (8%) and Muslims (5%).

- A majority of the respondents belong to Other Backward Caste (76%), Other Caste (20%) and Scheduled Caste/Scheduled Tribes (4%).

5.6.2 Nature and extent of victimization of the respondents

- A sizable per cent of the respondents faced victimization through their photos being circulated in the cyber space by the perpetrators (26%).

- A significant per cent of the respondents experienced victimization by receiving anonymous calls of obscene nature (26%). Of the 26% of the respondents who received anonymous calls of obscene nature, 11% of the respondents experienced once, 3% of the respondents experienced twice and 12% of the respondents experienced thrice and above.
• Also, 17% of the respondents received spam mails and vulgar and abusive SMS and 14% of the respondents were victimized by the creation of fake profiles and defamation.

• 12% of the respondents received threatening calls and victimized by impersonation by hacking into E-mail accounts and requesting money from persons in the contact list for financial gain.

• The respondents faced other forms of victimizations such as harassment (8%), morphing (7%), phishing mails (6%), threatening to upload offensive photos (4%), credit card frauds (4%) and stalking (3%).

• The extent of victimization of the respondents has been categorized as low (46%), moderate (30%) and high (24%).

5.6.3 Online behaviour of the respondents

• A majority of the respondents used mobile phone (62%), laptop (61%), desktop (52%) and tablet (11%) every day. A meagre per cent of the respondents occasionally use internet through tablet (1%), laptop (2%), desktop (5%), and mobile phone (6%).

• The frequently used online activity is E-mail (85%). Of the 85% of the respondents, 39% of them use it sometimes, 28% of them rarely use it and 18% of them used it often.

• Texting is another online activity used by a significant per cent of the respondents (75%). Of the 75% of the respondents, a significant per cent of them use it rarely (39%), sometimes (28%) and often (8%).

• 40% of the respondents involved in chatting. With regard to online Social Networking Sites account, 47% of the respondents had one
account, 2% of the respondents had two accounts and 1% of the respondents had more than three accounts.

- Among the account holders of the Social Networking Sites, a majority of them were using the Social Networking Sites for the last 5 years (91%). A significant per cent of the respondents had their profile with half-truth and half-false information (55%).

- 40% of the respondents had genuine profile, 3% of them had three-fourth of true information and 2% had fake profile. While a majority of them secured their social networking account (93%), a small percentage of the respondents had not secured the accounts (7%).

- A majority of the respondents had online friends between 101 and 300 persons (53%). A significant per cent of the respondents had less than 100 online friends (42%) and a meagre per cent of the respondents had online friends between 301 and 600 persons (6%).

- A majority of the respondents revealed their name (97%), profile picture (83%), date of birth (81%), marital status (72%) and interest (59%), email ID (53%). A sizable per cent of the respondents revealed their gender (38%), contact numbers (25%), family photos (24%), friend’s photos (18%), job title (14%), address (10%), scenery (6%) pet’s picture (5%), and other information (2%).

- 20% of the respondents opened unfamiliar attachments and similar per cent of the respondents opened web links from their email account (20%). A notable per cent of the respondents stated that they did not mind sharing their passwords with others (16%). 15% of the respondents deleted suspicious E-mails and similar per cent of the respondents preferred storing important files online (15%).
5.6.4 Causes of the victimization

- 29% of the respondents stated that financial gain was the cause for their victimization. One-fourth of the respondents said defamation was the cause for their victimization (25%). 22% of the respondents observed hate and anger was the cause of their victimization. 21% of the respondents stated that character assassination was the cause of their victimization.

- 17% of the respondents said that fun and obsession for love were the causes of their victimization. 16% per cent of the respondents observed revenge as the cause for their victimization. The other causes cited by the respondents for their victimization include sexual perversion (9%), ego (8%) and jealousy (8%).

5.6.5 Victim-offender relationship

- The most common communication tool employed by the offender as stated by the respondents was mobile phone (43%). A significant per cent of the respondents stated that the perpetrators contacted them through email (39%). 27% of the respondents were contacted through Social Networking Sites by the perpetrators. A meagre per cent of the respondents were contacted through telephone (4%), chat room (2%) and instant messenger (1%).

- Majority of the offenders who committed cybercrimes against the respondents were male (61%). One-fourth of the perpetrators constitute friends and relatives (25%) and strangers (24%).
5.6.7 Reporting behaviour of the respondents

- A majority of the respondents said that the reason for reporting the victimization was to trace the offender (51%). About half of the respondents reveal that the reason for reporting the victimization was to secure themselves from re-victimization (45%). A significant percent of the respondents reported the victimization to stop the issue getting worse (41%). The other reasons stated by the respondents for reporting the victimization include ‘felt the issue more serious’ (36%), ‘to get back the lost money’ (24%), ‘to punish the offender’ (23%), ‘to prevent misuse of personal data’ (19%) and ‘disturbed persistently’ (18%).

5.6.8 Attitude towards the police and the outcome of the case

- Majority of the respondents agreed that police were very supportive (84%). However, 14% of the respondents disagreed that police were very supportive.

- A majority of the respondents perceived that they were treated well by the police (84%) and 12% of the respondents disagreed with that.

- A significant percent of the respondents disagreed that police handled their case satisfactorily (44%). Further, a sizable percent of the respondents disagreed that the police were well-equipped to deal with cybercrimes (36%).

- A significant percent of the respondents stated that no action was taken by the police on their complaints (46%). 16% of the respondents observed that the police closed their complaint without taking any action.
• 12% of the respondents stated that the police warned the perpetrators. 8% of the respondents withdrew the complaints due to fear of publicity and revenge from the perpetrator. Similar per cent of the respondents stated they do not know about the outcome of the case (8%).

5.6.9 Impact of victimization on the respondents

➢ Financial Impact

• A significant per cent of the respondents had lost their money due to online fraud and cheating (44%). 26% of the respondents stated other financial impacts such as sold their property, pledged their jewels, availed bank loans and borrowed money from others for interest due to the victimization. A meagre percentage of the respondents suffered the following financial impact due to the victimization such as legal expenses (10%), loss of job (9%), loss of pay (4%), bribing the police (3%), demotion (3%) and coping expenses (2%).

➢ Social Impact

• A significant per cent of the respondents were blamed by their husbands for their victimization (31%). 23% of the respondents were verbally abused by their husbands. 21% of the respondents stated that there was a misunderstanding between them and their husbands due to the victimization. The other social impacts of victimization from the spouses include lost trust (8%), deleted SNS account (5%), deserted (5%), sexual abuse (3%), issued divorce notice (3%) and sent to parent’s place (3%).
• 17% of the respondents experienced loss of reputation from friends. 9% of the respondents suffered loss of faith from their friends. 6% of the respondents were subjected to harassment by their friends and 5% by the relatives, 5% by the in-laws and 2% by their parents due to the victimization. A small per cent of the respondents were blamed for their victimization by the relatives (7%), 6% by friends, 6% by their parents and 5% by the in-laws.

➢ Career, Academic and Internet Impact

• A significant per cent of the respondents stated that their ability to work had reduced due to the victimization (37%). 19% of the respondents said that the time spent on the office had decreased as they have to take leave often to follow up the case. 18% of the respondents stated they lost their concentration and were unable to continue the job due to the victimization.

• Of the 205 respondents, 12% of the respondents were pursuing their studies at the time of victimization. A significant per cent of the respondents had lost their concentration on studies due to victimization (48%).

• A significant per cent of the respondents were watchful and alert on the internet usage after the victimization (32%). One-fifth of the respondents reduced the online activities due to the victimization (20%). 17% of the respondents stopped posting pictures and 12% deleted their E-mail IDs. 8% of the respondents stopped using the internet due to the victimization.
Psychological Impact

- Findings on overall psychological impact indicate that 23% of the respondents had low psychological impact, 64% of the respondents had moderate psychological impact and 13% of the respondents had high psychological impact due to the victimization.

- Based on the mean sub-scores, it was found that most of the respondents experienced anxiety and insomnia, followed by social dysfunction and then somatic symptoms and finally severe depression got the least mean sub-score.

5.6.10 Associations

- There is a significant difference between the income of the respondents and the extent of victimization ($P = 0.003$).

- A highly significant difference is found between the type of family of the respondents and the extent of victimization ($P = 0.000$).

- There is a significant difference between the marital status of the respondents and the impact of victimization ($P = 0.000$).

- There is a significant difference between the reporting behaviour of the respondents with respect to age ($P=0.048$), educational qualification ($P=0.001$) and the community ($P=0.002$) of the respondents.

- A significant difference was found between age of the respondents and their attitude towards the police($P=0.005$).
There is a highly significant difference between online behaviour of the respondents with respect to age (P=0.000), marital status (P=0.000), educational qualification (P=0.001) and occupation (P=0.000). The null hypotheses were rejected at 1% level of significance.

A significant difference is found between online behaviour of the respondents with respect to income (P=0.029) and community (P=0.025). The null hypotheses were rejected at 5% level of significance.

There is a highly significant association between posting photos and personal information online by the perpetrators and revenge (P =0.000) at 1% level of significance.

There is a significant association between morphing and sexual perversion of the perpetrators (P = 0.002) at 1% level of significance.

There is an association between sending vulgar and abusive SMS by the perpetrators and character assassination of the respondents (P =0.013) at 5% level of significance.

A significant association is found between extent of victimization with respect to the reporting behaviour(P = 0.001), psychological impact of victimization (P= 0.003) and attitude of the respondents towards the police (P= 0.000). The null hypotheses were rejected at 1% level of significance.

An association is found between the level of impact of victimization with respect to the online behaviour(P =0.037) and the level of attitude towards the police (P= 0.004). The null hypotheses were rejected at 5% and 1% level of significance respectively.
An association is found between the level of psychological impact with respect to the level of online behaviour (P = 0.026) and the level of attitude towards the police (P = 0.006). The null hypotheses were rejected at 5% and 1% level of significance respectively.

A highly significant association is found between victim-offender relationship with respect to the extent of victimization (P = 0.000), level of impact of victimization (P = 0.007) and the level of reporting behaviour of the respondents (P = 0.016). The null hypotheses were rejected at 1% and 5% levels of significance respectively.

It was found through Spearman’s rank correlation test that there is 23% positive relationship between extent of victimization and the social impact of victimization of the respondents and is significant at 1% level of significance.

17% positive relationship was found between extent of victimization and the psychological impact of victimization of the respondents and is significant at 5% level of significance.

There is 22% positive relationship between extent of victimization of the respondents and the causes of victimization and is significant at 1% level of significance.

20% positive relationship was observed between financial impact and the career impact on the respondents and is significant at 1% level of significance.
• 16% positive relationship was found between financial impact on the respondents and the psychological impact and is significant at 5% level of significance.

• There is 17% negative relationship between financial impact and the online behaviour of the respondents.

• 39% positive relationship was found between social impact and the psychological impact on the respondents and is significant at 1% level of significance.

• There is 16% positive relationship between social impact and the causes of victimization of the respondents and is significant at 5% level of significance.

• 15% positive relationship was found between career impact and the causes of victimization of the respondents and is significant at 5% level of significance.

• 14% positive relationship was found between career impact of the respondents and their reporting behaviour.

• 14% negative relationship was found between psychological impact and online behaviour of the respondents and is significant at 5% level of significance.

• There is 16% negative relationship between psychological impact of the respondents and their attitude towards the police and is significant at 5% level of significance.
• 18% positive relationship was found between online behaviour of the respondents and their attitude towards the police and is significant at 5% level of significance.

• The multiple linear regression analyses reveal the coefficient of type of family, religion and downloading video/movie are significant and positively associated with extent of victimization. The value of R-square is0.232 means that about 23.2% of the variation in dependent variable is explained by the independent variables and R-square value is significant at 1% level of significance.

• The coefficients of the cyber defamation, posting and circulating personal information, cheating through spam mails are significant and positively associated with social impact. The value of R-square is0.330 means that about 33% of the variation in dependent variable is explained by the independent variables and R-square value is significant at 1% level of significance.

• The coefficients of marital status, social impact, posting and circulating photos and personal information is significant and positively associated with psychological impact. The value of R-square is0.233 means that about 23.3% of the variation in dependent variable is explained by the independent variables and R-square value is significant at 1% level of significance.

• Educational qualification (β= 0.230; p<0.01) and occupation (β= 0.221; p<0.01) were significant and positively associated with reporting behaviour. Nature of victimization (spam mails (β= -0.151; p<0.05), harassment (β= -0.155; p<0.05), fake advertisement (β= -0.145; p<0.05), posting and circulating personal information(β= 0.133; p<0.05), credit card frauds (β= -0.140; p<0.05) are
significant and positively associated with reporting behaviour. Career impact is significant and positively associated with reporting behaviour ($\beta=0.153; \ p<0.05$). The value of R-square is $0.252$ means that about 25.2% of the variation in the dependent variable is explained by the independent variables and R-square value is significant at 1 % level of significance.

5.7 LIMITATIONS OF THE STUDY

The present study included only the women victims of cybercrime and the men victims were not included in the study. The present study focused only on reported cases of cybercrime victimization in Chennai city for the period of 5 years from 2009 to 2013. The researcher was unable to include all the women victims of cybercrime who had reported their victimization due to several reasons such as shifting of their place of residence and the unwillingness to participate in the study. There could be many more women victims of cybercrime who had not reported their victimization. The present study has not included the unreported cases. The present study is confined to Chennai city due to unavailability of the data concerning the cases of cybercrime victimization by women in other parts of Tamil Nadu. The present research does not have a control group of the non-victims. The causes of victimization have been studied from the perspective of the victims who have reported their cases to the Cyber Crime Cell and the findings of the study do not reflect the perspective of the perpetrators on the causes of cybercrime. The study has not included the challenges faced by the police in handling cybercrime cases. The future researchers may dwell upon these limitations.

5.8 CONCLUSIONS

Based on the findings of the present study, the following conclusions have been drawn:
• With regard to the demographic characteristics of the respondents, most of the victims are in the age group of 26 years and above. Majority of the respondents are married and most of them are graduates and post graduates. Majority of them belong to the Other Backward Caste. Most of them belong to nuclear family.

• The cybercrime victimization shows a pattern of decreasing risk, as the income level of the victims goes up.

• Women in cyber space are likely to face the following nature of cybercrime victimization such as circulating photos, anonymous calls of obscene nature, online hacking and misuse, fake profile, defamation, threatening calls, impersonation by hacking, harassment, morphing, phishing mails, stalking, etc.

• The causes for cybercrime victimization of women include financial gain, defamation, hate and anger, character assassination, entertainment, obsession for love, revenge, sexual perversion, ego, jealousy, etc.

• One-third of the women victims of cybercrime are likely to receive vulgar and abusive SMS intended for character assassination.

• One-third of the women victims whose photos and personal information were being circulated in the cyber space is primarily because of the revenge on the part of the perpetrators.

• One out of five women victims of morphing is likely to be harassed by the perpetrators for their sexual perversion.

• Unmarried women are more likely to spend more time on internet than married women.
• Though everyone use internet irrespective of their education level, the frequency of internet usage is more among highly educated people.

• Women who are working in private organizations frequently use internet.

• The women who share their passwords with others are more likely to face crime victimization in cyber space.

• Those who have relatively high online exposure are likely to have positive attitude towards police.

• The perpetrators of cybercrime against women use email, Social Networking Sites and mobile phones to contact the potential victims.

• Majority of the offenders of cybercrimes against women are male.

• Women face cybercrime victimization more from known individuals than others. Close to half of the perpetrators of cybercrime against women are known to the victims of cybercrime. The perpetrators include friends, relatives and the acquaintances.

• The women victims of cybercrime are more likely to complain to the police, if the perpetrators are known to them.

• The various reasons for reporting cybercrime victimization to the police are to trace the offender, to secure from re-victimization, to stop the issue form getting worse, to get back the lost money, to punish the offender, to prevent misuse of personal data, alert others and create awareness, etc.
• Mostly, police are kind enough and offered a seat to the women victims of cybercrimes. However, for some women victims of cybercrime, police are indifferent, reluctant to file case, blaming, humiliating and rude.

• Police are supportive and treat the women victims well. Further, since the police are not well-equipped, they are unable to handle cases of cybercrime satisfactorily.

• In almost half of the cybercrime cases reported by the victims, no action is taken by the police. The other outcome of the cases include police closes the complaint without taking any action, warned the perpetrators, victims withdrew the complaints due to fear of publicity, revenge from the perpetrator, etc.

• It appears that police do not take any concrete action on the complaints by the women victims of cybercrime.

• The women victims aged 36 years and above are most likely to have negative attitude towards police.

• Highly educated women victims of cybercrimes are more likely to report their victimization to the police.

• The women victims of cybercrime who have high level of the extent of victimization are likely to receive better treatment from the police.

• The women victims of cybercrimes belong to Other Caste are more likely to report their victimization.

• Close to half of the women victims of cybercrime are likely to have financial impact on them.
• One out of four married women victims of cybercrime suffer social impact from their husbands, which range from blaming to issuing divorce notice due to the victimization.

• Some women victims of cybercrime suffered various forms of social impact from their friends, relatives, in-laws and parents.

• Cybercrime victimization affects the women’s ability to work and loss of concentration in their studies.

• The cybercrime victimization is likely to influence the women victims to be watchful and alert and in some cases the victims tend to stop using internet.

• The women victims of cybercrime who are likely to have high extent of victimization are more likely to have severe psychological impact on them.

• Those who have good exposure and awareness on the internet are likely to have low impact of victimization.

• The women victims of cybercrime with higher psychological impact have negative attitude towards the police.

5.9 SUGGESTIONS

The following suggestions have been made from the field experience of the researcher and findings of the present study.

• **Cybercrime unit**: There should be cybercrime unit in every police station for receiving complaints of cybercrimes and investigation of cybercrimes. The presence of more women police officers in
cybercrime units may encourage more women victims to come forward and lodge their complaints without any fear of secondary victimization. The cybercrime victims should be informed about the progress of the case by the police. It is the responsibility of the police to keep them informed.

- **Training**: The police training module should enable that all police officers should be given a basic literacy on internet and telecommunication services, so that they can have the basic understanding of cybercrimes. Those police officers who are dealing with cybercrimes should be provided periodical in-depth training programs to keep them updated and technically competent to investigate the emerging forms of cybercrimes.

- **Victim Crisis Centre**: Victims Crisis Centres (VCC) should be setup by the State government to provide support and assistance to the women victims of cybercrimes. The centre should provide counselling to the victims, immediate family members and legal assistance on a need basis. The police can also collaborate with Non-Governmental Organizations (NGOs) for providing the services to the victims.

- **Helpline**: Toll-free helpline should be introduced by the police department exclusively to receive complaints regarding cybercrime victimization. This will facilitate the women victims to make the complaints of cybercrime victimization without any fear or intimidation.
• **Awareness:** Workshops and seminars should be conducted in all schools and colleges to create awareness on cybercrime victimization. Further, short duration courses can be conducted with a minimal fee by public and private sectors to teach the public about security measures needed to be adopted while using emails, social networks, messaging services, discussion forums, online banking services, mobile phones, etc.

• The State government should produce documentaries to create awareness and sensitization on cybercrimes, victimizations and the related laws. Efforts should also be initiated to screen such documentaries in public malls, theatres, bus terminals, railway terminals and in other places where public gather in huge number.

• The women should not respond to spam mails, fake job mails, online lottery mails and SMSs, etc. In case of receiving such mails, the women should forward the same to the cybercrime unit immediately to prevent potential cybercrime victimization.

• The personal details of the victims should not be disclosed in media without the informed consent from the victims.

• **Internet usage:** Self-defense is the first step to control cybercrime. It is the duty of every netizen to adopt safe practice of internet usage by not revealing personal information to others, particularly strangers.