P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

TAXONOMY AND RELATIONSHIP OF CYBERCRIMES AND SECURITY MEASURES BEFORE AND DURING COVID-19: A SEM APPROACH

Dr. (Ms.) Tarannum Mohan,
Assistant Professor, Punjabi University Regional Centre for IT and Management,
Mohali-160062, Punjab, Email Id: tarannummohan@gmail.com

Abstract

The aim of this study was to understand how most vulnerable section that is girl students classifies cybercrimes and security measures before and after advent of pandemic. In qualitative aspect, types of cybercrime and corresponding security measures were judged through personal interview of experts. The quantitative aspect used deduced dimensions to collect data from randomly selected 510 girl students from under-graduate colleges of nine major cities of Punjab. SEM analysis was applied to examine responses to latent dimensions. Four attributes of cybercrimes were classified, namely, stalking, privacy violation, financial risks and pornography. To counter these crimes three cyber security measures of general security, password protection and awareness about attacks were categorized. Lastly, significant difference was found between understanding of various cybercrimes and application of various security measures before and during pandemic.

Keywords: cybercrime, cyber security, girl students, SEM, covid-19.

Introduction

In 2017, more than 34% of Indian population accessed internet which increased to over 52% by 2020. India with 688 million internet users by January 2020 makes it the second largest internet market in the world only after China. Data shows that on an average an individual would spend 155 minutes daily on internet through smart phones whereas daily internet consumption per capita on other devices would be only 39 minutes (www.statista.com). This huge consumption of internet and being online always exposes individuals to online attacks (Geetha & Phamila, 2016). Cybercrimes are escalating at higher rate, generally virtual friends take advantage of their female friends by gaining their confidence and misuse their personal information for harassment and abuse. Moreover, attacks try to defame women by salacious emails, stalk women on dating sites or on social media, morph images for pornography etc. (Chaithanya & Veena, 2019). Still, most of the women are unaware about these crimes, until it happens with them than they come to know about the truth, but then it gets too late (Geetha & Pagutharivu, 2010). Undoubtedly, cybercrimes are easy to commit with little resources, but its damage can be huge to the privacy and security of women (Umadevi et al., 2019).

Social media has provided new way to socialize and has become part of everyone’s life. It fulfils need of curiosity to know what is unknown along with giving opportunity to discover untried paths (Obar & Wildman, 2015). It helped women to fight for equality as now they can share their struggles, experiences, feelings, success, failure and emotions to whole world (Li, 2015). Internet is a boon of advanced society (Ottis & Lorents, 2015) but it also has dark side that is trapping women's life and security known as cybercrime against women. Modern innovations have provided equal rights to women and made their lives easy, but on contrary, these innovations also raised the violence against women (Singh, 2015).

Cybercrime, also known as computer-oriented crime threaten a person, organization or country's financial health and security **(**Sankhwar & Chaturvedi, 2018**)**. Cyber crime from gender perspective has been defined as "Intentionally, crimes against women with motive to hurt victim physically and psychologically, by using modern communication networks such as internet, computers and mobile phones" (Halder, et al. 2012). Privacy and security of an individual has come under at risk with the development of technology (Chang, 2020). Crimes in cyber world against person include harassment through email, cyber stalking, defamation and unauthorized control and access over computer device etc. (Kethineni & Cao, 2020).

Though literature has discussed these issues however no study examined a change in attitudes towards different types of cybercrimes, awareness levels regarding cybercrimes and cybersecurity measures to counter such attacks after covid-19. This study as highlighted studied these aspects and their effect on girl students of Malwa region in Punjab before and after setting of Covid. The study tested the hypothesis that girl students would have become more aware and adopted stringent measures to cybercrimes after Covid. This was done in three steps: firstly, attitude towards cybercrimes was summarized into groups indicating crime considered to be affecting most; secondly, attitude towards different cybersecurity measures was summarized to understand which measure was considered important and adopted; lastly, variation in importance of both attitudes with regard to summarized dimensions was inferred before and after Covid.

Conceptual framework

Cybercrime classification

Cybercrimes in the form of sexual abuse, stalking, vulgar gestures and using of obscene language through phishing, morphing and other means particularly attack women (Kandpal & Singh, 2013, Konradt et al., 2016). Cybercrimes have various versions that attackers use to disrupt. They could take the form of financial frauds, password hacking, vulgar content among others. Proper understanding of meaning of each type of attack would help in knowing ways attackers apply for an attack. Definitions of various types of attacks should be understood not only by experts but by a common user to make a significant effect on understanding (Chandra & Snowe, 2020).

Internet addiction provides significant problems and challenges related to cyber abuse. Online abuse such as online friendship and relationship abuse, cyber sexual internet abuse, criminal internet abuse and internet information abuse is a critical occupational issue (Griffiths, 2010). Bullying, aggressive behaviour and individualism have been found to increase on cyber world. However, findings revealed that highest cyber aggression has seen in Indian adolescents as compared to China and Japan (Wright et al., 2015). *Cyber Stalking* involve false allegations, threats, monitoring, identity stolen, data damage, collecting information that can use to harass (Sheridan & Grant, 2007). This is one of the most discussed cybercrimes generally, occur with children and women by adult perpetrator, or paedophiles or men (Sethi & Ghatak, 2018). Some results show (Reyns et al., 2012)

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

40.8% people experienced cyber-stalking and approximately 4.9% had perpetrated cyber-stalking. Cybercrime that involves character assassination is another online crime against women termed as *cyber defamation*. It happens when perpetrator uploads defamatory matter on social media or website or sends emails to all person's friends and family members **(**Gunjan, et al., 2013**)**. As per survey report of Centre for Cyber Victim Counselling (CCVC) 2010, around 71.1% was defamed due to cyberspace (www.cybervicitims.org)**.** Sending fake emails consisting of malicious activity in which source of sender is altered is referred to as *email spoofing* (Pandove et al., 2010). Real identity of email sender is not disclosed (Hu & Wang, 2018). It involves tricking users into innocuous looking online content that could be a malicious email or a link that would inadvertently lead to a virus attack. Hacking of email accounts and passwords is a common way of spoofing (Dinev, 2006; Anesa, 2020). *Cyber pornography* has been defined as creating sexual arousal through explicit depiction of persons in images or words through online medium (Fernandez et al., 2017, Powell et al., 2019). It involves obscenity that deals with influencing minds through obscene and vulgar content (Sahoo, 2018). Studies (Verma, 2012; Math et al., 2014) have shown how to measure awareness about cyber pornography, its measurement for different demography and its consequences both physically and mentally (Dombrowski et al., 2007; Grubbs et al., 2010). *Cyber Morphing* means taking pictures of some persons and modifying them by using computer animation in such a way that it becomes unrecognizable. Such insane activities harm infinitely both socially and psychologically to persons whose pictures have been morphed (Karnold, 2000; Halder & Jaishankar, 2011).

Huge variance in cybercrime classification could be attributed to large variance in socioeconomic, psychological and geopolitical characteristics of perpetrators. Incorporating social and contextual factors provide better understanding of cybercrime classification that could further enable better application of security measures (Ibrahim, 2016). Taking this into consideration our study intends to firstly identify these aspects among girl students and their importance in both pre and after Covid period. This study importantly attempts to classify cybercrime taxonomy by restricting effect of cyber attacks to girl students only. Different societal strata faces different types of cybercrimes and none of the studies have focussed such classification.

Cyber security measures

To mitigate the effect of cybercrimes it is vital to find possible solutions of threats posed by such crimes and what preventive measures should be taken by individuals and organizations (Boddy, 2018). Over-indulgence in usage of online mediums through different devices, negligence towards level of harm a cyber attack and lack of knowledge about cybercrimes were considered to be major reasons of cybercrime victimization (Cheng et al., 2020). Online financial transactions have become increasingly susceptible to frauds due to active interventions by cyber criminals. Institutions taking cognizance of such aggravated threat have been forced to incorporate various technological measures such as firewalls, stringent password security measures and anti-spam software. Application of such measures remains incomplete without understanding effect of cybercrimes (Epps, 2017). Security of financial transactions was found to be proportionally dependent on awareness of customers. Higher awareness and attributing importance to cyber security measures would enable mitigation of cybercrimes and secure transactions (Ali, 2019).

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

Awareness about robust, cost effective and convenient to use cyber security measures are key in their adoption. Adoption of any measure depends on understanding role of awareness, dealing and perceived threat among individuals (Martens et al., 2019). Congruence between human intervention such as inclination towards applying security measures and technology tools such was considered as an effective defence system against dangerous cyber attacks (Donalds & Osei-Bryson, 2019). Knowledge about cybercrimes would facilitate their early detection leading to application of specific security measures. For instance, certain criminal attacks can be effectively handled by using simple and easily applicable technological tools (De Kimpe et al., 2020). However, crimes involving financial frauds and vulgar messages require more measures that are serious. Taking cognisance, considering it important and reporting about cybercrime if attacked is necessary in successfully dealing with cybercrime victimization (Conteh & Schmick, 2016). Individuals who do not report as they feel embarrassed or ignore it as unimportant are more prone to be attacked again and being victims. These crimes can be reduced with tough laws from government along with providing education and awareness to people especially women (Eddolls, 2016).

Thus, it becomes important to examine awareness about cybercrimes and security measures individuals would prefer to prevent them.

Cyber Security Importance in the era of COVID-19

Past year saw world affected by Covid-19 pandemic forcing people to carry all of their personal, financial and professional activities online. This provided cybercriminals to increase their attacks exponentially. The period saw three of the biggest ransom-ware attacks affecting global companies (Cobb, 2018). Major businesses and individual users were found wanting to face severity of various cyber attacks. Security measures ranging from simple to tedious were adopted. However, people required certain skills to use and operate these measures especially that require complex processes like installing software (Chang & Coppel, 2020). Thus, robust understanding of these measures by local and less aware audience was found to be essential.

According to CSC e-Governance Service India, there is extreme rise in internet data consumption from 2.7 TB (terabyte) on March 10 to 4.7 TB on March 30, which has shown 100 percent increase in 20 days. However, such huge and sudden shift to online medium by businesses and education institutions also highlighted the vulnerabilities of the medium. Users faced risks from various types of cybercrimes as perpetrators found lot of victims easily due to lot of people shifting to online medium. Persons behind carrying out cybercriminal activities primarily targeted girls making them easy victims when online medium is so extensively used (Weil & Murugesan, 2020). A study (Lallie et al., 2020) showed that first cyber-attack pertaining to covid-19 pandemic occurred on 19th January 2020; 30 days after first reported incident in China. After that second attack occurred after 14 days. This frequency kept increasing. Study found that 86% cases involved phishing; 5% involved hacking; 65% pertain to malware whereas 34% related to financial fraud. Maximum number of these cases i.e. 25% occurred in China whereas 14% were reported from both USA and UK. Phishing cases such as asking donation for vaccine development, impersonating of communication platforms such as Zoom and Google were most prominent cyber-attacks along with extortion by threatening to infect with virus if ransom is not paid.

Above examination of literature highlights the importance of studying types of cybercrimes affecting girl students and what measures they have adopted to mitigate their disastrous effects. The

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

study becomes relevant by undertaking a comparison between adoption of cybersecurity measures before and after advent of covid-19 pandemic. This understanding led to formulation of following hypothesis:

Hypothesis 1: Importance attributed to different cybercrimes during covid-19 pandemic is different from before pandemic period.

Hypothesis 2: Importance attributed to different cyber security measures during covid-19 pandemic is different from before pandemic period.

Research Methodology

Research design

The attack of cybercrimes is subtle and due to social stigma attached to sexual harassment matters girls most of the time do not disclose them. Thus in first step of study to identify types of cybercrimes and security measures a *qualitative method* of research was applied by taking a judgmental sample of 10 experts from industry and academia who have substantial experience in the subject of cybercrimes and security. Personal interview with each of the expert provided number of dimensions pertaining to these two constructs. Content analysis was carried out to remove ambiguous and repetitive responses. In conjunction with literature this analysis provided a list of 24 statements relating to different types of cybercrimes and 18 pertaining to cyber security measures.

In second step of study *quantitative research* was conducted involving large sample size and structure undisguised questionnaire. All set of questions would have close ended questions so as to collect data reliably, quickly and from large sample. Thus research design would be primarily *descriptive* type as the purpose would be to characterize usage of cyber space, find relations among various constructs under study and identify certain causes about effects under study.

Sampling methodology

The study was conducted in the Malwa region of Punjab for following reasons. Punjab is segregated primarily into three major regions namely Malwa, Doaba and Majha. Malwa region of Punjab is largest both geographically covering an area of 32806 sq.km. i.e. 65.14% of total area (https://www.esopb.gov.in/static/PDF/Abstract2019.pdf) and population wise. It consists of 09 major districts and its population adds up to 1.64 crores which is approximately 52.50% of total population of Punjab. Population was girl students enrolled in graduate and post-graduate courses of colleges affiliated to Punjabi University which fall in the nine districts comprising Malwa region. This data was collated from official website of Punjabi University (www.punjabiuniversity.ac.in/Pages/Images/Forms/list_of_affiliated_colleges.pdf). Data base indicated that there are 270 colleges affiliated to university. These colleges are categorized as Govt., Private-aided and Private self-financing. Data regarding total number of students enrolled in various courses in all three types of colleges of 09 cities of Malwa region, namely, Patiala, Fatehgarh Sahib, Sangrur, Barnala, Bathinda, Mansa, Faridkot, Rupnagar and Sahibzada Ajit Singh Nagar (SAS). Total population of students in the age group of 18-23 from these cities was calculated to be 59,530. Total girl student population which was approximately 60% of total students came out to be 35,718. This entire population size was firstly segregated with regard to cities and; secondly with regard to number of girl students in rural and urban colleges of each city. The segregation was done on these two strata because of our objectives which compared cyber security awareness among rural and

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

urban girl students of all cities of Malwa region of Punjab. From these defined strata which have finite and known population a limited sample would be selected randomly. Thus *disproportionate stratified random sampling* was considered to be appropriate method of sampling for selecting girl students.

Sample size

Sample size of girl student from each strata was calculated by using Cochran's formula at 10% margin of error. This formula was considered appropriate because of relatively large known population size of each stratum. Formula is shown below:

Cochran's formula = $Z^2(pq)/e^2$

Where Z is derived from established confidence interval (C.I.). Commonly C.I. of 90% is used so value of Z=1.645.

p means proportion of success, for instance, in this case success is selection of urban students from a particular city say Patiala. To illustrate further in this case:

p = number of urban girl students in Patiala /total number of girl students in Patiala

p = 4848/7422 = 0.6532.

q = 1-p; and

e = margin of error depending on variability in data from respondents. As variability is significant among responses from urban and rural respondents so 10% of margin of error was decided.

By using the formula sample size of each stratum of each city would be:

City	*Patiala*	*Fatehgarh*	*Sangrur*	*Barnala*	*Bathinda*	*Mansa*	*Faridkot*	*Rupnagar*	*SAS*
Population	4848	912	2691	1820	4296	420	900	1500	1302
Sample	61	59	55	45	56	36	68	63	67

So total sample examined was 510 girl students.

Data collection

Part A of the questionnaire gathered responses from selected number of girl students in the Malwa region regarding different types of cybercrimes they have encountered or are aware. Responses were gathered on 5 point Likert scale where '5'implied high degree of acceptance towards occurrence of a cybercrime and '1'meant lowest degree implying respondent did not consider it to be important as effecting their work. Along with each statement participants were asked to rate from 1 to 5 the significance of it both before and after the advent of covid-19. This was done to evaluate the variation in importance of different cybercrime dimensions. Part B of the questionnaire similarly involved all identified 18 statements pertaining to cyber security measures. Their degree of effectiveness if participants adopt any of them was again evaluated on a 5 pint Likert scale where '1'meant that respondents consider it to be unimportant whereas '5'meant it to be highly important in saving from dangers of cybercrimes. Lastly to examine the importance of different cyber security

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

measures before and after pandemic respondents were asked to signify each dimensions importance on a scale of 1 to 5 where '1' meant lest important and '5' implied a dimension to be of highest importance.

Results

Identification of relevant cybercrimes affecting girl students

The results of SEM analysis are shown in Table 1. KMO value obtained was 0.782 which was greater than 0.5 indicating sampling adequacy (Kaiser 1974). Significant chi square value (121.84; p=0.000<0.05) fulfilled assumption of Bartlett's test of sphericity indicating all possibility of obtaining differentiated factors (Tabachnick & Fidell, 2001). The results reduced number of relevant attributes to 17 from 24 that were grouped in four factors namely *cyber-stalking, privacy violation, financial risks and pornography*. Each of these factors had Eigen value greater than threshold value of one making them as relevant factors.

All dimensions loaded reliably with their respective factors as correlation coefficients indicated acceptable level of contribution of each dimension in explaining the factor. Item-to-total correlation values were also in acceptable area of greater than 0.4 (McKelvey, 1976) indicating that all dimensions are measuring the same construct of employability skills.

Table 1: Reliability results of Cybercrime construct

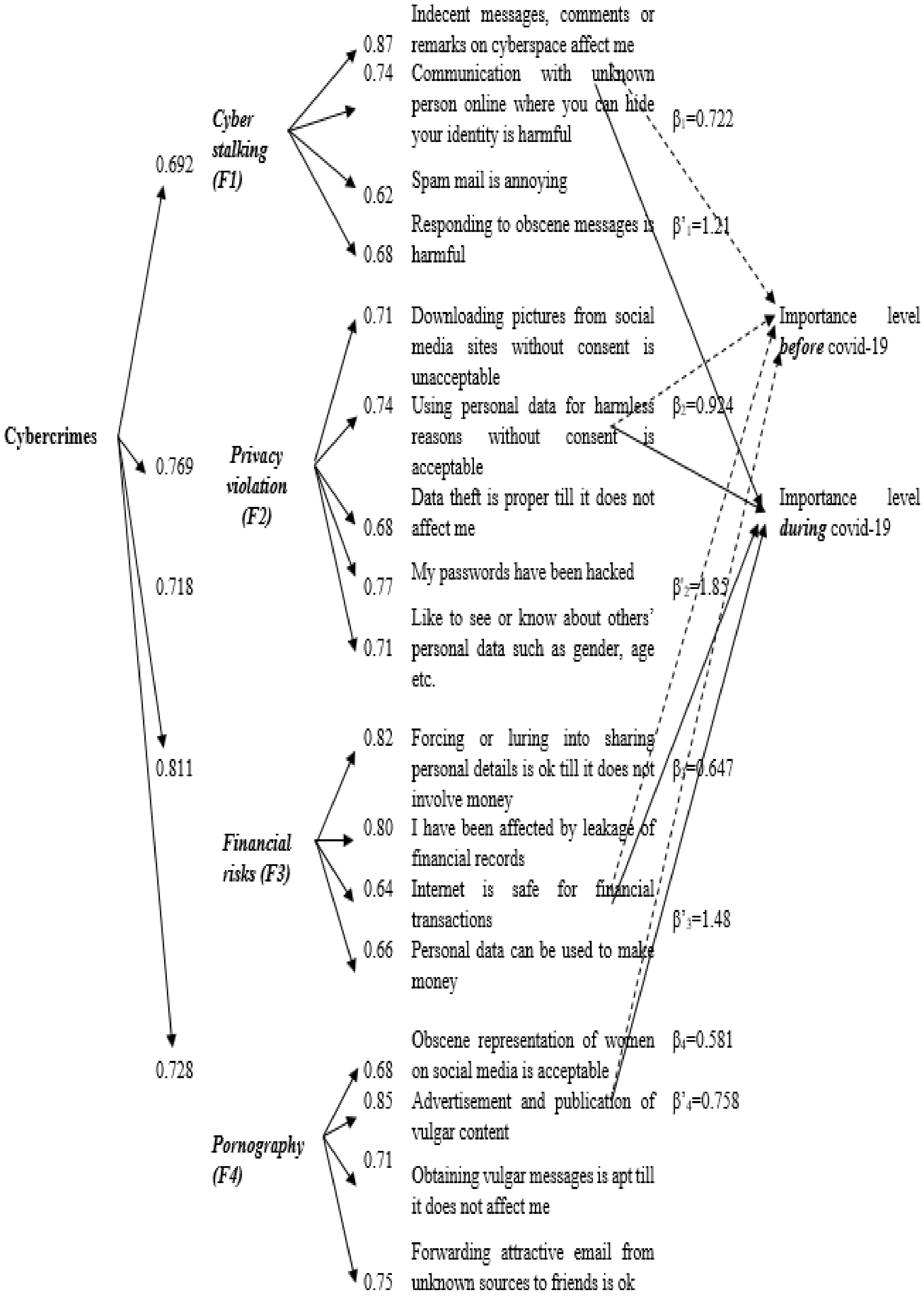
Factors	**Factor Loadings**	**Item-to-total correlation**
Cyber stalking (F1)		
Indecent messages, comments or remarks on cyberspace affect me	0.87	0.81
Communication with unknown person online where you can hide your identity is harmful	0.74	0.82
Spam mail is annoying	0.62	0.80
Responding to obscene messages is harmful	0.68	0.79
Cronbach alpha= 0.714; Eigen value=6.271; Average variance explained=23.47%		
Privacy violation (F2)		
Downloading pictures from social media sites without consent is unacceptable	0.71	0.77
Using personal data for harmless reasons without consent is acceptable	0.74	0.81
Data theft is proper till it does not affect me	0.68	0.78
My passwords have been hacked	0.77	0.74
Like to see or know about others' personal data such as gender, age etc.	0.71	0.72
Cronbach alpha=0.827; Eigen value=7.452; Average variance explained=31.87%		
Financial Risks (F3)		

Forcing or luring into sharing personal details is ok till it does not involve money	0.82	0.68
I have been affected by leakage of financial records	0.80	0.71
Internet is safe for financial transactions	0.64	0.69
Personal data can be used to make money	0.66	0.74
Cronbach alpha=0.665; Eigen value=5.186; Average variance explained=18.72%		
Pornography (F4)		
Obscene representation of women on social media is acceptable	0.68	0.65
Advertisement and publication of vulgar content	0.85	0.68
Obtaining vulgar messages is apt till it does not affect me	0.71	0.69
Forwarding attractive email from unknown sources to friends is ok	0.75	0.71
Cronbach alpha=0.632; Eigen value=4.217; Average variance explained=15.42%		

Lastly, Cronbach alpha values indicating internal consistency of deduced factors were found to be greater than decided threshold value of 0.7 (Peterson, 1994). It is a good measure of reliability of factors as it indicates that there is positive and strong association between identified factors and dimensions involved in each one of them.

Convergent validity was examined by significant and high correlations between identified factors and cybercrimes construct. The results show that correlation coefficient of cyber stalking, privacy violation, financial risks and pornography with the construct were 0.692 ($p=0.021<0.05$), 0.769 ($p=0.018<0.05$), 0.718 ($p=0.015<0.05$) and 0.728 ($p=0.004<0.05$) respectively indicating that all four factors converge to measure same phenomenon (shown in Fig.1).

Figure 1: SEM analysis of Cybercrime


Cybercrimes
0.692
0.769
0.718
0.811
0.728
Cyber stalking (F1)
0.87
Indecent messages, comments or remarks on cyberspace affect me
0.74
Communication with unknown person online where you can hide your identity is harmful
0.62
Spam mail is annoying
0.68
Responding to obscene messages is harmful
Privacy violation (F2)
0.71
Downloading pictures from social media sites without consent is unacceptable
0.74
Using personal data for harmless reasons without consent is acceptable
0.68
Data theft is proper till it does not affect me
0.77
My passwords have been hacked
0.71
Like to see or know about others' personal data such as gender, age etc.
Financial risks (F3)
0.82
Forcing or luring into sharing personal details is ok till it does not involve money
0.80
I have been affected by leakage of financial records
0.64
Internet is safe for financial transactions
0.66
Personal data can be used to make money
Pornography (F4)
0.68
Obscene representation of women on social media is acceptable
0.85
Advertisement and publication of vulgar content
0.71
Obtaining vulgar messages is apt till it does not affect me
0.75
Forwarding attractive email from unknown sources to friends is ok
β_1=0.722
β'_1=1.21
β_2=0.924
β'_2=1.85
β_3=0.647
β'_3=1.48
β_4=0.581
β'_4=0.758
Importance level before covid-19
Importance level during covid-19

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

Discriminant validity was examined through chi-square values that were considered as an excellent measure of goodness of fit. Chi-square values by merging two factors at a time were found to be: F12 (F1 is merged with F2), F3 & F4 = 34.71, F13 (F1 is merged with F3), F2 & F4 = 47.18, F14 (F1 is merged with F4), F2 and F3 = 39.28 which were significantly higher than of original model (19.57). Thus merged models showed bad model fit making original model with four distinct factors as measuring similar phenomenon but with different contribution.

Lastly measuring construct validity by applying regression analysis showed that all four factors significantly contributed in explaining 68.27% (adjusted R square=67.46%) of importance attributed to awareness regarding cybercrimes during pandemic period.

Table 2: Regression results

Dependent variable	**Independent variables**	**Regression coefficient (p value)**	**R square (Adjusted R square)**	**F value (p value)**
Importance level ***before*** covid-19	Cyber stalking (F1)	β_1=0.722 (0.112)	47.82% (46.92%)	18.741 (0.004)*
	Privacy violation (F2)	β_2=0.924 (0.041)*		
	Financial Risks (F3)	β_3=0.647 (0.243)		
	Pornography (F4)	β_4=0.581 (0.002)*		
Importance level ***during*** covid-19	Cyber stalking (F1)	β'_1=1.241 (0.042)*	68.27% (67.46%)	25.684 (0.001)*
	Privacy violation (F2)	β'_2=1.853 (0.023)*		
	Financial Risks (F3)	β'_3=1.482 (0.031)*		
	Pornography (F4)	β'_4=0.758 (0.041)*		

**significant at 5% p value*

This was significantly more than importance exuded to cybercrimes before pandemic (R square=47.82%) wherein only two cybercrimes privacy violation (β_2=0.924; $p=0.041<0.05$) and pornography (β_4=0.581; $p=0.002<0.05$) were considered impacting girl students leading to acceptance of H1. Also high value of regression coefficients associated with four types of cybercrimes in after pandemic period imply their contribution to respondents' consideration towards imparting significance to a particular cybercrime as compared to before pandemic period coefficients. For instance β'_2=1.853 (0.023) pertaining to privacy violation after pandemic as compared to β_2=0.924 (0.041) indicated increased risk of respondents being impacted by such cybercrime. This information would help in finding cyber security measures adopted or considered

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

important by same girl students in order to counter the effect of important cybercrimes. It has been examined in next section.

Identification of relevant cyber security measures affecting girl students:

The results of SEM analysis are shown in Table 3. KMO value obtained was 0.714 which was greater than 0.5 indicating sampling adequacy.

Table 3: Reliability results of Cyber security measures construct

Factors	**Factor Loadings**	**Item-to-total correlation**
General security (F1)		
I always log out from my account before leaving computer/phone	0.75	0.74
Scanning frequently system is helpful	0.69	0.72
Making profile data public on social media sites is safe	0.70	0.74
Leaving computer or mobile on without auto lock poses danger to data	0.77	0.72
Installing security software is important even if it is time consuming and difficult	0.71	0.62
Cronbach alpha= 0.782; Eigen value=5.627; Average variance explained=32.18%		
Password security (F2)		
I frequently change my passwords	0.77	0.71
Do not share passwords with family members or close friends	0.72	0.68
For remembering passwords I do not write them somewhere	0.69	0.62
Memorizing passwords is easy	0.75	0.77
Robust passwords secure me from any cyber crimes	0.81	0.74
Cronbach alpha=0.754; Eigen value=4.238; Average variance explained=29.37%		
Awareness (F3)		
I want to know more about cyber security measures even if it consumes time	0.84	0.71
By installing security software I feel more secure	0.74	0.72
Using anti-virus is essential	0.73	0.77
Opening of unknown emails is harmless	0.69	0.79
Cronbach alpha=0.742; Eigen value=3.285; Average variance explained=19.81%		

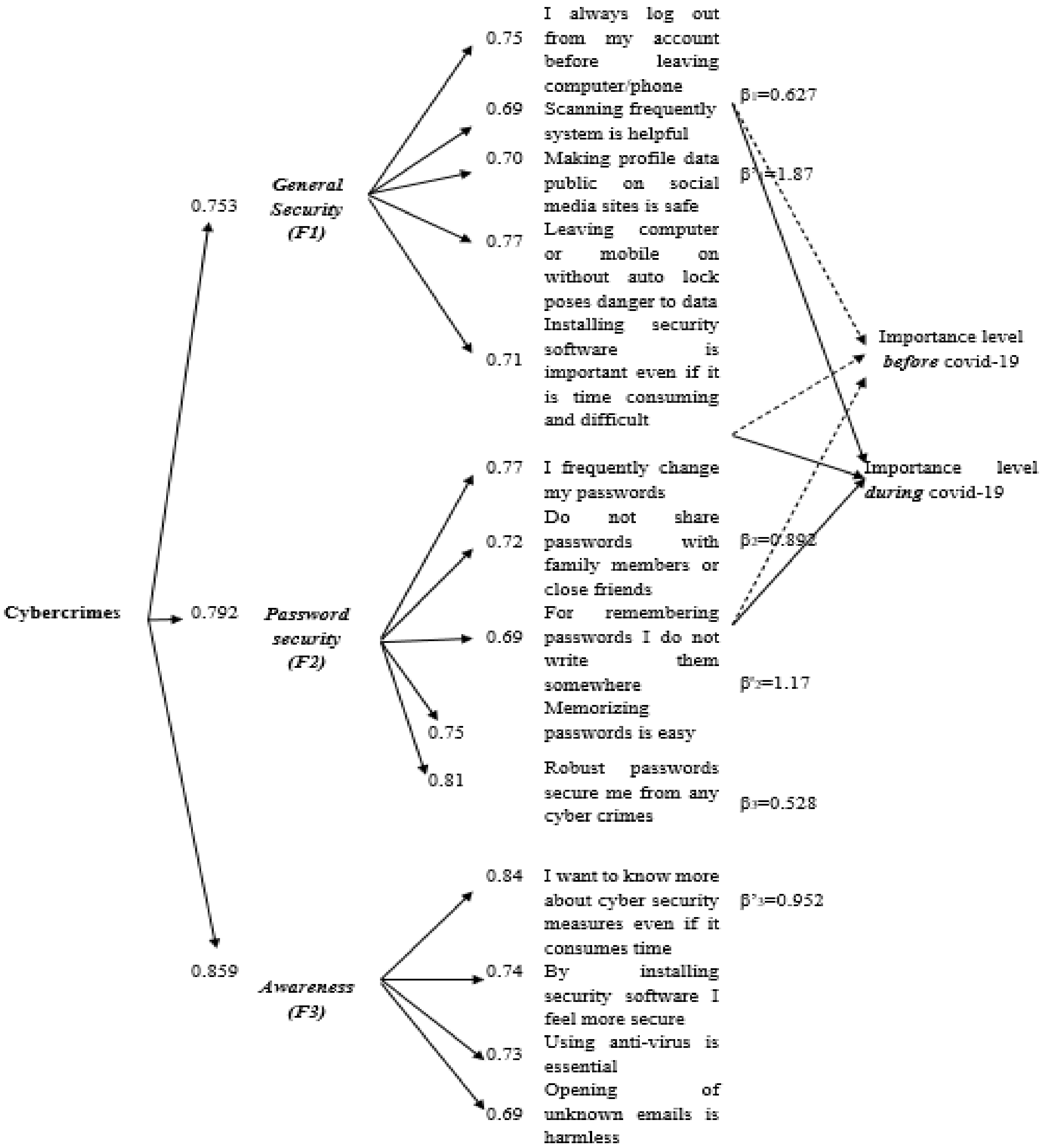
P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

Significant chi square value (87.56; p=0.000<0.05) fulfilled assumption of Bartlett's test of sphericity indicating all possibility of obtaining differentiated factors. The results reduced number of relevant attributes to 14 from 22 that were grouped in three factors namely *general security, password security and awareness.*

Each of these factors had Eigen value greater than threshold value of 1 making them as relevant factors with general security attribute having maximum (5.627) implying its significant contribution towards awareness about security measures.

In addition, this attribute with maximum average variance explained of 32.18% indicated respondents' willingness to adopt these measures for cyber security improvement. Reliability measures of Cronbach alpha and item-to-total correlation were also found to be appropriate. Thus, dimensions comprised in particular factor were considered to be acceptable.

Figure 3: SEM analysis of cyber security measures


Cybercrimes
0.753
0.792
0.859
General Security (F1)
Password security (F2)
Awareness (F3)
0.75
I always log out from my account before leaving computer/phone
0.69
Scanning frequently system is helpful
0.70
Making profile data public on social media sites is safe
0.77
Leaving computer or mobile on without auto lock poses danger to data
0.71
Installing security software is important even if it is time consuming and difficult
0.77
I frequently change my passwords
0.72
Do not share passwords with family members or close friends
0.69
For remembering passwords I do not write them somewhere
0.75
Memorizing passwords is easy
0.81
Robust passwords secure me from any cyber crimes
0.84
I want to know more about cyber security measures even if it consumes time
0.74
By installing security software I feel more secure
0.73
Using anti-virus is essential
0.69
Opening of unknown emails is harmless
β1=0.627
β'1=1.87
β2=0.892
β'2=1.17
β3=0.528
β'3=0.952
Importance level before covid-19
Importance level during covid-19

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

Convergent validity examined by significant and high correlations between identified factors and cybercrimes construct showed correlation coefficient of general security, password security and awareness with the construct of cyber security measures to be 0.753 ($p=0.032<0.05$), 0.792 ($p=0.022<0.05$) and 0.859 ($p=0.033<0.05$) respectively indicating that all three factors converge to measure same phenomenon (shown in Fig.2).

Discriminant validity examined through chi-square showed: F12 (F1 is merged with F2), & F3 = 29.37, F13 (F1 is merged with F3) & F2 = 35.64 were significantly higher than of original model (15.68). Thus merged models showed bad model fit making original model with three distinct factors as measuring similar phenomenon but with different contribution.

Lastly measuring construct validity by applying regression analysis (Table 4) showed that all three factors significantly contributed in explaining 53.56% (adjusted R square=62.33%) of importance attributed to awareness regarding significance of cyber security measures during pandemic period. This was significantly more than importance exuded to cyber security measures before pandemic (R square=22.75%) as only one measure of password security ($\beta_2=0.892$; $p=0.023<0.05$) was considered to be important measure which would safeguard from cybercrimes. High and significant value of all three security measures general security ($\beta'_1=1.872$, $p=0.028<0.05$), password security ($\beta'_2=1.171$, $p=0.011<0.05$) and awareness ($\beta'_3=0.952$, $p=0.042<0.05$) implied increased awareness about significance of different security measures (accepting hypothesis H2) in mitigating threat of cybercrimes especially of privacy violation and financial risks as these were considered to be biggest contributor to lack of awareness about cybercrimes.

Table 4: Regression results

Dependent variable	**Independent variables**	**Regression coefficient (p**	**R square (Adjusted R square)**	**F value (p value)**
Importance level ***before*** covid-19	General security (F1)	β_1=0..627 (0.231)	22.75% (21.54%)	11.634 (0.019)*
	Password security (F2)	β_2=0.892 (0.039)*		
	Awareness (F3)	β_3=0.528 (0.185)		
Importance level ***during*** covid-19	General security (F1)	β'_1=1.872 (0.028)*	62.33% (61.28%)	18.27 (0.021)*
	Password security (F2)	β'_2=1.171 (0.011)*		
	Awareness (F3)	β'_3=0.952 (0.042)*		

**significant at 5% p value*

Discussion

The study examined classification of cybercrimes and cyber security measures among girl students of Malwa region of Punjab. The study generates its importance in two ways. Firstly literature showed that taxonomy of cybercrimes is not standard and varies with demographics, societal structure and frequency of usage of online medium among others. Appropriate understanding of definition of various cybercrimes was important in order to effective application of specific security measures. No study was found to operationalize types of cybercrimes encountered by girl students despite of them being one of the most vulnerable segments. Secondly, advent of pandemic with subsequent nationwide lockdown changed the ways education was imparted and occupied. Humungous increase in internet consumption also made girl students more vulnerable to cybercrimes. This study compared the significance attached to deduced cybercrimes and security measures before and after advent of pandemic. Such a comparison underscored importance of taking necessary cognisance to understanding of cybercrimes affecting girl students and security measures that would facilitate mitigating their harmful effects.

SEM findings of the study revealed all four factors were found to contribute to the extent of 89.48% in explaining formation of cybercrimes construct. Out of four deduced cybercrimes privacy violation to be considered as most important as its average variance to explain construct of cybercrimes was maximum followed by cyber stalking, financial risks and lastly threat of pornography. Similar analysis of cyber security measures indicated three prime attributes of general security, password protection and awareness about different measures as contributors to the extent of 81.36% in explaining formation of cybercrimes construct. This was important in order to understand security measures girl students apply or are aware about. They could be different for other demographics and gender. Most importantly the study majorly intended to examine effect of Covid-19 pandemic on understanding or importance that participants attributed to both cybercrimes and corresponding security measures. The findings helped in recognizing specific security measures that girl students would adopt to encounter crimes they have faced or are aware about. The study showed that before pandemic participants appreciated threats of only privacy violation and pornography. To encounter them they comprehended using only password security measures. However after pandemic respondents encountered all four identified types of crimes and they attributed high and significant importance to application of deduced security measures to alleviate their harmful effects. The study thus very importantly examined before and after effects of pandemic on understanding and assigning importance to different cybercrimes and security measures.

Implications:

The study has implications especially for educationists involved in designing curricula in schools and under-graduate institutions. Imparting education as part of course curricula should be promoted to enhance individuals' awareness about cybercrimes. Providing awareness and knowledge not at higher education level but at school or under-graduate level is essential to instil behavioural measures of protection and prevention against cybercrimes (Venter et al., 2019). Online users indulge in using free online services like chats and entertainment. Thus paying for cyber security measures is sometimes considered as extra unnecessary cost. However studies how expending on such measures goes a long way in preventing long-term damage like lost data or privacy intrusion (Lloyd, 2020). Thus, study also encourages technology solutions providers to design and provide easy to use reasonably priced security measures to individual users.

Future research:

The study has limited its scope to understanding cybercrimes and security measures considered important by only urban girl students studying in colleges of specific region. For further researches

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

findings can be used to make a comparative study among urban and rural girl students as it is generally hypothesized that rural students are less aware and knowledgeable about technology driven activities. In addition, study applied research purpose to under-graduate students, as their higher number would allow more generalization. However, future researches can use the template provided to compare with university girl students. Thus, future researches can apply the findings for demographic and geographic comparisons.

References

Ali, L. (2019) Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study of the Online Banking Sectors In GCC) The Journal of Developing Areas, 53(1)

Anesa, P. (2020) Lovextortion: Persuasion strategies in romance cybercrime. Discourse, Context and Media, 35, 100398.

Boddy, M. (2018) Phishing 2.0: the new evolution in cybercrime. Computer Fraud and Security, 2018(11), 8-10.

Chaithanya, B. N., and Veena, R. (2019) Emerging trends and challenges in advanced technologies on cyber security. IJO-International Journal of Computer Science and Engineering, 2(1), 01-16.

Chandra, A., and Snowe, M. J. (2020) A taxonomy of cybercrime: Theory and design. International Journal of Accounting Information Systems, 38, 100467.

Chang, L. Y., and Coppel, N. (2020) Building cyber security awareness in a developing country: lessons from Myanmar. Computers and Security, 97, 101959.

Chang, W. J. (2020) Cyberstalking and Law Enforcement. Procedia Computer Science, 176, 1188-1194.

Cheng, C., Chan, L., and Chau, C. L. (2020) Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior, 108, 106311.

Cobb, M. J. (2018) Plugging the skills gap: The vital role that women should play in cyber-security. Computer Fraud and Security, 2018(1), 5-8.

Conteh, N. Y., and Schmick, P. J. (2016) Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31.

Donalds, C., and Osei-Bryson, K. M. (2019) Toward a cybercrime classification ontology: A knowledge-based approach. Computers in Human Behavior, 92, 403-418.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., and Hardyns, W. (2020) Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. Computers in Human Behavior, 108, 106310.

Dinev, T. (2006) Why spoofing is serious internet fraud. Communications of the ACM, 49(10), 76-82.

Dombrowski, S. C., Gischlar, K. L., and Durst, T. (2007) Safeguarding young people from cyber pornography and cyber sexual predation: A major dilemma of the Internet. Child Abuse Review: Journal of the British Association for the Study and Prevention of Child Abuse and Neglect, 16(3), 153-170.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

Eddolls, M. (2016) Making cybercrime prevention the highest priority. Network Security, 8, 5-8.

Epps, C. (2017) Best practices to deal with top cybercrime activities. Computer Fraud and Security, 4, 13-15.

Fernandez, D. P., Tee, E. Y., and Fernandez, E. F. (2017) Do Cyber Pornography Use Inventory-9 scores reflect actual compulsivity in internet pornography use? Exploring the role of abstinence effort. Sexual Addiction and Compulsivity, 24(3), 156-179.

Geetha, B., and Pagutharivu, R. (2010) Internet–A Dangerous Web for Women. The Indian Police Journal, Vol. LVII-No. 4, (October – December), 55-62.

Geetha, S., and Phamila, A. V. (Eds.) (2016) Combating security breaches and criminal activity in the digital sphere. IGI Global.

Griffiths, M. (2010) Internet abuse and internet addiction in the workplace. Journal of Workplace Learning. 22 (7), 463-472.

Grubbs, J. B., Sessoms, J., Wheeler, D. M., and Volk, F. (2010) The Cyber-Pornography Use Inventory: The development of a new assessment instrument. Sexual Addiction and Compulsivity, 17(2), 106-126.

Gunjan, V. K., Kumar, A., and Avdhanam, S. (2013, September) A survey of cyber crime in India. In 2013 15th International Conference on Advanced Computing Technologies (ICACT) (pp. 1-6) IEEE.

Halder, D., and Jaishankar, K. (2011) Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. Victims and Offenders, 6(4), 386-398.

Halder, D., and Jaishankar, K. (2012) Cyber Crime Against Women and Regulations in Australia. In Cyber Crime: Concepts, Methodologies, Tools and Applications 757-764, IGI Global.

Ibrahim, S. (2016) Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice, 47, 44-57.

Kaiser, H. F. (1974) An index of factorial simplicity. Psychometrika, 39(1), 31-36.

Kandpal, V., and Singh, R. K. (2013) Latest face of cybercrime and its prevention in India. International Journal of Basic and Applied Sciences, 2(4), 150-156.

Karnold, S. (2000) The cyber world of child pornography and the child pornography act of 1996: Thoughts on morphing, virtual imaging, and the first amendment. Journal of Information Ethics, 9(2), 60.

Kethineni, S., and Cao, Y. (2020) The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 30(3), 325-344.

Konradt, C., Schilling, A., and Werners, B. (2016) Phishing: An economic analysis of cybercrime perpetrators. Computers and Security, 58, 39-46.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., and Bellekens, X. (2021) Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, 102248.

Li, Z. (2015) Does power make us mean? An investigation of empowerment and revenge behaviors in the cyberspace (Doctoral dissertation, University of Miami)

Lloyd, G. (2020) The business benefits of cyber security for SMEs. Computer Fraud and Security, 2, 14-17.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2022.28.04.150

Martens, M., De Wolf, R., and De Marez, L. (2019) Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Computers in Human Behavior, 92, 139-150.

Math, S. B., Viswanath, B., Maroky, A. S., Kumar, N. C., Cherian, A. V., and Nirmala, M. C. (2014) Sexual crime in India: is it influenced by pornography? Indian Journal of Psychological Medicine, 36(2), 147.

Obar, J.A. and Wildman, S.(2015) Social media definition and the governance challenge: An introduction to the special issue. Telecommunications policy, 39(9), 745-750.

Ottis, R., and Lorents, P. (2010, April) Cyberspace: Definition and implications. In International Conference on Cyber Warfare and Security (p. 267) Academic Conferences International Limited.

Pandove, K., Jindal, A., and Kumar, R. (2010) Email spoofing. International Journal of Computer Applications, 5(1), 27-30.

Powell, A., Henry, N., Flynn, A., and Scott, A. J. (2019) Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. Computers in Human Behavior, 92, 393-402.

Reyns, B. W., Henson, B., and Fisher, B. S. (2012) Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. Deviant Behavior, 33(1), 1-25.

Sahoo, G. P. (2018) Legal Framework of Information Technology in India: With Special Reference to Cyber Obscenity. In Contemporary Issues in International Law, 475-500, Springer, Singapore.

Sankhwar, S., and Chaturvedi, A. (2018) Woman harassment in digital space in India. International Journal of Pure and Applied Mathematics, 118(20), 595-607.

Sethi, D., and Ghatak, S. (2018) Mitigating cyber sexual harassment: An Insight from India. Asian Themes in Social Sciences Research, 1(2), 34-43.

Sheridan, L. P., and Grant, T. (2007) Is cyberstalking different? Psychology, crime and law, 13(6), 627-640.

Tabachnick, B.G. and Fidell, L.S. (2001) Using Multivariate Statistics. Fourth Edition. Needham Heights, MA: Allyn and Bacon.

Umadevi, K. S., Amali, G. B., and Subramanian, L. (2019) An Indian and Global Perspective on Cybercrime. In Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems. 45-63, IGI Global.

Verma, A. (2012) Cyber pornography in India and its implication on cyber cafe operators. Computer Law and Security Review, 28(1), 69-76.

Venter, I. M., Blignaut, R. J., Renaud, K., and Venter, M. A. (2019) Cyber security education is as essential as “the three R's”. Heliyon, 5(12), e02855.

Weil, T., and Murugesan, S. (2020) IT Risk and Resilience—Cybersecurity Response to COVID-19. IEEE Computer Architecture Letters, 22(03), 4-10.

Wright, M. F., Aoyama, I., Kamble, S. V., Li, Z., Soudi, S., Lei, L., and Shu, C. (2015) Peer attachment and cyber aggression involvement among Chinese, Indian, and Japanese adolescents. Societies, 5(2), 339-353.