

A STUDY OF CONSUMER AWARENESS ON CYBERCRIMES & CYBERLAW AMONG INDIAN YOUTH

ADITHYA NUKALA



**BHARTI SCHOOL OF TELECOMMUNICATION
TECHNOLOGY AND MANAGEMENT
INDIAN INSTITUTE OF TECHNOLOGY DELHI
JULY 2025**

© Indian Institute of Technology Delhi (IITD), New Delhi, 2025

A Study of Consumer Awareness on Cybercrimes & Cyberlaw among Indian Youth

by

Adithya Nukala
(2018BSZ8120)

Bharti School of Telecommunication Technology and Management

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy to the



Indian Institute of Technology Delhi

July 2025

CERTIFICATE

This is to certify that the thesis entitled – “**A Study of Consumer Awareness on Cybercrimes & Cyberlaw among Indian Youth,**” submitted by Mr. Adithya Nukala to the Indian Institute of Technology Delhi for the award of the degree of the Doctor of Philosophy, is a record of bonafide research work carried out by him. He worked under our supervision for the submission of this thesis, which, to the best of our knowledge, has reached the requisite standard.

The research reports, and the results presented in this thesis have not been submitted in parts or in full to any other University or Institute for the award of any degree or diploma.

Prof. Mahim Sagar
Dept. of Management Studies
Indian Institute of Technology Delhi
New Delhi

Dr. Medudula Murali Krishna
Asst. General Manager
Reliance Jio
New Delhi

Dedicated to my Parents and my Mentor

ACKNOWLEDGMENTS

Understanding this Ph.D. has been eye-opening for me, and it would not have been possible without the support and guidance I have received from many people. First and foremost, I am grateful to the Almighty God for keeping me healthy and brightening my mind to accomplish this work.

I would like to begin by expressing my heartfelt gratitude to my supervisor, Prof. Mahim Sagar, for his endless encouragement, patience, wisdom, and humour he has given me during the course of my study. I honestly thank him for dedicating his effort and time to my thesis work. I express my deepest gratitude to my supervisor, Dr. Medudula Murali Krishna, for his valuable advice and guidance despite his busy schedule throughout this research work. His experience, knowledge, and substantial feedback brought it all together. I am blessed to have two experts from academic and industry backgrounds who have given me insights into both worlds. Their indispensable assistance and invaluable guidance have helped me significantly contribute to society. I am eternally grateful for their kindness, helpful advice, discussions, and timely help. I owe my sincere, heartfelt thanks and deep sense of gratitude to them, and I have been fortunate to have them as my supervisors.

I am grateful to all the members of my Student Research Committee (SRC), Prof. Harish Chaudhry, Prof. Arpan Kumar Kar, and Prof. Varsha Singh, for their educational guidance, valuable suggestions, and advice relating to my research, which is very useful to my thought process. I want to thank the Bharti School of Telecommunication Technology and Management and the Department of Management Studies, IIT Delhi, for giving me this opportunity to carry out this research work. I want to thank one more person, Dr. Rojaline Pradhan, who helped me in every

step of my research work. Her valuable suggestions are unforgettable. I want to thank all the participants who took part in the data collection process and spent their time providing useful information, without whom the study would not have been completed. Their willingness to participate in this research work is highly appreciated.

Along with my family, my friends shape the other pillar of my life. I am very grateful to my friends who supported me in my journey. Special thanks to all my research colleagues: Shiksha Kushwa, Vishakha Chauhan, Shefali Khare, Sonal Arora, Richa Kondal, Amardeep Prasad, Honey Yadav, Priyanka, and Rohini Sharma for their unconditional support and encouragement. Special thanks to Project Staff: Swathi Kaushik and Delma Momi. Many thanks to IIT Delhi CEP-QIP Staff Om Prakash, Sagar, Ashwini Sharma, Jay Kumar, Simrath Kaur, and Sheela Madam for their help and kindness. My acknowledgment would be incomplete without thanking Charru Hasti, madam, for motivating me during thesis writing.

My Mom and Dad, I would not have been here today without you. Thank you for always being with me, believing in me, and never giving up on me. Special thanks to my wife, Shyamalambica, my better half for being patient during my journey. Her endless love and support helped me to focus on my research work.

Thank you all from the depth of my heart.

Date

(Adithya Nukala)

ABSTRACT

Technology has changed people's life the way they live. It has changed people's mindset and their lifestyles. Though the Internet was introduced in the late 90s, its usage started in 2000 and has continued until the present. The combination of computers and the development of technology through media gave birth to the Internet. The Internet is nothing but networks of networks. This internet is used mainly by young consumers (Youth) compared to middle-aged and older consumers. Youth is defined as someone who comes under the age between when they leave compulsory education and enter their first employment. The most prominent smartphone usage in India is by youth only. Good quality, new features, and being under budget attract consumers efficiently. Consumers, especially youth, are well-educated, tech-savvy, and well-versed with the technologies and their applications. They assume that they are on the safe side and think that nobody can enter their digital world. Young consumers are aware of the front side of the technology rather than the dark side of the technology.

Consumers are victims of cybercrimes until and unless someone says they (consumer) became a cybercrime victim. Though the consumer becomes a victim of cybercrime, what is the next step? What is the consumer's next agenda? To whom he should approach. What types of cyber laws and policies (Information Technology Act, 2000 and Information Technology (Amendment) Act, 2008) are against these cyber crimes? This gap made me study consumer awareness of cyber law among Indian youth. The main objective of this research is to develop a consumer awareness framework of cyber law among Indian Youth. The sub-objectives of this research study are (i). To explore and identify consumer awareness factors of cyber law among Indian Youth (ii). To develop a consumer

awareness framework of cyber law to create awareness among Indian youth, and (iii). To validate the framework using empirical studies. These three objectives are achieved in three studies.

Study 1 focuses on consumer awareness factors of cyber law. These factors are explored using the grounded theory methodology. Grounded Theory Methodology is used in an area where previous research was not done. Expert interviews are taken using a semi-structured questionnaire, recorded interview process, and converted into transcripts. MaxQDA software was used for data analysis, and factors were identified. The factors identified in the study are Digital Protection Measures, Cyber Risks & Attacks, Information Sharing, Technology Adoption, Cyber Acts & Policies, Governing Mechanisms, Consumer Experience, and Educational Curriculum.

Study 2 relates the factors and develops a hierarchical interrelationship among factors using Total Interpretive Structural Modelling (TISM). TISM questionnaire was designed and again approached to the experts for their opinion. Based on the expert opinion, the TISM process is done. A digraph is formed showing hierarchical interlinkages among factors. Hierarchical factors and linkages will help us analyze how one factor will influence other factors and their role in consumer awareness of cyber law. In the digraph, the factor Educational Curriculum is in the base stage while the Governing Mechanism is in a dependency state. In the digraph, Digital Protection Measures and Information-sharing constructs have two-way communication. Similarly, Cyber Risks & Attacks and Technology Adoption also have two-way communication. In contrast, technology adoption has transitive communication with cyber acts and policies, and cyber acts and policies directly communicate with technology adoption.

Study 3 relates the validation of the consumer awareness framework using empirical studies. Structural Equation Modeling is used. Quantitative research is done with a sample size of 410. The convenience sampling method is used for this study. The target sample is students, employees, and entrepreneurs. Seven constructs positively contribute to the model in the Structural Equation Modeling. Technology Adoption, Cyber Risks & Attacks, Cyber Acts & Policies, Information Sharing, Governing Mechanism, Consumer Experience, and Educational Curriculum. At the same time, other constructs, such as Digital Protection Measures and Awareness Channels, are not shown much in the SEM model.

This study attempts to develop a consumer awareness framework about cyber law in the Indian context. The study begins with understanding the consumer perception of various threats/cybercrimes in the context of cyber law. This study considers Indian youth as a unit of analysis while examining consumer awareness of cyber law. The interlinkages among the key factors are discovered, and a hierarchical framework is developed.

Keywords: *Consumer Awareness, Consumer, Youth, Cybercrimes, Cyberlaw, Information Technology Act, 2000, Information Technology (amend) Act, 2008, Grounded Theory Methodology, Total Interpretive Structural Modelling (TISM), Structural Equation Modeling (SEM). Consumer Protection Act, 1986, Consumer Protection Act, 2019.*

सार

प्रौद्योगिकी ने लोगों के जीवन जीने के तरीके को बदल दिया है। इसने लोगों की मानसिकता और उनकी जीवनशैली को बदल दिया है। हालाँकि इंटरनेट 90 के दशक के अंत में पेश किया गया था, लेकिन इसका उपयोग 2000 में शुरू हुआ और आज तक जारी है। कंप्यूटर और मीडिया के माध्यम से प्रौद्योगिकी के विकास के संयोजन ने इंटरनेट को जन्म दिया। इंटरनेट कुछ और नहीं बल्कि नेटवर्क का नेटवर्क है। इस इंटरनेट का उपयोग मुख्य रूप से युवा उपभोक्ताओं (युवा) द्वारा किया जाता है, जबकि मध्यम आयु वर्ग और वृद्ध उपभोक्ता इसका उपयोग नहीं करते हैं। युवा को ऐसे व्यक्ति के रूप में परिभाषित किया जाता है जो अनिवार्य शिक्षा छोड़ने और अपने पहले रोजगार में प्रवेश करने के बीच की आयु में आता है। भारत में सबसे अधिक स्मार्टफोन का उपयोग युवा ही करते हैं। अच्छी गुणवत्ता, नई सुविधाएँ और बजट के भीतर होना उपभोक्ताओं को कुशलतापूर्वक आकर्षित करता है। उपभोक्ता, विशेष रूप से युवा, अच्छी तरह से शिक्षित, तकनीक-प्रेमी और तकनीकों और उनके अनुप्रयोगों से अच्छी तरह वाकिफ हैं। वे मानते हैं कि वे सुरक्षित हैं और सोचते हैं कि कोई भी उनकी डिजिटल दुनिया में प्रवेश नहीं कर सकता है। युवा उपभोक्ता तकनीक के अंधेरे पक्ष के बजाय तकनीक के सामने वाले पक्ष से अवगत हैं।

उपभोक्ता तब तक साइबर अपराध के शिकार होते हैं जब तक कोई यह न कहे कि वे (उपभोक्ता) साइबर अपराध के शिकार बन गए हैं। हालाँकि उपभोक्ता साइबर अपराध का शिकार बन जाता है, लेकिन अगला कदम क्या होता है? उपभोक्ता का अगला एजेंडा क्या होता है? उसे किससे संपर्क करना चाहिए। किस प्रकार के साइबर कानून और नीतियां (सूचना प्रौद्योगिकी अधिनियम, 2000 और सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008) इन साइबर अपराधों के खिलाफ हैं? इस अंतर ने मुझे भारतीय युवाओं में साइबर कानून के बारे में उपभोक्ता जागरूकता का अध्ययन करने के लिए प्रेरित किया। इस शोध का मुख्य उद्देश्य भारतीय युवाओं में साइबर कानून के बारे में उपभोक्ता जागरूकता ढांचा विकसित करना है। इस शोध अध्ययन के उप-उद्देश्य हैं (i)। भारतीय युवाओं में साइबर कानून के उपभोक्ता जागरूकता कारकों का पता लगाना और उनकी पहचान करना (ii)। भारतीय युवाओं में जागरूकता पैदा करने के लिए साइबर कानून के बारे में उपभोक्ता जागरूकता ढांचा विकसित करना, और (iii)। अनुभवजन्य अध्ययनों का उपयोग करके ढांचे को मान्य करना। इन तीन उद्देश्यों को तीन अध्ययनों में प्राप्त किया गया है।

अध्ययन 1 साइबर कानून के उपभोक्ता जागरूकता कारकों पर केंद्रित है। इन कारकों का पता ग्राउंडेड थ्योरी पद्धति का उपयोग करके लगाया जाता है। ग्राउंडेड थ्योरी पद्धति का उपयोग ऐसे क्षेत्र में किया जाता है जहाँ पहले शोध नहीं किया गया था। अर्ध-संरचित प्रश्नावली, रिकॉर्ड की गई साक्षात्कार प्रक्रिया का उपयोग करके विशेषज्ञों के साक्षात्कार लिए जाते हैं, और उन्हें प्रतिलेखों में परिवर्तित किया जाता है। डेटा विश्लेषण के लिए MaxQDA सॉफ्टवेयर का उपयोग किया गया, और कारकों की पहचान की गई। अध्ययन में पहचाने गए कारक डिजिटल सुरक्षा उपाय, साइबर जोखिम और हमले, सूचना साझाकरण, प्रौद्योगिकी अपनाना, साइबर अधिनियम और नीतियाँ, शासी तंत्र, उपभोक्ता अनुभव और शैक्षिक पाठ्यक्रम हैं।

अध्ययन 2 कारकों को जोड़ता है और कुल व्याख्यात्मक संरचनात्मक मॉडलिंग (TISM) का उपयोग करके कारकों के बीच एक पदानुक्रमित अंतर्संबंध विकसित करता है। TISM प्रश्नावली तैयार की गई और फिर से विशेषज्ञों से उनकी राय के लिए संपर्क किया गया। विशेषज्ञ की राय के आधार पर, TISM प्रक्रिया की जाती है। कारकों के बीच पदानुक्रमित अंतर्संबंधों को दिखाते हुए एक डायग्राम बनाया जाता है। पदानुक्रमित कारक और संबंध हमें यह विश्लेषण करने में मदद करेंगे कि एक कारक अन्य कारकों को कैसे प्रभावित करेगा और साइबर कानून के बारे में उपभोक्ता जागरूकता में उनकी भूमिका क्या होगी। डायग्राम में, कारक शैक्षिक पाठ्यक्रम आधार चरण में है जबकि शासी तंत्र निर्भरता अवस्था में है। आरेख में, डिजिटल सुरक्षा उपाय और सूचना-साझाकरण निर्माणों में दो-तरफा संचार होता है। इसी तरह, साइबर जोखिम और हमले तथा प्रौद्योगिकी अपनाने में भी दो-तरफा संचार होता है। इसके विपरीत, प्रौद्योगिकी अपनाने का साइबर कृत्यों और नीतियों के साथ सकर्मक संचार होता है, और साइबर कृत्य और नीतियाँ सीधे प्रौद्योगिकी अपनाने के साथ संवाद करती हैं।

अध्ययन 3 अनुभवजन्य अध्ययनों का उपयोग करके उपभोक्ता जागरूकता ढांचे के सत्यापन से संबंधित है। संरचनात्मक समीकरण मॉडलिंग का उपयोग किया जाता है। 410 के नमूना आकार के साथ मात्रात्मक शोध किया जाता है। इस अध्ययन के लिए सुविधा नमूनाकरण विधि का उपयोग किया जाता है। लक्षित नमूना छात्र, कर्मचारी और उद्यमी हैं। संरचनात्मक समीकरण मॉडलिंग में सात निर्माण मॉडल में सकारात्मक रूप से योगदान करते हैं। प्रौद्योगिकी अपनाना, साइबर जोखिम और हमले, साइबर अधिनियम और नीतियाँ, सूचना साझाकरण, शासी तंत्र, उपभोक्ता अनुभव और शैक्षिक पाठ्यक्रम। साथ ही, डिजिटल सुरक्षा उपाय और जागरूकता चैनल जैसे अन्य निर्माण, SEM मॉडल में बहुत अधिक नहीं दिखाए गए हैं।

यह अध्ययन भारतीय संदर्भ में साइबर कानून के बारे में उपभोक्ता जागरूकता ढांचा विकसित करने का प्रयास करता है। अध्ययन साइबर कानून के संदर्भ में विभिन्न खतरों/साइबर अपराधों के बारे में उपभोक्ता धारणा को समझने के साथ शुरू होता है। यह अध्ययन साइबर कानून के बारे में उपभोक्ता जागरूकता की जांच करते समय भारतीय युवाओं को विश्लेषण की इकाई के रूप में मानता है। प्रमुख कारकों के बीच अंतर्संबंधों की खोज की जाती है, और एक पदानुक्रमित ढांचा विकसित किया जाता है।

CONTENTS

1. Introduction and Research Overview	1
1.1 Introduction	1
1.2 Background of the Study	3
1.3 Motivation of the Study	8
1.4 Introduction of Cyberlaw	10
1.5 Introduction of Consumer Awareness	12
1.6 Youth and Cybercrimes	15
1.7 Need for Consumer Awareness in Cyberlaw	20
1.8 Research Objectives and Research Questions	22
1.9 Scope of the Study	22
1.10 Methodological Overview	23
1.10 Expected Outcomes	24
1.11 Concluding Remarks	24
1.12 Structure of the Thesis	25
2. Literature Review	28
2.1 Introduction to Cyber law	28
2.1.1 Information Technology Act, 2000	29
2.1.2 Information Technology (Amendment) Act, 2008	33
2.2 Cyberlaw across Globe	38
2.2.1 Malaysia	38
2.2.2 Indonesia	40

2.2.3	Japan	41
2.2.4	United Kingdom	43
2.2.5	United States	43
2.2.6	Canada	45
2.2.7	Greece	46
2.2.8	Vietnam	48
2.2.9	South Korea	48
2.2.10	Australia	48
2.3	Cybercrimes	50
2.4	Consumer Awareness	64
2.4.1	Youth as Consumer	85
2.5	Issues and Challenges	89
2.6	Research Gaps	92
3.	Research Design and Methodology	94
3.1	Introduction	94
3.2	Research Objectives	99
3.2.1.	Research Objective 1	99
3.2.1.1	Grounded Theory Methodology	100
3.2.2.	Research Objective 2	108
3.2.2.1	Total Interpretive Structural Modelling	109
3.2.3.	Research Objective 3	111
3.2.3.1	Structural Equation Modelling	112
3.3	Research Design	114

3.4 Sampling Design	114
3.5 Conclusion	116
4. Exploratory Study of Consumer Awareness factors on cyberlaw among Indian Youth	118
4.1 Introduction	118
4.2 Restatement of Research Objective 1	120
4.3 Research Methodology and Sample selection criteria	120
4.4 Coding process	124
4.4.1 Digital Protection Measures	134
4.4.2 Cyber Risks & Attacks	135
4.4.3 Information Sharing	136
4.4.4 Technology Adoption	137
4.4.5 Awareness Channels	138
4.4.6 Cyber Acts & Policies	138
4.4.7 Governing Mechanism	139
4.4.8 Consumer Experience	139
4.4.9 Educational Curriculum	139
4.5 Synthesis and Findings	146
4.5.1 Category 1 – Digital Protection Measures	148
4.5.2 Category 2 – Cyber Risks & Attacks	151
4.5.3 Category 3 – Information Sharing	154
4.5.4 Category 4 – Technology Adoption	157
4.5.5 Category 5 – Awareness Channels	163

4.5.6	Category 6 – Cyber Acts & Policies	170
4.5.7	Category 7– Governing Mechanism	175
4.5.8	Category 8 – Consumer Experience	178
4.5.9	Category 9 – Educational Curriculum	184
4.6	Conclusion	189
5.	Development of a hierarchical model of Consumer Awareness factors on cyberlaw and contextual evidences	190
5.1	Introduction	190
5.2	Restatement of Objective 2	190
5.3	TISM – Total Interpretive Structural Modeling	191
5.3.1	Overview of Methodology	191
5.3.2	Steps for Total Interpretive Structural Modeling	193
5.3.2.1	Step 1 – Identify and define elements	193
5.3.2.2	Step 2 – Define contextual relationship	194
5.3.2.3	Step 3 – Interpretation of Relationship	195
5.3.2.4	Step 4 – Interpretive logic of pair-wise comparison	195
5.3.2.5	Step 5 – Reachability Matrix and Transitivity check	203
5.3.2.6	Step 6 – Level Partition on reachability matrix	204
5.3.2.7	Step 7 – Developing a Diagraph	207
5.3.2.8	Step 8 – Interaction Matrix	208
5.3.2.9	Total Interpretive Structural Model	213
5.4	Interpretation and Findings	215
5.5	MICMAC Analysis	219

5.6 Contextual Evidences	221
5.6.1 Contextual Evidence 1	224
5.6.2 Contextual Evidence 2	227
5.6.3 Contextual Evidence 3	233
5.6.4 Contextual Evidence 4	236
5.6.5 Contextual Evidence 5	240
5.6.6 Contextual Evidence 6	246
5.7 Conclusion Remarks	250
6. Empirical Validation of Cyberlaw in the Context of Indian Youth	253
6.1 Introduction	253
6.2 Objective of the Study	253
6.3 Survey Instrument	254
6.4 Sampling and Data Collection	258
6.5 Sampling Demographic Profile	258
6.6 Methodology	260
6.7 Hypothesis Development	261
6.7.1 Technology Adopation	261
6.7.2 Governing Mechanism	262
6.7.3 Educational Curriculum	263
6.7.4 Consumer Experience	263
6.7.5 Cyber Acts & Policies	264
6.7.6 Cyber risks & Attacks	264
6.7.7 Information Sharing	265

6.8	Stastical Analysis	265
6.8.1	Descriptive Analysis	265
6.8.2	Measurement of Model	267
6.8.2.1	Common Method Bias	268
6.8.2.2	Reliability	269
6.8.2.3	Validity	271
6.9	Structural Model Analysis	274
6.9.1	Collinearity Checks	274
6.9.2	Hypothesis Testing	275
6.10	Confirmatory Factor Analysis	276
6.11	SEM Model	281
6.12	Concluding Remarks	282
7	Discussion and Conclusion	284
7.1	Introduction	284
7.2	Reconsidering the research questions and study approach	285
7.3	Summary of Key Findings	287
7.4	Research Contributions	291
7.5	Implications of the Study	293
7.6	Limitations of study	295
7.7	Directions for Future Research	297
7.8	Conclusion	298
8	Organisation of Thesis	300
9	List of Publications	301

10 References	302
11 Appendix	349

LIST OF FIGURES

Figure: 1.1 Number of users using Internet in Mobile phones	5
Figure: 1.2 Total No. of Wireless Data subscribers in the last 5 years	5
Figure: 1.3 Total No. of Internet users from 2010 to 2040	6
Figure: 1.4 Total No. of Smartphone users from 2010 to 2040	7
Figure: 1.5 Consumption of data in gigabytes	7
Figure: 1.6 Cybersecurity ranking across 20 countries	18
Figure: 1.7 Research Roadmap for the study	25
Figure: 2.1 List of countries where consumers lodge complaints on online fraud	64
Figure: 2.2 Changes between CPA 1986 & CPA 2019	79
Figure: 3.1 Research Methodology for Study 1	100
Figure: 3.2 Research Methodology for Study 2	109
Figure: 3.3 Research Methodology for Study 3	111
Figure: 3.4 Model fit indices description	113
Figure: 3.5 Research Framework of the study	114
Figure: 4.1 Steps for Grounded Theory Methodology	120
Figure: 4.2 Steps for MAXQDA process	122
Figure: 4.3 Process of Grounded Theory Methodology	133
Figure: 4.4 An instance from MAXQDA	140
Figure: 4.5 Category 1 - Digital Protection Measures and its codes	141
Figure: 4.6 Category 2 – Cyber Risks & Attacks and its codes	141
Figure: 4.7 Category 3 - Information Sharing and its codes	142

Figure: 4.8 Category 4 - Technology Adoption and its codes	142
Figure: 4.9 Category 5 - Awareness Channels and its codes	143
Figure: 4.10 Category 6 – Cyber Acts and Policies and its codes	143
Figure: 4.11 Category 7 - Governing Mechanism and its codes	144
Figure: 4.12 Category 8 - Consumer Experience and its codes	144
Figure: 4.13 Category 9 - Educational Curriculum and its codes	144
Figure: 4.14 Code Cloud of Consumer Awareness on Cyberlaw Factors	145
Figure: 4.15 Code Portrait of codes from MAXQDA	145
Figure: 5.1 Basic process of TISM Model	192-193
Figure: 5.2 Diagraph view	208
Figure: 5.3 Level Partition	210
Figure: 5.4 A Diagraph Model	214
Figure: 5.5 Results of MICMAC Analysis of Factors	220
Figure: 5.6 Contextual Evidence 1	226
Figure: 5.7 Contextual Evidence 2	232
Figure: 5.8 Contextual Evidence 3	235
Figure: 5.9 Contextual Evidence 4	239
Figure: 5.10 Contextual Evidence 5	245
Figure: 5.11 Contextual Evidence 6	249
Figure: 6.1 Confirmatory Factor Analysis Model	280
Figure: 6.2 Final SEM Model	281
Figure: 8.1 Organisation of Thesis	300

LIST OF TABLES

Table: 2.1 Acts amended in IT Act, 2000	29-30
Table: 2.2 Sections in IT Act, 2000 and IT (Amend) Act, 2008	31-32
Table: 2.3 Sections related to IPC	32-33
Table: 2.4 Cybercrimes amended in IT (amend) Act, 2008	35-36
Table: 2.5 Prohibited Acts in ITE law, Indonesia	41
Table: 2.6 Cyber laws in Japan	42
Table: 2.7 Greece Cyber Laws	47-48
Table: 2.8 Cyber laws in Australia	49
Table: 2.9 Definition of Cybercrime	52-55
Table: 2.10 Types of Cybercrime	56-61
Table: 2.11 Ways to overcome/handle attacks	62-63
Table: 2.12 Consumer Awareness rights	66
Table: 2.13 Consumer Awareness details	69-73
Table: 2.14 List of factors from consumer awareness research papers	75-78
Table: 2.15 Definition of youth by different organisations	86
Table: 3.1 Difference between Qualitative research and Quantitative research	97-98
Table: 3.2 Types of Qualitative Research	98
Table: 3.3 Comparison of Strauss and Corbin and Glaser GTM	102
Table: 3.4 Different approaches of GTM from researchers	103-104
Table: 3.5 Comparison of Grounded Theory Methodology (GTM) types	105-107
Table: 3.6 Data collection methods	116
Table: 4.1 Interview Expert Details	123

Table: 4.2 List of open codes generated from transcripts	124-128
Table: 4.3 List of selected open codes from the study	128-129
Table: 4.4 Definition of Each Category	130-133
Table: 5.1 Element Number and Element Name	193
Table: 5.2 Identified Elements with authors	194
Table: 5.3 Interpretive Logic Knowledge Base	195-202
Table: 5.4 Initial Reachability Matrix	203
Table: 5.5 Final Reachability Matrix (* Transitive Relations)	204
Table: 5.6 Reachability Matrix for Iteration I	205
Table: 5.7 Reachability Matrix for Iteration II	205
Table: 5.8 Reachability Matrix for Iteration III	206
Table: 5.9 Reachability Matrix for Iteration IV	206
Table: 5.10 Reachability Matrix for Iteration V	207
Table: 5.11 Reachability Matrix for Iteration VI	207
Table: 5.12 List of factors and their levels	207
Table: 5.13 Interpretive Matrix	209
Table: 5.14 Binary Matrix	209-210
Table: 5.15 Interaction Matrix	211-213
Table: 5.16 Element Linkages & Respondent responses	217-219
Table: 5.17 Driving power and dependence power of MICMAC analysis	219-220
Table: 5.18 MICMAC Rankings of Factors	220
Table: 5.19 Categories and Subcategories of the study	221-224
Table: 5.20 Factor Relationships with Contextual Evidence 1	224-225

Table: 5.21 Factor Relationships with Contextual Evidence 2	227-231
Table: 5.22 Factor Relationships with Contextual Evidence 3	233-235
Table: 5.23 Factor Relationships with Contextual Evidence 4	236-238
Table: 5.24 Factor Relationships with Contextual Evidence 5	240-241
Table: 5.25 List of countries having cyber legislations	242-244
Table: 5.26 Factor Relationships with Contextual Evidence 6	246-249
Table 6.1 Independent Variables (Constructs) questionnaire	254-257
Table: 6.2 Demographic profile of age of respondents	259
Table: 6.3 Demographic profile of gender of respondents	259
Table: 6.4 Demographic profile of occupation of respondents	259
Table: 6.5 Demographic profile of education of respondents	259
Table: 6.6 Demographic profile of income level of respondents	260
Table: 6.7 Demographic profile of location of respondents	260
Table: 6.8 Descriptive statistics of empirical studies	266-267
Table: 6.9 Mean, Variance, and S.D. of constructs	267
Table: 6.10 Mean, Variance, and S.D. & Cronbach Alpha of Consumer Awareness	267
Table: 6.11 Common Method Bias	268-269
Table: 6.12 Cronbach Alpha and Composite Reliability of constructs	269
Table: 6.13 KMO Value, Eigenvalues, and total % of variance	270
Table: 6.14 KMO Value, Eigenvalues, and total % of variance & factor loadings of consumer awareness	270
Table: 6.15 Factors Loading & Average Variance extraction of constructs	271-272
Table: 6.16: Discriminant validity of all constructs with correlation values	273

Table 6.17: Discriminant validity of all constructs according to Fronell-Larcker criteria	273-274
Table 6.18: Threshold value and VIF of constructs	275
Table 6.19: Hypothesis Testing Result	276
Table 6.20: Model fit values of Confirmatory Factor Analysis of SEM Model	277
Table 6.21: Model fit estimate values of CFA values in SEM	278-279
Table 6.22: Model fit indices of final SEM Model.	282