Advances in Social Sciences Research Journal – Vol.4, No.6
Publication Date: March 25, 2017
DoI:10.14738/assrj.46.2901.

Sooriyabandara, V. (2017). An Analysis of the Legitimate Coverage to Minimize the Cybercrimes in Sri Lanka. *Advances in Social Sciences Research Journal,* 4*(6)* 187-206

An Analysis of the Legitimate Coverage to Minimize the Cybercrimes in Sri Lanka

Vishakha Sooriyabandara (Attorney At Law)
Senior Lecturer in Political Science, Department of Political science
University of Sri Jayewardenepura
Sri Lanka

ABSTRACT

The purpose of this study is to find out the legitimate rules and regulations to minimize the cybercrimes in Sri Lanka and to find out the existing weaknesses of the cybercrime law and the level of minimization of cybercrimes. The research study first analyses what is really meant by cybercrimes and the reasons for the emergence of cybercrimes. Then the study closely looks at how cybercrimes can be categorized under different sub units and cybercrime examples for each of such sub units. The latter part of the research study highlights the importance of cyber rules and regulations in a situation where there is an increasing trend towards cybercrimes. Within this part it first looks at the current level of internet security in Sri Lanka. Subsequently it examines the level of awareness of the cybercrime laws and the level of strangeness of such laws. Finally the research study evaluates the behavior of cybercrimes in terms of changes in the current level of internet security; the level of awareness of the cybercrime laws and the level of strengthens of such laws. The research findings emphasize that there is a strong relationship between the level of internet security in Sri Lanka, the level of awareness of cyber laws and the level of strength of such laws separately with the number of cybercrimes in Sri Lanka and it also evidences that there is an influential effect of aggregate impact of the three independent variables on the number of cybercrimes in Sri Lanka. Based on the research findings, the level of existing weaknesses of cyber laws in Sri Lanka have been identified and suggestions to minimize such crimes have been provided accordingly.

Key words: cybercrimes, cyber laws, internet security

INTRODUCTION OF THE STUDY

Background of the study

Emergence of cybercrimes

The advancements of the modern technology have helped countries in developing and expanding their communication networks enabling faster and easier networking and information exchange. Currently there are nearly three billion internet users (www.internetlivestats.com/internet-users/, 24/11/2015) and over five billion mobile phone users worldwide (www.statista.com/statistics/274774/forecast-of-mobile-phone-users worldwide/, 24/11/2015). Everyday billions of emails and phone messages are exchanged all over the world. Most people around the world now depend on consistent access and accuracy of these communication channels.

The growing popularity and convenience of digital networks, however, come at a cost. As businesses and societies in general increasingly rely on computers and internet based networking, cybercrimes and digital attacks are increasing rapidly around the world.

Cybercrimes and its classifications

These cybercrimes can generally be defined as ''any illegal activity that uses a computer as its primary means of commission'' (searchsecurity.techtarget.com/definition/cybercrime, 24/11/2015).

Cybercrimes can be broadly classified as cybercrimes against persons, cybercrimes against property, cybercrimes against governments and cybercrimes against society.

Cybercrimes against persons

- Harassment via E-Mails
- Cyber-Stalking
- Dissemination of obscene material
- Defamation
- Hacking
- Cracking

Cybercrimes against property

- Intellectual property crimes
- Cyber squatting
- Cyber vandalism
- Transmitting viruses
- Cyber trespass
- Internet time theft

Cybercrimes against governments

- Cyber terrorism
- Cyber welfare
- Distribution of pirated software
- Possession of unauthorized information

Cybercrimes against society

- Cyber trafficking
- Online gambling
- Financial crimes
- Forgery
- Childpornography

Need of cyber rules and regulations

The users of cyberspace are rapidly increasing and the range of online interactions is expanding. Therefore there is a significant room for growing cybercrimes. Due to these consequences there is a need to adopt strict laws by the cyber space authorities to regulate criminal activities relating to cyber and to provide a better administration of justice to the victims of cybercrimes.

In the modern cyber technology world, it is very much necessary to regulate cybercrimes and most importantlycyber laws should be made stricter in the case of cyber terrorism and hackers. Mostly people are less aware about the available cyber laws. So the current need is making aware the society about cyber laws in order to minimizing the possible threats from cybercrimes in an effective manner.

Objectives of the study

The objectives of the study can be identified in relation to two main areas. They are

- To find out the existing legitimate rules and regulations to minimize the cybercrimes in Sri Lanka
- To find out the existing weaknesses of the cybercrime law and the level of minimization of cybercrimes

Scope of the study

This research study is basically carried out by taking the perceptions of 40 respondents regarding the cybercrimes in Sri Lanka and various factors that affect to the behavior of cybercrimes.

The respondents include both employed and unemployed persons. The perceptions of those respondents have been gathered majorly under four age categories. They are the 20-25, 25-30, 30-35 & 35-40. And also the research study has gathered the perception of both male and female respondents as well.

LITERATURE REVIEW

Summary of the selected research paper

The selected research paper is "the effects of crime on legitimate businesses'' by Frank J Marine in 2006.

As asserted by Marine, F, J (2006), the purpose of this paper is to examine the development and nature of organized crime in the USA over the past 50 years, emphasizing organized crime's corruption and victimization of legitimate businesses and describing law enforcement's efforts to combat organized crime through specific case studies.

First, the paper analyses the control over and corruption of legitimate businesses in USA by the La Cosa Nostra ("LCN" or the American mafia), including the industries such as Las Vegas gaming; moving and storage; garment; waste – hauling; and, construction, and the following unions: the International Brotherhood of teamsters; Laborers international Union of North America; and, the International Longshoreman's Association.

The research paper also describes the success of the law enforcements' efforts to combat such corruption through the use of criminal and civil racketeering laws and specific prosecutions. The paper then discusses the emergence in the mid – 1980s of non-traditional organized crime groups in USA, including various Asian ethnic groups and large scale human trafficking organizations that impact Europe and Asia as well as the USA.

As per Marine, F, J (2006), the findings of this research article concludes that the nontraditional criminal groups not only prey on the legitimate businesses in ethnic Asian communities in the USA, but they also engage in complex crimes, alien smuggling, drug trafficking, credit card frauds, money laundering and, other financial crimes. A new era has been emerged for organized crimes that began in the 1990s with the fall of the former Soviet Union and the emergence of transnational organized crime groups emanating from the nations comprising the former Soviet Bloc. These organized crime groups engage in a wide variety economic crimes including extortion, fraud, illicit appropriation of natural resources, and public corruption. Such extensive corruptions threaten the stability of some of these emerging nations.

Marine, F, J (2006), emphasizes that this paper will be effectively used by law enforcement officers and policy makers to assist them to understand the scope and nature of organized crime's adverse effects upon business and economic interests and to develop tools to combat such criminal activities.

Summaries of other research papers relevant to the research topic

Cybercrimes

A cybercrime refers to "any illegal activity that occurs in the virtual world of cyberspace" (Henson, Reyns and Fisher, 2011). Most of the definitions refer internet crimes as cybercrimes. But some wrongly defined computer crimes as internet crimes (Henson, Reyns and Fisher, 2011). Cybercrimes can also be defined as "any criminal offense that is committed or facilitated through the use of the communication capabilities of computers and computer systems.

Categories of cyber crimes

As per Saini, H, Rao, Y, S. and Panda, T, C. (2012, pp.202-209), cybercrimes can be categorized as follows.

Data crime

Data interception

An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a latter attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. The most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variant the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted.

Data modification

In a data modification attack, an unauthorized party on the network intercepts data in transits and changes parts of that data before retransmitting it. In a replay attack, an entire set of valid data is repeatedly interjected onto the network. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. Privacy of communication is essential to ensure that data cannot be modified or viewed in transits.

Data theft

This is the term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security, numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely the individual will be prosecuted to the fullest extent of the law.

Network crime

Network interferences

These crimes involve network interfering with the functioning of the computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing network data.

Network sabotage

Network sabotage or incompetent managers trying to do the jobs of the people they normally are in charge of? It could be the above alone, or a combination of things. But if Verizon is using the help the children, hindering first responders line then they might be using network problems as an excuse to get the government to intervene in the interest of the public safety.

Access crime

Unauthorized access

This is an insider's view of the computer cracker underground. Unauthorized access looks at the personalities behind the computers screens and aims to separate the media hype of the outlaw hacker from the reality.

Virus dissemination

This concerns malicious software that attaches itself to other software and destroys the system of the victims. Examples for such malicious software are viruses, worms, Trojan horse, Time bomb, Logic bomb etc…

Related crime

Aiding and abetting cybercrimes

There are three elements of most aiding and abetting charges against an individual. The first is that another person committed the crime. The second, the individual being charged had knowledge of the crime or the principals' internet. The third is the individual provided some form of assistance to the principle.

Computer related forgery and fraud

Computer forgery and computer related fraud constitute computer related offenses.

Content related crimes

Cybersex, unsolicited commercial communications, cyber defamation and cyber threats are included under this category.

Impact of cybercrimes on society

As per Pariyani R, some major impacts of cybercrimes can be identified under potential economic impact, impact on market value, impact on customer trust and impact on national security.

Potential economic impact

These crimes make a large economic impact because it involves losses of millions of dollars per year. Since the consumers today have been dependent on computers, networks and internet database therefore they restored and preserved information in internet is used by the criminal and therefore risk of being subjected to victimization becomes high (PTI Contents, 2009). Every day, new attacks on the confidential, integrity, and availability of computer system can be heard. This could range from the theft of personally identifiable information to denial of service attacks.

As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber criminals. Today talks are traded to internet, purchase are made using plastic money, banking transactions can be done online, and many such other activities are carried out through internet and all these instances consists of chances of final fraud by cyber criminals and hence affect the economy. Similar the disturbances of international financial markets create big impact on international economic position. Hence many attacks on cyberspace related with financial activities send shock waves outside of the market which is the source of problem. The productivity today is also risks attacks from worms and viruses etc… take productivity time away from the user. Machines may be made to perform slowly, networks are jammed and other attacks are done to negative by the organization activities. In addition to all these the potential fraud committed against online shoppers during transactions also considered to make laws to the economic zone and the breach of thrust against the consumer repercussions and bear going into more detail.

Impact on market value

The cybercrimes make a greater impact on the market value of a country also. The economic impact of security breaches of interests to companies trying to decide where to place their information security budgets as well as for insurance companies "that provides cyber risk policies". Micro stated that physical damage is restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality (Ariz, D. 2000). These kinds of damages affect more severely as many firms rely on information systems in general and the internet in particular to conduct their business due to these reasons also, many insurance companies are bound to compensate businesses for the damage caused by such cyber-attacks for other security breaches. As the characteristic of security breaches change, companies continually reassess there is environments of threats (Kelly, B, J. 1999). However, assessing the financial loss from a potential IS security breach is a difficult step in the risk assessment process for the following reasons.

- It is not possible for many organizations to quantify their financial losses due to security beaches (Power, R. 2011).
- Due to lack of historical data many security breaches are unreported. In similar situation, companies are reluctant to disclose these breaches due to management embarrassments, fear of future crimes (Hoffer, J.A, Straub, D.W. 1989), and fear of negative publicity.
- Additionally, there is a fear of negative financial consequences resulting from public disclosure of security breach (Sprecher, R, Pertl, M. 1988).

Impact on consumer trust

The consumers hold the major impact of market and breach of their trust amounts to a huge impact on economic position through cyberspace. Hence such attackers enter into other space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The disputed site is termed as fraudulent but the master mind criminal as not recognized as its main cause. This makes the loss of confidence in the customer and in the internet and its strengths.

It is also a perception that the internet is widespread with credit card fraud and security hazards are growing. It can be seen as a serious problem for e commerce. Also, any concern over the credibility of an e business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception security risk on e –commerce, seriously paralyzes the potential of business.

Impact on national security

Today most of the countries have advanced computer systems for their military system. But information warfare, including network attack, exploitation, and defense, isn't a new national security challenge. The crimes of this level are being increasing because of low cost, highly effectiveness and deniability to the attacker. Malware are being spread misinformation is also being spread with it. When the criminals find systems that are easy easily breakable they simply hack the system and the terrorists and criminals use information technology to execute the criminal activities. Because of advanced technology such crimes may be committed from any part of the world and therefore criminals find loopholes in the security system of the country to be targeted and perform the task from part of other country other than their own country to confuse the victim during investigation. The internet has helped funding of cybercrimes by means of fraudulent bank transactions, money transfer etc… in developed countries by which these crimes are done. Greater encryption is helping these criminal activities.

Cyber Security

As per Homeland Security, unlike other threats currently facing the country, cyber-attacks on individual citizens can have instant, wide – ranging consequences for the nation's broader national and economic security interests. No country, industry, community, or individual is immune to cyber risks, and no one government agency, company, or individual can solve the riddle of cyber security.

Across America, more than 800,000 law enforcement officers work to keep our nation safe and secure. The Department of homeland Security (DHS) collaborates with law enforcement in combating cybercrime through many ways including the following ways.

The Homeland Security Information Network (HSIN)

This provides law enforcement officials at every level of government with a means to securely collaborate with partners across geographic and jurisdictional boundaries. Law enforcement organizations use HSIN to quickly share information with mission specific contact lists including, Be on the Lookout (BOLOs), Requests for Information (RFIs), For Your Information (FYIs), Intelligence Reports and other sensitive documents.

National Network

To increase cyber security awareness across the country to people of all ages, the stop, think, connect. Campaign established the National Network, which is comprised of not for profit groups and organizations that advocate and promote cyber security. D.A.R.E is a member of the National Network and has collaborated with the campaign on local outreach efforts and resource distribution.

Cyber awareness coalition

Federal agencies and state, local, tribal, and territorial governments from the Federal Bureau of Investigation (FBI) to the state of California are engaged in the campaign. Coalition members through alerts, teleconferences, newsletters, and meetings make effective use of existing communications channels and outreach capabilities to spread the Stop, Think, Connect, messages.

Cyber Tours

Cyber tours directly engage communities in promoting awareness and dialogue about the dangers Americans face online. Through a series of events and forums, cyber tours with the help of law enforcement bring together federal, state and local entities, industry, academia, non-profits and individual citizens to emphasize theimpact internet safety has on all segments of a community.

Secondary data

As many developing and non-developing countries, now a day Sri Lankan community is also experiencing the cybercrimes and its related impacts. This is mainly due to the widely spread use of the internet facilities, mobile phones and computers etc… in day today activities.

According to the Central Bank - Sri Lanka, (www.lankabusinessonline.com/sri-lankas-mobile-internet-usage-grows-85-8-pct-in-2014-cb/, 24.11.2015) total internet connections have grown by 68.4 per cent during 2014 raising internet penetration (connections per 100) to 16.4.And also the numbers of mobile phone connections have increased by 8.9 per cent while fixed wire line telephone connections recorded a 5.7 per cent growth in 2014.

Those factors have contributed more in the increasing trend in cybercrimes in Sri Lanka. Therefore it is crucial to look at the available law enforcements and other relevant authorities that have been established aiming at minimizing the level of cybercrimes in Sri Lanka.

Computer Crimes Act, No.24 of 2007

Computer Crimes Act, No.24 of 2007 is the main law enforcement in Sri Lanka enacted by the parliament of the democratic Socialist Republic of Sri Lanka. The objective of this act is "to provide for the identification of computer crime and to provide the procedure for the investigation and prevention of such crimes; and to provide for matters connected therewith and incidental thereto" (Computer Crimes Act, No.24 of 2007).

According to the computer Crimes Act, a person who breaches the provisions prescribed in the act is liable for either a fine, imprisonment or both.

Sri Lanka Computer Emergency Readiness Team | Coordination Centre (CRET)

CERT is the single trusted source of advice about the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from cyber-attacks (www.slcert.gov.lk, 24.11.2015). This was set up in June 2006, in collaboration with the Information and Communication Technology Agency (ICTA) of Sri Lanka.

CERT provides three services to its constituency. They are,

- Responsive services
- Awareness services
- Consultancy services

CERT provides several channels to report an accident relating to cyber. It facilitates to fill the accident reporting form on the web site, to contact through telephone or to send a fax or email. CERT disseminates information about the incident and the precautions that need to be taken, through all publicly accessible media.

All the above secondary data gathered has been used to get more knowledge and an idea on preparing the Part 2, 3, 4 and 5 of the questionnaire.

RESEARCH METHODS

Data Collection Methods

For the research study, the relevant data is collected mainly through a developed questionnaire. The questionnaire basically includes five parts. The first part of the questionnaire gathers all the demographic data in relation to the respondents. It collects the information such as gender, age, employability of the respondents etc…

The rest of the parts of the questionnaire basically deal with the Likert scale questions asked in relation to the different perspectives of the respondents regarding the determined dependent variable and the three independent variables.

In that, the second part examines the perceptions of the respondents regarding the cybercrimes in Sri Lanka and the third part of the questionnaire gathers the perceptions regarding the level of internet security in Sri Lanka. Subsequently the forth part collects the perceptions about theawareness of the cyber laws and regulations. Finally, the fifth part gathers the data in relation to the level of strength of the cyber laws.

Types of Variables

In the research study, mainly two types of variables have been identified. They are;

1. Independent variables
2. Dependent variables

Those variables have been created in line with the objectives recognized. The research study includes only one dependent variable. That has been identified as “Number of cybercrimes in Sri Lanka”.

In addition to this dependent variable, there are three significant independent variables have been identified. Those are “Level of internet security in Sri Lanka”, “Awareness of cyber laws and regulations” and “Level of strength of cyber laws in Sri Lanka”.

LIST OF HYPOTHESES

Based on the objectives determined and the variables developed, the relationships between each three independent variables with the dependent variables have been emphasized. In relation to this, three key hypotheses are developed that is expected to be tested in the data analysis part of the research study. Those developed hypotheses are as follows.

Hypothesis 1

Ho1 – There is no relationship between the level of internet security and number of cybercrimes in Sri Lanka

Ha1 - There is a relationship between the level of internet security and number of cybercrimes in Sri Lanka

Hypothesis 2

Ho1 – There is no relationship between the awareness of cyber laws and regulations and number of cybercrimes in Sri Lanka

Ha1 - There is a relationship between theawareness of cyber laws and regulations and number of cybercrimes in Sri Lanka

Hypothesis 3

Ho1 – There is no relationship between the level of strength of cyber laws and number of cybercrimes in Sri Lanka

Ha1 - There is a relationship between the level of strength of cyber laws and number of cybercrimes in Sri Lanka

SAMPLE

The sample for the study is selected based on the convenience sampling method. Hence the respondents are selected in a random manner by assuming the sample is properly representative.

The total sample consists of forty respondents including both male and female respondents. The selected sample has been divided in to four based on the age of the respondents.

The sample represents the perceptions of the employed respondents as well as the unemployed respondents.

Data Analysis Methods

In this research study, all the collected data through the questionnaire has been basically analyzed by using,

1. Descriptive statistics
2. Hypotheses testing

Descriptive statistics

Descriptive statistics methods have been used to carry out an analysis of all the demographic data collected through the questionnaires. This study has employed several descriptive statistics methods. Those descriptive statistics have been used to provide a concise summary of demographic data numerically and graphically.

Hypotheses testing

This method of data analysis has been used to determine whether there is a relationship between the number of cybercrimes in Sri Lanka with each of the identified independent variables. That is hypotheses testing method has been used to determine whether the null hypotheses can be rejected or not.

DATA ANALYSIS

This part of the research study mainly built upon four major parts. They are analysis of demographic data, results of hypotheses testing, summary of findings and suggestions to mitigate cybercrimes in Sri Lanka.

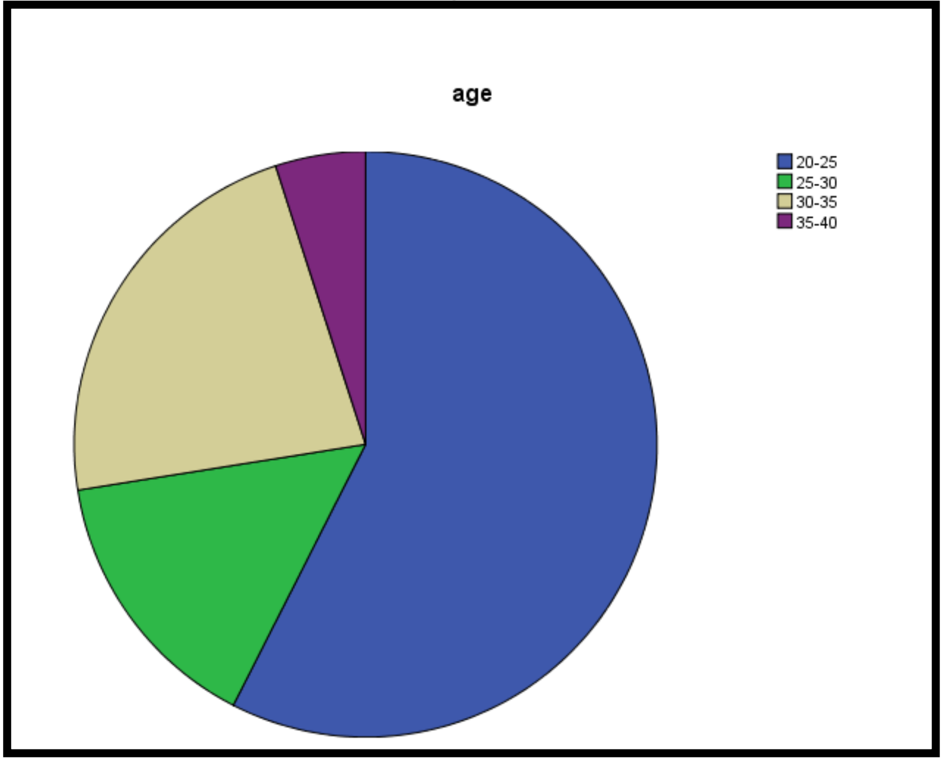
Analysis of demographic data

Age

Table 1

	Age Group	Frequency	Percent (%)	Valid Percent (%)	Cumulative Percent (%)
Valid	20-25	23	57.5	57.5	57.5
	25-30	6	15.0	15.0	72.5
	30-35	9	22.5	22.5	95.0
	35-40	2	5.0	5.0	100.0
	Total	40	100.0	100.0	

Figure 1



The age of the respondents were gathered under four age categories. Those are 20-25 age group, 25-30 age group, 30-35 age group and 35-40 age group. From the total respondents, most of the respondents are included under the age category of 20-25. It is 57.5% which is amounted to 23 out of 40 respondents.

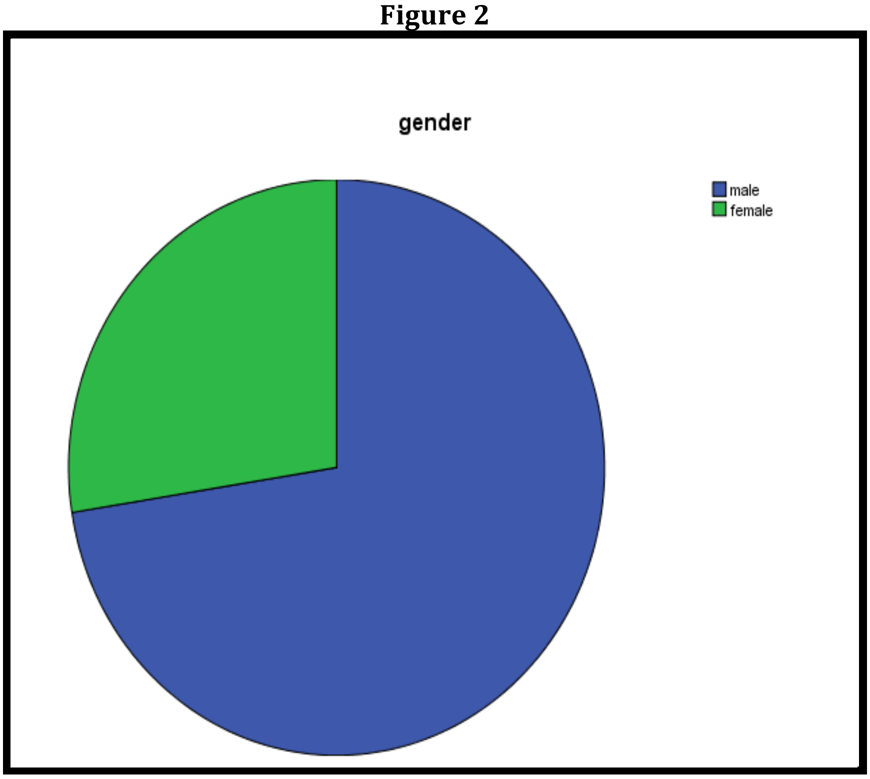
35-40 age group represents the least number of respondents. It is 5% from the total respondents. 25-30 age group and 30-35 age group include 6 and 9 respondents respectively. The respective percentages of those age groups are 15% and 22.5%.

Gender

Table 2

Gender Group		Frequency	Percent (%)	Valid Percent (%)	Cumulative Percent (%)
Valid	Male	29	72.5	72.5	72.5
	Female	11	27.5	27.5	100.0
	Total	40	100.0	100.0	

Figure 2



From the total of 40 respondents most of the respondents are male respondents. They represent a 72.5% which consist of 29 respondents.

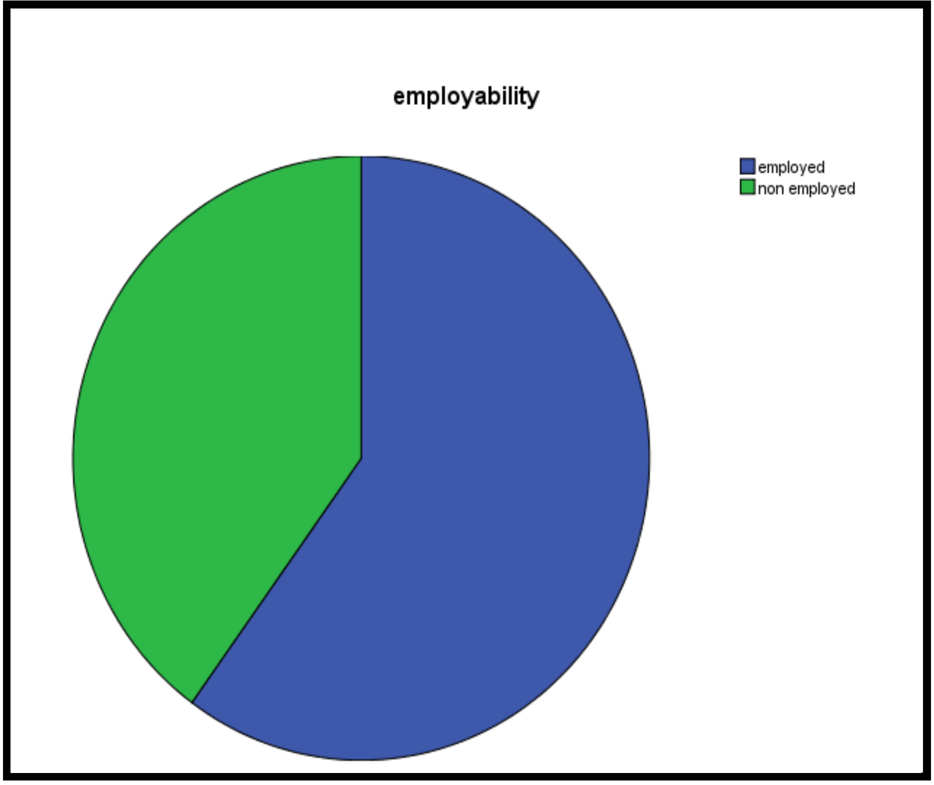
The balance portion of 27.5% represents the female respondents. Number of female students in the selected sample is 11 out of 40 respondents.

Employability

Table 3

	Employability	Frequency	Percent (%)	Valid Percent (%)	Cumulative Percent (%)
Valid	Employed	24	60.0	60.0	60.0
	Non employed	16	40.0	40.0	100.0
	Total	40	100.0	100.0	

Figure 3



The questionnaire also examined the employability of the respondents. Most of the respondents within the selected sample are employed in various jobs. The employed category symbolizes a 60% which is amounted to 24 numerically.

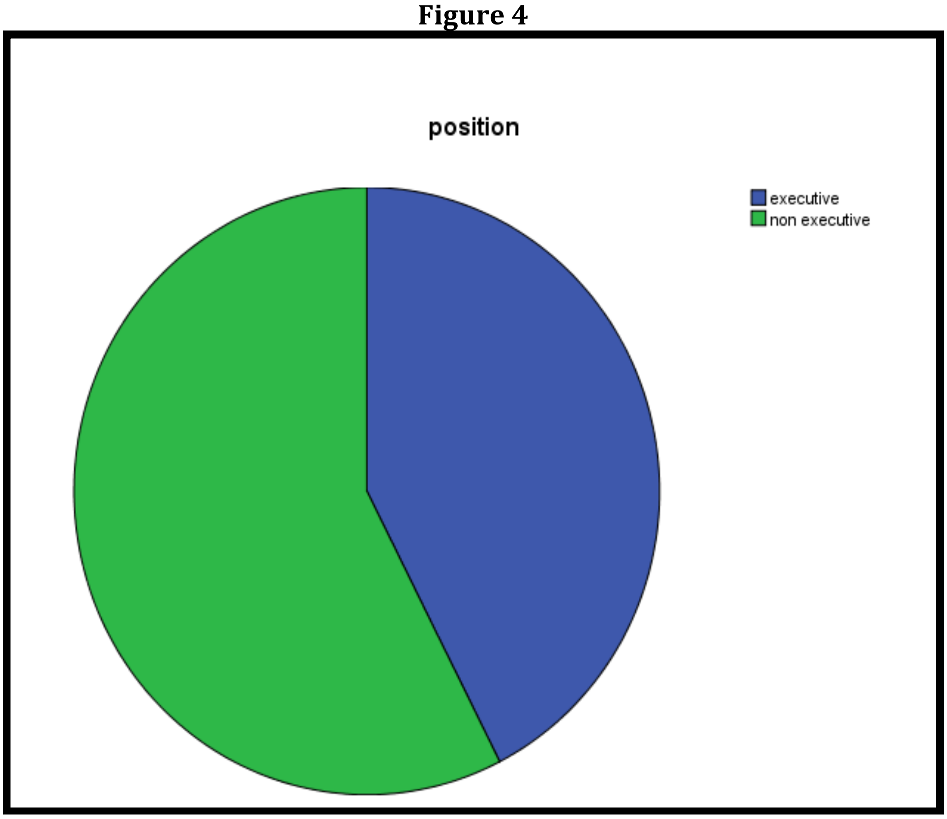
The remaining portion of the respondents is not employed in any occupation. They are 40% as a percentage. Numerically that is 16 out of total respondents.

Position

Table 4

	Position	Frequency	Percent (%)	Valid Percent (%)	Cumulative Percent (%)
Valid	Executive	10	41.6	41.6	41.6
	Non executive	14	58.4	58.4	100.0
	Total	24	100.0	100.0	

Figure 4



After questioning the employability of the respondents, the questionnaire was arranged to embrace the position of the employed students. The position of the employed students was gathered basically under two groups as "executive" and "non Executive".

From 24 employed students, majority represents the non executive group. That portion is 58.4 as a percentage and amounted to 14 respondents.

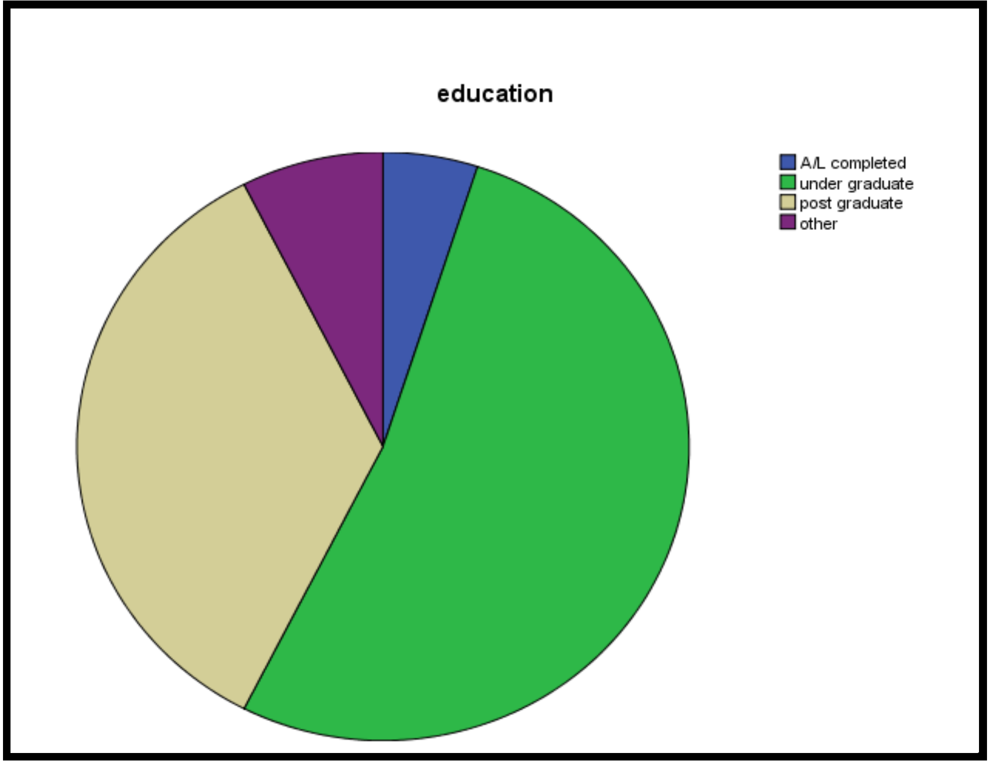
The rest of the sample represents the employed respondents who engage in executive positions. That is 41.6 as a percentage which is amounted to 10 out of 24 employed respondents

Level of Education

Table 5

	Level of Education	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	A/L completed	2	5.0	5.0	5.0
	Under graduate	21	52.5	52.5	57.5
	Post graduate	14	35.0	35.0	92.5
	Other	3	7.5	7.5	100.0
	Total	40	100.0	100.0	

Figure 5



Finally the level of education was tested within the part 1 in the questionnaire. The education level of the respondents was gathered basically under four categories as “A/L completed”, “Under graduate”, “Post graduate”, and “Other”.

From the provided four categories, the majority represents the under graduate category. That is a 52.5 as percentage which numerically represents 21 respondents. The rest of the sample represents the post graduate category, other category and the A/L completed category. The numbers of respondents that are amounted to each three categories are 14, 3 and 2 respectively. It is 35, 7.5 and 5 as a percentage of total number of respondents.

Hypotheses testing

Hypothesis 1

Hypothesis 1 is developed to see whether there is a relationship between the level of internet security in Sri Lanka and number of cybercrimes in Sri Lanka. Based on the respondents' answers, the following results were generated.

Table 6
Model Summary table

Model	R	R square	Adjusted R Square	Std. Error of the Estimate
1	.950[a]	**.903**	**.900**	.22474

a. Predictors: (Constant), average level of internet security

As per the table 6, the independent variable, the average level of internet security accounts for 90.3% of the variability of the dependent variable, average number of cybercrimes. After adjusting for the number of regresses it is 90%.

Table 7
ANOVA table

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	17.856	1	17.856	353.516	**.000[a]**
Residual	1.919	38	.051		
Total	19.775	39			

a. Predictors: (Constant), average level of internet security
b. Dependent Variables, average number of cybercrime

As reflected by the significant value of table 7, the null hypothesis of "there is no relationship between the level of internet security and number of cybercrimes in Sri Lanka" is highly rejected.

Hypothesis 2

Hypothesis 2 is developed to see whether there is a relationship between the awareness of cyber laws and regulations and number of cybercrimes in Sri Lanka. Based on the respondents' answers, the following results were generated.

Table 8
Model Summary table

Model	R	R square	Adjusted R Square	Std. Error of the Estimate
1	.883[a]	**.779**	**.773**	.33911

a. Predictors: (Constant), average awareness of cyber laws and regulations

As per the table 6, the independent variable, the average awareness of cyber laws and regulations accounts for 77.9% of the variability of the dependent variable, average number of cybercrimes. After adjusting for the number of regresses it is 77.3%.

Table 9
ANOVA table

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	15.405	1	15.405	133.966	**.000[a]**
Residual	4.370	38	.115		
Total	19.775	39			

a. Predictors: (Constant), average awareness of cyber laws and regulations
b. Dependent Variables, average number of cybercrime

As reflected by the significant value of table 9, the null hypothesis of "there is no relationship between the awareness of cyber laws and regulations and number of cybercrimes in Sri Lanka" is highly rejected.

Hypothesis 3

Hypothesis 3 is developed to see whether there is a relationship between the level of strength of cyber laws and number of cybercrimes in Sri Lanka. Based on the respondents' answers, the following results were generated.

Table 10
Model Summary table

Model	R	R square	Adjusted R Square	Std. Error of the Estimate
1	.859[a]	**.737**	**.730**	.36967

a. Predictors: (Constant), average strength of cyber laws

As per the table 10, the independent variable, average strength of cyber laws accounts for 73.7% of the variability of the dependent variable, average cybercrimes. After adjusting for the number of regresses it is 73%.

Table 11
ANOVA table

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	14.582	1	14.582	106.705	**.000**[a]
Residual	5.193	38	.137		
Total	19.775	39			

a. Predictors: (Constant), average strengths of cyber laws
b. Dependent Variables, average number of cybercrime

As reflected by the significant value of table 11, the null hypothesis of "there is no relationship between the level of strength of cyber laws and regulations and number of cybercrimes in Sri Lanka" is highly rejected.

The overall validity of the model

Table 12
Model Summary table

Model	R	R square	Adjusted R Square	Std. Error of the Estimate
1	.965[a]	**.931**	**.926**	.19425

a. Predictors: (Constant), average strength of cyber laws, average awareness of cyber laws, average level of internet security

The model accounts for 93.1% of variability in the dependent variable. After adjusting for the number of regresses it is 92.6%.

Table 13
ANOVA table

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	18.417	3	6.139	162.691	**.000**[a]
Residual	1.358	36	.038		
Total	19.775	39			

a. Predictors: (Constant), average strength of cyber laws, average awareness of Cyber laws, average level of internet security
b. Dependent Variables, average number of cybercrime

The significant value as depicted by table 14 asserts that there is a strong relationship between the aggregate impact of the identified three independent variables and the cybercrimes in Sri Lanka.

SUMMARY OF FINDINGS

The results of the data analysis provide that approximately 75% of the respondents from the total sample are below 30 years. The majority of the sample represents male respondents. When evaluating the employability of the respondents, it evidences that most of the respondents are employed. From the employed respondents the majority is engaged in non executive job positions. On the other hand, the majority of the respondents reflect the under graduate and post graduate education levels. This is approximately 88% from the total sample. These results may be generated mainly due to the employed convenience sampling method which basically attended to the community associated with the University of Sri Jayewardenepura.

On the other hand, the majority of the non executive job holders which is 58.4% can be justified by the majority of undergraduates which is 52.5%.

As per the three hypotheses tested within the research study, it emphasizes that all the three null hypotheses can be strongly rejected.

That is, firstly there is a strong relationship between the level of internet security in Sri Lanka and the number of cybercrimes in Sri Lanka. As per the tested results, secondly there is a strong relationship between the level of awareness of cyber laws and regulations and the number of cybercrimes in Sri Lanka. And also finally, there is a strong relationship between the level of strength of cyber laws and the number of cybercrimes in Sri Lanka.

In addition to the separate results of the three hypotheses, the overall model indicates that, there is a strong relationship between aggregate impact of the three independent variables and the dependent variables.

SUGGESTIONS TO MITIGATE CYBERCRIMES IN SRI LANKA

Therefore as emphasized by the research findings, it is important to focus on increasing the level of internet security, the level of awareness regarding cyber laws and regulations and the level of strength of cyber laws in Sri Lanka as a solution to the increasing number of cybercrimes occurring within the country and across countries.

The national governing body of the country has a major role to implement actions in preventing and mitigating such internet related crimes. In doing so, assisting the rule makers to deal with cybercrimes and digital evidence is essential. Sri Lanka's justice system must provide an effective framework for investigation and prosecution of cybercrimes. In addition to that the Computer crimes act enacted in Sri Lanka need to essentially reflect the society's requirements by appropriately criminalizing the offences and providing adequate punishment mechanisms. It is mostly required by the national government to facilitate adequately to reforms in cyber laws to take account of more complex situations emerging on cyber related matters.

0n the other hand it is also important to enhance the capabilities and capacities of the cyber related agencies in Sri Lanka such as Information and Communication Technology Agency (ICTA), Computer Emergency Readiness Team (CERT) etc… to perform their duties in a more efficient manner.

Another key suggestion to the national government in Sri Lanka is to educating the community to protect themselves against internet related crimes. The government should be able to assist the internet users to understand the protective actions and to recognize the possible warning messages. This may be highly effective specially in mitigating financially motivated cybercrimes.

It is also suggested to partnering with the private sector industries to tackle the shared issues of cybercrimes by providing an adequate level of education and resources to such industries. This will lead the private sector to take responsibility for its own protection and to assist their clients to do the same.

References

Ariz, D. (2000), American guarantee & liability insurance co. v. Ingram Micro, Inc. Civ, pp. 99-185.

Computer Crimes Act No.24, (2007). Sri Lanka.

Henson, B., Reyns, B., & Fisher, B. (2011). Internet Crimes. In W. Chambliss (Ed.), Key issues in Crime and Punishment: Crime and Criminal Behaviour. Sage publications, pp. 155-168

Hoffer, J, A. and Straub, D, W. (1989), The 9 to 5 undergound: Are you policing computer crimes?. Slogan Management review, pp. 35-43.

http://searchsecurity.techtarget.com/definition/cybercrime, 24.11.2015.

Kelly, B, J. (1999), Preserve, protect and defend, Journal business strategy, 20(5), pp. 22-26.

Marine, F, J. (2006) "The effects of organized crime on legitimate businesses". Financial crime 13 (2), pp. 214-234

Pariyani, R, Online crimes and their impacts: A review

Power, R. (2001), 2001 CSI/FBI Computer Crime and security survey, Computer security issues and trends, 7(1), pp. 1-18.

PTI Contents. (2009), India: A major hub for cybercrimes

Saini, H, Rao, Y, S. and Panda, T, C. (2012), Cyber-crimes and their impacts: a review, Vol.2, pp. 202-209.

Sprecher, R. and Pertl, M. (1988), intra – industry effects of the MGM Grand Fire, Quarterly journal of Business and Economics.

www.internetlivestats.com/internet-users/, 24/11/2015.

www.lankabusinessonline.com/sri-lankas-mobile-internet-usage-grows-85-8-pct-in-2014-cb/, 24.11.2015.

www.slcert.gov.lk, 24.11.2015.

www.statista.com/statistics/274774/forecast-of-mobile-phone-users worldwide/, 24/11/2015.