Application of Protective Motivation Theory in cyber safety context: Human factor in risk mitigation

MAVS Edirisuriya [1], LS Liyanage[2]

[1]ICT Branch, Ministry of Education
[2]General Sir John Kotelawala Defence University
[1], vasana.edirisuriya@ gmail.com
[2]liyanagelakshika@gmail.com

Abstract— *Popularity of Internet usage has increased drastically in recent years. Being ICT natives; youth, become one of the highest beneficiaries of the internet. At the same time they become more vulnerable to threats associated with the internet. Elimination of all cyber threats is less practical. Most of the time internet users are part of the problem and solution as well. Therefore inculcating cyber safety behaviours among users is productive in order to mitigate cyber threats.. The purpose of this paper is to analyse the suitability of application of Protective Motivation Theory as a cyber-risk mitigation mechanism in Sri Lankan context with special focus on youth. Protective Motivation Theory is a behavioural science theory mostly used in health context. The sample consist of 40 set of secondary data consist of journal articles, conference proceedings and research reports. Theses secondary data and 10 case studies analysed qualitatively using grounded theory method and the results show the positive impact of generating self and coping efficacy as a cyber safety mechanism. The application of protective motivation concept critically subjected to PESTAL analysis against the political, economic, social, technological, environmental and legal aspects of Sri Lanka. The study shows the changing human behaviour is the most important and positively affect reducing cyber threat, especially in a developing country like Sri Lanka.*

Key words: *Protection Motivation Theory, Cyber Safety Behavior, threat appraisal, coping appraisal*

I. INTRODUCTION

The internet is one of the fastest growing technologies. Further, due to its novelty and dynamic nature it can become a centre of attention. There is a trend that the crimes and threats related to the internet have increased as the same pace of users. A fairly large amount of victims and accuses of the internet related incidents are teenagers and young adults. They are vulnerable to the potential threats which may cause social problems and can be a threat to national security in future. It is very difficult to conceal all security vulnerabilities physically; as the hacker, criminal or terrorist needs just one security hindered point. Therefore none of the cyber threats can be seized completely. Only the safety precautions can counteract and mitigate the risks or the effect.

II. CYBERATTACKS AND CYBER SECURITY

Cyber attacks, network security and information pose complex problems that reach into new areas for national security and public policy.(Lewis, 2002)World Economic Forum ranked cybercrime as number one technological risk in 2012 and risk of cyber attack as priority concern in 2013. (Hathaway, 2013)

Cyber security or cyber safety plays an important role in the ongoing development of information technology, as well as Internet services. International Telecommunication union (2008) defines cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. (Sharma, 2012)

Cyber threats are the activities which cannot predict in advance or prevent completely. The possibilities are minimizing vulnerabilities and mitigating risks incorporated with the threats in order to regain the previous status within short lifespan. Since the effects of cyber threats not only causes harm to physical resources but also for the human being the preventing and contingency mechanism is very vital.

III .CYBER ATTACKS AND YOUTH

Conceptual Overview on Youth at Risk and ICT report (Cullen et, al,2011) states that young Europeans in the 16-24 age group enjoy widespread access to ICTs, and that accessibility has been steadily increasing over the year. Evidence shows negative effects associated with the use of ICTs by at risk young people. This includes: risk of isolation associated with high online internet use; adoption of greater 'risk' behaviours leading to greater exposure to unsuitable and harmful on-line experiences.

Teenagers are on a transition period of life between childhood and maturity. They are naturally an active, dynamic, sensitive and altruistic group of the society. On the other hand they are the most emotionally vulnerable social group due to the feelings of adventure, courage and emotions that supersede the feeling of comfort, shyness and logic. (Alkan and Citak, 2007) Being ICT natives; teenagers commonly show interest on cyber activities. Thus they become victims of cyber crimes and potential targets of cyber terrorism acts. Teenagers can tend to involve in cyber criminal and terrorist activities due to their natural curiosity, considering the heroism and publicity of such acts. The vulnerability and malleability make them susceptible exploitation by both criminals and terrorists. (Shelly, 2008)

IV.RESAERCH METHODOLOGY

The research was done as a secondary research. 40 articles including journals, conference proceedings, reports and empirical studies are studied and analysed and 10 real life cases happened within Sri Lanka and outside Sri Lanka. The data was analysed qualitatively following grounded theory approach. Data was coded and subjected to constant comparison in order to build up conclusion.

V. PROTECTIVE MOTIVATION THEORY: THEORY AND GLOBAL CONTEX

Protective Motivation Theory (PMT) was originally conceived (by Rogers, 1975) to understand the impact of health communication messages targeting risky behaviour. However it was successfully applied in other areas such as road safety, crime control, and environmental protection, preventing nuclear war and preventing child abuse. In its current form, PMT states that protective behaviour is motivated by perceptions of the threat, efficacy, and consequences associated with taking protective measures and maintaining maladaptive behaviours.

The theory mainly describes two appraisal processes – threat appraisal and coping appraisal. The most obvious safety message is fear. Threat appraisal is the process by which user access the threats towards themselves, including the severity of the threats and one's susceptibility to them. (La Rose et al, 2008)

Users also evaluate their ability to respond to threats by performing a coping appraisal. Response efficacy, or the belief that the recommended behaviour will be effective, and coping self-efficacy, the belief in one's capability to carry out the recommended behaviour, are the two efficacy variables.

Building self efficacy or confidence in one's ability and in the safety measure used is perhaps the most effective education strategy. (La Rose et al,2008)

Micheal Workman (2007) conducted an empirical study on social engineering attacks which proved that threat severity and vulnerability positively support the behaviours which prevent social engineering attacks.

The research proved that there is a positive relationship between online safety behaviour with self efficacy and coping efficacy. The study was carried out with College students in USA. Protection Motivation Theory was used as a theoretical framework to empirically test the reasons for backing up data on personal computers. This was tested using 112 surveys collected using paper and online data sources. The findings show that computer self-efficacy and response efficacy both positively affect the backing up of data, (Croseller , 2010)

The study conducted Chai, et al (2009) substantiate the positive relationships between the variables of perceived information privacy importance and information privacy protection behaviour, Information privacy self-efficacy and perceived information privacy importance, Information privacy self-efficacy and information privacy protection behaviour, Information privacy exposure and information privacy self-efficacy, Past bad experience and affect information privacy anxiety, External information privacy anxiety and information privacy protection behaviour. Further study reveals that information privacy protection behaviour and perceived information privacy importance vary by gender. The study was done with pre teens who are middle school students in two states of the United States namely Maryland and New York.

La Rose et al (2005) was carried out a research with undergraduates of classes in telecommunication and advertising at a major Midwestern university. The sample consists of 46 % females and 54% males with a median age of 20 years. The study substantiated the positive hypotheses between coping efficacy and online safety protection behaviour, response efficacy and online safety protection behaviour, perceived benefit of the safe behaviour and online safety protection behaviour; whereas the negative hypotheses between cost of safe behaviour and online safety protection behaviour.

VI. SRI LANKAN CONTEXT

Nielson Sri Lanka year in review 2013 and opportunities in 2014 (2013) report shows that there are 2.8 million of internet users in Sri Lanka and 21% of them can be considered as daily users. The involvement of internet to areas such as education, commerce and marketing, communication, media and health are increasing rapidly. However the threats and conflicts associated with internet has caught up its pace as equal as the increase of internet users.

The reports published by Sri Lanka Computer Emergency Readiness Team (SL CERT) shows (Nafeel, N., 2015) the cyber threats have increased rapidly within last seven years. Computer cyber crime unit of the Police Department for the time period of 2006-2015 shows similar trend in reported cybercrimes. Further suicides and mental trauma due to cyber threats increase rapidly during last few years.

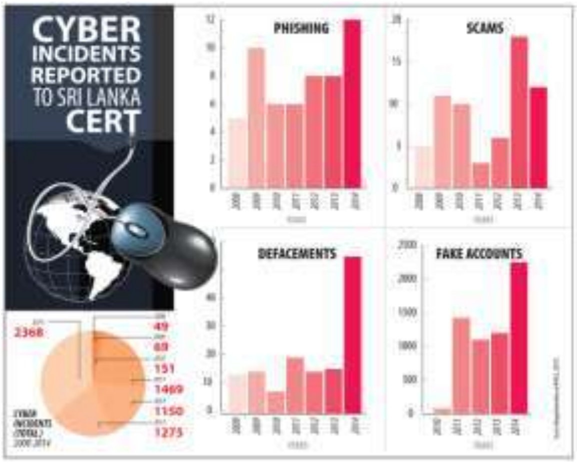

Table 1-Cyber incidents Reported to SL CERT(Adapted from Daily News 05-11-2015)

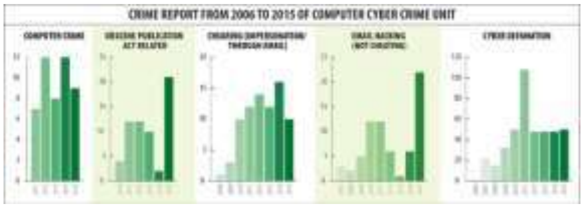

Table2-Reported incidents to Computer Cyber Crime Unit – SL Police(Adapted from Daily News 05-11-2015)

Sri Lanka will experience a massive wave of cyber attacks in the near future due to inadequate prevention methods and privacy laws as well as non-compliance, according to the state's Computer Emergency Response Team Co-ordination Centre. (Wettasingha, 2014)

VII. ANALYSIS

The threat appraisal process of Protective Motivation Theory is proved in the researches of Crosellor (2010) on backing up of data and Workman(2007) on social engineering attacks.

Further the coping appraisal process of Protective motivation theory is proved by the researches of Chai et al (2009) on online privacy and La Rose(2005) on online safety protection behaviour. The all researches' samples were pre-teens, early teen's teenagers and young people in early twenties.

The following table shows the results analysis of case studies.

Issue	Behavior	Effect after incident	Result
Online sharing of pictures	Publishing Personal data, Low concern on Privacy	Punishment Defame	Suicide
Fake profile (created by own)	Low concern on responsible behaviour online	Loss of romantic affair	Suicide
Fake profile (published by peers)	Low concern on Privacy	Cyber bulling on-line and off line harassment	Emotional distress, depression, disturbance to study
Fake profile (published by peers)	Low concern on Privacy	Online & offline harassment	Emotional distress, depression, disturbance to study
Fake profile (published by unknown)	Weak Passwords, Low concern on Privacy	Online harassment	Emotional distress

Hacked Accounts	Sharing password	Loss the accessibility of social media account	Emotional distress
Hacked Accounts	Sharing password	Loss the accessibility of social media account / e-mail	Emotional distress
Hacked account	Low concerns on security	Loss the accessibility of social media account / e-mail	Emotional distress
Hacked account	Weak passwords	Loss the accessibility of social media account / e-mail	Emotional distress Loss of memory
Hacked account	Low concerns on security	Legal Issue Defame	Legal Action and Punishment

Table 3- Analysis of case studies

PESTLE analysis provides a framework for investigating and analysing the external environment for an organization. When considering the applicability of concepts in Protective Motivation theory in Sri Lanka; it is analysed against the feasibility perspectives which used in “PESTEL” analysis; - political, economical, social, technological and legal.

South Asia has becoming the potential trouble spot in the world including geographical and political favourability to cyber crimes and risks. Being a South Asian country Sri Lanka is facing or has faced similar problems with other regional countries terrorism and poverty which provide incubators to raise crimes including cyber crimes. The cyber threats are becoming potential security threats where the nation needs to find sustainable solution.

Sri Lanka as a developing country cannot afford the higher cost for technical solutions which developing countries practice to detect cyber crimes and combat against the cyber terrorism. On the other hand Sri Lanka having strength to carry out awareness and education programs and streamline the existing ones with the support of government, private and non government organizations with the minimal cost.

Social media has become popular among the Sri Lankan youth and it has given a signal that social media can influence the mind set of general public especially young people from recent political and social incidents. Further the cyber related sever incidents such as suicides directly or indirectly involve with cyber activities have given publicity through electronic, print and social media. This results a favourable social environment to develop strategies against cyber crimes and threats. Since many reported incidents are avoidable through the change of online privacy behaviour the psychosocial risk mitigating mechanism highly important.

The use of internet and mobile phones has drastically increased as the number of mobile subscriptions exceeding the total population of the country. However any technical solution cannot guarantee the total cyber safe environment as it is need to conceal all vulnerabilities; but cyber attacker needs only one security hindered point to intrude.

Sri Lanka passed the Computer Crimes Act no. 24 in 2007 which can consider as the first move to enforce legal framework to reduce cyber risk incidents. In 2015 Sri Lanka has become the first South Asian country to enter the Council of Europe (CoE) Cyber Crime Convention also known as the Budapest Convention. (Nafeel, N., 2015) This opens a new path to with regard to cyber crimes. Some of the benefits getting from this convention are ,adhere to the data protection and privacy safeguards, open 24/7 contact points in Sri Lanka to get mutual assistance from other member countries, ability to investigate and prosecute offences by Criminal Justice Authority.

VIII. RECOMMENDATION AND CONCLUSION

The writer's recommendation in line with that “Human factor is the most important in mitigating cyber risks" highlighting the importance of motivating the safe behaviour.

Cyber security has become a potential problem to Sri Lanka with the increasing popularity and accessibility to internet. Young people -the potential workforce of the country are on the verge of danger. Since the threat severity related to threat appraisal discussed at the Protective Motivation Theory cannot be controlled intentionally; cyber risk mitigation programs should focus on coping appraisal. Since the coping appraisal mainly concerns building one’s ability to do perform right action at the right time and building confidence on be secure in cyber space performing the said actions.

Cyber safety education can play vital role in developing self and coping efficacy. The programs should align with the awareness of cyber risks, their effects and the safety behaviours to be followed in order to overcome them. Dramas, role plays, short films and eye catching advertisement in print and electronic media may add colour to the programs.

Since social media is highly effective mode to give a message to youth; the same mode can be used to do the awareness.

Poster campaigns and awareness programs can be conducted in schools and in youth centres. Formation of Provincial level trained trainers' pool including school teachers, volunteer youth leaders could be ideal to make a start. Rewarding students through competitions would be an ideal motivation to inculcate safe behaviours.

The general and school level counselling services should be empowered with the knowledge to handle issues related to cyber incidents. 24 x7 call centre and help desk for counselling should be formulated to handle cyber incidents.

Using behavioural science in mitigating cyber risks is comparatively less discussed area. Therefore further researches should be carried out in the field of psychology, sociology, behavioural science and Information and Communication Technology on this area for finding proper mechanism and strategies

Sri Lanka is categorized as developing country. However it is in the top of other South Asian and Asian countries in terms of literacy and human capital is the best asset of the country. Therefore motivating the positive behaviour in cyber safety is one of the best and effective method to mitigate cyber threats.

VII .REFERENCES

- Alkan, N. ,Citak, M.C. (2007). *Youth and Terrorism, in Understanding and Responding to Terrorism*, Proceedings of the NATO Advanced Research Workshop on Policing Responses to Terrorist Operations, IOS Press, Netherlands, pp 285-286, viewed 18 September 2014, <http://books.google.lk/books?hl=en&lr=&id=jZjqavWoRfkC&oi=fnd&pg=PR1&dq=Understanding+and+Responding+to+Terrorism&ots=GxDfC-XlKv&sig=2gs2HtmH4mpB-BkZvXplowdHM0I&redir_esc=y#v=onepage&q=Understanding%20and%20Responding%20to%20Terrorism&f=false>

- Croseller, E.R., (2010), *Protection Motivation Theory:Understanding Determinants to Backing Up Personal Data,* Proceedings of the 43rd Hawaii International Conference on System Sciences

- Chai, S., Bagchi-Sen, S., Morellel, C.,Rao, H.R., Upadhyaya., S.J., (2009). *Internet and Online Information Privacy:An Exploratory Study of Preteens and Early Teens,* IEEE Transactions on professional Communication, Vol.52.No.2

- Cullen,J., Cullen, C., Hamilton,E., Maes, V. (2011). Mapping and Assessing the Impact of ICT-based Initiatives for the Socio-economic Inclusion of Youth at Risk of Exclusion: Conceptual Overview on Youth at Risk and ICT, pp 23-58, Viewed 18 September 2014, <http://is.jrc.ec.europa.eu/pages/EAP/eInclusion/documents/FINALConceptualOverviewwithTavArcolacovers.pdf>

- Hathaway, O.A, Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. (2011). *The Law of Cyber Attacks*, California Law Review

- International Telecommunications Union (ITU). ITU-TX.1205: series X: (2008). *Data networks, open system communications and security: telecommunication security: overview of cyber security*

- Larose, R., Rifon,N., Liu, S., Lee, D.(2005). Paper presented to the Communication and Technology Division International Communication Association, New York, pp.3-14

- Lewis, J., A., (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats:,* Center for Strategic and International Studies, viewed 26November 2015 < http://www.steptoe.com/publications/231a.pdf>

- Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society, *International Journal of Scientific & Engineering Research*, Volume 3, Issue 6, pp. 1

- Shelly , L. (2008). *Youth , Crime and Terrorism*, Political Violence, Organized crimes, Terrorism and Youth, pp. 133-139, IOS Press, Netherlands, viewed 18 September 2014, http://books.google.lk/books?hl=en&lr=&id=xCW6nVReyAcC&oi=fnd&pg=PA133&dq=.+(Shelly,+2008)+terrorism&ots=RAhYqxggZN&sig=JP00T0knyB6u0d40kFw2hV7rDTU&redir_esc=y#v=onepage&q&f=false

- Wettasingha, C. (2014)., *Sri Lanka Highly vulnerable to cyber attacks:CERT| CC* ,Daily Mirror, 29 September , Viewed 20 August 2015, <http://www.dailymirror.lk/53078/sri-lanka-highly-vulnerable-to-cyber-attacks-certcc>

- Workman, M., (2007)., *Methods for Understanding and Reducing Social Engineering Attacks,* Viewed 25 August 2015, < https://www.sans.org/reading-room/whitepapers/engineering/methods-understanding-reducing-social-engineering-attacks-36972>

- Nafeel,N. (2015). *New laws to curb cyber crimes*, Daily news, 06 November ,viewed 26November 2015,<http://www.dailynews.lk/?q=2015/11/05/features/new-laws-curb-cyber-crimes-0>

Acknowledgment

I would like to extend my sincere gratitude to Ministry of Education for sponsoring my research study , Director and staff of ICT Branch Ministry of Education for all the support given . Further the supervisor of my PhD Dr. Lakshika Liyanage for the guidance.