PalArch's Journal of Archaeology of Egypt / Egyptology

"AWARENESS AND PREPAREDNESS TOWARDS CYBER RISK AMONG ONLINE USERS"

Dr. V Gajapathy[1], Ms. Reshma M Patil[2]

[1]Professor, Presidency University
vgajapathy@presidencyuniversity.in
[2]Research Scholar, Presidency University
reshmasibichan@gmail.com

Dr. V Gajapathy[1], Ms. Reshma M Patil[2], "AWARENESS AND PREPAREDNESS TOWARDS CYBER RISK AMONG ONLINE USERS",-- Palarch's Journal Of Archaeology Of Egypt/Egyptology 18(9). ISSN 1567-214x

Keywords: Cyber Risk, Digitization, Cyber Insurance, Risk Management.

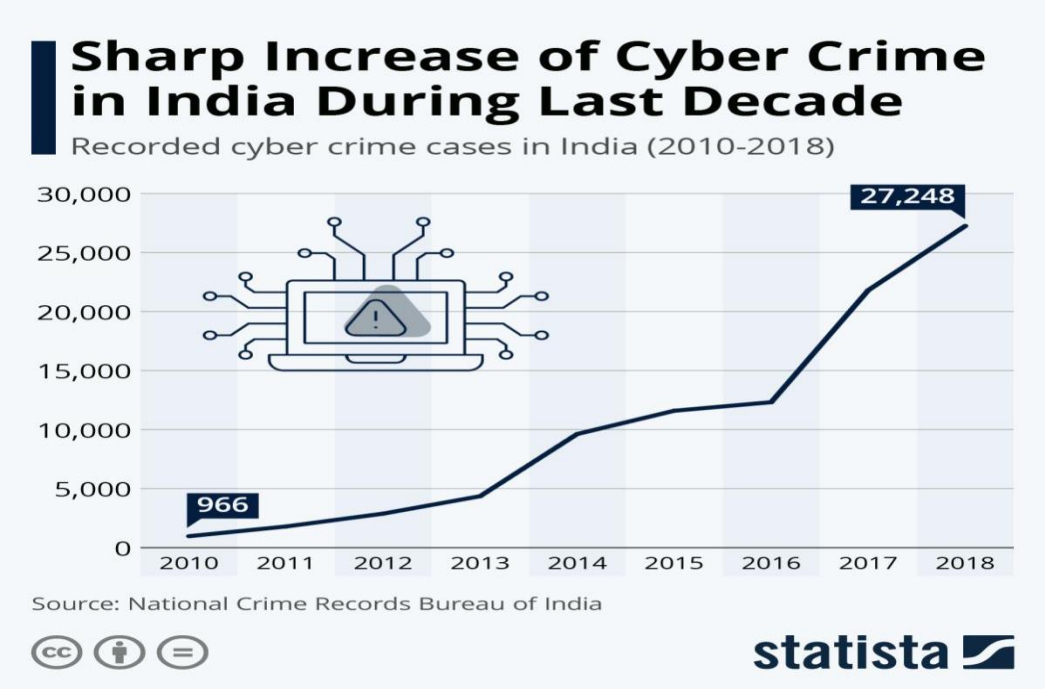
ABSTRACT

Cyber-attacks are increasing with every ticking second. Individuals by nature are risk averse and even the risk takers assess the risk before investing or venturing into new foray. Individuals have ventured into digital transformation taking the cyber space by storm. The technology has given us the leverage to explore new horizons and reap maximum mileage from it. On the flipside are cyber-attacks which are on the rise. As an aftermath of these risks, individuals have to deal with financial loss, damaged credibility and psychological problems arising from it. The challenge for the cyber-attack victim is that they themselves have to deal with the loss as there are no bearers of cyber risk to whom the risk can be transferred. This paper intends to evaluate the awareness and preparedness of individuals toward cyber risk. The study is conducted using Primary Data which is collected by administering questionnaire. The data collected is analyzed using statistical tools.

JEL Classification: G22, G28, G32, K24.

Introduction

Cyber World, connectivity, technology and its innovations has kept the wheel moving for human advancements in all spheres of life. In this time of pandemic situations which has brought the physical transit to a standstill the world over, there has been no stopping of ecommerce activities and the flow of traffic over the cyber world has kept the economies moving required for its survival. With the increase in number of internet users and their activities, it has opened up increased cyber-crimes the world over. Cyber-crimes knows no geographical boundaries and are identical globally(Iqbal, Juneed; Beigh, 2017)



REVIEW OF LITERATURE

(Abdul Rahman & Binti Omar, 2015) state that Higher the knowledge of cyber-crimes, high is the awareness level of cyber-crimes. (Iqbal, Juneed; Beigh, 2017) mentions that there are bilateral treaties signed by India with various countries on cyber laws. However, the need of the hour for India is to have a multilateral treaty which will complement its regulations by a shared criminal policy which can help in fighting cybercrimes at international levels.

(Enst et al., 2015) They observed that one of the current difficulties in tackling cyber risk is the absence of standards, shared language, and standardized practices which are best in the industry. Insurance sector can play a pivotal role in creating awareness of cyber risks among the individuals.

(Franke & Brynielsson, 2014) A review paper on cyber risks indicated that there is no much research being done in the area of understanding cyber risks and the position on the level of awareness, the risks of coning, or the issue of cyber fight and destruction assessment in armed operations.

(Böhme & Schwartz, 2006) This study presented a novel grouping of correlation properties of cyber-exposures built on a twin-tier method. Tier one shows the correlation of cyber-exposures inside the firm and the a firm i.e. correlated letdown of its internal system and its network. Tier two highlights the correlation of global cyber exposures and stand alone firms in the portfolio of the insurers. A beta-binomial model is used here.

(Biener, Eling, & Wirfs, 2015) The adequacy of insurance for handling cyber-risk is emphasized here. Insurability of cyber risk by review of cases in a systematic manner has been initiated by Berliner (1982). A number of substantial issues ensuing from interrelated damages, data inadequacy, and information asymmetries hamper the progress of market for cyber insurance.

(Shackelford, 2012) They have arrived at the conclusion that to decrease corporate

risk, they need to be proactive and invest in augmenting cybersecurity and analyze if their existing insurance coverage, covers them from the risk of cyber-crimes and if the coverage is not adequate, measures should be taken to increase the coverage.

(Kosub, 2015) The focus of this study is to understand the key constituents of a cyber risk controlling method. Effective cyber risk handling comprises of handling the internal system and process with all diligence and they should not limit it to the same and go further with transferring the risk to third parties and cyber insurance may be an option as it still needs clarity on the pricing and the risks that it can absorb.

(Xia Zhao., 2013) In this work they explore in what way businesses use risk management methods, "third-party cyber insurance", "managed security service (MSS)" and "risk pooling arrangement (RPA)", address the concern of investment ineffectiveness. Cyber Insurance and MSS offer comprehensive risk handover and of the two, MSS, brings more effectual distribution of security resources.

(Kopp, Kaffenberger, & Wilson, 2017) This research reflects the characteristics and components of cyber risk, deliberates the reason why private market are unsuccessful to offer the socially ideal level of security from cyber risks and discover how complete cyber risk intermingles with other financial constancy risks. Policy measures can surge the flexibility of the financial structure to systemic cyber risk.

(Mukhopadhyay, Chatterjee, Bagchi, Kirs, & Shukla, 2019) **T**hey offered (CRAM) frame which is "cyber-risk assessment and mitigation" to assess the possibility of an attack by means of generalized linear models (GLM), It is suggested to use a dataset which has additional data points than CSI–FBI for demonstrating cyber risk.

Research Gap

From the review of literature, it shows that various researches have been conducted on cyber risk in various countries and also in India but this study mainly focuses on awareness of cyber risk among the individuals in Bengaluru is not been conducted, thus this is the research gap of the study

Objectives:

1. **To study the awareness of exposures of cyber risk amongst the individuals**
2. **To study whether there is a relationship between occupation and usage of internet.**
3. **To study whether there is an association between installation of antivirus software and the awareness of cyber risk.**
4. **To study the awareness of cyber schemes**

Research Methodology

Collection of data: Data was collected through a questionnaire that was administered through google forms. The data collected was collated and coded in MS Excel for the purpose of analysis.

Tools used for analysis:

Descriptive Statistics was used to cluster the profiles of the respondents based on their age, gender, education and income.

I. **To study the awareness of cyber risk among the individuals**

- **Gender, Age group have an effect on Awareness of cyber risk.**

H01: There is no relationship concerning gender and awareness of cyber risk.
H02: There is no relationship amid age and awareness of cyber risk.
H1: There is relationship concerning gender and awareness of cyber risk.
H2: There is relationship amid age and awareness of cyber risk.

Descriptive Statistics			
	Mean	**Std. Deviation**	**N**
GENDER	0.56	0.499	102
AGE GROUP	1.33	0.848	102
AWARENESS	3.02	0.901	102

Correlations				
		GENDER	**AGE GROUP**	**AWARENESS**
GENDER	**Pearson Correlation**	1	-0.164	-0.135
	Sig. (2-tailed)		0.100	0.177
	N	102	102	102
AGE GROUP	**Pearson Correlation**	-0.164	1	0.030
	Sig. (2-tailed)	0.100		0.763
	N	102	102	102
AWARENESS	**Pearson Correlation**	-0.135	0.030	1
	Sig. (2-tailed)	0.177	0.763	
	N	102	102	102
****. Correlation is significant at the 0.01 level (2-tailed).**				

A Pearson's correlation was conducted to examine the awareness of cyber risk that is gender and age group has an effect on awareness. Awareness of cyber risk is more strongly correlated to age group, **r (98) = 0.763, p > 0.001** than to gender which is negatively related, **r (98) = -0.13, p < 0.001.**
These findings show that

- There is no relationship concerning gender and awareness of cyber risk. Hence, Null Hypothesis cannot be rejected.
- There is relationship amid age and awareness of cyber risk. Hence, Null hypothesis is rejected.

II. To study whether there is a relationship between occupation and usage of internet.

Null Hypothesis
H01: There is no relationship between occupation of an individual and usage of internet
Alternative Hypothesis
H1: There is a relationship between occupation of an individual and usage of

internet.

Descriptive Statistics			
	Mean	**Std. Deviation**	**N**
OCCUPATION	1.97	1.424	102
USAGE OF INTERNET	2.32	0.914	102

Correlations			
		OCCUPATION	**USAGE OF INTERNET**
OCCUPATION	Pearson Correlation	1	-0.221
	Sig. (2-tailed)		0.026
	N	102	102
USAGE OF INTERNET	Pearson Correlation	-0.221	1
	Sig. (2-tailed)	0.026	
	N	102	102

****. Correlation is significant at the 0.01 level (2-tailed).**

The above correlation analysis shows that usage of internet is negatively correlated with the occupation of the individuals, **r (98) = -0.221, p < 0.01**. It indicates that the null hypothesis cannot be rejected. It indicates that there is no relationship among occupation and internet usage of individuals.

III. To study whether an association between installation of antivirus software and awareness of cyber risk exists.

H01: There is no relationship between installation of antivirus software and the awareness of cyber risk.

H1: There is relationship between installation of antivirus software and the awareness of cyber risk

Descriptive Statistics			
	Mean	**Std. Deviation**	**N**
ANTIVIRUS SOFTWARE	1.28	0.453	102
AWARENESS	3.02	0.901	102

Correlations			
		ANTIVIRUS SOFTWARE	**AWARENESS**
ANTIVIRUS SOFTWARE	Pearson Correlation	1	-0.159
	Sig. (2-tailed)		0.110
	N	102	102
AWARENESS	Pearson Correlation	-0.159	1

	Sig. (2-tailed)	0.110	
	N	102	102

****. Correlation is significant at the 0.01 level (2-tailed).**

The above analysis shows that installation of antivirus software is negatively correlated with the awareness of cyber risk, **r (98) = -0.159, p < 0.01**. It indicates null hypothesis cannot be rejected and there is no relationship between installation of antivirus software and awareness of cyber risk.

IV. To study the awareness of cyber schemes

- Gender, age group have an effect on the awareness of cyber schemes.

Null Hypothesis

H01: There is no relationship between gender and awareness of cyber schemes.

H02: There is no relationship between age group and awareness of cyber schemes.

Alternative Hypothesis

H1: There is relationship between gender and awareness of cyber schemes.

H2: There is relationship between age group and awareness of cyber schemes.

Descriptive Statistics			
	Mean	**Std. Deviation**	**N**
GENDER	0.56	0.499	102
AGE GROUP	1.33	0.848	102
AWARENESS OG CYBER SCHEMES	2.66	0.980	102

Correlations				
		GENDER	**AGE GROUP**	**AWARENESS OF CYBER SCHEMES**
GENDER	**Pearson Correlation**	1	-0.164	-0.191
	Sig. (2-tailed)		0.100	0.054
	N	102	102	102
AGE GROUP	**Pearson Correlation**	-0.164	1	0.067
	Sig. (2-tailed)	0.100		0.500
	N	102	102	102
AWARENESS OF CYBER SCHEMES	**Pearson Correlation**	-0.191	0.067	1
	Sig. (2-tailed)	0.054	0.500	
	N	102	102	102
****. Correlation is significant at the 0.01 level (2-tailed).**				

Correlation was conducted to examine the awareness of cyber schemes that is gender and age group has an effect on awareness. Awareness of cyber schemes is more strongly correlated to age group, **r (98) = 0.067, p > 0.001** than to gender

which is negatively related, **r (98) = -0.191, p < 0.001.**
These findings show that

- There is no relationship between gender and awareness of cyber schemes. Hence, Null Hypothesis is not rejected.
- There is relationship between age group and awareness of cyber schemes. Hence, Null hypothesis is rejected.

CONCLUSION

The problems arising from cyber risk is encountered by all nations in the present world; nevertheless there are only a few nations that have legislated laws to regulate cyber risk with an international viewpoint. Cyber risk has a universal personality and the wrongdoer may be seated at a remote location and the crime may be committed thousands of miles afar in another place. Thus the dynamic teamwork of the worldwide community is essential to reduce and minimize cyber risks. Cyber risk is one amongst the severest nationwide security in recent times, all are fronting currently. The study results show that people are aware of cyber risk and they don't trust online security, but they don't give much importance to password security. There are numerous agreements and organizations that compact with threat of cyber risk and assist the developed and developing nations in legislating cyber laws. However, it unacceptable that close by are many states that offer safe spaces to cyber offenders and few other countries that does not treat some offenses as crimes in their country, which are considered as criminalities in the law of other nations, and it poses a major threat and problem when crimes involving cyber world are committed across nations. This situation can certainly be fixed if all nations join hands and practice a model law on which each country endorses their home laws and increase the awareness of cyber risks and cyber schemes to all strata of the society cross all demographic borders.

References:

Abdul Rahman, R., & Binti Omar, N. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia Anti-money laundering a View project Compliance and Effectiveness Analysis of the Mutual Evaluation Reports of Financial Action Task Force Member Countries View pr. *Article in Journal of the Social Sciences*, (September 2016). https://doi.org/10.3844/jssp.2015

Bennis, W., Boccaccio, V., Pagani, M., Oestreicher-singer, G., Zalmanson, L., English, L., … Pavlou, P. A. (2013). M Anaging I Nformation Q Uality –. *Data Base*, *37*(2), 633–635.

Biener, C., Eling, M., & Wirfs, J. H. (2015). *I NSURABILITY OF C YBER R ISK : A N E MPIRICAL A NALYSIS W ORKING P APERS ON R ISK M ANAGEMENT AND I NSURANCE N O . 151 C HAIR FOR R ISK M ANAGEMENT AND I NSURANCE Insurability of Cyber Risk : An Empirical Analysis Every reported incident of data breach o*.

Böhme, R., & Schwartz, G. (2006). Models and Measures for Correlation in Cyber-Insurance. *2006 Workshop on the Economics of Information Security (WEIS)*, (June 2006), 1–26.

Enst, M., Anab, R., Tez, D., Dan, L. U., Yılmaz, S., Baran, Z., … Enstġtüsü, S. B.

(2015). No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, *16*(1), 24–25. https://doi.org/10.30798/makuiibf.323102

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness - A systematic review of the literature. *Computers and Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Iqbal, Juneed; Beigh, B. M. (2017). Cybercrime in India : Trends and Challenges. *International Journal of Innovations & Advancement in Computer Science*, *6*(12), 187–196.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. *IMF Working Papers*, *17*(185). https://doi.org/10.5089/9781484313787.001

Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift Fur Die Gesamte Versicherungswissenschaft*, *104*(5), 615–634. https://doi.org/10.1007/s12297-015-0316-8

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, *21*(5), 997–1018. https://doi.org/10.1007/s10796-017-9808-5

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4), 349–356. https://doi.org/10.1016/j.bushor.2012.02.004