International Journal of Computer Engineering and Technology (IJCET)
Volume 15, Issue 3, May-June 2024, pp. 12-20, Article ID: IJCET_15_03_003
Available online at https://iaeme.com/Home/issue/IJCET?Volume=15&Issue=3
ISSN Print: 0976-6367 and ISSN Online: 0976-6375
DOI: https://doi.org/10.17605/OSF.IO/BQ2WC
Impact Factor (2024): 18.59 (Based on Google Scholar Citation)

ANALYSIS ON CYBER RISK EXPOSURES AND AN EVALUATION OF THE ELEMENTS THAT GO INTO BEING READY TO DEAL WITH CYBER THREATS

Kaushik Reddy Muppa
Advisory Manager, Deloitte, Ashburn, VA, United States

ABSTRACT

In today's world, which is getting closer to a cashless and paperless economy, digitization is the key to success for any organization or business. The risk of cyberattacks has been growing and is significantly higher than the risk that is thought to be associated with cyberspace. Even though efforts have been made to encourage digitalization, cyber risk has been overlooked. It has taken several days and months for certain establishments to recover from the destabilizing effects of cyberattacks, which are causing widespread concern around the world. In other instances, cyberattacks have caused certain enterprises to become unstable. in addition to the other operational challenges, the recovery period was accompanied by a financial liability and a loss of market share. Through the identification of the role that awareness of cyber risks, experience with cyber risks, attitude towards cyber risks, and the online behavior of respondents play in determining an individual's preparedness to deal with cyber risks, this research has focused on determining the factors that determine an individual's preparedness to deal with cyber risks. Following the administration of a structured questionnaire to 385 respondents, the researcher coded and modified the data acquired to conduct further analysis. The researcher has utilized ANOVA, t-test, and Regression to bring forth the framework of the study. The data that was collected was subjected to Univariate, Bivariate, and Multi-Variate Analysis before being analyzed. The findings suggest that there is a correlation between an individual's online behavior and their awareness of the risks associated with cyberspace, which ultimately results in preparation to deal with cyber risks. To improve one's readiness to deal with cyber threats the findings will be an important input that may be utilized by an individual.

Keywords: Cyber Risk, Cyber Security, Assessment, Risk Exposures

Cite this Article: Kaushik Reddy Muppa, Analysis on Cyber Risk Exposures and An Evaluation of The Elements That Go into Being Ready to Deal with Cyber Threats, *International Journal of Computer Engineering and Technology (IJCET)*, 15(3), 2024, pp. 12-20.
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_3/IJCET_15_03_003.pdf

1. INTRODUCTION

1.1. Introduction

Cyber Risks are the major risks being faced by many with the ever-changing technology and digitalization of the economy and also with online marketing and e-commerce being the way of business and life. Digitization has become the keyword of every organization big and small alike, established companies and startups included, and also for individuals to enhance their business or to move ahead in their career, knowledge seeking, ease of managing and doing daily activities both in their domain and work front. Every individual is seeking to get answers and manage all activities connected with their life concerning family and friends at their fingertips in the comfort of their home and office [1,2].

This has given rise to cyber bullies who are lurking to see any vulnerable situation that can be taken advantage of. Cybercrime can be attributed to any instance where there has been a breach of data or any crime that has been committed using a computer over the internet. Managing Cyber Risks begins with an individual or an organization identifying the areas of risk exposures so that all the exposures can be taken care of to reduce the incidence of cyber-attacks.

The number of cyber crimes happening in India and globally has been showing an increasing trend in terms of numbers and also percentages [3]. More instances of such crimes and also the writing on the walls that the next world war is a war in cyberspace commends more studies and research to be conducted to manage cyber risks and also to be secure in cyberspace.

1.2. Background of the Research

In [4] Viral attacks, denial-of-service (DoS) attacks, financial fraud, system penetration, and theft of proprietary information are all examples of cyber threats that are frequently used by malicious external attackers. On the other hand, malicious internal attackers use unlawful access to put the integrity, confidentiality, and accessibility (CIA) of data belonging to individuals, businesses, and nations in jeopardy. This results in a loss of opportunity for firms, in addition to having a detrimental effect on market capitalization and the value of their brand value. Information technology (IT) security consumes a sizeable portion of the expenditures allocated to information technology (IT) by both private companies and public administrations (including technologies for perimeter and core security). Nevertheless, there are numerous instances of security deficiencies. An approach for cyber-risk evaluation and mitigation (also known as CRAM) is described in this scientific investigation. Generalized linear models (GLM), most notably logit and probit, are utilized to confirm the estimations that are being offered and to make predictions regarding the likelihood of an attack.

Whereas in [5] One of the most significant problems that have arisen as a result of the growing use of networks in industrial control systems is the issue of cybersecurity, which may be described as information security to prevent cyberattacks. The purpose of this study is to present a model that integrates fault tree analysis, decision theory, and fuzzy theory to (i) determine the current reasons for failures in cyberattack prevention and (ii) evaluate the vulnerability of a specific cybersecurity system. We evaluate the potential consequences of such attacks, which include data transmission, data alteration, data destruction or loss, and service disruption, in terms of monetary damages and the amount of time it takes to restore the service. The model was utilized to evaluate the cybersecurity risks that are associated with attacks on websites, e-commerce, and enterprise resource planning (ERP), as well as the potential consequences of such attacks. The findings of the model application indicate its value and emphasize the sensitivity of e-increased commerce to cybersecurity threats when compared to websites or ERP. This vulnerability is due, in part, to frequent operator access, credit transactions, and user authentication concerns that are specific to e-commerce.

2. REVIEW OF LITERATURE

In [6] it is obvious that a major increase in public awareness of cybersecurity is necessary to ward off the fast-rising number of cyber-attacks. Therefore, it is obvious that it is crucial to spread this knowledge through specially created programs for both people and groups, in the public and private sectors. To lessen the likelihood that people may be the target of such attacks, several initiatives might be developed to further enlighten the populace.

The advent of the virtual office means more networks, more gadgets, and a tremendous increase in interconnectedness for businesses worldwide. The most significant outcome of this expansion for providers of cyber insurance is an ever-rising amount of risk to insure. These carriers implement increased premiums as a result, which reflects the rising risk. Cyber insurance can compensate for lost revenue and fixed costs incurred during unanticipated outages, but as risks increase and more claims are made, premiums skyrocket. I believe that in the end, purchasers of cyber insurance must have realistic expectations regarding the benefits of the engagements. Organizations who anticipate that cyber insurance will cover all of their issues and serve as a "get out of jail free card" may be dissatisfied, frustrated, and possibly found legally and publicly responsible. Although it must be included in a risk management strategy, cyber insurance is not a cure-all [7].

In [8], cyber insurance is considered one of the effective preventive strategies that help to decrease the unfavorable repercussions of cybercrime intervention. Cyber insurance is recognized as offering several benefits. The article divides the market for cyber insurance into different segments according to the size of the insurance business and the geographic location of the company. The findings of the analysis indicated that enterprises based in the United States hold a dominant position in the market for cyber insurance. A claim asserts that the sectoral distribution of people who purchase cybersecurity plans generally tracks developments in the sectoral distribution of cybercrime. This is the case since the two are generally related. Several issues have been recognized, and they are preventing the growth of cyber risk insurance. The key ones are as follows: there is a lack of a common standard for filling insurance services in the realm of cyber insurance, and there is a high level of information entropy during the process of assessing cyber risk. Bringing up the fact that insurance firms have a future in the market for cyber insurance is something that should be emphasized. The reason for this is due to the costs associated with cyberattacks as well as the significant rise in the number of cyber threats.

In [9] the end of the cyber risk spectrum's characteristics have changed over time, and national governments and criminal gangs are increasingly focusing their attention on commercial operating systems. The ability of a business to operate, store data securely, access vital data, and generate revenue is directly undercut by this act. Cyber insurance will continue to develop as a result of the threat posed by severe, knowledgeable, and well-resourced threat actors. There are currently only a few insurance companies and little business community awareness of cyber insurance in Australia. Small premium pools, combined with some cyberattacks' growing sophistication and malice, have put a lot of strain on insurers and businesses alike. Given the high cost and difficulty in pricing cyber risk due to its continually changing profile, many insurers are hesitant to offer cyber insurance or instead provide limited insurance coverage.

The study reveals that there is no review of all these studies shows that there is no agreement on the definition of cybercrime and quantifying the impact of cyberattacks. The corporate executives are not able to evaluate the impact the cyberattacks will have on their clients [10].

3. RESEARCH METHODOLOGY

3.1. Introduction

Here the approach that was utilized in this investigation has been expounded over in great detail. Detailed explanations have been provided for the primary components of methodology, which include the research design, the numerous variables that were utilized in the study, the hypothesis that was developed, the sample design and the procedure of sampling, the tools for data collecting, the processing of data, and the analysis of the extracted data. The statistical tools that were utilized in the analysis of the data that was gathered are also explained here.

3.2. Research Design

The primary aim of the research is to determine the relationship that exists between demographic variables like Gender, Age, Income, and Education which are the independent variables with the dependent variables like Awareness, Preparedness, Attitude, Online Behaviour, and Experience toward Cyber Risks in a population. States that quantitative research design can be classified as conclusive research and exploratory research. Based on his explanation, we can say that this research is Exploratory research as it facilitates the researcher to discover research problems in detail. It may be said that it is the foremost research as it paves for conclusive research, highlights the purpose of carrying out exploratory research and the main reason is to satiates the curiosity of a researcher and their wholesome understanding, to confirm the scope for further research.

3.3. Data Collection

3.3.1: Primary Data

In this study, the collection of data was done using a simple random sampling technique from 389 individuals who use the internet in Bengaluru. The respondents were communicated personally, through mail, and through phone calls to collect their responses. Additionally, physical forms and Google forms were utilized in the administration of the questionnaire. The link was distributed via email and several social media platforms to collect responses from the individuals. The respondents were given the option to fill out the questionnaire at their convenient time.

3.3.2: Secondary Data

The researcher collected data from the National Crime Records Bureau (NCRB) which has given the number of cybercrime cases in India and also from Statistia.com which has given the trend of increase in cyber crimes in India over the last decade. Additionally, data from secondary sources has also been collected to complete the requirement of the research in understanding cyber risks.

3.3.3: Data Collection

The structured questionnaire was prepared using simple English language so that it could be easy to understand and leave no space for ambiguity in the tool. The questionnaire was framed keeping in mind that it would be self-administered by the respondents. The respondents were contacted personally or through mail phone or social media for to fill out the forms. Most of the forms were filled through Google Forms and the researcher met with individuals in companies, colleges, and homes to collect data personally from the respondents.

Once the questionnaires were filled and completed, the researcher took time to ensure that there was ample awareness being made concerning cyber risks involved especially to individuals working in organizations and also to students.

Table 1: Reliability Statistics

Items	Cronbach's Alpha	Percentage (%) of reliability	Validity	Number of Items
Awareness	0.614	61%	Acceptable	5
Preparedness	.715	71%	Acceptable	4
Experience	.915	91%	Excellent	6
Online Behavior	.910	91%	Excellent	20
Attitude	.836	83%	Excellent	10

Respondents have our word that all data will remain private and utilized solely for the research at hand, with no plans to share or sell their information at any point.

The reliability of the claims studied in this research is very dependable and appropriate for the continued analysis of the study, according to the statistical findings shown in Table 1.

4. RESULTS AND DISCUSSION

4.1. Gender of the Respondents

The gender of an individual is an important factor as they have different behavior pattern in different situations and understanding them is crucial for any study.

Table 2 Gender of the respondents

Frequencies of Gender		
Gender	**Frequency**	**% of Total**
Male	128	33%
Female	261	67%

From Table 2 it is evident that of the 389 respondents, 128 of them are male which forms 33% of the total respondents, and 261 respondents are females and they form 67% of the total respondents.

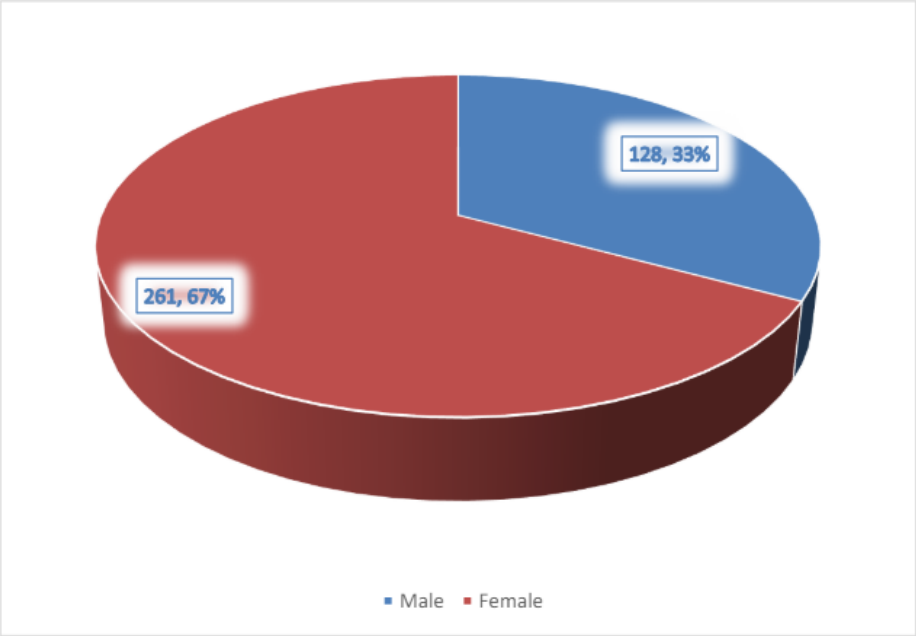

Figure 1. Respondent's Gender

From Figure 1 above, it is obvious that the majority of the respondents for this study are females and they constitute 67% of the sample and only 33% of the sample are men.

4.1.1. Age of the respondents

Age is a primary variable in the demographic factor which is measured in analysis. The risk-bearing capacity of an individual varies over the years. The age group has been classified in four groups, the first one is for individuals below the age of 25, second group has individuals of the age group of 25 – 35 years, the third set has individuals in the age group of 36 – 45 of years and the last group has individuals above the age of 45 years. The same has been represented in the below-given table

Table 3. Respondent's Age:

Age Group	Frequency	% of Total
Below 25yrs	115	29.6 %
25yrs – 35yrs	165	42.4 %
36yrs – 45yrs	61	15.7 %
Above 45yrs	48	12.3 %

The age distribution of the respondents is shown in Table 3. Between the ages of 25 and 25, 165 respondents were found; 115 were younger than 25; 61 were in the 36–45 age bracket; and 48 were older than 45.

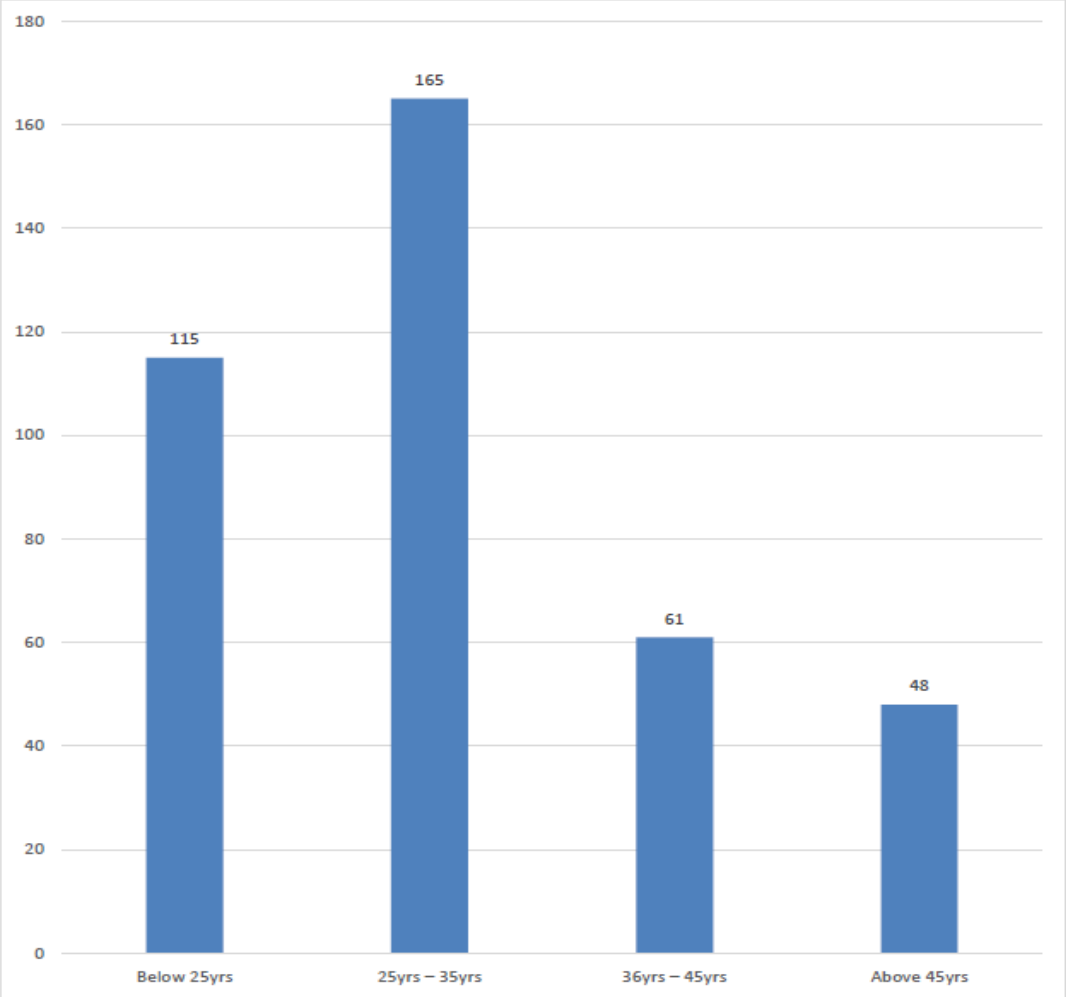

Figure 2. Respondent's Age

Figure 2 indicates that 42% of the respondents fall in the age group of 25 yrs – 35 yrs followed by 30% of the respondents below the age 25 yrs, 16% of respondents in the age cluster of 36 yrs – 45 yrs and 12% of respondents are above the stage of 45 years.

4.1.2. Qualification of the Respondents

Qualification is another demographic factor that has been looked into in this study. The respondents have been classified into two main categories as individuals who have their highest qualification as graduation and the other as individuals who have completed their post-graduation and any other higher degree.

Table 4. Qualification of respondents

Frequencies of Qualification		
Levels	**Counts**	**% of Total**
Graduate	173	44.5 %
Post Graduate	216	55.5 %

Table 4 indicates that the number of respondents who have completed their graduation is 173 and 216 respondents have completed their post-graduation or any other higher degrees.

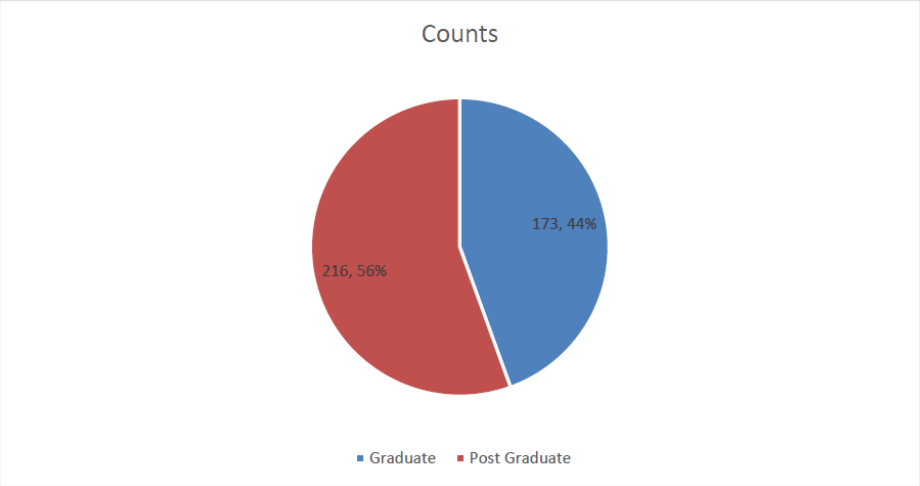

Figure 3. Qualification of respondents

Figure 3 indicates that 56% of the respondents for this study have completed a postgraduation degree and 44% were graduates or diploma holders.

5. CONCLUSION

The consequences of being a victim of cybercrime are many. It can make a person lose confidence in himself/herself and will have a feeling that they are being watched and stalked all the time. This can hamper the growth and potential of an individual to move forward. In this digital era, it is very important to be tech-savvy and also to perform all the tasks over the internet as this will lead to savings in time, and resources and also to stay ahead of competitors. Due to the dynamic nature of ICTs, internet users must make it a practice to regularly refresh their knowledge in this area. As a result, they will be able to protect their information from cybercriminals by staying up-to-date on the latest trends in cybercrime and learning about the different types of cybercrime and how cybercriminals carry out their bad activities. The necessity for individuals to exercise internet-related self-control and heightened vigilance when using the internet is growing in proportion to the persistence of cybercrime.

Every motivation should be provided to increase awareness about cyber risks, inculcate the right etiquette of online behavior, and encourage people to come and share their experiences with cyber risks, as a victim or how they were able to dodge a cyber intrusion or a cyber-attack as all these go a long way in increasing the preparedness to handle cyber risks at an individual level which will have its cascading effect of an organization being prepared, a society being prepared and an entire nation being prepared to handle cyber risks.

REFERENCES

[1] Bennis, W., Boccaccio, V., Pagani, M., Oestreicher-singer, G., Zalmanson, L., English, L., Godfrey, a B., Woodard, C. J., Tschang, F. T., Trategy, D. I. B. U. S., Mithas, S., Tafti, A., Mitchell, W., Drnevich, P. L., Croson, D. C., Grover, V., Markus, M. L., Loebbecke, C., Tim, V. P., … Pavlou, P. A. (2013). M Anaging I Nformation Q Uality –. Data Base, 37(2), 633–635.

[2] Betts, L. R., & Spenser, K. A. (2017). Developing the Cyber Victimization Experiences and Cyberbullying Behaviors Scales. Journal of Genetic Psychology, 178(3), 147–164. https://doi.org/10.1080/00221325.2017.1295222

[3] Bharadwaj, S. K., & Bba, H. (2016). Cyber Liability Insurance in India: Growing Importance. Imperial Journal of Interdisciplinary Research, 2(1), 2454–1362.

[4] 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

[5] Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara e Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. International Journal of Information Management, 43. https://doi.org/10.1016/j.ijinfomgt.2018.08.008

[6] Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

[7] Howard, D. J. (2018). Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents (Issue June). https://scholarcommons.usf.edu/etd/7306/

[8] Kurmaiev, P., Seliverstova, L., Bondarenko, O., & Husarevych, N. (2020). Cyber insurance: the current situation and prospects of development. Revista Amazonia Investiga, 9(28), 65–73. https://doi.org/10.34069/ai/2020.28.04.8

[9] Here, T. G. (2022). Cyber Insurance: Protecting our way of life, in a digital world. Insurance Council of Australia, March, 1–21.

[10] Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. Crime, Law and Social Change, 1–24.

Citation: Kaushik Reddy Muppa, Analysis on Cyber Risk Exposures and An Evaluation of The Elements That Go into Being Ready to Deal with Cyber Threats, International Journal of Computer Engineering and Technology (IJCET), 15(3), 2024, pp. 12-20

Abstract Link: https://iaeme.com/Home/article_id/IJCET_15_03_003

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_3/IJCET_15_03_003.pdf

✉ **editor@iaeme.com**