Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3364 - 3371
Received 05 March 2021; Accepted 01 April 2021.

A Study on Cyber Security in Financial Services Sector

[1]mary Benitta Rani, [2]sridevi Narayanan

[1]Assistant Professor,College of Administrative and Financial Sciences,AMA International University, Kingdom of Bahrain,
[2]Assistant Professor, College of Computer Studies, MA International University, Kingdom of Bahrain,

ABSTRACT:

A cyber security meant to assist a corporation mitigate risk exposure by offsetting costs involved recovery after a cyber-related security breach or similar event. Security vulnerabilities available in cyber security systems cause virtual and physical damages to financial systems which successively cause national- and individual-level security issues. Today's world is being shaped by digital technology, and cyber threats to information constitute a big risk factor for businesses. This study explores the cyber security risks the economic system may encounter. The status of monetary system, a system which incorporates variety of online services, in Tamilnadu with reference to cyber security risks and therefore the current risks are assessed and presented alongside possible solutions. This study analyzes cyber security and cyber risk insurance. Nevertheless, cyber risk insurance, an emerging tool for cyber risk management, was analyzed intimately. With this background, the researcher has taken this topic to analyse the Cyber Security in Financial Services sector in Chennai District.

Keywords: Financial sector, cyber security, Level of perception

INTRODUCTION

Many nations present radical solutions against cyber-attacks and make investments in such solutions. Variety of countries like better to protect their critical communications of cyber security on the market level, while nations like Israel developed state-centric security strategies. Many cyber security specialists stated that it's impossible to adopt an efficient defense and counteracting security regimen without cooperation with the stakeholders from the private sector, because the state services are backed by variety of personal service providers and telecommunication companies. Cyber risk may be a sort of risk which incorporates any unexpected technical failure of the IT infrastructure of a business or any cyber-attack targeting such infrastructure which results in possible financial losses and damaged brand value. Today, any commercial establishment starting from Small- and Middle-sized Enterprises (SMEs) to international businesses face the financial consequences of the risks arises from cyber threats. As a result, a replacement market has emerged with the increasing interest in cyber security products. Cyber-attacks brought with them a replacement opportunity for insurance companies which supply their services during a highly competitive market which want to expand their product range. Many companies

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3364 - 3371
Received 05 March 2021; Accepted 01 April 2021.

have already introduced their cyber insurance productsand lots of more are preparing to launch their productsconsistent with the survey by ABI Research, it's expected the worldwide cyber risk insurance market will reach up to US$10 billion in market price by 2020.

OBJECTIVES OF THE STUDY

- To know the online financial risk faced by the financial sectors
- To know the level of perception towards cyber security

HYPOTHESES FRAMED

Ho: There is no significant relationship between the age of the company and level of awareness towards cyber security.

RESEARCH METHODOLOGY

Research Design

The researcher has used both descriptive and exploratory research design.

Data used

The researcher has used both Primary and Secondary Data. The Primary data were collected through Structured and Pre tested Questionnaire. The Secondary data were collected from the Published Books, Journals, News Papers, Magazines, websites etc.

Data collection method

The researcher may collect data through the structured questionnaire.

Target population of the study

The researcher has targeted companies from financial sector functioning in Chennai District.The financial sector is a section of the economy made up of firms and institutions that provide financial services to commercial and retail customers. This sector comprises a broad range of industries including banks, investment companies, insurance companies, and real estate firms. The researcher has targeted those companies functioning in Chennai District.

Sampling Design

The researcher has used Purposive Sampling method. The researcher purposively selected companies from the financial sector. The researcher has selected 80 companies for the present research work.

LIMITATIONS OF THE STUDY

1. The study had been carried out in financial sector only and hence the findings of the study are valid to this particular sector only.
2. The researcher has concentrated on selected study area only.
3. The reliability of the data depends upon the responses given by the respondent

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3364 - 3371
Received 05 March 2021; Accepted 01 April 2021.

AGE OF THE COMPANY AND LEVEL OF AWARENESS TOWARDS CYBER SECURITY OF FINANCIAL SECTOR COMPANIES

S.No	CYBER SECURITY ATTRIBUTES	Chi Square Value	Sig.Valu	Sig Or Not
1	Safety towards account details	18.445	0.361	Not Sig
2	Privacy of accounts	49.995	0.515	Not Sig
3	Legal regulation	2251.903	0.000*	**Sig**
4	Good Governance	2180.338	0.000*	**Sig**
5	Risk Management	2280.350	0.000*	**Sig**
6	Security Management	2079.604	0.000*	**Sig**
7	Technology Management	2158.698	0.000*	**Sig**
8	Incident Management	2325.235	0.000*	**Sig**

From table above it is observed that out of 8 selected variables, six variables such as Legal regulation, Good governance, Risk management, Security Management, Technology management and Incident management have significant association with the level of awareness towards the attributes of cyber security. The remaining 2 variables namely, safety and privacy do not have significant association with company's level of awareness towards the attributes of cyber security.

PERCERPTION TOWARDS CYBER SECURITY

Factor analysis is used to identify and define the underlying dimensions (factors) in the original variables. Here 14 factors are identified tostudy the perception towards cyber security. The variables are stated in the form of statements to collect opinion from the respondents. They are asked to give their opinion for all the 14 statements in the Likert's five point scale with alternate options such as strongly disagree, disagree, neither agree nor disagree, agree and strongly agree. A closer examination of the correlation matrix may reveal variables which do not have any relationship. Therefore, all the 14 variables have been retained for further analysis.

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.971
Bartlett's Test of Sphericity	Approx. Chi-Square	979.896
	Df	91
	Sig.	.000

KMO and Bartlett's Test

The Kaiser – Meyer – Olkin test is based on the correlations and partial correlations of the variables. If the test value of KMO measure is closer to one, it is good to use factor analysis. If KMO measure is closer to zero, the factor analysis is not a good idea for the variables and data. The value of KMO measure of sampling adequacy is 0.971.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3364 - 3371
Received 05 March 2021; Accepted 01 April 2021.

Another test namely, Bartlett's test of sphericity is used to test whether the correlation matrix is an identified matrix i.e., all the diagonal terms in the matrix are zero. The significant value of Bartlett test is 0.000. Hence, there exists significant relationship among the variables. The measure of KMO test and value of Bartlett test indicate that the present data are useful for factor analysis.

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.985	35.606	35.606	4.985	35.606	35.606	2.944	21.031	21.031
2	2.461	17.577	53.183	2.461	17.577	53.183	2.907	20.767	41.797
3	1.749	12.491	65.675	1.749	12.491	65.675	2.838	20.275	62.072
4	1.315	9.396	75.071	1.315	9.396	75.071	1.517	10.839	72.911
5	1.154	8.246	83.316	1.154	8.246	83.316	1.457	10.405	83.316
6	.679	4.851	88.167						
7	.454	3.241	91.408						
8	.416	2.974	94.382						
9	.284	2.026	96.408						
10	.232	1.658	98.066						
11	.145	1.038	99.103						
12	.062	.445	99.548						
13	.050	.360	99.907						
14	.013	.093	100.000						
Extraction Method: Principal Component Analysis.									

The next step in the process is to decide about the number of factors to be derived.Principal Component Analysis (PCA) method is applied to choose the number of factors for which "Eigen Values" with greater than unity. The component matrix so framed is further rotated orthogonally using varimax rotation algorithm. All the statements are added on the two factors. The results so obtained have been given in the tables separately along with factor loadings. Of the five factors, the first factor which accounts for 35.606 percent of variance is the primacriteria considered to study the respondents' (traders or company) perception towards cyber security. The second factor accounts for 17.577 percent. The third factor accounts for 12.491 percent and the fourth and fifty factor explained 9.393 and 8.246 percent. The cumulative variance of all five factors is 83.316 percent. The following table gives the factor matrix where principal component analysis extracted five factors.

Rotated Component Matrix[a]	
	Component

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3364 - 3371
Received 05 March 2021; Accepted 01 April 2021.

	1	2	3	4	5
Cyber attacks	.928				
Cyber security risk	.819				
Online financial risk	.687				
Types of Cyber risk	.651				
Hackers		.893			
Malware		.860			
Web jacking		.782			
Denial of service attack		.651			
Logic bombs			.916		
Virus diffusion			.901		
Cyber Stalking			.831		
Data Diddling			.522		
Govt Initiatives				.826	
Cyber laws					.893
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.					
a. Rotation converged in 6 iterations.					

Table above reveals that the factor loadings (co –efficient) indicate how much weight is assigned to each factor. The factors with large co-efficient for a variable are closely related to that variable. Thus the 14 variables in the data are reduced into five factor models and each factor is identified with the corresponding variables as given below.

Factors	**Statements**
Factor 1 – (Risk Factors)	Cyber attacks
	Cyber security risk
	Online financial risk
	Types of Cyber risk
Factor 2 – (External Factors)	Hackers
	Malware
	Web jacking
	Denial of service attack
Factor 3 - (Internal Factors)	Logic bombs
	Virus diffusion
	Cyber Stalking
	Data Diddling
Factor 4 – (Government factor)	Govt Initiatives
Factor 5 – (Law factor)	Cyber laws

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3364 - 3371
Received 05 March 2021; Accepted 01 April 2021.

CLUSTER ANALYSIS

The selected companies perception towards cyber security can be classified in three categories based on choice criteria using the cluster analysis. They are classified into three segments because the difference between the co–efficient is significant only on three cases on the hierarchical cluster. For the purpose of classification of traders (company) K- means cluster is used.

Final Cluster Centers			
Factors	Cluster		
	1	2	3
Risk	.84797	.18320	.69193
Internal security	.54627	.41255	.74418
External security	.26715	.75646	.17505
Government	.40094	.92115	.14226
Law	.21867	.94759	.32801
Average	2.281	3.22095	2.08143
Rank	**II**	**I**	**III**

The final cluster centers' table above shows the mean values for the three clusters which reflect the attributes of each cluster. The high mean value for the first cluster, second cluster and third cluster are 3.22, 2.281 and 2.08 respectively. This means that the first cluster respondents have medium perception, second cluster respondents have low perception and third cluster respondents have high perception towards cyber security.

The following table presents the cluster means square, error mean square and F- value.

ANOVA						
	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
Risk	18.748	2	.539	77	34.783	.000
Internal security	14.869	2	.640	77	23.241	.000
External security	6.711	2	.852	77	7.880	.001
Government	10.372	2	.757	77	13.709	.000
Law	10.520	2	.753	77	13.976	.000

The ANOVA table above indicates that the difference existing among the three clusters in the mean values is significantly different. The significant value for the factors is 0.000. This means that the above five factors have significant contribution on dividing traders (company) into three segments based on choice criteria.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3364 - 3371
Received 05 March 2021; Accepted 01 April 2021.

Number of Cases in each Cluster		
Cluster	1	30.000
	2	18.000
	3	32.000
Valid		80.000
Missing		.000

Table above reveals that out of the 80 respondents, 32 (40%) respondents have high perception, 30 (37.5%) respondents have moderate perception and only 18 (22.5%) respondents have low perception. It is important to note that very low percentage of the respondents (59.7%) have very low perception towards cyber security.

SUGGESTIONS AND CONCLUSION

The developing period of digitalization asks the requirement for cyber insurance. The business can bear the cost of the protection inclusion against these cybercrimes. The individual clients ought to likewise profit by such protection. The digital protection cover keeps the people from the dread of malicious harms. They don't catch any weakness in dealing with individual information. Yet, the protection cover ought to be given surveying the danger related. The sort and setting of the individual data managed, instruction and preparing of people are to be thought of while surveying the danger. It ought to likewise consider the degree of security of cell phones that convey touchy data. The Government should start mindfulness about the danger just as its counteraction. The impact of globalization is positive in monetary development and improvement. Yet, it has likewise offered ascend to numerous issues around the world. As India is an agricultural nation, the framework and other making sure about and promising improvements are not quickly in the range, yet could be reached. The lead time between, causes tension and concern. The essential need is felt being developed of hey tech framework outfitted with against hazard. Without a doubt India is continuing onward with the serious edge. However, it is slacking in protecting such advancements. At present the digital protection idea is felt uniquely in the West though in India it is restricted distinctly to few business houses. At the point when we are sharp during the time spent digitalization, and demand straightforwardness and responsibility it is the duty of the change to secure the change. Rustic India is the most exceedingly terrible hit during the time spent digitalization. It is genuinely felt at this point, the requirement for Cyber protection.

Reference

1. https://en.wikipedia.org/wiki/Cyber-Insurance
2. www.aig.com/business/insurance/cyber-insurance
3. https://www.onlinejournal.in/IJIRV2I1/004.pdf
4. https://www.britannica.com/topic/cybercrime

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3364 - 3371
Received 05 March 2021; Accepted 01 April 2021.

5. https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html
6. https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf
7. http://www.cyberriskinsuranceforum.com/sites/default/files/CIS%20Cyber%20Insurance_FINAL.pdf
8. http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/06/WEIS_2017_paper_28.pdf
9. Dr. D.PaulDhinakaran, *"*Exports and Imports Stagnation in India During Covid-19- A Review*"* GIS Business (ISSN: 1430-3663 Vol-15-Issue-4-April-2020).
10. Shree Krishna Bharadwaj.H(2016), "Cyber liability insurance in India: Growing importance", Imperial Journal of Interdisciplinary Research (IJIR) – Volume 2 Issue 1 2016, ISSN: 2454-1362.
11. Dr. D.PaulDhinakaran, *"Community Relations Of Tamilnadu State Transport Corporation Ltd"*International Journal Of Research And Analytical Reviews (E ISSN 2348-1269, print ISSN 2349-5138) Special Issue March 2019.