IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study On Risk Management Strategies For E-Commerce Technology In Business Special Preference Within Tamilnadu

1Dr .M.R. Chandrasekar, 2M. Suman

1Dr, 2student

1Dr. N. G.P. Arts and Science college,

2Dr. N.G.P Arts and Science college

ABSTRACT:

The growth of e-commerce has been significant in India over the past few years, and it has provided a platform for businesses to reach consumers in a much more efficient way. However, this also exposes consumers to various digital risks. Digital risks refer to the various risks that consumers face when they engage in e-commerce activities. Some of the significant digital risks include data breaches, cyber-attacks, phishing, identity theft, and fraudulent transactions. These risks can cause significant damage to both consumers and e-commerce businesses. Consumers can lose their personal information, suffer financial losses, and even face reputational damage. E-commerce businesses can face significant financial losses, damage to their brand reputation, and legal issues. Effective risk management strategies are essential for mitigating these risks and ensuring the continued growth and success of e- commerce businesses. Companies must adopt a proactive approach to identify, assess, and manage potential risks to protect both their assets and their customers' interests.

INTRODUCTION:

E-commerce businesses should also have clear and concise terms and conditions, privacy policies, and data protection policies. These policies should inform consumers about the data that e-commerce businesses collect, how they use it, and how they protect it. E- commerce businesses should also provide consumers with the option to opt-out of any marketing communications and should not share their data with third parties without their explicit consent. E-commerce businesses should also provide consumers with a secure payment gateway to protect their financial information. They should use encryption to protect payment information and should not store consumers' payment information unless

explicitly permitted by the consumers.

The following are some of the consumer protection issues that e-commerce businesses face:

1. Product quality: E-commerce businesses need to ensure that the products they sell are of good quality and meet the standards set by regulatory authorities.
2. Delivery issues: E-commerce businesses need to ensure that products are delivered to customers on time and in good condition.
3. Payment issues: E-commerce businesses need to ensure that payment systems are secure and that customers' payment information is protected.
4. Customer service: E-commerce businesses need to provide good customer service to ensure customer satisfaction and loyalty.

STATEMENT OF THE PROBLEM:

The exponential growth of e-commerce has led to increased exposure to various technological risks, including cyber security threats, data privacy concerns, transaction fraud, and system downtime. Many businesses, especially small and medium enterprises (SMEs), struggle to implement adequate risk management strategies, leading to financial losses, reputational damage, and operational disruptions.

Despite the availability of advanced security tools and frameworks, businesses often lack the knowledge, resources, or strategic approaches to effectively mitigate these risks. Additionally, evolving cyber threats and regulatory requirements further complicate risk management efforts in the e-commerce sector.

This study aims to examine the key risk factors affecting e-commerce businesses and evaluate existing risk management strategies to identify best practices. The research will also explore technological solutions, legal frameworks, and policy recommendations to help businesses enhance their risk resilience. By addressing these challenges, this study seeks to provide a comprehensive understanding of how businesses can secure their e-commerce operations while maintaining growth and innovation.

OBJECTIVES:

Primary objective

To study on risk management strategies for E-Commerce technology in business

Secondary objectives

- To understand the major technological risks faced by e-commerce businesses.
- To analyses risk change techniques used by businesses
- To evaluate the impact of risk management on business performance
- To monitoring the risk management through legal and regulatory compliance.

SCOPE OF THE STUDY:

This scope helps clarify the depth and breadth of the study, focusing on practical, technological, and strategic aspects of risk management within e-commerce environments. It also highlights how businesses can leverage technology to proactively manage risks, ensuring smooth operations and long-term success.

RESEARCH METHODLOGY:

Research methodology is the systematic way to solve the research problems. It gives an idea about various steps adopted by the researcher in a systematic manner with an objective to determine various manners,

Research design:

Research design is the scheme of work undertaken by the researcher at various stages. The research design includes the mode of data to be collected, the sample to be selected and the analysis part of research. In order to study the human research development activities, the researcher has adopted descriptive design.

Method of Data collection

Basically, there are two methods of data collection

1. Primary data
2. Secondary data

Primary Data

Primary data are those which are collected afresh and for first time, and thus happen to be original in character, there are several methods of collecting primary data. The method used here is questionnaire method.

Secondary Data

Secondary data means that are already available i.e., they refer to the data which have already been collected and analyzed by someone else. It was collected from company records, files and internet sources.

Sample size

The sample size is 120 respondents.

Statistical tools used analysis

Statistical tools are the mathematical techniques used to facilitate the interpretation of numerical data secured from groups of individual or groups of observation individual.

For the purpose of the study the following tools are used

- Simple Percentage Method
- Chi-Square Method

The results of the survey were represented through tables and exhibits

LIMITATIONS OF THE STUDY

1. Some of the respondents of the survey may be unwilling to share information,
2. There might be a possible tendency of respondents to give inaccurate or untruthful answers for various reasons
3. The study is confined to Tamil Nadu only.

REVIEW OF LITERATURE:

Su (2024)[1] examines these challenges and proposes optimization strategies, including strengthening compliance and risk management, improving logistics and supply chain efficiency, and enhancing information security protocols. These measures aim to provide guidance for the robust operation of cross-border e-commerce platforms.

Vos et al., (2023) The intrusion of cyber criminals into the companies' critical infrastructure has become a major concern to risk managers, resulting in introduction of sophisticated techniques for data protection. One such strategy is digital signature, which is a critical feature in risk mitigation that involves a cryptographic tag that can only be calculated. This feature helps to curb such activities as hacking through unique encryption of information.

Piotrowicz & Cuthbertson, (2023) The security of online transactions depends on various features that are incorporated into the data protection systems to minimize the risk of cyber activities. Digital envelopes are among the critical developments that have been found to play a significant role in the protection of companies' critical infrastructure. Firms in the e- commerce business continue to introduce new features into their risk management techniques in order to respond adequately to emerging in modern conditions, new attacks emerge from technological evolution, prompting the risk managers to invest in technologies that will enhance protection of information resources in their companies.

DATA ANALYSIS:

SIMPLE PRECENTAGE:

TABLE SHOWING GENDER OF THE RESPONDENTS

Gender	Number of respondents	Percentage
Male	80	67
Female	40	33
Total	**120**	**100**

INTERPRETATION:

It is inferred that 67% of the respondents are male and 33% of the respondents are female. **Majority of the respondents are male. CHI-SQUARE TEST:**

To find the significant association between Type of industry e commerce business operating and the biggest technological risks their business faces.

Hypothesis.

Null Hypothesis = There is no significant association between Type of industry e commerce business operating and the biggest technological risks their business faces.

= There is significant association between Type of industry e commerce business

TABLE NO: 4.28 (a)

Type of industry e commerce business operating * The biggest technological risks their business faces cross tabulation					
	ogical risks their business faces				
Type of industry e commerce business operating	Cyber attacks	ayment fraud	Data privacy breaches	System failures and downtime s	ota l
Retail	3	7	2	2	14
Services	13	21	7	5	46
Digital products	8	16	12	12	48
Others	2	8	1	1	12
Total	26	52	22	20	120

TABLE NO: 4.28 (b) CHI-SQUARE TABLE

Chi-Square Tests	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10.094[a]	9	.343
Likelihood Ratio	9.999	9	.351
Linear-by-Linear Association	1.142	1	.285
N of Valid Cases	120		

Level of Significant =5 % Degree of freedom-(R-1) (C-1)

(3-1) (5-1) = 8

INTERPRETATION

Since the p value is 0.343 which is greater than 0.05 at 9 degrees of freedom and 5 percentage level of significance, we accept the alternate hypothesis. Hence there is a significant association between Type of industry e commerce business operating and the biggest technological risks their business faces

s operating and the biggest technological risks their business faces.

FINDINGS:

- 43% of respondents consider payment fraud to be the biggest technological risk their business faces
- 58% of respondents report that their company experiences security-related incidents occasionally
- 42% of respondents use real-time monitoring tools to monitor their e-commerce systems for potential risks

SUGGESTIONS:

- Educate customers on safe online transaction practices to prevent phishing and payment fraud.
- Encourage the use of tokenization and block chain technology to enhance transaction security.
- Use AI-based fraud detection systems to identify suspicious activity.
- Monitor customer purchasing behavior for signs of account takeovers or fraudulent activity.

CONCLUSION:

The project entitled "**Risk Management Strategies for E-Commerce Technology in Tamil Nadu** "was carried out with sample size of 120. The statistical tools used for the study is Percentage analysis, Chi-square and weighted average with ranking. Majority of respondents are from medium-sized e-commerce businesses and report that their company experiences security-related incidents occasionally. Majority of the respondents believe that their risk management strategies are very effective in preventing security breaches.

The study highlights the critical need for businesses to adopt a proactive and integrated approach to managing risks. As the e-commerce industry grows rapidly in Tamil Nadu, businesses face increasing threats related to cyber security, payment security, supply chain disruptions, and regulatory compliance.