

ABSTRACT

This study investigates the level of cyber-law awareness among small business owners who conduct digital operations such as online sales, marketing, and data storage. While digital tools enable growth and efficiency, they also expose businesses to cyberattacks and legal liabilities. Using a mixed-methods approach—online questionnaires completed by 25 participants and follow-up interviews—the research assesses owners' understanding of key legal requirements surrounding data privacy, electronic transactions, and cybersecurity standards.

Findings reveal that most respondents possess only limited or fragmented knowledge of cyber law, often neglecting critical practices like strong data-protection measures, customer-consent protocols, and compliance with privacy regulations. This lack of awareness increases vulnerability to data breaches, financial penalties, and reputational harm. Root causes include insufficient access to affordable legal guidance, low prioritization of cyber risks, and underestimation of the consequences of cybercrime. The study concludes that improving legal awareness is vital for the resilience of small enterprises and the broader digital economy. It recommends comprehensive education programs, user-friendly compliance resources, affordable legal and cybersecurity services, and the promotion of a proactive cybersecurity culture. These measures can help small business owners safeguard digital assets, meet legal obligations, and maintain customer trust in an increasingly connected marketplace.

TABLE OF CONTENTS

Sr.no	Particulars	Pages.no
1.	Abstract	
2.	Table of contents	
3.	List of figures and tables	
4.	Chapter 1: Introduction	
5.	Chapter 2: Iteration Review	
6.	Chapter 3: Methodology	
7.	Chapter 4: Field work Description , Observation and Analysis	
8.	Chapter 5: Conclusion and Recommendation	
9.	References	
10.	Appendices	

List of figures and tables



MR. Paresh Rawal is filling the survey form.



Gain knowledge about cyber law



Coordinating with us for
Field project.



Spreading awareness of
cyber law



Participating in the survey

Chapter 1: Introduction

Small businesses increasingly rely on digital tools for operations like online transactions, marketing, and data storage. While this digital shift offers many benefits, it also brings risks such as cyberattacks and data breaches. Cyber laws are designed to regulate online behavior and protect digital assets. However, many small business owners lack awareness of these laws, leaving them vulnerable to legal and financial risks. This study explores their level of awareness and understanding of cyber law.

Many small business owners are unaware of their legal responsibilities related to cybersecurity. This lack of awareness increases the risk of legal violations and exposure to cybercrime. Despite their vulnerability, small businesses are often overlooked in cyber law research, creating a gap that this study aims to fill.

- To assess the level of cyber law awareness among small business owners.
- To identify challenges faced in understanding and complying with cyber laws.
- To recommend ways to improve cyber law awareness and compliance.

The study focuses on small business owners who operate digitally. It does not include large enterprises, government bodies, or technical cybersecurity measures. The emphasis is on legal awareness only.

This study highlights the need for greater legal awareness among small business owners. Its findings can help shape training programs, inform policymakers, and assist small businesses in improving their legal compliance and cybersecurity practices.

Chapter 2: Literature Review

1.science 2025:

- ❖ [Human-centric **cyber** security: Applying protection motivation theory to analyse micro **business owners'** security behaviours](#) [H Jamil](#), [T Zia](#), [T Nayeem](#), [MT Whitty](#)... - Information & Computer ..., 2025 - emerald.com.
- ❖ [Enhancing **Cybersecurity Awareness**: mitigating phishing risks for employees in a **small company**](#)
D Mercuri - 2025 - theseus.fi

2.Science 2024:

- ❖ [**Cybersecurity, cyber** insurance and **small-to-medium-sized enterprises**: a systematic Review](#) [R Adriko](#), [JRC Nurse](#) - Information & Computer Security, 2024 - emerald.com
- ❖ [**Cybercrime In The Digital Era: Impacts, Awareness, And Strategic Solutions For A Secure Future**](#) [P Pandey](#), [A Kapoor](#) - Sachetas, 2025 - sachetas.in

3.Sort by relevance:

- ❖ [\[PDF\] **E-Commerce Adoption in Distribution Channel: Evidence from Retail Enterprises in Vietnam**](#) [HD NGUYEN](#) - Journal of Distribution Science, 2025- researchgate.net
- ❖ [**Cybersecurity** and Global Data Protection **Laws**: Post-gDPR Era Analysis](#) [A Palanissamy](#) - Tech Fusion in **Business** and Society, 2025 - Springer

4.Review:

- ❖ [**Balancing Act: Navigating Privacy and Security in the Cookie-Enabled Web**](#)[A Jaiswal](#), [BK Basnet](#), [P Ghimire](#)... - ... IEEE Consumer Life ..., 2024 - ieeeexplore.ieee.org

Chapter 3: Methodology

3.1 Research method:

- **Type:** Descriptive and exploratory
- **Approach:** Mixed methods (quantitative surveys + qualitative interviews)
- **Objective:** Assess the level of awareness, sources of knowledge, and gaps in understanding of cyber law among small business owners.

3.2 Tool used:

1. Questionnaires: Digital platforms like Google Forms, Microsoft Forms.
2. Interviews: To gain deeper insights into perceptions, experiences, and challenges.
3. Software/Apps: Google Forms or Microsoft Forms – for creating and distributing questionnaires

3.3 Sample size:

- The survey was completed by 25 peoples .

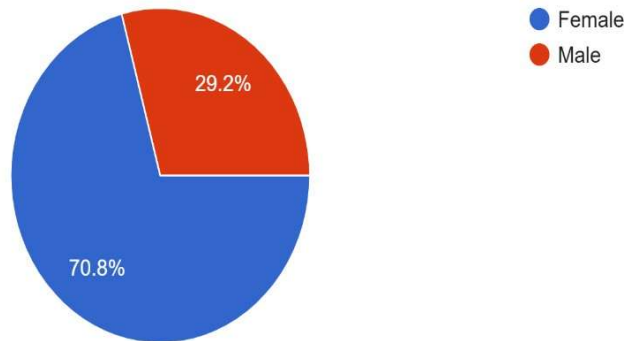
3.4 Sample Method:

- **Quata Sampling:** Within each subgroup, choose participants using convenience or judgment sampling (e.g., approaching business owners in local markets or via online directories).

3.5 Data Analysis:

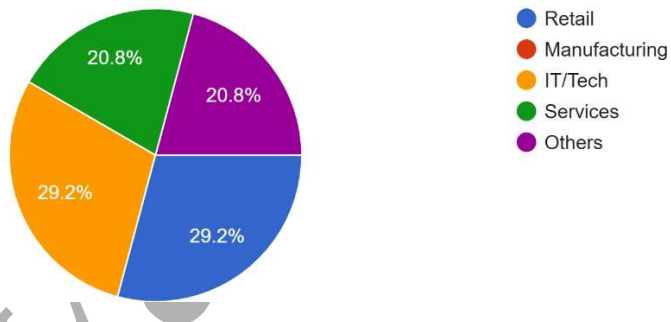
Gender

24 responses



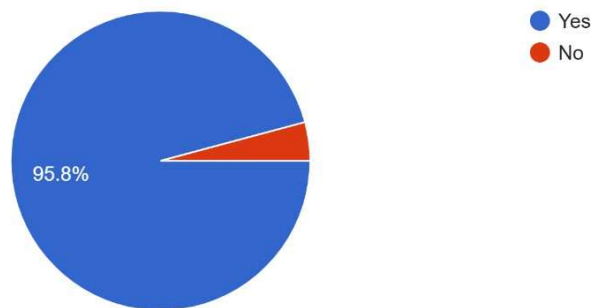
Businesses Sector

24 responses



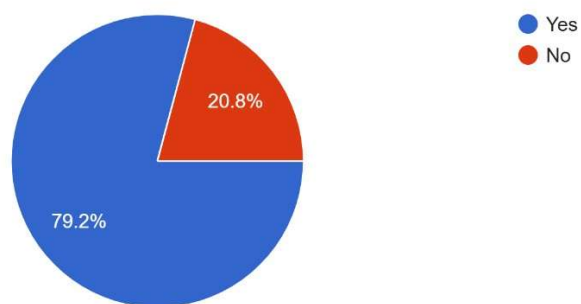
Are you aware of term "cyber law "?

24 responses



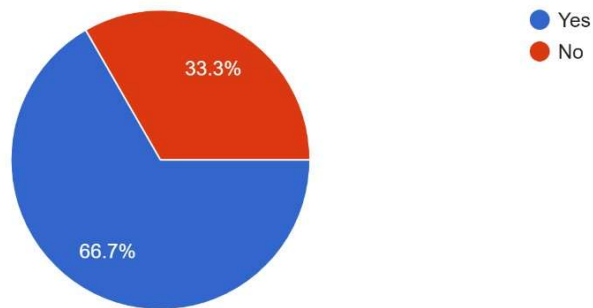
Do you use digital platforms for businesses (e-commerce, online payments, etc)

24 responses



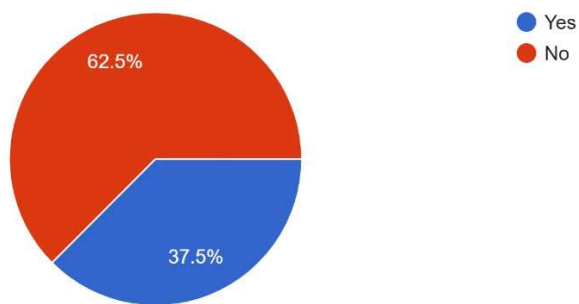
If no been interested in training secession of cyber law for small business

24 responses



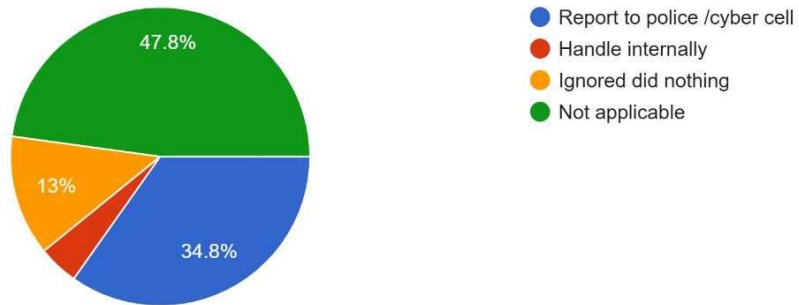
Have you or your business ever face cyber incidents (fraud, phishing, hacking, etc)

24 responses



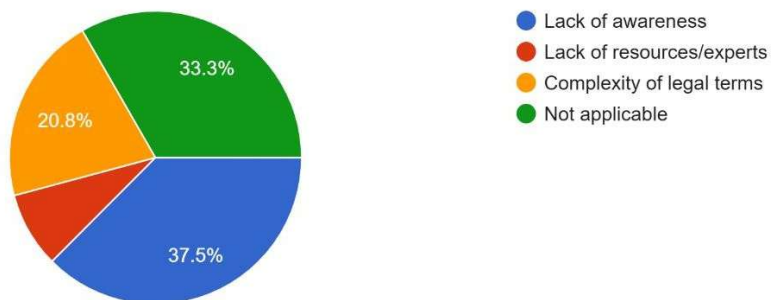
If yes, how did you respond to this incident ?

23 responses



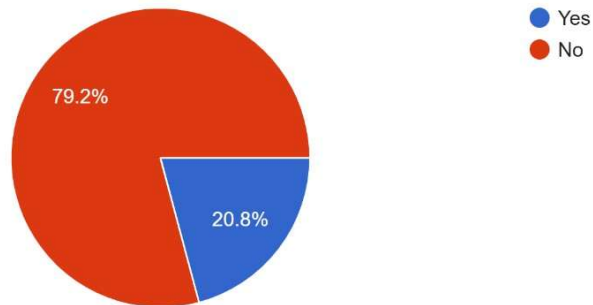
What challenges do you face in following cyber law?

24 responses



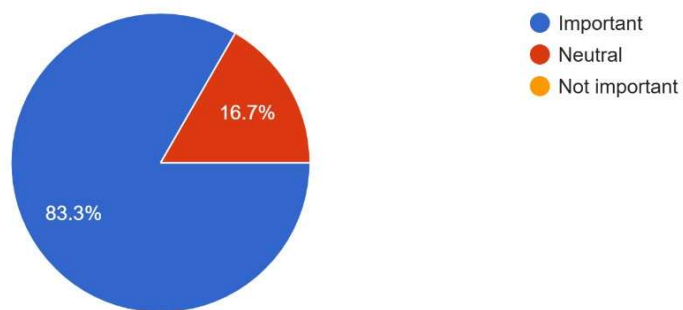
Have your business ever received training or workshops on cyber security/cyber law?

24 responses



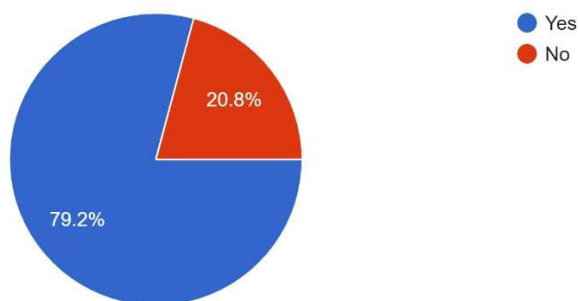
In your opinion how important is *cyber law awareness* for small businesses ?

24 responses



Do you know where to report cyber crime cases?

24 responses



Chapter 4: Field work description, observation and analysis

4.1 Description:

Cyber law refers to the legal framework that governs activities in the digital environment, including internet usage, data privacy, electronic contracts, cybercrimes, intellectual property rights online, and cybersecurity standards. For small business owners, understanding cyber law is essential because it affects how they collect, store, and protect customer data, conduct e-commerce, communicate electronically, and handle digital transactions.

4.2 Observation:

Despite the increasing integration of digital technologies in small businesses, many owners have limited or fragmented knowledge of cyber law. Surveys and studies indicate that a significant number of small business owners do not fully understand legal obligations around data privacy or cybersecurity. This often leads to inadequate security measures like weak passwords, lack of encryption, or absence of privacy policies on websites. Furthermore, many are unaware of the legal implications of data breaches or cyber-attacks, leaving their businesses exposed to risks such as financial loss, fines, or reputational harm.

4.3 Analysis:

The limited awareness of cyber law among small business owners is a critical vulnerability in today's digital economy. Small businesses are increasingly targeted by cybercriminals because they often lack robust defenses. Ignorance about legal requirements means many fail to implement necessary compliance measures, such as obtaining customer consent for data collection or securing sensitive information, which can lead to severe penalties under laws like GDPR or local

equivalents. Additionally, cyber incidents can disrupt operations and erode customer trust, directly impacting business sustainability. The root causes of this lack of awareness include insufficient access to affordable legal and cybersecurity resources, low prioritization of cyber risk due to other pressing business concerns, and a general underestimation of cyber threats. Addressing this gap requires targeted education programs, accessible legal guidance, and incentives for small businesses to adopt cybersecurity best practices. By enhancing awareness and compliance, small business owners can better protect their enterprises and contribute to a safer digital marketplace.

Jiiva Nakum

Chapter 5: Conclusion and recommendation

5.1 Conclusion:

In today's rapidly evolving digital landscape, small business owners are increasingly dependent on online platforms for operations, sales, and customer engagement. However, their awareness of cyber law remains notably limited, exposing them to significant vulnerabilities. This lack of knowledge often results in inadequate data protection, weak cybersecurity practices, and non-compliance with legal requirements, which can lead to severe consequences such as data breaches, financial penalties, loss of customer trust, and damage to their business reputation. Given that small businesses typically lack the resources and expertise to manage these risks effectively, their cyber law ignorance represents a critical gap in overall business resilience. Addressing this issue is essential not only for safeguarding individual businesses but also for strengthening the broader digital economy's security and trustworthiness.

5.2 Recommendation:

To bridge the awareness gap and enhance the cyber law readiness of small business owners, a multifaceted approach is needed:

1. Comprehensive Education and Awareness Programs:

Governments, business associations, and cybersecurity organizations should collaborate to design and deliver targeted education initiatives. These could include workshops, webinars, and e-learning modules specifically tailored for small business owners that cover the fundamentals of cyber law, data privacy, cybercrime risks, and compliance obligations.

2. Development of Clear, Accessible Resources:

There is a need for simple, jargon-free guides, checklists, and

toolkits that explain cyber law requirements clearly and provide practical steps for compliance. These resources should be easily accessible online and translated into local languages where necessary.

3. Affordable Access to Legal and Cybersecurity Services:

Many small businesses cannot afford dedicated legal counsel or cybersecurity experts. Governments and industry bodies should facilitate access to subsidized or low-cost consulting services, including legal advice and cybersecurity audits, to help small businesses identify vulnerabilities and implement appropriate safeguards.

4. Encouraging a Proactive Cybersecurity Culture:

Small business owners should be encouraged to integrate cybersecurity into their overall business strategy. This includes adopting best practices such as strong password policies, data encryption, regular software updates, secure payment systems, and employee training on phishing and social engineering attacks.

References

- **Chatgpt:-** <https://chatgpt.com/>
- **Perplexity:-** <https://www.perplexity.ai/>
- **Google Scholar:-** <https://scholar.google.com/>
- **Microsoft Excel:-** <https://www.microsoft.com/en-in/microsoft-365/excel>
- **Gemini:-** <https://gemini.google.com/?hl=en-IN>