Confronting The Challenges Posed by Cybersecurity Issues

Pradeepa Kumar K V[1], Dr. Ajoy Joseph[2]
[1]*Research Scholar, Srinivas University, Mangalore*
[2]*Professor and Head, MBA Department Srinivas Institute of Technology, Mangalore*

***Abstract*—It is believed in well-informed circles that India's cybersecurity regime is challenged by outdated legal frameworks, fragmented coordination across institutions, acute shortage of skilled professionals and poor public awareness, among other things. Rapid digitization followed by rapid digitalisation of the country's economy and the rising sophistication of cyber threats, such as AI-driven attacks and ransomware renders the challenge even more challenging, so to speak. Given the current pace of growth of the country's digital footprint, the rising vulnerabilities of the country's cyber infrastructure have been coming to the fore every other day. Public and private sectors have become the prime target of cyber criminals and neither of the sectors is fully immune to cyber-attacks. The current status of the cybersecurity issues led the researcher to identify the key problems the country must contend with, in its cybersecurity space, so the researcher could recommend measures that the cyber administration must take to defend the country's cyber space Towards this end, the researcher interacted with two important categories of respondents associated with the cyberspace, namely, owners of business enterprises and practising lawyers. The interaction led the researcher to recommend that advanced cybercrime laboratories be established in our universities and at least in all sensitive government departments to begin with, to minimise the country's reliance on foreign hardware and software for its cybersecurity infrastructure. Additionally, given the demographic diversity of the country, the government should incentivise local players to invent tools that reckon the country's ecosystem, which is characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances in the main. Shockingly, even SMEs do not have adequate exposure to cyber hygiene. Hence, industry and trade bodies should train the SMEs in the art and science of handling cyberthreats lest the SMEs should miss the forest for the trees, given their weak wherewithal!**

***Index Terms*—cybersecurity; digitalisation; digitisation fragmented; wherewithal**

I. THEORETICAL BACKGROUND OF THE TOPIC

India's digital journey has been impressive so far. What started off sedately as a frugal exercise in innovation, suddenly got its second wind and raced ahead of its rivals, particularly in the digital public infrastructure (DPI) space. Wealthier and technologically more advanced countries figure in the list of the rivals the country overtook. Platforms like Aadhaar, Unified Payments Interface (UPI), and the India Stack have led a big chunk of Indians, including those from the remotest corners of the country, to access financial services, and government benefits, seamlessly and effortlessly. UPI alone accounts for 84 percent of all digital payment volumes, with transactions amounting to 800 percent plus of the country's GDP (Dharshan, 2025). Additionally, India has globalized its digital innovation, with Bhutan, Singapore, the UAE, and Qatar adopting UPI. The International Monetary Fund (IMF) calls India a leader in fast payments. India's G20 presidency positioned DPI as a global public good. Obviously, India's innovations are export-worthy given that they serve as blueprints for inclusive growth.

II. STATEMENT OF THE PROBLEM

India's achievements in the cyberspace have their flip side too -- businesses face cyberattacks. Since digital services span banking, health, commerce, and governance, the aftermath of the attacks can be easily visualised. Given that India's digital fabric spans dozens of languages, diverse user behaviours, and regulatory complexities, securing the digital fabric requires solutions that reckon these realities. Hence, making out a strong case for homegrown cybersecurity

champions is not just aspirational – it is existential, as one of the studies reviewed in a subsequent assert. This warrants that the country identifies the key problems it must contend with, in its cybersecurity space. It will help the country to define measures it must take to defend its cyberspace.

III. REVIEW OF LITERATURE

In the following paragraphs, some of the studies on the research topic are reviewed:

1. Abhiraj states that cybersecurity risks have been rising; they have been becoming more complex and more hazardous too, with enterprises increasingly chasing digitalisation (Abhiraj, 2025). By 2025, hackers will be exploiting emerging technology to take advantage of the weaknesses obtaining in enterprises of every kind, adds the researcher for good measure. Businesses that ignore cybersecurity risks will have to contend with financial losses, dented reputation, and legal repercussions. Even governments, corporations, and individual customers have been targeted because of which the cybersecurity landscape is changing quickly and appropriately. Workplace options like remote work and rapid deployment of artificial intelligence (AI) and increasing reliance on the cloud have opened newer pastures for the hackers. According to the researcher, Advanced Persistent Threats (APTs), Zero-Day Exploits and Nation-State Attacks figure among the latest threats our enterprises must contend with.
2. Ashok Kumar remarks that India has become a major target for cyber-attacks, given its growing digital footprint (Ashok, 2025). The growth has unveiled the rising vulnerabilities in the country's cyber infrastructure. The vulnerabilities in turn, have led to a surge in cybercrimes. To prove his point, the researcher recalls the 2020 cyber-attack on the Kudankulam Nuclear Power Plant. The attack exposed the state of security of critical infrastructure. In the circumstances, robust cybersecurity measures are called for. To prove that the government sector is a prime target of cyber criminals, the researcher cites the Aadhaar data leak of 2018 which exposed sensitive personal information of Aadhaar cardholders. Nor is the corporate sector immune to cyber-attacks, adds the researcher. He rues that many organizations lack basic cybersecurity practices; nor do they hire skilled professionals to combat cyber threats. On its part, the Government of India (GoI) has launched several initiatives. The framing of a National Cyber Security Policy and the constitution of an Indian Computer Emergency Response Team (CERT-In) are examples of such initiatives. They will ensure a secure and resilient cyberspace. However, these measures are not adequate. The Personal Data Protection Bill which seeks to enhance data protection laws and user privacy is a move in the right direction. On its part, the private sector has been taking proactive steps by investing in advanced security technologies and promoting awareness of cybersecurity. The researcher believes that collaboration between the public and private sectors is crucial to ensure cybersecurity. The exercise should be supplemented through cooperation at the global level. Promoting awareness, investing in skills and infrastructure, and enhancing policy frameworks are important among the measures needed to build a resilient cyberspace and secure a digital future for the associated stakeholders.
3. Tejas Bharadwaj asserts that a country's cybersecurity administration should ensure the safety, accessibility, and equitability of its cyberspace for its citizens (Tejas, 2025). The National Cybercrime Reporting Portal defines cybercrime as any unlawful act that involves the use of a computer, communication device, or computer network. India's digital economy is projected to account for 20 percent of its GDP by 2030. The country registered a record 18.3 billion digital payment transactions in March 2025. A driver of social and economic progress, Indians use cyberspace to exercise their fundamental rights and access public welfare services, reminds the researcher. Thus, the onus devolves on the government to protect the cyberspace from attacks. With multiple State / Central agencies / departments / actors participating, India's cybersecurity administration structure lacks clarity, adds the researcher. For example, which agency should deal with which aspect of cybersecurity, is a question that goes unanswered often. Currently, agencies and departments operating at the national and state levels follow a decentralized approach, allowing each sector to be

proactive about cybersecurity without waiting for directions from the top. This arguably allows for quick decision making for a cyberspace as large as India's and aligns with the quasi-federal structure. But how the agencies at the State and Central levels will coordinate with each other is a question that remains unanswered. Advancements in AI have been contributing to a significant rise in internet-connected smart devices and appliances in the last five years. In the circumstances, an adaptive cyber administration is imperative to deal with the evolving landscape and complexity of cyber threats through advancements in AI and quantum computing and their cyber nexus. India's current cybersecurity administration demonstrates an attempt to enforce a unified but differentiated responsibility that involves multiple stakeholders, including government agencies, the private sector, academia, and, most importantly, its citizens. While the national cybersecurity coordinator within the NSCS (National Security Council Secretariat) is tasked with coordinating strategic directions whenever functions overlap, lack of an explicit framework to handle inter-ministerial / agency coordination may disrupt a unified approach, cautions the researcher. Towards this end, more clarity is needed on inter-ministerial and agency coordination. Emerging threats posed by AI and quantum may require a recalibration of the existing structure, including within new agencies and functions under existing ministries. The researcher adds, tongue in cheek, that for now, India appears to have adopted the age-old idiom, "If it works, don't touch it."

4. Prakash, Rakesh avers that even as the country races ahead in its digital journey, AI has been emerging as the most dangerous weapon in the cybercriminal's arsenal (Prakash, 2025). A whopping INR 22,812 crore or USD 2.78 billion was lost to digital frauds in 2024 alone. The loss was triggered by AI frauds. The frauds were committed not only in cities like Bengaluru but also across rural India, asserts the researcher, citing a report captioned "The State of AI-Powered Cybercrime: Threat and Mitigation Report, 2025" (Report, hereafter) jointly released by GIREM (Global Initiative for Restructuring Environment and Management) and automotive tech firm Teklon. According to the Report, cybercriminals leveraged AI to craft phishing emails, clone websites and even spin up deepfake-driven scams. AI tools were involved in 80 percent of the phishing mails, implying that AI was exploited in eight out of every 10 phishing campaigns. Quoting Jay Vijayan, founder and CEO of Teklon, the researcher states that phishing scams, identity thefts and cyber slavery are no longer abstract dangers. AI has turned them into a daily reality. Recalling that organised e-crime syndicates like FIN7 have been targeting the auto industry in US, the researcher states that such syndicates now use AI to target hospitality chains and restaurants in India. This proves that the latter are vulnerable, although they boast of well-defended corporate networks. The Report suggests that a few cyber defence measures be taken: integrate digital safety and cybersecurity education in schools and workplaces; establish advanced cybercrime laboratories in universities and police departments; deploy AI-based threat detection systems across critical infrastructure; launch public awareness campaigns in local languages; strengthen international cooperation to combat cyber slavery and transnational crimes.
5. Dharshan, Shanthamurthy rues that India's digital journey has often been described as one of frugal innovation, although the country has outgrown that label (Dharshan, 2025). India's digital public infrastructure (DPI) rivals and in some cases surpasses, the systems of wealthier nations. Platforms like Aadhaar, Unified Payments Interface (UPI), and the India Stack have helped hundreds of millions access identity, financial services, and government benefits seamlessly. UPI alone accounts for 84 percent of total digital payment volumes, with transactions amounting to more than 800 percent of GDP. Additionally, India has globalized its digital innovation. Bhutan, Singapore, the UAE, and lately Qatar have adopted UPI. The International Monetary Fund calls India a leader in fast payments. India's G20 presidency positioned DPI as a global public good, proving that our innovations are also exportable as blueprints for inclusive growth. However, the achievement has its flip side too -- businesses face more than 3,000 cyberattacks per week. Since digital services span banking, health, commerce, and governance, the aftermath of the attacks can be

easily visualised. In the circumstances, the country must view cybersecurity not as a compliance checkbox but as a core pillar of national competitiveness. Resilience cannot be ensured with patchwork defences or generic global tools, cautions the researcher. Given that India's digital fabric spans dozens of languages, diverse user behaviours, and regulatory complexities, securing the digital fabric requires solutions that are deeply attuned to these realities. Without context-driven resilience, India's digital success story risks a collapse. Trust is the glue that holds digital economies together. Lose trust, and you lose adoption. Thus, the case for homegrown cybersecurity champions is no longer aspirational but existential, declares the researcher emphatically.

IV. RESEARCH GAP

The learned researchers have highlighted some of the problems the country must contend with to effectively secure its cybersecurity. To resolve the issues and ensure cybersecurity, certain measures must be taken in the short-term and the long-term. Only then the country can succeed in defending its cyberspace continuously, constantly and relentlessly, with no pauses or reduction in intensity. It is this aspect of the problem that the reviewed research has not focused adequately on, thus engendering a research gap. It is this gap the present study proposes the bridge.

V. SCOPE OF THE PRESENT STUDY

The study confines itself to two categories of respondents 50 entrepreneurs (owners of business enterprises) and 50 practising lawyers (specialising in the cyberspace domain). Both the categories are based in Bengaluru (Urban) and Bengaluru (Rural) districts.

VI. OBJECTIVE OF THE STUDY

The objective of the study is to

1. Identify the key problems India must contend with, in its cybersecurity space
2. Recommend measures the country must take to defend its cyber space

VII. HYPOTHESIS PROPOSED TO BE TESTED

The study proposes to test the following hypothesis:
"The suggested measure that the government should incentivise local players to develop tools that reckon the country's ecosystem characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances and the category the respondents belong to, are independent".

VIII. RESEARCH DESIGN

The following paragraphs furnish the research methodology.

8.1 Research methodology

The study is descriptive in nature and has used the 'fact-finding' survey method.

8.2 Sources of data

Data required for the research has been collected from both primary and secondary sources. Primary data has been collected from the 50 entrepreneurs and the 50 practising lawyers.
Secondary data has been collected / downloaded in hard version / digital version, from the various websites of the government of Karnataka (GoK), the government of India (GoI), the financial press and journals.

8.3 Sampling plan

Entrepreneurs: The researcher selected 50 entrepreneurs familiar with the issues associated with cyberspace. He used the purposive or judgement sampling technique under the non-probability method for the purpose.
Practising Lawyers: Given the limited number of lawyers practising in the cyberlaw space, the researcher used the purposive or judgement sampling technique under the non-probability method to select 50 such lawyers.

8.4 Data collection instruments

The researcher administered interview schedules to the respondents and interacted with them for collection of primary data.

8.5 Data processing and analysis plan

The researcher used manual and mechanical methods for data processing. He used the Microsoft Excel spreadsheet package for data analysis, reporting and

deployment. To collect primary data, he used a 4-point Likert scale to elicit the respondents' replies to the queries raised in the Interview Schedule. The researcher used the 4-point Likert scale to ensure that the respondents are obliged to express their views.

8.6 Limitations of the study

The researcher has deduced primary data through constant topic-oriented discussions with the respondents too. Possibly a certain degree of subjectivity has influenced the views of the researchers. However, the researcher is confident that the subjectivity, if any, will not affect the quality of the findings of the study.

IX. ANALYSIS OF PRIMARY DATA COLLECTED FROM 50 ENTREPRENEUR RESPONDENTS.

In the following paragraphs, the primary data collected from the 50 entrepreneur respondents is analysed.

9.1 Key problems India must contend with, in its cybersecurity space

Various views have been doing the rounds on the key problems India must contend with in its cybersecurity space. Hence the researcher sought to know from the respondents if they would agree with the views that are tabulated below. The respondents' agreement or otherwise with the views is expressed at four levels, namely, Strongly Agree, Agree, Disagree and Strongly Disagree. These variates are assigned the values 1, 2, 3 and 4 respectively.

Table-1. Key problems India must contend with, in its cybersecurity space

Sl No	Key problems	Strongly agree (1)	Agree (2)	Disagree (3)	Strongly disagree (4)	Total (5)
a)	Legal and policy frameworks where updates are overdue	19	24	5	2	50
b)	Poor coordination across agencies tasked with overseeing cybersecurity	13	27	7	3	50
c)	Dearth of cybersecurity talent	24	21	3	2	50
d)	Vulnerability to cyber-attacks in infrastructure of critical sectors that persist with legacy systems	13	24	9	4	50
e)	Excessive reliance on foreign hardware and software for cybersecurity infrastructure	16	23	7	4	50
f)	Strict enforcement of cyber regulations dented by jurisdictional issues which are rooted in the cross-border nature of cybercrimes	13	21	11	5	50
g)	The country's response to threats to its cybersecurity has been reactive rather than proactive, by default.	16	27	5	2	50
	Total	134	192	50	24	400

43 respondents agree that legal and policy frameworks where updates are overdue, pose a key problem. The remaining seven beg to differ. 40 respondents agree that poor coordination across agencies tasked with overseeing cybersecurity poses a key problem. The remaining 10 beg to differ. 45 respondents agree that dearth of cybersecurity talent poses a key problem. The remaining five beg to differ. 37 respondents agree that vulnerability to cyber-attacks on infrastructure in critical sectors that persist with legacy systems poses a key problem. The remaining 13 beg to differ. Excessive reliance on foreign hardware and software for cybersecurity infrastructure poses a key problem, according to 39 respondents. The remaining 11 beg to differ. Strict enforcement of cyber regulations dented by jurisdictional issues which are rooted in the cross-border nature of cybercrimes, poses a key problem, according to 34 respondents. The remaining 16 beg to differ. The country's response to threats to its cybersecurity has been reactive rather than proactive, by default and this poses a key problem, according to 43 respondents. The remaining seven beg to differ.

9.1 Measures the country must take to defend its cyberspace

Having apprised himself of the key problems the country must contend with in the cybersecurity space, the researcher sought to ascertain from the respondents the measures the country must take to defend its cyberspace. Their replies to the query are tabulated below. The replies are expressed at four levels, namely, Strongly Agree, Agree, Disagree and Strongly Disagree. These variates are assigned the values 1, 2, 3 and 4 respectively.

Table-2. Measures the country must take to defend its cyberspaces.

Sl No	Measures	Strongly agree (1)	Agree (2)	Disagree (3)	Strongly disagree (4)	Total (5)
a)	Government should proactively promote collaboration between public and private sectors to ensure cybersecurity.	16	29	3	2	50
b)	Government must ensure the clarity and effectiveness of its cybersecurity administration.	15	23	9	3	50
c)	Government must ensure that agencies at the State and Central levels coordinate with each other perfectly in the cyberspace.	17	22	7	4	50
d)	Advanced cybercrime laboratories should be established in our universities and sensitive government departments like the police department	16	28	3	3	50
e)	Government should launch public awareness campaigns in local languages	29	16	3	2	50
f)	Government should deploy AI-based threat detection systems across critical infrastructure	31	16	2	1	50
g)	Government should incentivise local players to develop tools that reckon the country's ecosystem characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances	19	20	7	4	50
	Total	143	143	34	19	350

Government should proactively promote collaboration between public and private sectors to ensure cybersecurity, assert 45 respondents. The remaining five would beg to differ. Government must ensure the clarity and effectiveness of its cybersecurity administration, assert 38 respondents. The remaining 12 respondents would beg to differ. Government must ensure that agencies at the State and Central levels coordinate with each other perfectly in the cyberspace, assert 39 respondents. The remaining 11 respondents beg to differ. Advanced cybercrime laboratories should be established in our universities and sensitive government departments like the police department, assert 44 respondents. The remaining six beg to differ. Government should launch public awareness campaigns in local languages, assert 45 respondents. The remaining five beg to differ. Government should deploy AI-based threat detection systems across critical infrastructure, assert 47 respondents. The remaining three would beg to differ. Government should incentivise local players to develop tools that reckon the country's ecosystem characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances, assert 39 respondents. The remaining 11 would beg to differ.

X. ANALYSIS OF PRIMARY DATA COLLECTED FROM THE 50 PRACTISING LAWYER RESPONDENTS

In the following paragraphs, the primary data collected from the 50 practising lawyer respondents is analysed.

10.1 Key problems India must contend with, in its cybersecurity space

Various views have been doing the rounds on the key problems India must contend with in its cybersecurity space. Hence the researcher sought to know from the respondents if they would agree with the views that are tabulated below. The respondents' agreement or otherwise with the views is expressed at four levels, namely, Strongly Agree, Agree, Disagree and Strongly Disagree. These variates are assigned the values 1, 2, 3 and 4 respectively.

Table-3. Key problems India must contend with, in its cybersecurity space

Sl No	Key problems	Strongly agree (1)	Agree (2)	Disagree (3)	Strongly disagree (4)	Total (5)
a)	Legal and policy frameworks where updates are overdue	26	20	3	1	50
b)	Poor coordination across agencies tasked with overseeing cybersecurity	23	20	5	2	50
c)	Dearth of cybersecurity talent	27	16	4	3	50
d)	Inadequate exposure of the populace and even SMEs to cyber hygiene	24	19	5	2	50
e)	Vulnerability to cyber-attacks on infrastructure in critical sectors that persist with legacy systems	15	28	5	2	50
f)	Excessive reliance on foreign hardware and software for cybersecurity infrastructure	21	25	3	1	50
g)	Strict enforcement of cyber regulations dented by jurisdictional issues which are rooted in the cross-border nature of cybercrimes	20	22	5	3	50
h)	The country's response to threats to its cybersecurity has been reactive rather than proactive, by default.	19	24	4	3	50
	Total	175	174	34	17	400

46 respondents agree that legal and policy frameworks where updates are overdue, pose a key problem. The remaining four beg to differ. 43 respondents agree that poor coordination across agencies tasked with overseeing cybersecurity poses a key problem. The remaining seven beg to differ. 43 respondents agree that dearth of cybersecurity talent poses a key problem. The remaining seven beg to differ. 43 respondents agree that inadequate exposure of the populace and even SMEs to cyber hygiene poses a problem. The remaining seven beg to differ. 43 respondents agree that vulnerability to cyber-attacks on infrastructure in critical sectors that persist with legacy systems poses a key problem. The remaining seven beg to differ. Excessive reliance on foreign hardware and software for cybersecurity infrastructure poses a key problem, according to 46 respondents. The remaining four would beg to differ. Strict enforcement of cyber regulations dented by jurisdictional issues which are rooted in the cross-border nature of cybercrimes, poses a key problem, according to 42 respondents. The remaining eight beg to differ. The country's response to threats to its cybersecurity has been reactive rather than proactive, by default and this poses a key problem, according to 43 respondents. The remaining seven beg to differ.

10.1 Measures the country must take to defend its cyberspace

Having apprised himself of the key problems the country must contend with in the cybersecurity space, the researcher sought to ascertain from the respondents the measures the country must take to defend its cyberspace. Their replies to the query are tabulated below. The replies are expressed at four levels, namely, Strongly Agree, Agree, Disagree and Strongly Disagree. These variates are assigned the values 1, 2, 3 and 4 respectively.

Table-4. Measures the country must take to defend its cyberspace.

Sl No	Measures	Strongly agree (1)	Agree (2)	Disagree (3)	Strongly disagree (4)	Total (5)
a)	Government should proactively promote collaboration between public and private sectors to ensure cybersecurity.	19	22	3	6	50
b)	Government must ensure the clarity and effectiveness of its cybersecurity administration.	13	29	5	3	50
c)	Government must ensure that agencies at the State and Central levels coordinate with each other perfectly in the cyberspace.	19	25	3	3	50
d)	Advanced cybercrime laboratories should be established in our universities and sensitive government departments like the police department	20	27	2	1	50
e)	Government should launch public awareness campaigns in local languages	19	24	4	3	50
f)	Government should deploy AI-based threat detection systems across critical infrastructure	27	17	3	3	50
g)	Government should incentivise local players to develop tools that reckon the country's ecosystem characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances	26	21	2	1	50
	Total	143	165	22	20	350

Government should proactively promote collaboration between public and private sectors to ensure cybersecurity, assert 45 respondents. The remaining five would beg to differ. Government must ensure the clarity and effectiveness of its cybersecurity administration, assert 38 respondents. The remaining 12 respondents would beg to differ. Government must ensure that agencies at the State and Central levels coordinate with each other perfectly in the cyberspace, assert 39 respondents. The remaining 11 respondents beg to differ. Advanced cybercrime laboratories should be established in our universities and sensitive government departments like the police department, assert 44 respondents. The remaining six beg to differ. Government should launch public awareness campaigns in local languages, assert 45 respondents. The remaining five beg to differ. Government should deploy AI-based threat detection systems across critical infrastructure, assert 47 respondents. The remaining three would beg to differ.

XI. CONCLUSIONS

Conclusions are inferences / generalisations drawn from the findings and relate to hypotheses. They are answers to the research questions or the statements of acceptance or rejection of hypotheses. As explained already, this study proposes to test the following hypothesis.

11.1 Testing of hypothesis

"The suggested measure that the government should incentivise local players to develop tools that reckon the country's ecosystem characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances and the category the respondents belong to, are independent".

Hence, H_o and H_a are as follows:

H_o: The suggested measure that the government should incentivise local players to develop tools that reckon the country's ecosystem characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances and the category the respondents belong to, are independent

H_a: The suggested measure that the government should incentivise local players to develop tools that reckon the country's ecosystem characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances and the category the respondents belong to, are not independent

Based on the primary data collected from the respondents, vide Tables: 2 and 4, the researcher applied a chi-square test to ascertain the association, if any, between the variables. The following Table reveals the computation made using MS-Excel:

		Observed Values		
	Category	Agree	Disagree	Total
	Entrepreneurs	39	11	50
	Practising lawyers	47	3	50
	Total	86	14	100
		Expected Values		
	Category	Yes	No	Total
	Entrepreneurs	43	7	50
	Practising lawyers	43	7	50
	Total	86	14	100
		Yes	No	
	o-e	-4.0000	4.0000	
2		4.0000	-4.0000	
	(o-e)^2	16.0000	16.0000	
		16.0000	16.0000	
	((o-e)^2)/e	0.3721	2.2857	
		0.3721	2.2857	
	CV	0.7442	4.5714	5.3156
	TV			3.8415
	p			0.0211

The calculated value of χ^2 is 5.3156, greater than the table value of 3.8415 for an alpha of 0.05 at one degree of freedom. p=0.0211<0.05, the alpha level. Hence H_0 is rejected.

XII. RECOMMENDATIONS

The following are the researcher's recommendations in the light of the findings arrived at:

1. It is true that the country's legal and policy frameworks are not updated promptly and this could compromise cybersecurity. For example, in November 2025, the government notified Digital Personal Data Protection Rules, 2025, although the Digital Personal Data Protection Bill received parliament's nod in 2023!
2. Advanced cybercrime laboratories should be established in our universities and in sensitive government departments. This will eventually lead the country to minimise reliance on foreign hardware and software, for its cybersecurity infrastructure.
3. Government should launch public awareness campaigns in local languages too, given the country's linguistic diversity.
4. Additionally, given the demographic diversity of the country, the government should incentivise local players to develop tools that reckon the country's ecosystem, which is characterised by linguistic diversity, informal economy, poor connectivity, regulatory frameworks, and cultural nuances.
5. It is unfortunate that even SMEs do not have adequate exposure to cyber hygiene. Industry bodies / trade associations should prevail on the SMEs to adhere to cyber hygiene. The latter should be adequately trained in the art and science of handling cyber threats.
6. The country's approach to cybersecurity should be proactive and not reactive, by default. It amounts to closing the stable door after the horse has bolted. By default, the approach should be proactive, given that the reactive approach could cost the country, its industry and other stakeholders, in more ways than one.

7. Much as one may dislike it, the private sector is always ahead of the public sector in addressing cybersecurity issues. However, the public sector can access certain privileges which the private sector cannot, for various reasons. In the circumstances, it will be ideal if the two sides join hands to address the issues concerning cybersecurity, given that such an association will lead to a win-win situation for both the sides.
8. Government should deploy AI-based threat detection systems across critical infrastructure, given that it is better placed to do it than the private sector.

REFERENCES

[1] Abhiraj. (2025, 17 August). Home: Cybersecurity Challenges in Businesses. Retrieved from Craw Academy Web site: https://www.craw.in/cybersecurity-challenges-in-businesses?srsltid=AfmBOoqalKo-K9KVvck0WtXXp17cIPF6unakiozKsOy7hgpH7Sza2qOu

[2] Ashok, K. T. (2025, February 26). News: Express Computer. Retrieved from Express Computer Web site: https://www.expresscomputer.in/guest-blogs/indias-cybersecurity-challenges-rising-threats-in-a-rapidly-digitalizing-nation/122160/

[3] Dharshan, S. (2025, October 5). ET Edge Insights: Cyber Security. Retrieved from ET Edge Insights Web site: https://etedge-insights.com/technology/cyber-security/atmanirbhar-in-cyberspace-building-indias-own-security-champions/#:~:text=India's%20cybersecurity%20budget%20must%20reflect,failure%20is%20not%20an%20option.

[4] Prakash, R. (2025, June 25). Trending: Times of India. Retrieved from Times of India Web site: https://timesofindia.indiatimes.com/city/bengaluru/ai-driven-cybercrime-threatens-indias-digital-future-rs-23000-crore-lost-in-2024/articleshow/122066377.cms

[5] Tejas, B. (2025, September 1). Home: Carnegie India. Retrieved from Carnegie India Web site: https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025?lang=en