

SAFEGUARDING INDIA'S FUTURE: A COMPARATIVE STUDY OF
CYBERSECURITY EDUCATION AT THE HIGH SCHOOL LEVEL,
ANALYZING INTERNATIONAL PRACTICES

by

Abhijit Das

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

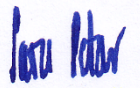
May, 2026

SAFEGUARDING INDIA'S FUTURE: A COMPARATIVE STUDY OF
CYBERSECURITY EDUCATION AT THE HIGH SCHOOL LEVEL,
ANALYZING INTERNATIONAL PRACTICES

by

Abhijit Das

APPROVED BY



Prof.dr.sc. Saša Petar, Ph.D., Dissertation chair

RECEIVED/APPROVED BY:



Admissions Director

ABSTRACT

SAFEGUARDING INDIA’S FUTURE: A COMPARATIVE STUDY OF
CYBERSECURITY EDUCATION AT THE HIGH SCHOOL LEVEL,
ANALYZING INTERNATIONAL PRACTICES

Abhijit Das
2026

The need for faster communication and enhanced connectivity has driven the evolution of the information technology industry. Internet-enabled devices support a wide range of functions from video conferencing and social media to smart home automation and real-time monitoring through the “Internet of Things” (IoT). However, this convenience comes with increased vulnerability to privacy breaches, identity theft, financial fraud, data misuse, and cyberattacks. Educational institutions, particularly schools, have become frequent target to cyber threats, with sensitive data being exploited on the dark web. Despite the growing concern, many educators lack the awareness and resources to teach cybersecurity effectively, and institutional support remains limited.

This study investigates cybersecurity education in Indian high schools by comparing global practices, evaluating teaching approaches, curriculum design, and

analyzing stakeholder awareness. Using a mixed-method approach, the study integrates literature review and empirical data from 198 students, 126 parents and 121 educationalists. Data collected through structured surveys were analyzed to understand variations in awareness, engagement, and digital safety practices across stakeholder groups.

Research suggests that international programs emphasize early awareness, collaborative parent-teacher engagement, and foundational cyber-safety skills. Common recommendations include gamified and practical learning, virtual labs, and progressive curricula that build both ethical and technical competence. Cybersecurity education in India, however, remains largely theoretical, often embedded within basic computer literacy, resulting in limited practical exposure and inconsistent learning outcomes. Stakeholder analysis reveals moderate awareness among students, parents, and educators. Parental involvement is primarily supervisory, and educationalists have access to technical knowledge but limited pedagogical application. Online practices among students was significant with regard to safety in behaviors alongside parental involvement and lapses were observed in the more complex areas such as password handling and phishing awareness.

The study concludes that improving cybersecurity education in India needs a multi-tiered strategy: a structured curricula integrating technical and ethical skills; comprehensive teacher training; active parental participation; and coordinated government-industry participation. Adapting global best practices to the Indian context can foster digital safety and critical thinking. equipping students with skills needed to navigate online world safely and contribute to building a future-ready cybersecurity workforce.

Keywords: Cybersecurity, Digital Literacy, Digital Safety in Schools, India Cybersecurity Landscape, Cyber Awareness, Cyber Workforce Development.

TABLE OF CONTENTS

List of Tables	vii
List of Figures	ix
List of Abbreviations	xii
CHAPTER I: INTRODUCTION.....	1
1.1 Introduction.....	1
1.2 Research Problem	24
1.3 Purpose of Research.....	27
1.4 Significance of the Study	28
1.5 Research Purpose and Questions	29
CHAPTER II: REVIEW OF LITERATURE	32
2.1 Theoretical Framework.....	33
2.2 The Space Transition Theory.....	33
2.3 Self-Determination and Social Cognitive Theory.....	37
2.4 Introduction to Global Insights on Cybersecurity Education	40
2.5 The growing importance of Cybersecurity in the digital era	42
2.6 Role of education in building cyber awareness and resilience	44
2.7 From Growing Threats to Growing Talent: Aligning Education with Cybersecurity Needs.....	48
2.8 Global Practices in Cybersecurity Education and Training.....	52
2.9 Comparative Insights: India vs. International Approaches.....	54
2.10 Current landscape of Cyber Safety in Schools	57
2.11 Cybersecurity Governance Frameworks in Education	64
2.12 Best Practices for Cyber Safety Curriculum Design.....	67
2.13 Summary	73
CHAPTER III: METHODOLOGY	75
3.1 Overview of the Research Problem	75
3.2 Operationalization of Theoretical Constructs	76
3.3 Research Purpose and Questions	77
3.4 Research Design.....	78
3.5 Population and Sample	79
3.6 Participant Selection	81
3.7 Instrumentation	82
3.8 Data Collection Procedures.....	85
3.9 Data Analysis	87
3.10 Research Design Limitations	89
3.11 Conclusion	90

CHAPTER IV: RESULTS.....	91
4.1 Research Question One.....	91
4.2 Research Question Two	96
4.3 Research Question Three	102
4.4 Research Question Four	107
4.5 Summary of Findings.....	186
4.6 Conclusion	188
CHAPTER V: DISCUSSION.....	189
5.1 Discussion of Results	189
5.2 Discussion of Research Question One	191
5.3 Discussion of Research Question Two	193
5.4 Discussion of Research Question Three	196
5.5 Discussion of Research Question Four	198
CHAPTER VI: SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS.....	202
6.1 Summary	202
6.2 Research contributions of the study	203
6.3 Implications.....	206
6.4 Recommendations for Future Research	207
6.5 Conclusion	208
REFERENCES	211
APPENDIX A: DATASET.....	243

LIST OF TABLES

Table 3.1: Sample Size Distribution	81
Table 3.2: Reliability Analysis (Cronbach's Alpha) for All Respondent Groups	84
Table 3.3: Process of Selecting Past Studies	86
Table 4.1: Strength Analysis of Cybersecurity Education.....	92
Table 4.2: Weakness Analysis of Cybersecurity Education	94
Table 4.3: Comparison and Summary of Cybersecurity Curriculum Approaches	96
Table 4.4: Summary of Different Countries' Teaching Methodologies, Learning Resources, Curriculum Design, and Teacher Development with Recommendations for India.....	98
Table 4.5: Analysis of Government Approaches to Cybersecurity Education in Indian High Schools Compared with Global Practices.....	103
Table 4.6: Demographic Details of Students	107
Table 4.7: How often do you use the internet for schoolwork or personal purposes?.....	113
Table 4.8: Devices Most Frequently Used to Access the Internet.....	114
Table 4.9: Primary Online Activities of Respondents	115
Table 4.10: How well do you understand the term Cybersecurity?.....	116
Table 4.11: Awareness Levels of Respondents on Different Cybersecurity Practices	117
Table 4.12: Have you ever received any formal training/workshops on cybersecurity?	122
Table 4.13: Would your awareness improve if Information and Communication Technologies (ICT) concepts were taught in the local language in addition to English?.....	123
Table 4.14: Usage of Online Techs.....	125
Table 4.15: Descriptive Statistics of the Students' Survey.....	130
Table 4.16: Demographic Details of Parents	132
Table 4.17: How aware are you of your child's online activities?	136
Table 4.18: How often do you talk to your child about online safety and responsible internet use?	138
Table 4.19: Have you ever received formal training/workshops on cybersecurity?.....	139
Table 4.20: Confidence Levels of Parents in Managing Cybersecurity Practices	140

Table 4.21: How often do you use the same passwords across websites/apps?	149
Table 4.22: How often do you use free public Wi-Fi for payments or banking?	150
Table 4.23: Would you like schools to organize workshops on cybersecurity for parents?	151
Table 4.24: Descriptive Statistics of Parents' Survey.....	155
Table 4.25: Demographic Profile of Teacher/School Administrator.....	157
Table 4.26: To what extent do you include cybersecurity topics in your curriculum/discussions?	163
Table 4.27: Have you ever received training/workshops on cybersecurity?	164
Table 4.28: How often would you like to receive cybersecurity training?	165
Table 4.29: To what extent are limited resources (funding, staff, technology, infrastructure) a barrier to implementing cyber-awareness programs in schools?	166
Table 4.30: Have you installed a firewall/antivirus in school systems?	168
Table 4.31: Familiarity Levels of Teachers with Cybersecurity Concepts.....	169
Table 4.32: Descriptive Statistics of the Teachers' Survey	179
Table 4.33: ANOVA Test Statistics.....	181
Table 4.34: Spearman's Rho Correlations of Cybersecurity Practices, Parental Awareness, and Training	184

LIST OF FIGURES

Figure 2.1: Space Transition Model derived from (Karupppannan, 2008) by (Danquah and Longe, 2011)	36
Figure 2.2: Initial and Emerging factors. Source (Harris et al., 2021)	39
Figure 4.1: Gender	112
Figure 4.2: Age-Group.....	113
Figure 4.3: How often do you use the internet for schoolwork or personal purposes	114
Figure 4.4: Which devices do you use most often to access the internet?	115
Figure 4.5: What are your main purposes of using digital devices?	116
Figure 4.6: How well do you understand the term Cybersecurity?	117
Figure 4.7: Phishing Email	118
Figure 4.8: Strong Password Practices.....	119
Figure 4.9: Safe social media behavior	120
Figure 4.10: Cyberbullying.....	121
Figure 4.11: Reporting suspicious activity	122
Figure 4.12: Have you ever received any formal training/workshops on Cybersecurity?	123
Figure 4.13: Would your awareness improve if Information and Communication Technologies (ICT) concepts were taught in the local language in addition to English	124
Figure 4.14: Use the same passwords across multiple websites/apps	125
Figure 4.15: Use free public Wi-Fi for online payments or banking.....	126
Figure 4.16: Share your location on social media.....	127
Figure 4.17: Perceived Risky Online Activities Among Students.....	128
Figure 4.18: Suggestions About Improving Cybersecurity Awareness in Schools	129
Figure 4.19: Gender	135
Figure 4.20: Age Group	136
Figure 4.21: How aware are you of your child's online activities	137
Figure 4.22: How often do you talk to your child about online safety and responsible internet use.....	138
Figure 4.23: Have you ever received formal training/workshops on cybersecurity?	139

Figure 4.24: Talking to children about cyber risks	141
Figure 4.25: Monitoring screen time	142
Figure 4.26: Identifying online threats.....	143
Figure 4.27: Creating strong passwords.....	144
Figure 4.28: Reporting suspicious activity	145
Figure 4.29: Using parental controls on digital devices	146
Figure 4.30: Promoting safe social media behavior.....	146
Figure 4.31: Protecting personal data	147
Figure 4.32: Recognizing phishing emails.....	148
Figure 4.33: Knowing your child's online friends	148
Figure 4.34: How often do you use the same passwords across websites/apps?	149
Figure 4.35: How often do you use free public Wi-Fi for payments or banking?	151
Figure 4.36: Would you like schools to organize workshops on cybersecurity for parents	152
Figure 4.37: Biggest Concern About Child's Online Presence According to Parents	153
Figure 4.38: Suggestions about improving cybersecurity awareness in schools	154
Figure 4.39: Gender	162
Figure 4.40 Age Group	163
Figure 4.41: To what extent do you include cybersecurity topics in your curriculum/discussions.....	164
Figure 4.42: Have you ever received training/workshops on cybersecurity?	165
Figure 4.43: How often would you like to receive cybersecurity training?.....	166
Figure 4.44: To what extent are limited resources (funding, staff, technology, infrastructure) a barrier to implementing cyber-awareness programs in schools?	167
Figure 4.45: Have you installed firewall / antivirus in school systems?	168
Figure 4.46: Safe social media behavior.....	170
Figure 4.47: Understanding data privacy laws	171
Figure 4.48: Identifying online threats.....	171
Figure 4.49: Student data protection	172
Figure 4.50: Talking to Students about cyber risks	173
Figure 4.51: Software / Hardware / Network Security	174

Figure 4.52: Reporting suspicious activity	174
Figure 4.53: Strong password practices	175
Figure 4.54: Cyber hygiene practices	176
Figure 4.55: Recognizing phishing emails.....	176
Figure 4.56: Administrator Support for Effective Cybersecurity Teaching	177
Figure 4.57: Suggestions about improving Cybersecurity awareness in schools	178
Figure 6.1: Holistic Cybersecurity Education Framework for High School Curriculum	205

LIST OF ABBREVIATIONS

Abbreviations	Full Form
ACM	Association for Computing Machinery
AI	Artificial Intelligence
ANOVA	Analysis of Variance
APTs	Advanced Persistent Threats
AWS	Amazon Web Services
BYOD	Bring Your Own Device
CBM	Capacity Building Model
CEAT	Cybersecurity Education, Awareness Raising, And Training
CERT-In	Indian Computer Emergency Response Team
CS	Cybersecurity
CSA	Cyber Security Agency, Singapore
CTF	Capture-the-Flag
EU	European Union
GII	Global Innovation Index
HEIs	Higher Education Institutions
ICT	Information and Communication Technology
IoT	Internet of Things
IPHS	Indian Public Health Standards
ML	Machine Learning
MOOC	Massive Open Online Course
NCHPC	National Critical Information Infrastructure Protection Centre
NCSP	National Cyber Security Policy

NEP	New Education Policy
SCT	Social Cognitive Theory
SDT	Self-Determination Theory
SPSS	Statistical Package for Social Sciences
STT	Space Transition Theory
STEM	Science, Technology, Engineering and Mathematics
WEF	World Economic Forum

Source: Compiled by author.

CHAPTER I: INTRODUCTION

1.1 Introduction

The development of computers and the subsequent rise of internet has had a transformative impact on the modern society, influencing virtually every aspect of life. In the 21st century, where each and every person across the globe has one or the other way of connecting to the digital world by means of mobiles, tablets, personal computers, laptops etc. find the internet revolution an indispensable asset. Social networking, online shopping, storing data, gaming, online studies, and online jobs; every possible thing one can imagine can be done through the medium of internet (Dar and Lone, 2020).

With the innumerable advantages that internet and its inter-connected devices do provide, there is a dark side of it that an uninformed or less informed entity such as corporations, government run facilities, or an individual may fall prey to. In the pre-internet era crimes were confined to physical space; with the growing usage of internet these crimes have transitioned to cyberspace. Traditional mail, once sent through post offices have largely been replaced by emails and text messages, leading to the rise of phishing and job scams. Similarly, acts of terrorism and related crimes have evolved into cyber-terrorism, exploiting the digital landscape to carry out malicious activities (Ige, 2020). This shift underscores the need for robust cybersecurity measures and greater awareness among internet users to mitigate the risks associated with digital crimes.

Most of the data in cyberspace is made publicly accessible and this openness promotes knowledge sharing, collaboration, and fostering innovation in various domains. However, some data are deemed confidential by individuals or organizations due to the sensitive nature of its content, such as nation's defense capabilities, ground-breaking health care research, and an organization's IT infrastructure. An individual's personal details,

including bank information, medical records, passport, and driving license details (commonly referred to as Personally Identifiable Information or PII), must remain confidential (Zote *et al.*, 2023; Verizon, 2022; Rahman *et al.*, 2020). Unintentional exposure or disclosure of such critical information may result in regulatory fines, reputational harm, revenue loss, and a decline in customer trust (Yashwant, 2021; Cheung *et al.*, 2011). Sensitive data must be safeguarded to maintain privacy and security, balancing the benefits of open access with the need for confidentiality.

In cyberspace, there are malicious elements that attempt to access digital devices to steal or lock confidential information (Manzil and Manohar Naik, 2023; Rattanabunno *et al.*, 2023; Amankwa, 2021). These cybercriminals, often called hackers may operate alone or in groups, and at times state-sponsored, aiming to sell data on the dark web, extort money, or disrupt opponent nations' systems for espionage, propaganda, or economic destabilization (AICTE, n.d.; Alam, 2022; Saxena and Mittal, 2022).

Cyberattacks are ranked among the top 5 global threats by the World Economic Forum (WEF) (World Economic Forum - GRR, 2024), emphasizing the importance of implementing strong cybersecurity measures. The WEF report (World Economic Forum - GCO, 2024) mentions that "The rapid spread of generative AI and other new technologies that can easily be used by cyber-attackers poses a serious threat both for business and in public life." The economic impact of these cyberthreats extends beyond immediate financial losses, affecting everything from small businesses to large corporations and even national economies (Francis *et al.*, 2024; Eling *et al.*, 2023).

India is now the world's most populous country (World Population Review, 2025) and is the second among the number of smart phone users (Statista, 2024), however there still exists serious lack of information security knowledge among the everyday citizens, posing a challenge for effective cyber hygiene and digital risk remediation. While the

country is making digital progress by leaps and bound, the lack of awareness of the dangers lurking in the world wide web (WWW) is often taken for granted (Business World, 2022). The COVID-19 pandemic has greatly accelerated digital transformation. Post-pandemic, there has been a significant increase in digital device usage for online education, remote work, adoption of digital business models by numerous firms, and a substantial rise in digital and online banking transactions (OECD, 2020).

Cybersecurity has increasingly become headline feature in news and print media owing to breach incidents and scams reported for financial institutions, telecoms, healthcare organizations, airlines and academic establishments. IT companies often offer basic information security programs for employees, while universities provide courses on cybersecurity for students enrolling specifically into IT disciplines. However, high school students lack awareness of information security, taking digital devices for granted and risking exposure to online threats like bullying, pornography, gambling, malware, stranger dangers, privacy violations, and phishing, which can compromise their confidential information. Thus, the need to focus on design and grass root level implementation of cybersecurity educational content for children is more pressing than ever.

According to (MassMediaLink India LLP SecurityLink India, 2024), the cybersecurity workforce gap requires an estimated 4 million professionals. Fortinet's 2024 Global Cybersecurity Skills Gap Report revealed that 80% of Indian organizations believe this skills shortage heightens their risks. This signifies the need for skilled cybersecurity professionals to reduce the complexities of modern-day cyber threats and safeguard digital boundaries. Other studies have also highlighted gender disparity (Merayo and Ayuso, 2023; AlDaajeh *et al.*, 2022) in cybersecurity workforce. According to (Kant, 2023; Kim, 2013), heavy users of digital devices are typically the ones who are least educated and lack cybersecurity awareness. Compounding to this issue is the existing gaps in cybersecurity

education, that fails to keep pace with rapidly evolving nature of cyber-threats and the disconnect between the skills taught in academic institutions and the competencies demanded by industry.

(Hyseni, 2024) highlights the critical role of cybersecurity awareness, defining it as the comprehension of digital threats, risks, and vulnerabilities, alongside the competencies required to safeguard individuals and organizations. This study underscores the value of implementing cybersecurity education at the high school level as a strategic measure to mitigate human error that is identified as one of the most prevalent contributors to security breaches in industry settings. Enhancing individuals' capacity to recognize and respond effectively to cyber threats will not only strengthen organizational resilience but also foster operational efficiency. Furthermore, cultivating interest in cybersecurity from an early age may encourage students to pursue advanced studies in the field, thereby enriching the community of practice and contributing to the reduction of the global cybersecurity workforce gap.

Cybersecurity education cannot be ignored in today's rapidly evolving digital landscape, with risks threatening safety of individuals, organizations, and society. High school students are particularly vulnerable due to their active digital presence and limited threat awareness. While countries like the US, UK, Singapore, and Australia offer structured cybersecurity education, including technical knowledge, ethical consciousness, and responsible behavior; India is still in its infancy phase of standardizing curricula and formulating policies for school students. India's growing dependence on digital platforms in academic, social, and personal lives underscores the urgent need to strengthen cybersecurity education especially among school students to ensure basic cyber hygiene.

As noted by (Kesavardhanan, 2022; Pal, 2022; PHDCCI and Grant Thornton Bharat, 2022; Yashwant, 2021), school curriculum in India lacks proper framework for

imparting cybersecurity education. To bridge this essential gap, this research undertakes a comprehensive comparison of international high-school cybersecurity curricula, identifying key insights that can be adopted to the Indian context. The study also looks into best practices from global government policies and industry partnerships on cybersecurity awareness that can be adopted and customized to facilitate successful learning among students, academicians and parents in India. The research provides recommendations that can be implemented by policymakers, educators, and school administrators as a way of encouraging a culture of cybersecurity awareness and digital resilience. The study ultimately seeks to safeguard India's digital future by proposing ways to foster technical competence, informed decision-making, and ethical digital behavior among high school students.

International Models Shaping Cybersecurity Education

Driven by the rapid integration of digital technologies across education, finance, healthcare industry, and governance, numerous countries have institutionalized cybersecurity instruction at school level to prepare students for the challenges of a digitally interconnected world. With the rising number of internet enabled devices among students to access social media platforms, online education, and other digital services; learners face a plethora of cyber threats, such as data breaches, identity theft, phishing attacks, and ransomware threats (Arishi *et al.*, 2024). The perception of these threats has caused several countries, including the US, UK, Singapore, and Australia to build extensive programs to equip youngsters with the knowledge and abilities they need to safely navigate the digital world. The goals of these programs extend beyond only improving students' knowledge of computer science; they also seek to prepare them for life after high school by teaching them to think critically, solve problems, and act ethically when using technology.

The current landscape of cybersecurity education in high schools globally mirrors a mix of progressive initiatives and pressing concerns. There are nations that have succeeded in introducing integrated curricula including courses in cybersecurity, practical laboratories, simulation activities, and certifications aligned to industry standards (Sağlam *et al.*, 2023). For instance, Singapore adopts real-life cyber defense exercises and project-based learning. US, on the other hand, concentrates on certifications and competitions as the motivation for the students. However, challenges such as the shortage of qualified educators, and disparities in technological access and curriculum implementation transcend national development status, affecting both emerging and developed education systems alike. By analyzing global experiences, India can derive actionable insights to tailor cybersecurity curricula, teaching methods, and policies to its educational context. As suggested by (Grimus, 2020), adopting insights from global successes will help shape content-rich, and effective cybersecurity education model tailored to local needs.

Children are engaging with digital technology at increasingly younger ages, prompting experts to advocate for early education in digital literacy and cybersecurity (Johnson *et al.*, 2023; Johnson *et al.*, 2022). Yet, significant barriers remain. Overloaded K-12 curricula leave little room for dedicated cybersecurity instruction, and restrictive policies further limit course development. With only a few computer classes per week, students lack sufficient exposure to these critical concepts (Johnson *et al.*, 2022). Compounding the issue, cybersecurity itself is rapidly evolving, making static curricula ineffective and outdated.

High profile cyber-attacks targeting airlines, healthcare industry, credit bureaus, government organizations, banks, and telecom companies have brought cybersecurity into sharp media focus in recent years (European Commission, 2017). As a result, multiple researches agree towards cybersecurity awareness as a crucial element to society's long-

term progress. To accomplish a task effectively while interacting with digital resources and services, one must possess a set of skills that encompass not only technical know-how but also the practical experience and education necessary for such work (Caulkins *et al.*, 2018). If a nation's workforce isn't prepared to mitigate the rising number of cybercrimes, its ability to adapt to a digital age will suffer. As emphasized by (Blažič, 2022), the digital economy will decide the winners and losers. It will be the key determinant of global competitiveness, making cybersecurity skills increasingly vital for future success.

In Summary, global high school cybersecurity education programs showcase a diverse range of innovative strategies designed to equip students with both theoretical understanding and practical expertise; and are often supported by government policies (Mukherjee *et al.*, 2024). However, even well-established programs face common challenges like unequal access to technology, teacher shortages, outdated curricula in the face of evolving threats, and at times, there is overemphasis on technical skills at the expense of socio-ethical knowledge. For India, these global experiences offer valuable insights; highlighting both effective practices and common pitfalls. By integrating scalable pedagogy, experiential learning, and informed policy support, India can build a robust high school cybersecurity education model that secures its digital future and cultivate cyber-aware, future ready, and skilled workforce motivated to pursue advanced studies in cybersecurity (Padmaja *et al.*, 2019).

International Cybersecurity Education Models: Successes and Shortcomings

The international high school cybersecurity education programs can serve as a vital yardstick for India, offering benchmarks and insights to guide the development of its own educational framework. Many developed economies, like US, UK, Singapore, and Australia, have enacted structured programs that integrate theoretical learning, laboratory work, interactive exercises, and cybersecurity contests (Mohanty *et al.*, 2024). In US,

programs such as Cyber Patriot offer students capture-the-flag competitions and real-world network defense exercises that allow them to gain skills in critical problem-solving and practical technical knowledge. Similarly, Cyber First and Cyber Discovery programmes in UK provide specific courses to students and initiatives aimed at increasing cybersecurity access for marginalized communities, particularly young women (Švábenský *et al.*, 2021). The Cyber Security Agency (CSA) Education program in Singapore involves virtual laboratories, internet-based learning programs, and industry mentoring to provide comprehensive picture of cyber threats and cyber hygiene. These international cybersecurity awareness programs can be adapted by India and transformed into local policies that set clear competencies, learning goals, and assessment standards; ensuring a consistent and structured approach across the education system. By drawing insights from these proven models, India can position itself to identify effective strategies that boost students' technical skills, digital literacy, and interest in higher education or careers in cybersecurity (Afzal *et al.*, 2023).

Global cybersecurity education programs offer a powerful blueprint; but they also reveal certain challenges that India should consider when developing its own cybersecurity education programs (Rahman *et al.*, 2020). One big problem is that not all schools have equal access to the tools and resources needed for learning, especially in rural or low-income regions; and this can create a big difference in students learning experience. Another key challenge is the shortage of qualified teachers who combine technical expertise with effective teaching skills. Additionally, cybersecurity curricula often lag behind, as evolving threats quickly render existing content outdated, leaving students ill-prepared on dangers lurking in the digital world. Some programs focus too much on technical skills but miss out on important lessons about ethics, laws, and social responsibilities in the digital world, like privacy, being a good digital citizen, and behaving

responsibly online (Dudley *et al.*, 2024). Recognizing these challenges will enable policy makers and educators create a system that mixes practical learning, clear standards for what students should know, and involve students, teachers, and parents in course curriculum design. India can draw lessons from success stories and shortcomings of global models and develop a robust, equitable, and future-ready cybersecurity curricula.

In today's global landscape, economies are increasingly driven by knowledge. As noted by (Deshpande, 2023), knowledge is produced nationally but shared globally fostering international collaboration and innovation. Universities worldwide are competing to attract students and train a workforce equipped for global challenges. By 2050, China and India are expected to contribute over 30% of the world's employment (Minocha *et al.*, 2018), underscoring their pivotal role in shaping the future workforce. In this light, the India's National Education Policy (NEP) 2020 marks a significant step towards preparing graduates who are not only future ready but also globally aware. The key objective of NEP is to make internationalization of education a priority. Bringing a global, intercultural, or international perspective to higher education's goals, practices, and operations is what's known as "internationalization of education" (Deaconu *et al.*, 2020). By encouraging the sharing of successful pedagogical and research methods across different educational systems around the world, internationalization of education seeks to raise the bar for educational excellence (Xu, 2024). Internationalization of education in essence is learning abroad and integrating global perspectives at home, fostering individuals with the skills, knowledge, and values needed to thrive in a globalized society. India by adopting internationalization of education like cross-border collaboration, adopting best practices, and investing in cybersecurity education can, not only strengthen its digital infrastructure but also emerge as a leading producer of skilled professionals for global stage.

In conclusion, India's cybersecurity education initiatives have a lot to learn from globally recognized programs. These programs have a distinctive edge, such as hands-on learning through real-life situations, well-planned, skill-based courses, strong government support, working with industry experts, and ways to incorporate all students (Mohanty *et al.*, 2024). Also to note that, these programs also have some inherent limitations, like not everyone having the same access to technology and resources, not having enough skilled teachers, course needs that change quickly, and not paying enough attention to ethical, legal, and social issues. By learning from these mistakes, Federal and state bodies and educational institutions can create a thoughtfully designed and inclusive system that can resolve challenges like uneven access, better teacher training, and inclusion of essential non-technical skills like digital ethics, privacy awareness, and responsible online behavior.

Teaching Cybersecurity: What Works in the Classroom

The way high school cybersecurity classes are planned and taught is really important for helping students learn technical skills, how to solve problems, and understand the digital world better. Good programs mix learning from textbooks with real-life activities, so students can use what they learn in situations like setting up secure networks, doing safe hacking practices in a controlled environment, and participating in competitions where they try to find and fix security issues (Ismail *et al.*, 2024). For example, in the US, the Cyber Patriot program uses both classroom lessons and competitions to help students learn about cybersecurity. In Singapore, the CSA has programs that use virtual labs and real-life situations to show students how cyber threats work. In the UK, Cyber First offers lessons on things like keeping data safe, securing networks, and online safety, along with projects that make students think and solve problems. These programs focus on clear goals, ways to measure students' progress, and methods to check how well students are learning.

Teaching methods are critical to the effectiveness of cybersecurity education, and they often decide how well pupils can understand difficult ideas. Countries with successful programs use blended learning methods that mix traditional classroom teaching with online modules, virtual labs, project-based learning, and peer collaboration to keep students interested and help them remember what they've learnt(Yadav, 2024). Gamification, problem-solving exercises, hackathons, and mentorship from industry professionals are all examples of interactive methods that help students improve their critical thinking, creativity, and ability to apply cybersecurity ideas in the real world (Asrifan *et al.*, 2025). Also, good teaching requires skilled teachers who are good at both technical and pedagogical abilities. International programs stress the need for teachers to continuously learn new things and getting exposure to the industry so they can stay up to date on new threats and technologies. India can use these international best practices to help create a high school cybersecurity curriculum that balances theoretical knowledge, hands-on practice, ethical awareness, and flexible teaching methods. This will empower students to become skilled, responsible, and digitally aware; ensuring competence to navigating the complexities of an evolving cyber landscape.

However, there is a lack of research comparing and analyzing cybersecurity curriculum design techniques. This paper provides a comprehensive analysis of current cybersecurity education curriculum design methodologies, including a critique and comparison of these methods. As highlighted by (Mouheb *et al.*, 2019), the goal is to gather insights that can contribute towards the development of a stronger cybersecurity curriculum.

To build a digitally literate workforce, governments globally are investing heavily in K-12 cybersecurity education. Yet, teachers face major hurdles especially in reaching out to marginalized students due to outdated teaching methods and a lack of age-

appropriate cybersecurity content. Bridging this gap is key to creating inclusive, future-proof digital education According to (Nieto *et al.*, 2025) in the context of China, majority of educators do not possess the knowledge or competence required to adequately instruct students in the field of cybersecurity. Teachers do not have enough opportunities for professional development and training to acquire research-based instructional strategies for teaching cybersecurity to students in grades K-12. Expanding early cybersecurity education can boost students' interest and enrolment in related university programs. This will assist universities fulfil the demand for cybersecurity experts (Nygard *et al.*, 2018).

In recent years, there has been a significant rise in the number and sophistication of cyberattacks targeting governments, organizations, and individuals. With the proliferation of mobile devices, the Internet of Things (IoT), and the so-called "Bring Your Own Device" (BYOD) trends, new cybersecurity threats have emerged and opened up opportunities for cybercriminals to attack vulnerabilities in these systems (Kaur *et al.*, 2023). The shortage of qualified cyber professionals makes matters worse in light of the ever-changing nature of threats. The availability of qualified cybersecurity experts is a persistent problem for businesses and other organizations (Yaacob *et al.*, 2023). This risks having critical data stolen, money lost, and reputation tarnished. The urgency around cybersecurity is rapidly intensifying, and there is a severe shortage of qualified candidates due to the complexity, velocity, and scope of cyberattacks (Li and Liu, 2021)

Bringing it all together, a well-designed cybersecurity curriculum paired with effective teaching methods is the key to building digital resilience in schools. Current research offers diverse approaches, but their impact hinges on thoughtful implementation within the classroom environment. International programs show that combining structured theoretical instruction with hands-on, experiential learning like virtual labs, simulations, ethical hacking exercises, and capture-the-flag competitions makes it much easier to

understand and remember what is learnt. Gamification, project-based learning, peer collaboration, and mentorship from industry professionals are all examples of interactive teaching methods that help students stay interested and think critically (Leung and Pluskwik, 2018). These methods also make sure that students can use cybersecurity principles in real life. Competency based frameworks like the US NICE framework and the UK Cyber First standards set explicit learning goals and verifiable outputs. India must tailor global best practices to its unique context by ensuring equitable access to resources, investing in teacher training, and keeping curricula aligned with evolving cyber threats. With the right approach, India can build a high school cybersecurity education system that equips students with essential skills while fostering responsible digital behavior, critical thinking, and resilience. This will save the digital future of the country and equip the future generation to handle the challenges of a more complex cyber environment (Amankwa, 2021).

Policy and Regulatory Support for Cybersecurity Education

Cybersecurity education programs thrive when guided by clear policies and regulatory support. Countries with successful models have implemented national frameworks and government led efforts to ensure uniform outcomes in every classroom. The NICE (National Initiative of Cybersecurity Education) Framework provided by US, in particular, provides a full-fledged framework that defines knowledge categories, skills competencies, and performance indicators (National Initiative for Cybersecurity Careers and Studies, 2024). The framework provides guidelines for curriculum development and teacher training as well as assessment methods. Implementation of the Cyber First programs in UK is also guided government regulations that promote inclusivity, secure funding, and support ongoing teacher development. The policy support of the CSA programme in Singapore, is very robust and ensures that educational objectives are aligned

to national cybersecurity objectives. Regulatory backing not only elevates cybersecurity education within national policy priorities but also facilitates its sustained growth, stability, and responsiveness to evolving technological challenges (Abrahams *et al.*, 2024). These policy guidelines assist in eradicating fragmentation in the curriculum delivery through a formalized framework. They also assist in aligning with the industry requirements and establishing a system of constant upgradation and control.

Strong policy and regulatory support are essential for scaling cybersecurity education. Beyond guiding curriculum development, it ensures equal opportunity, maintains educational quality, and funds critical resources like devices and online labs; allowing schools with diverse ICT capabilities to participate fully and effectively. Such frameworks also assist teachers acquire training, move along in their careers, and learn both technical and instructional skills (Hero, 2020). For example, Singapore's cybersecurity Education programs function inside a national policy framework that makes sure all schools follow the same laws, reaches out to groups that are often left out, and interacts with businesses to provide mentorship and help with tech skills. Likewise, policies in the US and UK bring together the public and private sectors making programs better, keep them up to date on the latest cyber threats, and give students real-world learning opportunities (Khando *et al.*, 2021). India can learn from global best practices to craft robust policies that support nationwide cybersecurity education in high schools. By standardizing teaching materials, ensuring inclusive access, fostering innovation, and strengthening collaboration among schools, industry, and government, India will be able to build resilient programs that evolve with emerging threats ultimately securing its digital future.

Cybersecurity is anchored by a CIA triad – confidentiality, Integrity, and Availability; which serves as a guiding framework for protecting digital assets. As per

(Tchernykh *et al.*, 2019), confidentiality is the restriction of access to authorized users only; integrity is the prevention of data corruption by malicious software; and availability is the guarantee that all networked devices are accessible to the authorized user. While technological defenses like encryption and access controls play a critical role in preserving data integrity, they are not sufficient on their own. Human awareness and responsible behavior are equally important, as many breaches stem from inadvertent actions, negligence, or social engineering tactics.

Human error drives a staggering 95% of cybersecurity breaches making people the weakest link in the security chain. The introduction of AI has deepened this imbalance, with AI generated phishing campaigns having four times more success rates than traditional methods. Most threats are designed to exploit human vulnerability, tricking individuals into unknowingly give up sensitive information (Zhadan, 2022). Integrating education with technology and services can help eradicate mistakes brought about by social engineering and carelessness while simultaneously raising users knowledge of the risks. As rightly pointed out by (Bolun *et al.*, 2021), cybersecurity education deserves investment from individuals, families, businesses, governments, and schools alike; it's a shared responsibility in today's digital world.

Bringing it all together, strong policies and government support are key to making high school cybersecurity education work well and last a long time. Examples from around the world show that when governments back these efforts, set clear standards for what students should learn, and keep funding steady, it helps schools deliver the same quality education everywhere. It also gives students access to important learning tools, online labs, and training for teachers (Reginald, 2023). These policies also help make sure that all students, even those in remote areas or small towns, can get quality cybersecurity education. When the government promotes collaboration among schools and businesses, it

introduces the reality world, expert tips and training that is on par with job market demands. In the case of India, it is of high significance to develop a similar mechanism of policies. It would assist in developing an effective, flexible, and robust cybersecurity program at high schools. This entails training the teachers suitably, application of learning plans that are in line with what the students are expected to know, providing all with equal opportunities to access the learning resources and ensuring that the program remains relevant to the emerging cyber threats (Morandini *et al.*, 2023).

Cybersecurity Awareness Among School Community

Educational institutions have steadily embraced technology since the onset of digital era, integrating it into teaching and administrative processes. Though this integration has many benefits, it also makes schools highly vulnerable to cybersecurity threats, jeopardizing the integrity of the education process and the confidentiality of data of students and teachers (Bada and Nurse, 2020; Pranggono and Arabo, 2021). Resource constraints are a defining challenge that heightens the risk of cyberattacks in educational institutions, making their network more prone to breaches and data theft (Muthuppalaniappan and Stevenson, 2021). Also, the rapid shift to e-learning platforms especially in the post COVID-19 pandemic era has increased the attack surface, which offers more possibilities to cybercriminals to take advantage of old or unpatched systems (Bada and Nurse, 2020; Jawaid, 2023).

Cyber threats demand foresight, not hindsight. Yet, many educational institutions have traditionally taken a reactive stance, responding to incidents, instead of preparing for them in advance. It is fundamental, and strongly desirable, to increase cybersecurity awareness and overall practice among all parties concerned, especially as the Internet becomes an essential element of educational infrastructure (Zurkarnain and Abdulsahib, 2023). Good cybersecurity awareness programs should involve large population with the

students being included in this as they should have proper guidance and supervision to handle the online risks without struggling (Rahman *et al.*, 2019).

Cybersecurity education is crucial for all members of the high school community, including students, teachers, and parents. Promoting digital safety awareness helps students develop the skills needed to explore online spaces responsibly (Jerman Blažič and Jerman Blažič, 2022). It is important that students learn how to identify cyber threats, safeguard personal and academic information, and use the internet securely. International studies highlight the value of embedding cybersecurity topics into everyday classroom teaching to build a safer digital learning environment. Interactive methods, such as workshops, gamified learning, competitions, and online challenges have proven effective in helping students internalize and apply cybersecurity concepts with greater confidence and retention (Altarawneh *et al.*, 2025).

Educators and parents have a significant role to play in teaching children online safety. By modelling responsible internet use and reinforcing key lessons, they can help create a culture that values caution and promotes digital responsibility (Santhosh and Thiyaagu, 2024). Teachers play a significant role in promoting cybersecurity awareness by integrating it into classroom environment, guiding students into safe internet practice, and encouraging responsible use of technology (Prümmer *et al.*, 2024). At home, parents, and caregivers are equally important, they should supervise online activity, reinforce safe digital behavior, and support participation in cybersecurity related programs and competitions. Countries such as Australia and Singapore have implemented effective initiatives to train both educators and parents, helping them stay informed about emerging cyber threats and foster healthy digital habits. In India, there are efforts like Cyber Surakshit Bharat and state-based awareness campaigns, that try to involve schools and families, but these programs are not widespread or consistent.

According to (Martínez-Domínguez and Fierros-González, 2022), cybersecurity measures in high school needs to ensure, sensitive information and systems cannot be accessed, disclosed, disrupted, altered, or destroyed by unauthorized individuals. To prevent unauthorized access, maintain system and data integrity, and prevent malicious software, phishing attempts, security measures should be implemented on computer networks and devices (Khando *et al.*, 2021). Seminars, workshops, and other forms of educational programming can be helpful to guide high school pupils about cybersecurity (Rahman *et al.*, 2019). Adopting strong passwords with multi-factor authentication, maintaining regular backups and system updates, and remaining vigilant will go a long way in minimizing cyber risks and ensuring the protection of sensitive data across digital platforms.

To conclude, ensuring that high school students, teachers, and parents are well informed about cybersecurity is vital for maintaining a resilient digital space and supporting the successful implementation of educational initiatives. Evidence from programs like Cyber Patriot in the U.S., Cyber First in the U.K., and CSA in Singapore indicates that combining student centered cybersecurity activities, along with training educators and involved parents enhances children's retention, ethical understanding of online conduct, and adoption of secure habits beyond the classroom (Altarawneh *et al.*, 2025). These initiatives are most effective when students, educators, parents, and mentors actively participate through structured events, interactive competitions, engaging educational games, and consistent guidance. In India, similar efforts like Cyber Surakshit Bharat, Digital India, and regional awareness campaigns have started to raise awareness about cybersecurity. Nonetheless, there are concerns such as imbalanced development, the absence of access to digital tools, and insufficient teacher and parental support. Integrating cybersecurity awareness into school curricula, government policies, and practical training

can help India build a more effective system that empowers students to recognize online threats, make informed decisions, and apply their knowledge in real-world scenarios. As per (Amankwa, 2021), cybersecurity awareness is not only a way of ensuring that people and schools become less vulnerable to cyber-attacks but also a way of assisting the nation in ensuring that its digital systems are protected.

Comparative View of Indian and Global Government Cybersecurity Initiatives and Challenges

Governments around the world play a critical role in assisting schools to teach cybersecurity by developing programs, guidelines, and rules that provide support, tools, and direction to schools. The NICE Framework is a national initiative in the United States that outlines the learning objectives, skill sets, and assessment strategies expected of students in cybersecurity education. It also serves as a foundation for curriculum development, teacher training, and student evaluation in schools (National Cyber Security Centre, 2022; Oyewole *et al.*, 2024). In a similar vein, the UK's Cyber First programs has government backed educational initiatives that offers students financial support, learning resources, competitions, and mentorship to strengthen cybersecurity skills, with a focus on inclusive participation, especially for girls. In Singapore, CSA's Cybersecurity Education programs integrate national policy, hands-on tools, virtual labs, engaging activities, and industry partnerships to deliver high-quality learning experiences (CSA SINGAPORE, 2024). These examples highlight how government intervention can support standardized cybersecurity education by providing resources and real-world training opportunities. They also underscore the need for adequate funding, industry collaboration, and clear policies to ensure long-term program effectiveness and growth.

Although these international initiatives have produced some success, there are issues that India must be cautious of while developing its own high school cybersecurity

initiatives. Aspects such as, disparities in access to digital infrastructure, particularly in rural and underfunded schools; absence of skilled teachers with ability to teach both technical and pedagogical material; and the fact that cyber threats are constantly evolving necessitating curriculum to be regularly updated to remain relevant, are some known challenges (Vigneswari *et al.*, 2025). In nations, where the programs are designed at the highest institutional authority level, it is often difficult to maintain the level of the consistency at the schools' levels, to incorporate the skills that may be helpful in the real world, and to make the balance between practical activities and the knowledge of the theory. India can shape sustainable, government-supported cybersecurity education programs by studying global models and ensuring strategic planning, adequate resources, and continuous collaboration among educators, students, and industry stakeholders.

Amid rising cyber threats in the digital era, the Indian government has taken numerous steps to create and execute a national cybersecurity plan. To protect the country's digital infrastructure, several initiatives have been launched, such as "National Cyber Security Policy" (NCSP), the "Indian Computer Emergency Response Team" (CERT-In), and sector-specific cyber cells (Oyewole *et al.*, 2024; Ahn *et al.*, 2024). Recent efforts to enact data protection legislation, the establishment of the "National Critical Information Infrastructure Protection Centre" (NCIIPC), and policies under the Digital India campaign; reflect governments intensifying focus to tackle cybersecurity risks. By encouraging cooperation between parties, capacity building, and establishing public-private partnerships in cybersecurity, these frameworks aim to develop a resilient cyber ecosystem. However, even with these recent efforts in policy and regulation amends, India still remains underprepared when it comes to cybersecurity. Critics argue that the policy landscape is not proactive enough, suffers from fragmentation across ministries, and face challenges in accountability and effective implementation (Darshini *et al.*, 2025; Alqurashi and Ahmad,

2024). The broader public lacks adequate awareness of safe technology practices, and there is a shortage of skilled cybersecurity professions. In addition, establishing global cyber rules and gaining international cooperation to combat cybercrime represent obstacles in diplomacy that India must ensure to navigate. As observed by (Kwilinski and Trushkina, 2024; Aksoy, 2024), it is critical to assess current cybersecurity frameworks, find areas to make improvements, and bring them in line with the changing character of cyber threats on a national and international scale.

Cyber intrusions attributed to foreign adversaries have emerged as global concern, threatening data sovereignty and the security of critical information systems. Malware, zero-day vulnerabilities, and digital propaganda have given rise to covert warfare and espionage in cyberspace, which has grown in importance as geopolitical tensions have escalated (AZUBUIKE, 2023). In light of these emerging dangers, India has re-evaluated and enlarged its national security architecture to incorporate robust cyber defense forces and institutional readiness. India has established several cybersecurity laws and established dedicated institutions to monitor cyberspace in reaction to these emerging threats (Iclg, 2024). While there have been notable advancements, India's overall cybersecurity landscape remains weak. Challenges include limited funding for cyber research and development, a shortage of skilled professionals, low public awareness, and the continued reliance on outdated IT systems by many government agencies (Sunita, 2024). Moreover, there hasn't been a chance to solidify how the business world, the military, and civic society work together; creating vulnerabilities that adversaries can exploit. The absence of robust international cooperation and a legally enforceable data protection framework further complicate India's cybersecurity effort. Addressing these gaps demands the inclusion of innovation in technology, legal reforms, capacity building, and strategic policy development.

In conclusion, at the heart of sustainable cybersecurity education lies strategic government involvement. Well-crafted policies and proper implementation are critical to maintaining the effectiveness and longevity of high school cybersecurity programs. These programs must ensure to provide clear structure, support, and strategic plans required to deliver instructions effectively, train educators and offer students hands-on learning opportunities (Vikasconcept, 2025). India stands at a pivotal moment in cybersecurity policy development. By studying international best practices and challenges, it can design frameworks that are both contextually relevant and globally informed.

Digital Awareness and Academic Performance: Perspectives from Students, Educators, and Parents

To truly measure the effectiveness of high school cybersecurity education, it's essential to understand the knowledge levels of students, teachers, and parents. These insights help shape programs that actually work. Most importantly, such initiatives have a direct impact on students; their ability to navigate digital environments safely and responsibly is shaped by what they know, how they think, and how they behave online. Without this foundational awareness, even the most well-designed curriculum may fail to achieve its objectives. Global research shows that students' knowledge varies greatly according to course content, instructor pedagogy, and students' exposure to real-world scenarios (Ciabo and Labadan, 2025). Students engaged in cybersecurity education programs, particularly those built around competency based modules and hands-on exercises demonstrate a strong understanding of digital risks, privacy protection, and responsible internet use (Waldock *et al.*, 2022). These learning experiences not only enhance their technical abilities but also nurture ethical awareness and proactive mindset; with students often showing a willingness to identify and respond to cyber threats,

indicating their evolution into informed and accountable members of the online community.

Equipping students with cybersecurity skills doesn't happen in isolation; it requires a supportive ecosystem. For this to happen, the awareness levels of teachers and parents are equally critical. When educators understand the importance of digital safety and parents as well as caregivers reinforce it at home, cybersecurity education becomes more effective, consistent, and lasting. Their involvement helps to bridge the gap between classroom learning and real-world application, creating a culture of responsible digital behavior. The responsibility of teachers entails teaching cybersecurity concepts in their classes, modelling good online behavior, educating students on technical and ethical practices, and keeping abreast about emerging threats and tools (Childers *et al.*, 2023). Similarly, parents role, in their children's education concentrates on certain aspects, including schoolwork, communication, family dynamics, expectations, and reading aloud to kids (Fan and Chen, 2001). In the scholarly article (Chen and Gregory, 2009), suggest that parental involvement is most effectively understood as a holistic concept; one that encompasses both behavioral actions and psychological engagement in a child's education. Understanding the levels of cybersecurity awareness among students, teachers, and parent; both in India and globally, offers valuable insight for educators and policymakers. By identifying gaps in knowledge and learning from successful international practices, schools and policy makers can design collaborative strategies that strengthen cybersecurity education (Cyberlite, 2023). This comparative approach enables the development of more informed, inclusive, and effective programs tailored to local needs while benefiting from global experience.

Understanding what drives student academic performance remains a complex challenge for educators, parents, and researchers alike. One useful approach is to view the influencing factors through two lenses: "in-school" and "out-of-school" conditions. In-

school conditions include teaching quality, curriculum design, peer interactions, teacher and administrative qualifications, and the learning environment (Straková *et al.*, 2018). Out-of-school conditions includes family support, access to technology, and socio-economic background (Roksa and Kinsley, 2019; Volante *et al.*, 2019). By recognizing and analyzing these dimensions, stakeholders can better identify where interventions are needed and how to create more supportive learning environments both inside and outside the classroom.

Analysis by (Nunes *et al.*, 2023), suggests that the difference in the way students, educators and parents interpret and rank the factors that define academic achievement are clear and meaningful. Teachers, because of their training and profession, are generally well aware of in-school factors, which include the teaching strategies, curriculum or syllabus design, classroom management and assessment strategies. Parents on the other hand, by virtue of their concerns about their children, are more aware of out-of-school factors, especially those that relate to socio-economic conditions, the learning resources available in homes, family support systems and health-related factors affecting the learning of children (Tabe, 2023). The level of awareness among students varies with some being aware of the importance of both school and home-based factors, but in most of the cases they underestimate the long-term effect of parental involvement, self-efficacy and their own learning habits. The gap in awareness levels can be bridged by intentional channels of communication, collaborative decision-making and awareness-raising programs in which students, educators and parents can build a common set of knowledge regarding important aspects of achievement, as well as collaborate in creating more inclusive and effective learning contexts (Ioannidi, 2025).

1.2 Research Problem

The basic idea behind the invent and the growth of information technology is speed of communication. People use devices connected to internet, not only for communicating with the outside world via video conferencing, social media posts, chats, emails etc. but use the technology inbuilt to navigate to newer places using maps and GPS, securing their homes, and using Internet of Things (IoT) to enable smart electrical appliances like TV's, refrigerators, cleaning homes and monitoring the activities of babies, elderlies and patients as well. While these technologies enhance convenience and real-time communication, they simultaneously heighten exposure to privacy breaches, data misuse, and cyberattacks; often requiring expensive efforts to restore trust and integrity to the damaged reputation.

In today's data driven landscape, just like government and commercial entities, even academic establishments including schools have become increasingly vulnerable to data breaches and cyber frauds. Sensitive student data, including names, addresses, identification numbers, and contact information can be exploited for identity theft, credit fraud, or manipulation, often without detection by victims or their families. This risk is intensified by a widespread lack of cybersecurity awareness among educators, many of whom feel ill-equipped to teach the subject. Moreover, the absence of guidance and support from government and industry bodies leaves schools without the necessary frameworks to implement robust cybersecurity education and practices. As well noted by (Taherdoost, 2024), raising awareness and knowledge is a crucial step towards cybersecurity, as technological defenses alone are not adequate to protect individuals or companies from online threats.

Recent research spanning diverse geographies including but not limited to United States, United Kingdom, and South Africa suggests an urgent need to equip parents and educators with digital literacy through collaborative seminars and workshops. The global

surge in cyberattacks, coupled with an acute shortage of cybersecurity professionals underscores the need to introduce cybersecurity education at an early age.

Children and adults alike have increasingly become vulnerable to cybercrimes, having collectively losing billions to online threats, reinforcing the argument that cybersecurity awareness should not be regarded as an optional skill, but as a foundational pillar of modern education. Despite consensus on the importance of early cybersecurity education, many teachers struggle to implement it effectively due to limited subject matter knowledge and a lack of age-relevant and psychologically appropriate resources and curriculum material for K-12 classrooms.

In the context of Indian sub-continent, cyber-hygiene awareness among students of higher education reveals a distinct urban-rural divide (Kant, 2023), with urban students exhibiting greater familiarity with digital safety practices. Alarmingly, a substantial proportion of users remain unaware of proper channels for reporting cyber-fraud, leaving them exposed in an increasingly hostile digital landscape.

While there have been multiple research projects published on cybersecurity awareness across multiple countries, there is a critical gap in localized studies addressing the Indian context. The high prevalence of cybercrimes mostly including financial fraud, underscores the urgency of investigating digital behavior among Indian youth, especially given their widespread use of internet-enabled devices and limited understanding of online risks. The unique socio-cultural dynamics and vast population of India calls for tailored intervention that reflects regional and linguistic needs and challenges. Bridging this research gap is essential for crafting context-sensitive cybersecurity strategies that not only protect young users but also empower schools and the community at large to foster a safer digital environment.

Research Objectives:

- To provide insights into the strengths and weaknesses of cybersecurity education programs in different countries and provide recommendations for improvement in Indian schools.
- To examine the teaching methodologies, resources and curriculum design used in other countries and identify best practices that can be applied in India.
- To investigate the role of government policies and regulations in promoting cybersecurity education at high school level in India.
 - To find the cybersecurity awareness level of educationalists, students and parents across India.

1.3 Purpose of Research

As digital technology becomes deeply embedded in everyday life, the need for strong cybersecurity education in schools is more urgent than ever. The research aims to explore how different countries approach cybersecurity education at the high school level and how their successful strategies can be capitalized to improve India's efforts in this area.

Students today face a range of online risks, from cyberbullying and phishing to privacy breaches and misinformation. While some countries have developed structured programs to address these challenges, India's approach remains largely inconsistent, often varying from one school to another without a unified framework. This study seeks to analyze global practices in cybersecurity education, focusing on teaching methods, curriculum design, teacher preparation, and resource allocation.

A key objective is to identify models that have proven effective elsewhere and identify how they can be adapted to suit India's diverse educational landscape. The research also examines the role of government policies, legal frameworks, and partnerships between public and private sectors in shaping successful cybersecurity initiatives.

In addition, the study investigates the current awareness level among students, teachers, and parents in both urban and rural settings. It considers how digital literacy, cultural context, and behavioral factors influence the success of educational programs. Ultimately, the goal is to offer practical recommendations to policymakers, educators, and curriculum developers to help build a safer, more informed digital environment for India's youth; empowering them to navigate the ever-evolving cyber world with confidence, responsibility, and in an ethical manner.

1.4 Significance of the Study

The study is significant as it addresses a critical gap in India's educational and policy landscape through systematic examination of: how high school cybersecurity education can be enhanced inspired by lesson plans and teaching methods from other countries as a reference. The accelerated pace of digitalization in India, coupled with high internet usage among youth, has led to a rise in cyber threats, including cyberbullying, fraudulent activity, and privacy violations. Despite these vulnerabilities, a standardized and robust cybersecurity curriculum remains absent from the national school system. By comparing the strengths and weaknesses of global best practices in cybersecurity education, this study offers practical guidance for creating culturally and region-specific teaching methods, resources, and curricula design for enhancing cyber programs in Indian schools. The study also highlights how government led policies, regulations, and cross-sector partnerships have advance early cybersecurity education abroad, serving as a guide for India's educational reform. Furthermore, the evaluation of awareness level among students, educators, and parents in India will provide insights into the gaps in behaviors and knowledge that signifies a barrier to effective cybersecurity practices at the grassroots level. The findings will have a broad application to many stakeholders in the area: Teachers who want to get trained on improved ways of teaching; Parents who wish to be able to

secure their children in the cyber world; Policymakers who want to develop evidence-based interventions; and Technology partners who are willing to contribute to the digital literacy efforts. Overall, the study aims to secure India's digital future by equipping the next generation with essential skills, ethical awareness, and a strong foundation, positioning cybersecurity as a fundamental part of early education.

1.5 Research Purpose and Questions

The modern digital landscape is exposed to a dual-edged crisis – First, the inherent anonymity provided by internet often impedes the ability of law enforcement agencies to accurately identify and apprehend cybercriminals. Second, the field of cybersecurity encompasses a broad spectrum of domain and specialized roles, rendering it difficult for any single educational program to comprehensively address all the requisite skills and competencies. However, some fundamental knowledge and skills are essential for daily life, academic pursuits, and critical job functions in our digital society. (Onyema *et al.*, 2021) accurately notes that “the increasing rate of cybercrimes underlines the need for increased cybersecurity awareness and education among people and organizations”.

Several scholarly investigations (Jayaraman, 2022; Pal, 2022; PHDCCI and Grant Thornton Bharat, 2022; Yashwant, 2021) have concluded that cybercrimes can occur at any time, regardless of location. The increasing prevalence of internet usage among adolescents and children poses significant risks to their cognitive, emotional, and social development, impairing their ability to form healthy relationships, and maintain attention; potentially exposing them to addictions like gambling, pornography, and cyberbullying. The best way to mitigate such threats is by incorporating cybersecurity education in learning institutions where students learn early on the ethics of interacting in the cyberworld. In the context of Indian sub-continent, there is a lack of proper framework for imparting cybersecurity education at high school level and as concluded by (Yashwant,

2021) very less research has been devoted towards cybersecurity education for high school students and school staff in India.

After conducting a thorough examination of the available literature, the paper investigates the need for cybersecurity education at school levels, identify ways for imparting cybersecurity education by comparing similar educational findings in other countries, identify challenges in implementing cybersecurity education and proposing ways to overcome such challenges. Drawing upon the interdisciplinary activities this paper intends to identify the awareness level and need for cybersecurity education at high school level and also suggest constructive ways in which teaching can be imparted that will help the students as well as the teachers realize the benefits of such education. The study employs a deductive research approach, employing surveys administered through Google forms, to reach out to students, parents, and educationalists and gain insights into the awareness level of cyberworld and cybersecurity among the students. In the end, the proposed study seeks to safeguard India's digital future by recommending best practices for curriculum enhancement, equipping students with necessary skills to operate in a secure, and ethical manner in the cyber world, empowering educationalists with the ability to teach effectively, and guiding policymakers with evidence-based strategies that promote digital safety, resilience, and literacy among youth.

Research Question

1. What are the strengths and weaknesses of cybersecurity education programs in different countries, and how can these inform improvements in Indian high schools?
2. Which teaching methodologies, learning resources, and curriculum designs used internationally can be effectively adapted to the Indian context?

3. What role do government policies and regulatory frameworks in India and abroad influence the implementation and effectiveness of high school cybersecurity education programs?
4. What is the current level of cybersecurity awareness among high school students, parents, and educationalists across India?

CHAPTER II: REVIEW OF LITERATURE

Cyberspace is a term commonly used to refer to the world of internet and the host of devices that are part of the ecosystem (Dobos and Csiszarik-kocsir, 2022; Van den Berg *et al.*, 2015). Within the cyber domain, there exists malicious actors known as cybercriminals or hackers that actively attempt to gain unauthorized access to digital systems and sensitive information, exploiting vulnerabilities in hardware, software, and communication infrastructures. These actors may operate alone or in groups, and at times state sponsored and are often motivated by financial gain, political agendas, espionage, or disruption. As per the study by (Okeke, 2024), common attack vectors include phishing, malware, ransomware, and distributed denial-of-service (DDoS) attacks.

(Ige, 2020) describes cybercrime as any criminal activity like cyber-hacking, identity theft, spamming, social engineering attack, programming attacks, online fraud, and data alteration executed using IT devices. (Halder and Jaishankar, 2011) defined these offences as acts against individuals or groups with the criminal intent to harm reputations using modern telecommunication networks. By highlighting the scope and nature of cybercrimes, these definitions underscores internet and the critical role of technology in facilitating these cyber-offenses and the urgent need for comprehensive cybersecurity education and awareness measures to protect against such threats.

(Taylor *et al.*, 2014) goes on to divide these cybercrimes into four categories. The first category is where computers or networks are the target, such as Denial of Service. The second is where computers are used as tools, such as fraud and harassment. The third is where computers are used as a product, such as for money-laundering, and the fourth where widespread use of internet enabled computing devices can be used for intellectual property infringement, counterfeiting and identity theft.

2.1 Theoretical Framework

“Space Transition Theory” and “Self-Determination Theory” are two well-known theories that provide complimentary insights within the academic field of Theoretical and Conceptual Frameworks for cybersecurity Education. Space Transition Theory (STT) is a concept from criminology that explains how individuals may behave differently in online environment compared to physical world. The theory suggests that anonymity and reduced sense of accountability found in virtual spaces may lead people to engage in harmful or illegal activities, that they would often avoid in the physical world. This framework helps educators and researchers better understand the psychological factors that drive negative behavior on the internet, such as cyberbullying or online fraud. Complementing this, the motivational theory known as the Self-Determination Theory (SDT) provides insight into how intrinsic basic psychological requirements of relatedness, competence, and autonomy influence individual behaviors. While SDT gives a useful framework for the "how" of encouraging healthy, safe, and self-motivated cybersecurity behaviors in individuals, STT offers an angle for comprehending the "why" behind harmful online actions. When combined, they offer a comprehensive perspective that aids in determining the true motives behind certain online behavior as well as creating instructional initiatives that successfully promote a cyber secure culture. These theoretical foundations support the study’s goal of recommending effective and psychologically informed cybersecurity education models for Indian schools.

2.2 The Space Transition Theory

The “Space Transition Theory” (STT) introduced by (Jaishankar, 2007), offers a criminological lens to explain the behavior of humans in cyberspace and how this differs from that of the physical world. Classic criminological theories paid much attention to physical environments, but the emergence of the internet and digital technologies made

theorists note that people sometimes behave in different ways when they are on the internet than when they interact with each other in real life. To address this gap, the author formulated a theory, STT, in 2007, and it was one of the first to provide a holistic theory to explain cybercrime and deviance in virtual space. The paper highlights cyberspace features, which include anonymity, invisibility, lack of physical barriers, and the capacity to create more than one, or false identities, and behavioral changes. Things that are not allowed to be done in the actual world because of societal expectations, fear of affecting others or punishment can be done freely in cyberspace. As an illustration, a person, who would not have committed harassment, fraud or identity theft in a real life would likely commit such acts in the cyber world due to the lower chances of being discovered, or in other words because of the anonymity provided by internet. In essence, cyberspace offers a sense of disinhibition, which stimulates behaviors that individuals would typically avoid in off-line situations. This theory has great relevance to cybersecurity research, because it explains why people especially the students and adolescents would use the internet in ways that are unsafe or immoral although they act responsibly in the physical world. Understanding this behavioral shift is crucial for developing effective educational strategies to promote safer digital practices.

The STT suggests that individuals, who suppress deviant behaviors in physical reality can find it easier to express them on the Internet. The absence of direct oversight, fear of punishment, and social accountability in online environment creates conditions where misconduct feels less risky and more permissible. Jaishankar states a number of propositions such as:

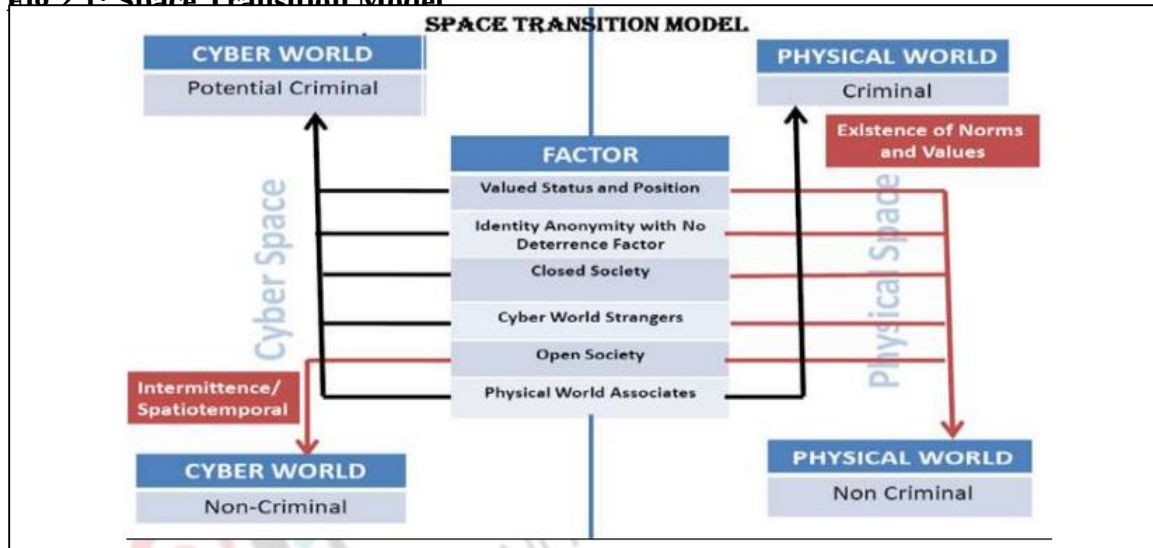
- **Transition of Behavior:** Individuals exhibit distinct behavioral pattern as they transition between physical environment and digital spaces.

- **Suppressions of Deviance:** Deviance that is unseen in the real world may be unleashed in the virtual world because of anonymity and invisibility.
- **Identity Flexibility:** In the virtual realm, people can form false identities or multiple identities and this facilitates deviance.
- **Less Fear of Authorities:** The perceived risk of being caught is decreased by the absence of direct law enforcement.
- **Global Connectivity:** The ability to interact with strangers across geographies, encourages both socially acceptable and deviant behaviors.
- **Continuation of Behavior:** Deviant behaviors acquired online may transition into the real world.

Applicability to the Current Study.

This theory has a lot of relevance to research on cybersecurity education in high school. Students being one of the most active internet users, tend to surf the cyber world without having a full insight of the dangers. STT provides an explanation as to why despite having good conduct in the physical world, the same students may still be exposed to unsafe behaviors in the virtual world, such as posting personal information, cyberbullying, and downloading pirated materials. This illustrates how cyberspace can alter perceptions of responsibility and authority, making young users more susceptible to deviant behavior or becoming victims of online threats. This shift in conduct highlights the urgent need to integrate cyberethics, cybersafety, and cybersecurity into school curricula, equipping students with the awareness and skills necessary to navigate digital realm responsibly.

Fig 2.1: Space Transition Model



Source: Compiled by author.

Figure 2.1: Space Transition Model derived from (Karuppannan, 2008) by (Danquah and Longe, 2011)

In the Figure 2.1 above, (Karuppannan, 2008) explains STT, as to how people's behavior changes when they migrate from the physical world to a virtual world. This hypothesis suggests that because of the unique nature of the online environment, individuals who are typically law-abiding in the real world may tend to have criminal or deviant inclinations in cyberspace. The existence of laws, values, and social standards deter criminal activity in the physical world. On the contrary, world of internet offers opportunities for anonymity, lack of deterrence, and contact with strangers, all of which may result in possible criminal activity. The pursuit of a valued status and position, identity anonymity, lack of deterrent, and the distinction between closed and open societies are some of the major reasons identified by the theory as influencing this behavioral shift. It also highlights the fact that people may behave differently while interacting with strangers online than they would with friends and family in real life. The theory highlights that, human behavior in the digital environment is often fluid, shifting between lawful and

unlawful actions depending on the context and circumstances, suggesting that deviant conduct online is not constant but influenced by temporal and situational factors. To conclude, the theory offers valuable psychological insight into cybercrime by proposing that the world of internet provides a platform where latent tendencies towards misconduct are more easily expressed; making it particularly relevant for analyzing patterns of online criminal behavior that may not manifest in offline interactions.

2.3 Self-Determination and Social Cognitive Theory

Deci and Ryan developed the idea of “Self-Determination Theory” (SDT) in the 1980’s (Deci and Ryan, 2013), as a motivating framework to explain why people decide to take specific actions. Fundamentally, SDT contends the satisfaction of three psychological needs that influences human motivation, they are: autonomy, competence, and relatedness. Autonomy is the ability to make decisions and feel in charge of one's behavior; Competence is the feeling of being able to learn or do things effectively; Relatedness focusses on maintaining a sense of community and support from others. The framework proposes that, individuals have a great capacity to be intrinsically motivated and, to pursue things for enjoyment, curiosity, and personal development rather than in response to rewards from other sources or fear of punishment. As the theoretical lens explains why, learning settings that foster choice, mastery, and collaboration increase student engagement, this idea is frequently used in the field of educational strategies.

Albert Bandura developed the idea of Social Cognitive Theory (SCT) in 1986 with the goal of examining how humans learn in social settings. SCT highlights the importance of learning through observation, where individuals adopt behaviors by watching the actions of peers, teachers, or role models. It also stresses the role of self-belief (self-efficacy) in driving motivation and learning success. Another idea in SCT is reciprocal determinism, which explains how individual actions, personal beliefs, and the surrounding environment

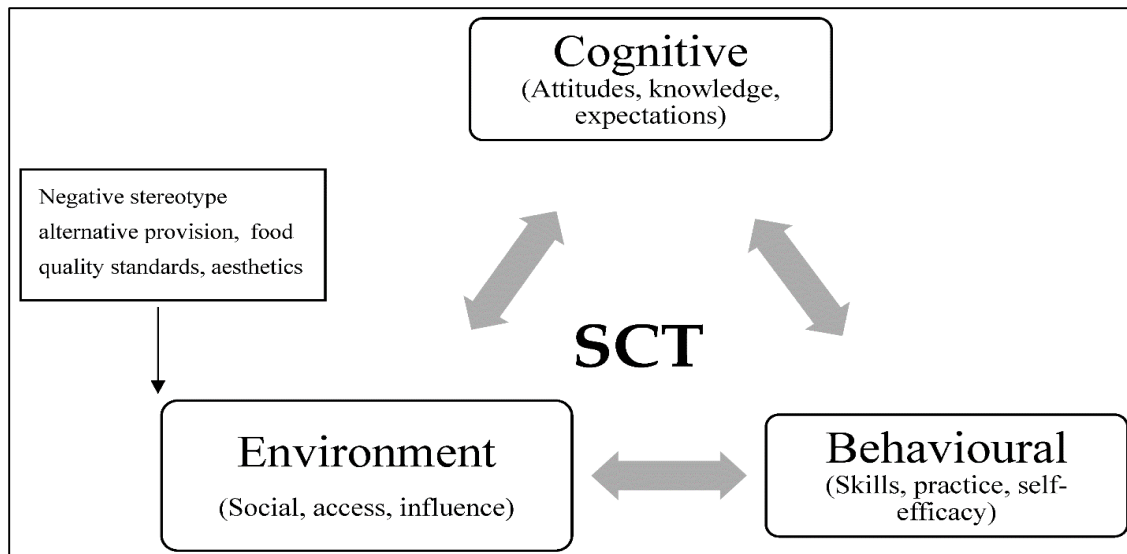
constantly influence each other. In educational settings, the theory explains how students develop skills, attitudes, and long-term habits through encouragement, and confidence-building exercises.

SDT is employed in this study as it suggests ways to encourage high school pupils to actively participate in cybersecurity courses. SDT offers a framework for creating learning experiences that give students a sense of control, competence, and connection to their teachers and classmates since it places an emphasis on the fulfilment of independence, abilities, and relatedness. Interactive approaches such as project-based tasks, game-based activities, and storytelling supports learners need for autonomy and skill development. These methods also encourage collaboration, helping students build a sense of belonging through shared group experiences; an element essential in fostering motivation as outlined by SDT. Teachers can foster intrinsic motivation in students, by designing cybersecurity course curricula that correlates to these motivational demands, that not only promotes safer online practices but also enhances their interest in exploring future careers in cybersecurity.

Social Cognitive Theory (SCT), in a similar manner, is highly relevant in the context of cybersecurity education, as it underscores the social nature of learning. Students not only absorb information from textbooks, but also acquire behaviors and skills by observing peers, teachers, and digital role models who demonstrate responsible online practices. Students while witnessing successful models of digital safety behaviors', internalize those behaviors as explained by SCT's observational learning principle. Furthermore, the focus on self-efficacy highlights how crucial it is to help students develop their confidence in managing cyber dangers as knowledge application in practical situations requires self-belief. Together, SDT and SCT substantiate the need for effective cybersecurity education curricula design and incorporate motivation, role modelling, and

confidence-building exercises in addition to technical resources, to make learning sustainable and successful.

Fig 2.2: Social Cognitive Theory



Source: Compiled by author.

Figure 2.2: Initial and Emerging factors. Source (Harris et al., 2021)

Figure 2.2 explains Social Cognitive Theory (SCT), a framework that shows how human behavior is influenced as a result of a dynamic and reciprocal interaction between three factors: Cognitive, Behavioral, and Environmental. The central triangle, with double-headed arrows illustrates this concept of reciprocal determinism, meaning each factor influences and is influenced by the other two. Cognitive factors include a person's thoughts, attitudes, and expectations, such as their knowledge about healthy eating. Behavioral factors refer to a person's actions, skills, and self-efficacy (their belief in their ability to succeed), for instance, their skill at cooking. Environmental factors are external influences like social pressure or the availability of certain foods. The additional box on the left provides specific examples of how the environment can influence this system, listing things like food quality standards or aesthetics. In essence, SCT explains that behavior is not

simply a product of one's thoughts or surroundings, but a constant interplay among thoughts, actions, and the environment.

To summarize, these theories provide a perspective that help teachers, governments, and cybersecurity experts understand how people learn and behave online. SCT explains that individuals learn by watching others and seeing consequences. For instance, if a student clicks a suspicious link and gets hacked, his / her peers learn not to do the same. SDT focuses on motivation and emphasizes that individuals do better when they feel autonomous, competent, and connected. For instance, if a student feels confident using strong password and knows his / her teacher supports such a practice, they keep practicing safe habits. STT explains why individuals behave differently in an online vs. an offline setting. For instance, a shy school student in classroom setting may act boldly and bully other in an online environment as they feel autonomous. These three theories in essence provides guidance to educators, policy makers and industry experts to make lessons more effective and engaging and help students become smart, safe, and ethical digital citizens.

2.4 Introduction to Global Insights on Cybersecurity Education

The scholarly contribution by (Payne *et al.*, 2021), discusses a collaborative effort brought together cybersecurity experts from five different fields to create a general education course free for everyone. The researchers identified that Cybersecurity, Technology, and Society should be considered interdisciplinary; and suggested to introduce students to cybersecurity through perspectives drawn from philosophy, computer science, engineering, business, criminal justice, and information technology. The study proposed course materials with an overview of the course's aims and purpose, a breakdown of the modules, details on the required readings and open educational resources, and an

inventory of the many types of assignments. The study in conclusion, offers advice to other researchers and educationalists developing similar programs.

The study presented by (Cabaj *et al.*, 2018), notes that with the continuous growth in digital data, vital infrastructures, and networked devices, cyberattacks are intensifying in occurrence, complexity, and severity. Despite rising concerns among diverse groups, the present workforce is not adequately equipped to meet the increasing demand for cybersecurity specialists, a deficit anticipated to grow. With this paper, the researchers investigated cybersecurity Master's programs at some of the best schools across countries like USA, UK, Australia, New Zealand, Estonia, Netherlands, Israel and Spain. The study examined subjects being covered and how they're taught. This article pays tribute to the work of the "Association for Computing Machinery" (ACM), an influential organization that helped shape early computer science courses like Information Assurance and Security Knowledge Areas and has since proposed new curricula design to back up the description of computer science degree programs at universities. The study evaluated 21 computer science master's programs across universities, taking into account each one's structure, curriculum, duration of programs, admission requirements, completion requirements, and historical development. The study recommends that, to remain relevant to the growing demands of the market, cybersecurity education programs must continuously evolve. India can also benefit from extensive evaluations of global cybersecurity courses to adapt best practices, strengthen its own curricula, and ensure that students are equipped with the skills needed to meet emerging challenges in the digital era.

The study by (Turkanović *et al.*, 2019), highlights that Information Technology (IT) has impacted every aspect of modern systems including vital infrastructure, healthcare, and strategic domains such as the military, asserting the importance of safe-guarding these assets. The study also points out that the escalating need for cybersecurity specialists

signals their soaring market value while underscoring the field's interdisciplinary character. The need for cybersecurity expertise has also been acknowledged by esteemed organizations such as ACM or IEEE, which have put up recommendations for the academic preparation of future cyber warfare fighters. Following the approach pioneered by the University of Maribor, this essay proposes an IT-driven and information systems-based perspective on computer science instruction.

2.5 The growing importance of Cybersecurity in the digital era

According to (Untawale, 2021), data protection has emerged as a key concern in the recent times and this concern over cybersecurity is mostly based on the rising tide of "digital violations". The paper highlights growing concerns over network security, with issues such as cybersecurity, digital psychological warfare, and broader network vulnerabilities posing significant risk. In particular, digital psychological warfare is identified as a threat capable of inflicting financial losses for organizations, amounting to billions. In essence, cybersecurity is not only considered as a technical challenge but also a socio-economic threat with far reaching implications.

This research study by (Adejumo and Ogburie, 2025), identifies cybersecurity to be essential in today's hyper-digital environment for safeguarding consumers, companies, and financial institutions against online threats. Data breaches, phishing attempts, ransomware, and financial fraud are some of the threats that the banking sector confronts due to its attractiveness to cybercriminals. With the rapid growth of digital transactions, online banking, and fintech innovations; robust cybersecurity measures have become increasingly critical. The study discusses key challenges and advanced solutions, identifying encryption, multi-factor authentication, blockchain, and AI-driven threat detection as essential tools for mitigating risks. The paper also stresses, the importance of consumer awareness and cyber hygiene, given the persistence of social engineering attacks.

As cyber-crime tactics evolve, continuous innovation in security practices is considered indispensable. Ultimately, the study argues that collaboration among banks, cybersecurity firms, and governments is vital to ensure the resilience, trustworthiness, and stability of financial systems in the digital age.

(Ervural and Ervural, 2018), observes that the global development industry is undergoing significant transformation to meet the complex demands of modern business. The emergence of Industry 4.0, driven by rapid technological progress, has introduced new challenges, particularly in cybersecurity. The rapid convergence of information and operational technology, coupled with widespread adoption of IoT, has heightened cybersecurity risks. This article takes a global, public–private perspective to analyze these threats, identifying the causes of cyberattacks, industrial challenges, and the pressing need for robust cybersecurity. It further discusses contemporary solutions, including frameworks and approaches designed to safeguard against evolving digital dangers.

The study addressed by (Sharma and Gupta, 2024), highlights that the integration of ICT has increased cybersecurity risks and enhanced digital convenience at the same time. It examines the complexity of emerging threats and parallel development of security applications designed to safeguard digital systems. The paper analyzes the challenges faced by IT professionals; critically assessing the effectiveness of current security solutions; and exploring the evolving landscape of security technologies. The paper addresses newly emerging threats such as supply chain vulnerabilities, ransomware, IoT risks, and Advanced Persistent Threats (APTs), supported by real world case studies. The paper also investigates security applications, focusing on blockchain, cloud security, endpoint protection, artificial intelligence, and machine learning. Ultimately, the study provides IT professionals, policymakers, and researchers with insights into dynamic cybersecurity

environment and to support the formulation of informed strategies for protecting digital ecosystems.

These studies reveal that as digital devices continue to evolve; with the rapid expansion of the Internet of Things (IoT) across sectors such as healthcare, manufacturing, transportation, energy, and finance has created vast opportunities; but also, significant risks translating into billions in losses every year from cyberattacks. Considering the growing threat landscape, there is an urgent need for strong partnerships among policy makers, industry experts, and academia to leverage the latest technologies, and support the formulation of informed strategies to ensure protection of critical infrastructure.

2.6 Role of education in building cyber awareness and resilience

(Odo, 2024) emphasizes that the digital age has woven a complex web, linking individuals' daily lives to the vast realm of cyberspace, spanning critical infrastructures such as power grids and financial systems to online communication and entertainment. The transition to digital world, has however, also unleashed a digital Pandora's box, exposing us to a relentless barrage of cyber threats and attacks with a sharp rise in the frequency and sophistication of cyberattacks. Empirical data indicate a persistent increase in malicious activity, with some reports estimating that cyberattacks occur every three seconds, translating to a staggering 26,000 incidents per day (Brooks, 2021). This surge of cyberattacks underscores the critical need for robust security measures. With threats continually evolving, and cybercriminals devising new methods to bypass defenses, makes protection of information assets increasingly complex. The paper observes that, given its extensive economic repercussions, cybercrime demands a comprehensive, multi-layered response to mitigate its growing impact.

According to IBM's 2024 Cost of a Data Breach Report (IBM, 2024), the global average cost of a data breach is estimated at \$4.88 million, a 10% increase from 2023. Skill

gaps were identified as the primary cause of breach. Healthcare sector, followed by financial firms had the highest average breach cost at \$375 million when 50 million records or more were compromised. The primary attack vectors were identified as stolen credentials followed by phishing attacks. These statistics highlight the immense financial burden cybercrime places on individuals, organizations, and governments. This study critically explores the contemporary cyber threat landscape, emphasizing the urgency to counter these vulnerabilities. By reviewing prior research and empirical investigations, the paper demonstrates the transformative role of comprehensive training and education in equipping individuals with knowledge, skills, and behaviors needed to recognize, mitigate, and respond to cyber risks in a dynamic digital environment. Through collective efforts by citizens, lawmakers, and other interested parties, digital assets can be safeguarded in an interconnected world. This research helps build a strong defense against the ever-changing threat landscape by combining findings from academic literature and empirical studies; and offers valuable ideas for designing and implementing comprehensive cybersecurity strategies.

(Burov *et al.*, 2020), examines the interplay between cybersecurity, digital education, and innovation in Ukraine's rapid digitalization. The study highlights that country's youth remain vulnerable, often targeted by cyber operations and are considered the weakest link in the system. Educational opportunities are crucial for fostering competence and talent; however, cybersafety awareness is limited by the lack of innovation in online classroom environment, where conventional measures fail to counter increasingly sophisticated attacks. To address these risks, the author proposes a generic model incorporating prompt defense, proactive and reactive threat hunting, and user resilience training. This model provides a standard framework that integrates cybersafety education and awareness to strengthen schools against cyber threats. Finally, the study underscores

the growing role of media in online learning. As individuals transition from being passive consumers to active prosumers in the digital environment, the media is changing into an information intermediary; facilitating educational access, enabling information, and supporting collaborative content creation, through platforms such as the creative commons.

The study by (Simola and Leppänen, 2025), highlights that new and more complex cybersecurity risks have emerged as a result of the rapid advancement of technology. Concurrently, there is a growing demand to improve comprehension of this ever-changing terrain. By training the workforce to recognize and report questionable emails and by improving security measures, organizations can develop policies and measures against perceived cyber dangers while still managing an adequate level of information security risks. The study emphasizes that, even though cybercriminals' tactics are often well-known and frequently reported in the media, the landscape of cybersecurity threats has remained relatively unchanged in recent years, and cyberattacks are becoming more sophisticated. Cybercriminals are becoming increasingly crafty and dangerous, testing the limits of human intelligence with methods like undetected zero-day vulnerabilities and social engineering. Cybersecurity experts are constantly on edge due to recent developments such as generative AI, changes in global geopolitics, and rapidly evolving ransomware campaigns. Through a comprehensive review of threat actor models, the study identifies emerging sources of threat in the context of European Union (EU). Findings from the survey highlight the significance of real-time data and recent publications in maintaining situational awareness, while also revealing major threat actors, new attack vectors, and key trends shaping the present cybersecurity landscape.

According to the research conducted by (Clark, 2022), A material civilization is giving way to what is more accurately described as an information civilization as a result of the rise of the information society. With digital technologies shaping every aspect of

life, new opportunities are emerging for social and economic growth. The internet is enabling new forms of work and learning that are changing the way society and businesses are structured. The work brings attention to the social effects of the information society's fast-paced development, specifically on the new online dangers that children and teenagers face, highlighting problems associated with the growing reliance on digital environments, particularly for younger generations that are more susceptible to online predators. The findings indicate that, everyone from parents and teachers to lawmakers and students should be informed of the dangers of cyberbullying. It stresses the need of education and legislation in protecting children and teenagers from cyberbullying and other forms of online abuse.

(Ayeyemi, 2023), presents a systematic examination of existing literature on cybersecurity education within K-12 settings. Given that adolescents increasingly rely on internet-enabled devices for both academic and personal use, it is essential that they develop a foundational understanding of cybersecurity and online safety. The study identifies that, despite the criticality, there remains limited clarity regarding formal requirements for cybersecurity instruction. To address the gap, the study employed a systematic literature review, drawing upon conclusions from four major scholarly databases like Scopus, Web of Science, ACM, and IEEE Xplore. Through a carefully defined inclusion and exclusion criteria, the study reviewed a substantial body of publications produced between 2012 and 2023. Findings reveal that cybersecurity has been integrated into K-12 school curricula through diverse student-centered pedagogical strategies, including game-based learning and project-based approaches. Workshops and online platforms emerged as the predominant environments for delivering these instructions. Methods that were uncovered for evaluating students' cybersecurity knowledge included quizzes, artefact collection, observation approaches, and self-

reporting questionnaires. However, the study highlights a notable absence of standardized evaluation tools capable of reliably measuring the effectiveness of cybersecurity education initiatives in enhancing students' knowledge.

These studies point to the critical role of education in fostering cyber awareness and resilience. In today's era, technology influences nearly every aspect of life, spanning from artificial intelligence to the Internet of Things, and redefining social, economic, and industrial landscapes. Along with this, threats are continually evolving as cybercriminals devise new methods of attack. These breaches not only result in millions of dollars in financial losses but also erode customer trust and confidence. Against this backdrop, education becomes essential in equipping individuals and organizations with the knowledge and skills needed to safeguard digital assets, adapt to emerging risks, and strengthen resilience in the face of an ever-changing cyber landscape.

2.7 From Growing Threats to Growing Talent: Aligning Education with Cybersecurity Needs

(Saxena *et al.*, 2012) defines cybersecurity as practice of implementing suitable technical and procedural safeguards to protect data and information systems, including databases, applications, networks, computers, and data centers. Technical solutions such as firewalls and antivirus software are necessary but as highlighted by the scholarly article, insufficient to guarantee security when it comes to personal data and computer networks. The article emphasizes on educating the population on the responsible use of cyber world. From an early age, students must be introduced to cyber-ethics, safety, and security, with emphasis on education, awareness, operations, and technology. The study highlights cybersecurity as a critical theme and outlines strategies for promoting awareness at the primary school level in India. However, it fails to capture current awareness levels among citizens and challenges faced by institutions in promoting digital safety awareness.

Similar findings by (Gaur, 2023) highlights initiatives at the primary and secondary school levels that employ strategies such as interactive workshops and classroom-based interventions to raise awareness. The study by (Statti and Torres, 2020), dives into examining and assessing recent studies on technology integration in community school curricula. It explores, current trends in online education and how community schools can integrate technology into their curricula. The essay considers potential collaborations between major tech corporations and community schools, and the benefits such alliances may yield. The study also examines the importance of technology education programs for parents and guardians, emphasizing the need for digital literacy among students and caregivers. Ultimately, it highlights how proficiency in digital skills can enhance family well-being, expand career opportunities, and support financial stability. These findings reinforce the importance of embedding cybersecurity within formal education while also drawing attention to the lack of standardized curricula and assessment tools.

Existing initiatives and policies related to Cybersecurity education

The study by (Shillair *et al.*, 2022), evaluates the role of cybersecurity education, awareness raising, and training (CEAT), in sustaining the vitality of internet services at the national scale. CEAT developed by the Global Cybersecurity Capacity Centre, represents one of the five dimensions within Cybersecurity Capacity Maturity Model (CMM), and is measured through indicators of education, awareness, and training. The article conducts cross-national research of CEAT's effects on internet use using comparative data from 80 nations. Considering controlling variables like national income and scale of internet adoption, the study demonstrates a positive and statistically significant relationship between CEAT initiatives and the vitality of internet services, while also revealing disparities in CEAT scores that highlight challenges faced by low-income and developing economies. A qualitative assessment of responses from these countries identifies

underlying reasons for varying levels of maturity. These includes: 1) Absence of a nationally coordinated awareness program; 2) Limited awareness at executive or board level; 3) Insufficient budgetary support; 4) Shortage of qualified cybersecurity educators; 5) Ongoing migration of skilled professionals; 6) High costs of professional certification; 7) Weak mechanisms for international knowledge transfer; 8) Language barriers between technical experts, non-specialists, and the general public; 9) Minimal involvement of community and local leadership. The literary article also proposes policies and practices to address the need for effective training, education, and awareness initiatives while acknowledging the limitations.

According to the paper published by (Catota *et al.*, 2019), safeguarding national critical infrastructure against cyberattacks requires a workforce equipped with appropriate knowledge and skills. While outsourcing or employing foreign experts may provide short-term relief, such measures are unsustainable and can introduce new challenges. Drawing on quantitative data from 28 semi-structured interviews with faculty and administrators across 13 Ecuadorian universities, the study identified present challenges in advancing cybersecurity education. Current initiatives in Ecuador tend to emphasize elementary-level instruction, with key obstacles identified being cybersecurity knowledge, organizational capacity, social cohesion, funding, and governance. The study argues for establishment of a national cybersecurity educational strategy supported by multi-stakeholder collaboration among academia, industry, and government. As suggested by the scholarly paper, complementary measures should aim to strengthen research and development, raise awareness, and improve teacher training and academic programs

Challenges in implementing structured Cybersecurity curricula

(Santos *et al.*, 2017) notes a significant rise in cyber incidents, some having severe consequences for governments establishments and organizations. The goal of cyberattacks

is to accomplish harm by taking advantage of various social and technological weaknesses to inflict damage, underscoring the need for skilled professionals with advanced knowledge of cybersecurity and cyber defense. As cyber threats intensify and training requirements expand, the research paper emphasizes the importance of institutionalizing agile learning methodologies within policy frameworks to ensure comprehensive cybersecurity awareness and preparedness. The paper underscores that, while cybersecurity and cyber defense training programs vary widely, many fail to adequately address the breadth and depth of learning and in linking training outcomes to career development. The paper proposes key considerations for structuring curriculum development for cybersecurity program at the graduate level.

(Knapp *et al.*, 2017) highlights the presence of extensive literature on developing cybersecurity curricula for Institutions of Higher Learning (IHL), underscoring the growing demand for guidance, maintenance, and improvement as more universities worldwide introduce such programs. Just as cybersecurity professionals must continually refine their skills to address evolving threats; academic programs must evolve to equip graduates with the competencies required for an ever-changing professional landscape. The paper emphasizes that, industry certifications play a crucial role in this process of upskilling individuals' knowledge; in turn, it also enables IHLs to keep curricula updated while also serving as key qualifications valued by employers. The study addresses a gap in the literature by examining the role of professional certifications in shaping and sustaining cybersecurity curricula. Through a literature review, it demonstrates how updates to industry certifications remain relevant for maintaining academic program quality. A case study of an undergraduate cybersecurity program at a mid-sized U.S. university is presented to illustrate this approach, with attention to experiential learning, and cybersecurity capstone courses. The paper observes that such an approach will provide

existing students with the necessary tools and study materials needed to successfully complete certification exams prior to graduation, thereby ensuring they enter the workforce with adequate skills and preparedness.

The scholarly article by (Mouheb *et al.*, 2019), highlights that, with the rapid rise of sophisticated and targeted cyberattacks worldwide, the demand for skilled and motivated cybersecurity professionals has become critical to prevent, detect, respond, and mitigate threats. Numerous undergraduate and graduate programs have been established, alongside initiatives by government and standard bodies such as NICE (National Initiative for CyberSecurity Education) aimed at shaping cybersecurity education. However, as noted by the paper, the interdisciplinary and often multidisciplinary nature of cybersecurity presents significant challenges for institutions in designing effective curricula. The article provides a comprehensive overview and comparison of existing curriculum design approaches, offering researchers and educators a consolidated perspective on current efforts. By synthesizing diverse approaches such as cybersecurity competitions, Virtualization, and education embedded with Gamification, the study underscores the importance of structured, adaptable, and comprehensive curricula that can evolve with emerging threats, while also offering recommendations for strengthening educational frameworks to build a capable cybersecurity workforce.

2.8 Global Practices in Cybersecurity Education and Training

(Parrish *et al.*, 2018) recognized the historical evolution of cybersecurity education, noting the growing demand for skilled professionals and the emergence of both traditional degree programs and alternative certification-based pathways. The author's conceptualizes cybersecurity as a “meta-discipline”, similar to “engineering” and “computing”. In other words, cybersecurity should be considered as an umbrella term that encompasses diverse sub-disciplines like computer science, law, ethics, policy, and risk management. The paper

emphasizes that by framing cybersecurity as a unifying discipline, a coherent educational structure that balances theoretical knowledge with practical skills can be developed, thereby ensuring the sustainability and maturity of cybersecurity education worldwide.

The study by (Armas and Taherdoost, 2025), emphasizes the growing vulnerability among institutions of higher education (IHL's) to cyberattacks, largely driven by social engineering attacks and human error. The research argues that awareness and training are critical to strengthen defenses; and to address these challenges, the authors propose a tailored Cybersecurity Awareness and Training Framework specifically designed for higher education; targeting students, faculty, and administrative staff. This framework derives from established standards such as NIST, ISO/IEC 27001, and CIS controls, while adapting them to the unique needs of academic environments. The study in essence, proposes a conceptual cybersecurity knowledge and training framework for higher education that embeds continuous awareness, training, and evaluation to build a sustainable security culture and enhance knowledge development, delivery method, and assessment across all institutional members.

Curriculum design, pedagogy, and assessment strategies

(Leat and Higgins, 2002), states that limited attention to teacher development has made it challenging to access how classroom practice have progressed since the introduction of the National Curriculum, despite rapid and frequent changes to the English and Welsh curricula. The study explains that strong teaching strategies, like asking questions, letting students explore, and talking about ideas, can change how schools' subjects are taught. As per the study, lesson instructions and engagement becomes better when teachers listen to students and use their feedback to improve curriculum content. Another study emphasizes that teachers can make lessons better when using smart teaching methods; for instance, teachers may help students understand ideas instead of memorizing

answers (Askew *et al.*, 1997). Together, these studies show that the way teachers teach, the subjects they plan, and the tests they give are all connected; and when done well, they help ensure that students learn in a deeper and more meaningful way.

(Al-Sharhan *et al.*, 2024) investigates the relationship between governmental support, organizational intentions, and the adoption of cybersecurity measures within the context of Kuwait. The study highlights that companies remain poorly equipped to counter the rising frequency and severity of cyberattacks, which can result in significant financial losses. Kuwait plans to upgrade and modernize its national infrastructure by 2035 to better support its citizens and communities. Using a quantitative approach, the authors demonstrate that both tangible and intangible benefits of cybersecurity adoption are strongly influenced by top level management support; offering policymakers a pathway to strengthen national cyber defenses and improving organizational resilience against evolving threats.

Taken together, these works illustrate that whether in traditional education or specialized fields like cybersecurity; curriculum design and organizational strategies must integrate pedagogy, leadership, and assessment mechanisms to ensure resilience, adaptability, and meaningful learning or performance outcomes.

2.9 Comparative Insights: India vs. International Approaches

The study by (Jacob, 2015), conducts sub-national comparative research on India and offers several recommendations for future inquiry. First, by carefully selecting sub-state regions allows for more valid conclusions about governance and the political economy of individual states, while also enabling cross-state comparisons. Second, the study emphasizes that more scope exists for intra-state comparisons that account for state-specific variables, identifying local context-specific factors that influence political and other outcomes. The study explains that researchers need to understand different types of

research methods and focus on a small number of cases to get meaningful answer; and suggests the use of numbers and statistics along with case studies to make the comparisons stronger.

(Thakur, 2023), in the research paper highlights that cybersecurity laws differ greatly from one country to another. This study compares and contrasts the cybersecurity legislation of several nations, including India, Japan, Germany, and Australia; focusing on issues such as data privacy, reporting cybersecurity incidents, and regulatory enforcement. The study goal was to identify each country's cybersecurity laws, their strengths and weaknesses, with the objective of enabling India to draw lessons from these experiences and enhance its own legal framework. The authors argue that aligning Indian laws with global best practices would strengthen resilience against cyber threats. The study concludes that effective cybersecurity governance requires not only robust legislation but also coordinated implementation, awareness, and international cooperation.

In the research study by (Ismail *et al.*, 2024), the authors highlight that cybercrime has emerged as a pressing global concern, and there is a growing need for cybersecurity experts who can identify, prevent, and mitigate the impact of cyberattacks. Governments and educational institutions have introduced specialized programs across schools, undergraduate, and master level programs; yet, there is a shortage of trained cybersecurity experts around the globe. The study observes that, as cyberattacks intensify, success in this domain requires interdisciplinary expertise and the integration of cybersecurity education not only within computer science but also across business, industry, and public policy, supported by standardized curricula to enhance adaptability. The paper provides a comparative examination of existing cybersecurity curriculum across multiple countries, revealing that while developed economies like Europe and North America rely on regulation and innovation, emerging nations such as Asia and Africa adopt adaptive,

community-based approaches, highlighting the need for integrated frameworks that balance technological advancement with socio-cultural adaptability.

Scholarly analysis by (Mishra, 2024), points to the fact that, as digital landscape has become increasingly integral to education, the need to incorporate cybersecurity education into school curricula has become more critical than ever. This study reviews best practices and case studies across educational levels, highlighting strategies such as interdisciplinary learning, project-based approaches, and industry collaboration. While emphasizing the role of educators and the need for professional development, it also identifies challenges including curriculum overcrowding, the digital divide, limited awareness, and lack of standardized guidelines. Overall, the paper underscores both the urgency and complexity of embedding cybersecurity education to equip learners with the tool and skills in an ever-growing world of digital threats.

As per the scholarly literature by (Tiwari and Dhiman, 2025), in today's digital era, where students increasingly depend on digital tools; safeguarding of educational institutions is very essential, and instructors play a key role in modelling cyber hygiene best practices. The study highlights the need to embed cybersecurity awareness into teacher training programs. This research looks at worldwide trends, gaps in the curriculum, and best practices for teacher readiness for digital safety using secondary data from scholarly articles, policy papers, and government publications. The findings reveal that pre-service teachers do not receive enough formal cybersecurity training, and suggests that, integrating dedicated cybersecurity courses into teacher education programs is essential to equip educators with the skills needed to address classroom cyber threats effectively.

Investigation conducted by (Kumar, 2024), provides a critical overview of India's cybersecurity landscape, tracing policy developments since the 2013 National Cyber Security Policy. It notes that amid rapid digital expansion through initiatives like Digital

India and Aadhar, there has been a significant rise of threats like ransomware, data breaches, and attacks on critical infrastructure. The study examines challenges in policy enforcement, stakeholder coordination, and the pressing need for public awareness and workforce training. By comparing India's policy measures with global best practices, including US frameworks and GDPR driven models, the paper suggests a forward-looking strategy emphasizing stronger regulations, sector specific guidelines, capacity building, and enhanced law enforcement to safeguard national digital infrastructure.

To conclude, comparative analysis reveals that while intra-state cybersecurity awareness remains uneven, valuable lessons can be drawn from international curriculum design, and legal frameworks and adapted to the Indian context. Success in this domain requires interdisciplinary expertise, with cybersecurity education integrated across computing, business, industry, and public policy through standardized curricula. Forward-looking strategies having stronger regulations, sector-specific guidelines, teacher readiness in digital safety, capacity building, and enhanced law enforcement to build a resilient national ecosystem needs to be implemented.

2.10 Current landscape of Cyber Safety in Schools

Schools are frequent targets of data theft, with cybercriminals often preferring children's personal information due to its high value in the dark web (Luna, 2021; Wilson, 2019). The value of stolen data can begin at just 1USD per record (Reisinger, 2016), making it highly lucrative for cybercriminals. This information can be used to open lines of credit or commit identity theft, and blackmail often leaving victims and their parents unaware. To exacerbate the issue, teaching staff show a lack of enthusiasm for teaching cybersecurity because of their insufficient understanding and schools typically lack the necessary frameworks, guidance, and support from government and industry experts to establish effective cybersecurity programs and practices.

Researchers have identified that humans are the weakest link in the security chain because human error, such as falling for scams, using weak passwords, or failing to apply security updates, can easily compromise even the most robust technical defense. The study by (Ricci *et al.*, 2019) in New Haven (CT. USA) highlights the necessity of joint seminars and workshops for parents and teachers to learn safe internet and mobile app practices. These sessions would educate on avoiding unsafe behaviors and accessing the safety of online activities. The study recommends for schools or local government bodies to sponsor seminars on home computing and cybersecurity concepts.

(Pusey and Sadera, 2011) explains Cyberethics, Cybersafety and Cybersecurity (C3) are three overlapping domains of knowledge. Cyberethics involves the moral choices individuals make while using internet technologies and digital media, addressing issues such as copyright, online etiquette, and hacking. Cybersafety encompasses actions to minimize dangers like online predators, viruses, and spyware, and includes awareness of how unsafe behaviors can spread malware and facilitate phishing or spoofing. Cybersecurity employs technical measures like antivirus software, firewalls, and password protection to safeguard data, identity information, and hardware from unauthorized access.

Human knowledge on safe digital practices is considered as the first line of defense. Raising awareness and knowledge is a crucial step towards cybersecurity, as technological defenses alone are not adequate to protect individuals or companies from online threats (Taherdoost, 2024). The C3 domains are often seen as the responsibility of others, with Cyberethics typically handled by parents and teachers, while the IT department manages cybersecurity. However, it is essential to recognize that raising awareness is a shared responsibility between individuals, educators, industry experts, and the government. This effort should commence with educating teachers and parents, who can then instill a culture of cyber awareness in students from an early age.

A child's education begins at home, under the guidance of parents, family members, and caregivers. Children often mimic the behaviors and activities they observe around them. Participating in educational activities with parents, such as reading books and using computers, supports cognitive development (Quayyum, 2024; Lauricella *et al.*, 2014). As such, family interactions provide a foundation for learning about online safety and appropriate behavior. In the digital space, parents and children do not necessarily work together, however, without adequate guidance from adults, children may struggle to independently understand Cyberethics due to their different maturity levels and cognitive abilities.

A survey by (Olmstead and Smith, 2017), revealed that many Americans lack awareness of key cybersecurity topics. While most could identify strong passwords and recognize public Wi-Fi, they were unfamiliar with two-factor authentication and website encryption. Additionally, (Abela, 2017) found that 80% of Americans admitted to risky behaviors such as using unsecured networks, clicking unfamiliar social media links, downloading files from third-party sources, opening unsolicited email attachments, and reusing passwords. The findings also indicated poor cybersecurity practices among adults, especially online shoppers. This puts students, adolescents and adults at risk exposing them to potential cybercrimes and compromising their online safety such as identity theft, exposure to inappropriate content, and cyberbullying. Educating adults on cyber-behavior is equally crucial for creating a safer digital environment for younger generations.

(Tsado, 2019) opined that US schools should leverage all available resources to attract and develop cybersecurity talent. This includes collaborating with local organizations and cybersecurity professionals to offer training, conduct seminars, and provide internships, and employment opportunities. The partnerships will ensure a steady flow of school talent into institutes of higher learning. These efforts will help cultivate a

dynamic cybersecurity community. (Chen *et al.*, 2021) identifies the rising number of cyberattacks and the shortage of cybersecurity professionals necessitate educating adolescents and children about cybersecurity in the US. Engaging and educating K-12 students in cybersecurity will likely boost university-level enrollments in this field. However, teachers face challenges in implementing effective education due to the lack of age-appropriate teaching materials and curriculum for K-12 students.

(Ige, 2020) analysis identified that South African citizens, including children lost \$7.45B to cybercrimes between 2014 and 2018. The security agencies trained in an analog era, faced challenges in tracing these incidents due to the anonymity provided by the internet. In the context of South Africa, (Venter *et al.*, 2019) advocates the need to treat cybersecurity and not merely Information and Communication Technologies (ICT) as a foundational skill alongside the basic “three R’s (reading, writing, and arithmetic)”. ‘Space Transition theory’ an idea proposed by (Jaishankar, 2007) points out that individuals are clueless when movement happens from one space to another (physical to cyber-world) and would exhibit conforming / non-conforming behaviors in these spaces particularly when interacting with anonymous individuals on the other side of planet using digital devices. These findings highlight the financial toll of cybercrimes and how a lack of cyberethics knowledge can drastically affect people’s lives and safety.

According to (Jerman Blažič and Jerman Blažič, 2022), cyber policy in UK allows to incorporate cyber-awareness education for students, starting at the age of 11. European High Educational Level (HEI) programs focus mainly on traditional cybersecurity topics as part of classical academic courses, and modern learning methods with hands on training that helps in building skills have been left behind. Similarly, as identified in the analysis by (Corradini and Nardelli, 2020), Italian school teachers' perceptions of their students' digital awareness found that students need to be educated on recognizing risks associated

with digital device usage. Student focus should be targeted towards protecting sensitive personal data and verifying the reliability of news on social media. Additionally, teachers expressed a desire for specific training in digital awareness to better support student learning. The findings suggest the need for a more inclusive approach to cybersecurity education so that adolescents, teachers and parents can navigate the digital world safely and responsibly.

(Kant, 2023) investigated cybersecurity awareness in India among students of higher education based on demographic and educational background such as gender, place of residence, level of study etc. revealing no difference regarding cyber-awareness based on gender. However, significant differences were observed based on residential location and academic disciplines, with students in urban areas demonstrating higher cybersecurity awareness compared to those in rural areas. According to (Kemp, 2024), population of India crossed 1.44 billion in Jan'2024 with 48.4% female and 51.6% male population. 36.6% of India's population lived in urban areas and 63.4% in rural areas, and 29.9% of the population are below 18 years. Internet penetration as per the report stood at 52.4% with more than 751 million internet users. Additionally, as report by (AAG, 2024), India experienced 212,485 cybercrimes in the first two months of 2022, surpassing the 208,456 cybercrimes reported for the entire year of 2018 with most of these cybercrimes relating to financial fraud. Findings by (Kant, 2023) also identifies that many Indian users are unaware of whom to contact or complain in the event of cyber fraud. These statistics warrants examining digital conduct among Indian students, given their high usage of digital devices and vulnerability in cyberspace.

Below is a compilation of prominent cybersecurity incidents worldwide that have caused service disruptions as well as theft of highly sensitive data from businesses, government agencies, and educational institutions.

1. In January 2023, the UK's postal service, Royal Mail, was targeted by the ransomware LockBit, leading to a temporary suspension of international deliveries. Royal Mail refused to pay the \$79.85M ransom suffering significant financial losses and spent approximately \$12.44M on ransomware remediation.

2. T-Mobile disclosed in Jan'2023 that 37 million customers' personal and account information was accessed in a malicious API attack. Additionally, another breach affecting personal and account data occurred in Feb / March 2023. These incidents have left millions of customers' data vulnerable to digital fraud.

3. British Library's online services were hit by ransomware attack in Oct'23. Forensic analysis revealed internal HR data was stolen and offered for sale on dark-web.

4. A North Carolina man in Sept'24 was charged with stealing royalties by using AI generated fake songs and listeners over listening platforms like Spotify and Apple music. This is the first criminal case involving AI generated music.

5. CrowdStrike's Falcon threat detection platform caused millions of Windows systems experiencing blue-screens of death and entering reboot loops in Jul'24. Major industries like airline services and healthcare organizations were impacted; with Delta airlines suing CrowdStrike for \$500M in damages.

6. In Aug'24, the Toronto District School Board (TDSB) reported that a LockBit ransomware attack compromised the data of 235,000 students, including names, email addresses, and dates of birth. Similarly, a ransomware attack on Highline Public Schools (Washington State) in Sep'24 led to the compromise of 17,500 students' data.

7. A 39-year-old software engineer lost 118M rupees to fraudsters within 18 days of digital arrest in Bangaluru (India) in Nov'24. The caller identified himself as senior police officer in Mumbai and that the victim's Aadhar (similar to SSN) card was used to

open bank accounts for money laundering and warned him of physical arrest if he does not cooperate with virtual investigation.

8. In Oct'23, cybersecurity agency Resecurity reported that Aadhar and passport details of 800 million Indian citizens were being sold in dark web for \$50,000.

These high-profile events highlight the critical need for improved cybersecurity policies and training in order to protect digital assets and preserve financial integrity in the face of expanding cyber threats (Francis *et al.*, 2024; Safitra *et al.*, 2023).

Federal Bureau of Investigation (FBI) has set-up an Internet Crime Complaint Centre (IC3), that allows the public to directly report a cybercrime. IC3 reported a total of 880,413 complaints received in 2023 from American public with potential loss exceeding \$12.5 billion (FBI - Internet Crime Complaint Center, 2023). This was a 22% increase in losses compared to 2022. Crimes incurring the greatest monetary losses encompass investment scams, Business Email Compromise (BEC), Tech Support / Government Impersonation scams, Personal Data Breach, Phishing and ransomware incidents. The IC3 report also highlighted that it received 18,174 complaints from people aged under 20 with losses over \$40.7 million. According to this report the top 5 countries from where IC3 received complaints includes – US, UK, Canada, India and Nigeria. These statistics emphasize the vital importance of cybersecurity awareness in the contemporary internet age, especially considering the potential for substantial financial losses.

The extensive collection of research unquestionably underscores the critical importance of cyber-hygiene awareness. The greater part of existing academic literature focus on schools in the US, UK. and South Africa, highlighting the significance of cybersecurity education measures in these regions. However, there is a notable lack of research focused on reach and impact of cybersecurity programs in the Indian subcontinent. This underscores the pressing need for targeted studies that address the unique challenges

and requirements of implementing effective cybersecurity education in this diverse and densely populated region. Addressing this research gap is crucial to ensure the development of tailored, effective cybersecurity strategies that can safeguard students and educational institutions in India.

2.11 Cybersecurity Governance Frameworks in Education

According to (Pusey and Sadera, 2011), US has two federal laws that affects K-12 education. The Children's Internet Protection Act (CIPA) mandates that schools implement comprehensive Internet safety policies and use filters to shield students from harmful content. The Broadband Data Improvement Act (2008) requires schools to educate students on proper online conduct. Additionally, the National Educational Technology Standards (NETS) insist on incorporating C3 content in educational curriculums. However, these guidelines often lack specificity and clear directives. Furthermore, the responsibility of providing C3 education falls heavily on schools, which face challenges not only due to teachers' limited knowledge in this area but funding challenges as well.

Similar research report by (Childers *et al.*, 2023; Yan *et al.*, 2021) have identified that teachers and students are a vulnerable group in relation to cyber-attacks and to compound to that cybersecurity education and awareness for K-12 teachers are limited. (National Initiative for Cybersecurity Careers and Studies, 2024; National Institute of Standards and Technology (NIST), 2023; Childers *et al.*, 2023) states that there is a national imperative to secure, protect, and continuously enhance current cybersecurity measures affecting educational initiatives in US. These efforts aim to address the need for developing and maintaining a robust cybersecurity workforce while also fostering a cyber-literate citizenry. The study suggests that the key to cyber workforce development is professional development of K-12 teachers' cybersecurity awareness and the ability to teach cybersecurity lessons.

As per a paper published by (Luna, 2021), in US, there are legislative process that tangentially affects schools' cybersecurity efforts. Family Education Rights and Privacy Act (FERPA) require schools to keep certain student information confidential and establishes the students and parents' rights to know the purpose and location of PII that educational institutes keep as part of their records (American Psychological Association (APA), 2012). Additionally, the Computer Fraud and Abuse Act (CFAA) criminalize cyber-data theft, so that people who steal data (names, addresses, phone numbers, parents' name, SSN's and school issued ID's) from schools could be prosecuted under the act (National Association of Criminal Defense Lawyers (NACDL), n.d.). Despite the seemingly remedial language of the statutes, in practice, they offer little relief to victims of data theft.

Certain states in US have developed their own legislation. Texas acknowledges the necessity for schools to address cybersecurity, yet the statute's language merely identifies this need (Luna, 2021; Goud, 2020). Questions persist about how schools should assess cybersecurity risks and develop mitigation plans, as effective risk mitigation is unattainable without known and documented risks. Virginia's cybersecurity bill parallels Texas's in substance, additionally requiring the Department of Education to appoint a Chief Data Security Officer to assist school districts in developing cybersecurity plans. In California, students are assigned an identification number instead of collecting SSNs, which is a positive step. Even if a student ID is exposed, which is not linked to SSN, the data is less useful to cybercriminals. If SSN data were available, the consequences could be catastrophic (Levinson, 2012).

The U.S. also has a CyberPatriot cyber education program (Ricci *et al.*, 2019) with focus on educating high school and middle school students at no cost, with the goal of sparking interest in cybersecurity careers. This program addresses the shortage of skilled

cybersecurity professionals in the country while also teaching students essential self-protection strategies in a connected world. Also, there is ‘Cyber Teacher’ certification program (cyberteachers.org) that helps teachers in grades 6 - 12 add cybersecurity lessons to their curriculum. Similarly, The National Integrated Cyber Education Research Center (NICERC) aims to develop cyber-based curricula for K-12 teachers in the United States. While there are multiple initiatives to address shortage of skilled cybersecurity professionals, it is also essential to educate an everyday internet user as many of us spend a lot of time in the cyberspace by browsing, for work or other online activities.

European commission in 2019 had setup cybersecurity competence centers – Concordia and Cybersec4Europe with the focus of re-shaping cybersecurity educational ecosystem (Jerman Blažič and Jerman Blažič, 2022). The Concordia consortium consists of 52 partners with representation from industry experts, European Universities and research centers with the purpose of addressing needs to “teach the teachers” by providing knowledge about the content and delivery methods of sustainable education among the high-school community. As part of the study a survey and subsequent interviews were conducted with teachers, students, parents, and high-school management representatives. The results (Cutas *et al.*, 2023; Jerman Blažič and Jerman Blažič, 2022; Hassan *et al.*, 2019) were alarming as majority of high-school students reported of experiencing online risks and they never discussed this with their parents or teachers. The findings reveal a high interest in cybersecurity education among teachers, parents, and students. The fact that most participants reported experiencing online risks underscores the urgent need to educate minors on online security and safety. Equipping the students with comprehensive cybersecurity education will help them navigate the digital ecosystem safely and protect them from potential threats.

In a similar vein, Italy as part of their efforts to digitally sensitize school students has developed 'Programma iL Futuro' project (Nardelli and Corradini, 2019) with a goal to increase cyber awareness based on scientific principles of digital technologies and on concepts of their responsible use. The objective is to arm young individuals with the knowledge and skills they need to recognize and respond to online dangers.

Indian government has established Computer Emergency Response Team (CERT-In) with the purpose of issuing guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents. CERT-In reported (India Today, 2024) more than 10,000 cyberattacks targeting educational institutions resulting in data breaches, financial losses and disruptions to educational services. The government has undertaken several initiatives to bolster cybersecurity in education sector including National Policy on Education (NEP) 2020, The Cyber Safety and Hygiene Awareness Network (CSHAN), and the Cyber Surakshit Bharat Mission. The initiatives aim to integrate cybersecurity awareness into school curriculum and raise awareness among students, parents, and teachers through workshops, training programs, and online resources. Despite these efforts, there is a lack of documented evidence on the effectiveness of these policies in enhancing cybersecurity awareness and practices in educational institutions. Research studies and media reports have yet to provide comprehensive evaluations of these initiatives, highlighting the need for more rigorous assessment and documentation of their impact.

2.12 Best Practices for Cyber Safety Curriculum Design

Cybersecurity spans a wide range of specialties and roles, making it impossible for a single educational program to cover all necessary skills. However, some fundamental knowledge and skills are essential for daily life, academic pursuits, and critical job functions in our digital society. Contemporary young generation can easily navigate the

latest cellphones without consulting the instruction manual, this does not mean they possess comprehensive digital literacy. Just as children are taught basic safety principles like “Don’t talk to strangers or take gifts from them”, “Always wear a helmet while biking or skating”, and “Look both ways before crossing the street”, similar approaches can be taken to instill a sense of digital safety and responsibility. Here, teachers and industry professionals have an important role to play in spreading awareness within the community about the safe and responsible use of internet-capable digital devices.

A study was executed as part of the AGENT (Advancing GenCyber Education for North Georgia Teachers) initiative involving K-12 teachers participating in a cybersecurity education workshop funded by the National Security Agency (NSA). The workshop included trainings on Confidentiality, Integrity and Availability (CIA), Think Like an Adversary, Defense in Depth (introduction to firewalls, reverse engineering), and Keep it Simple (programming principles and cryptography). Teachers assessed their self-confidence before and after the workshop, and the study (Childers *et al.*, 2023), revealed increase in self-confidence post-workshop. The findings indicate that professional development programs designed to enhance K-12 teachers’ cybersecurity knowledge can significantly contribute to creation and implementation of cybersecurity-related lesson plans benefiting both students and the broader community.

A study by (Pusey and Sadera, 2011) reveals that many teachers possess limited knowledge of C3 content and lack confidence in their ability to effectively model and teach this subject. This situation necessitates intervention not only from school administrators but also from the government and industry experts, to not only design a robust school curriculum but also allocate necessary funds for establishing computer labs. On similar lines, (Corradini and Nardelli, 2020) identified that teachers sometimes misuse terminologies related to cyberspace, (Chase *et al.*, 2020) also accentuates that teachers

often have no access to isolated computing networks required for hands on exercises in security. Therefore, it's crucial to develop training programs aimed at enhancing teachers' cybersecurity skills and ensuring they are well-equipped to support their students' learning journey.

In the past decade, concern about children's online etiquette and cybersecurity has received significant attention in the child-computer interaction (CCI) community. (Quayyum, 2024; Hartikainen *et al.*, 2016) proposes that involving children as co-designers can provide valuable insights for researchers, enabling them to create educational resources that effectively teach complex and diverse cybersecurity and privacy concepts. Consequently, there is a pressing need to focus on integrating children into the design process of these educational resources.

Numerous multimedia educational tools, such as games, comics and various training materials, have been created to enhance children's knowledge of security and privacy (Zhang-Kennedy and Chiasson, 2021). However, researchers often question the extent of children's participation in developing these resources and their effectiveness in engaging children in cybersecurity learning (Kumar *et al.*, 2018). As noted by (Quayyum, 2024), involving children in co-creation and design of educational resources is essential for developing relatable and effective solutions. One effective approach to achieving this is through storytelling.

Storytelling is a method that helps to promote imagination and creativity among children (Garzotto *et al.*, 2010), develops confidence and contributes to enforcing their relationships with peers and adults. (Kumar *et al.*, 2018; Quayyum, 2024) explored the Choose-Your-Own-Adventure (CYOA) scenario-based storytelling method to understand thoughts of Norway's children aged 9-12 years, about adult's role in given cybersecurity scenarios to understand how they perceived associated risks and possible consequences.

These scenarios include “a children finds a smartphone on the playground”; “a parent identifies that a game installed on her daughter’s mobile is sending a lot of information to other people” or “a children goes to a nearby donut shop where a stranger starts asking a lot of personal details”; and this set-up tried to identify how the children conceptualized the situations and perceived the risks. The study reveals that children often lack a comprehensive understanding of their actions and their consequences; and look up to their parents or the law-enforcers for guidance. It recommends a collaborative and participatory mediation approach between parents and children, to design cybersecurity instruction materials that a student can relate with. While the study provides valuable insights, its findings are limited by the sample size of 10 children, all of whom were recruited from a local technology club. Expanding the participant pool and including diverse perspectives would provide a more comprehensive understanding of the factors influencing effective cybersecurity education.

Based on survey followed by interviews conducted by (Jerman Blažič and Jerman Blažič, 2022) involving European high-school students, parents and teachers, the findings revealed that students identified some key topics for inclusion in the curriculum. This suggests the importance of co-designing programs with students as key stakeholders. Topics encompass “Being safe in online social platforms, “Recognizing fake accounts”, “Ensuring privacy in online activities”, “Creating strong passwords”, and “Using email applications in a secure way”. Participants expressed a preference for delivering cybersecurity content through educational videos and serious games, such as Target Attack, Permission Impossible, and Keep Traditions Secure. These methods were deemed most effective for high school students as by incorporating multimedia and gamification into the curriculum, educators can better capture students’ attention and foster a deeper understanding of online safety practices.

Cybersecurity programs can get very costly to implement - especially for schools with poor infrastructure, a lack of teaching materials, and limited funds; but the cost of identity theft and rectifying damages done by cybercriminals is even more expensive (Luna, 2021; Chatlani, 2017). The primary objective of cybersecurity awareness programs should be to enable students to better understand the environment where they interact every day or where they will act in future.

For K-12 cybersecurity education (Chiou *et al.*, 2021; Chen *et al.*, 2021) advocates six teaching methodologies for educationalists and students alike:

1) Problem-based learning: this teaching method stimulates students to learn concepts and principles to discover new knowledge and solve a set of cybersecurity problems.

2) Project-based learning: this teaching method lets students actively engage in real-world cybersecurity projects; such hands-on learning strengthens teamwork and problem-solving skills.

3) Game-based learning: this teaching method increases student's interest in single-user / multi-user gaming environments like Capture the Flag (CLT) and support collaborative learning.

4) Inquiry-based learning: in this learning, the problem is usually open-ended and starts by raising questions, problems and scenarios like "a children finds a smartphone on the play-ground, what should he/she do?"

5) Emerging-technology-based learning: this teaching process is incorporated with emerging technologies like AI and Virtual reality.

6) Case studies: using case-studies can help students understand the scenarios of real-world and also help distinguish genuine against the deceptive content.

(Bishop *et al.*, 2017) suggested curriculum design for K-12 cybersecurity education should include six essential knowledge areas:

1) Data Security: focuses on static data and dynamic data, and the teaching content should include encryption / hashing to protect data privacy.

2) Software Security: students should be able to protect software against malicious attack; and it focuses on design, development and implementation of software that meets security requirements.

3) System Security: it focuses on security of computer systems and supporting network infrastructure.

4) Human Security: focuses on protection of people's data in the context of an organization, personal life and their privacy.

5) Organizational Security: focuses on rules or procedures to protect organizational sensitive data.

6) Societal Security: focuses on ethics, cyber laws and regulations on cyberspace processes and technologies.

Such well-designed curriculum allows educators to plan sequenced courses or projects that target desired learning outcomes, ensuring students develop a solid foundation. However, as well pointed out by (Corradini and Nardelli, 2020) considering the age of the students, it may not be appropriate to talk about cybersecurity, instead it would be appropriate to talk about 'digital-awareness' or 'digital-hygiene'.

According to the Census 2011, India had 123 major languages (Translators without Borders, 2020), with English predominantly used in higher education and certain governmental areas. Hindi and Bengali are also widely spoken among the population. The student population is distributed across urban, semi-urban, and rural areas, where English may not be the primary language of instruction. Furthermore, there is a notable gender gap

in literacy, with an adult male literacy rate of 82.1% compared to 65.4% for adult females. Given this diversity, delivering cybersecurity education through a single medium poses significant challenges. Central and State governments need to develop multi-lingual and inclusive educational strategies that consider the linguistic and geographical diversity of the student population. These strategies should aim to bridge the literacy and gender gaps by making digital literacy initiatives accessible and comprehensible for all.

The governments should collaborate with educational institutions to ensure that teaching materials are available in multiple languages and tailored to different literacy levels. Additionally, they should leverage community resources, such as local leaders and influencers, to spread awareness about cybersecurity in ways that resonate with the diverse population. By adopting an inclusive approach to cybersecurity education, it will be possible to equip India's youth to navigate the digital world safely and responsibly, ultimately fostering a more secure and informed society.

2.13 Summary

This chapter offers a comprehensive review of the literature on high school-level cybersecurity education, situating India in the broader international context. It starts with the theoretical background, applying Space Transition Theory (STT) to interpret behavioral change in cyberspace and Self Determination Theory (SDT) to highlight student motivators in cybersecurity learning. The chapter then explores the concept of cybersecurity education emphasizing its importance in the digital era and its growing role in schools as foundation for awareness, resilience, and responsible digital citizenship.

The Indian context is then examined through policies such as NCSP, Digital India, and Cyber Surakshit Bharat, alongside challenges including limited teacher training, weak curricular integration, and lack of awareness among students, educators, and parents. The chapter then explores international practices such as those implemented in USA, UK, South

Africa, and Singapore emphasizing innovative pedagogy, structured curriculum design, and government industry partnerships. Comparative analysis highlights India's strengths and shortcomings, offering insights into potential reforms.

The comprehensive literature review encompassing multiple countries unequivocally underscores the significance of cybersafe behavior and awareness, highlighting that achieving this through cybersecurity education from an early age is imperative for creating a safer environment for children and adolescents. This will also help raise interest among school students to pursue higher education in the field of cybersecurity, eventually ensuring to remediate the gap in cybersecurity workforce by addition of skilled resources.

Most Indian research focuses on higher education or general digital literacy, with limited attention to policy design, implementation, and stakeholder engagement at the school level. A study was also conducted by (Kant, 2023) to investigate cybersecurity awareness among students of higher learning; but none of these studies address the need for cybersecurity education for Indian high-school students. Although, Federal and State governments in India have undertaken multiple initiatives for raising cybersecurity awareness among school students, parents and educationalists; the reach and impact of these initiatives remain undocumented across research studies and media reports. As concluded by (Yashwant, 2021) very less research has been devoted towards cybersecurity education for high school students and school staff in India.

This underscores the pressing need for studies targeted towards Indian high-school students and address the unique challenges and requirements of implementing effective cybersecurity education in this multilingual and densely populated country. Addressing this research gap is crucial to ensure the development of tailored, and effective cybersecurity strategies that can safeguard students and educational institutions in India.

CHAPTER III: METHODOLOGY

3.1 Overview of the Research Problem

Cybersecurity has emerged as a critical global concern, affecting individuals, institutions, and governments alike as digital connectivity expands (Admass *et al.*, 2024). Educational institutions, particularly schools, represent a vulnerable group due to their extensive reliance on internet-based technologies. Despite rapid technological advancement in learning environments, the integration of structured cybersecurity education within schools remains insufficient (Alnajim *et al.*, 2023). Educational institutions, including schools and universities, are increasingly exposed to sophisticated cyberattacks that exploit network vulnerabilities, compromise sensitive information, disrupt operations, and impose financial or reputational costs through ransom demands. Students face heightened risks of phishing, malware, data breaches, and online fraud, threatening both personal and institutional security. The problem is compounded by limited awareness among parents and educators, who play a crucial role in fostering safe online behavior (Panjani and Mudgal, 2025).

The challenge extends beyond the absence of a formal curriculum and includes weak government policies, inadequate school infrastructure, and limited stakeholder awareness. As noted by (Frank *et al.*, 2023) without coherent regulatory support, schools often lack the resources, trained staff, and standardized materials needed to deliver effective cybersecurity education. Addressing these gaps, alongside the limited awareness among students, parents, and educators, is essential to designing interventions that safeguard future digital citizens (Althibyani and Al-Zahrani, 2023).

Globally, several nations have introduced formal K-12 school cybersecurity programs with structured curricula and awareness initiatives; though their effectiveness,

accessibility, and scope vary widely (Pencheva *et al.*, 2020). In India, although digital literacy initiatives have gained significant momentum, cybersecurity education at the school level remains underdeveloped and lacks effectiveness, leaving a critical gap in preparing students for the challenges of the digital age (Jawaid, 2023). This gap underscores the urgent need for comparative research to identify best practices from international models that can be adapted and implemented within local education systems.

3.2 Operationalization of Theoretical Constructs

Operationalization refers to the process of specifying how abstract concepts and theoretical constructs of a study are operationalized or measured. The major theoretical constructs in this study are the cybersecurity awareness, the effectiveness of education, policy support, and stakeholder engagement (Ojha and Chattopadhyay, 2025). All these constructs have been meticulously converted to quantifiable variables so as to make the objectives of the study to be systematically discussed. In general, operationalization of cybersecurity awareness based on indicators includes the knowledge of students about online threats, safe internet usage, strong password practices, and responses to cyber threats (Verma and Pawar, 2024). The indicators are assessed using structured questionnaires with Likert-scale items, where a score of (1) represents minimal awareness and a score of (5) reflects the highest level of awareness.

Another key construct is educational effectiveness, which refers to the ability of high school programs to provide students with practical cybersecurity skills. As digital systems underpin modern life, cybersecurity is essential to protect information and infrastructure. The construct is operationalized by exploring the comprehensiveness of the curriculum, methods of teaching, access to resources and practical learning experiences (Saarsar, 2018). The indicators have been derived from secondary sources within the study's international comparative scope, including policy documents, program reports, and

academic literature. Policy support was operationalized through evaluation of existing government directives, regulatory frameworks, and funding mechanisms aimed at strengthening cybersecurity education. The study will thereby be able to uncover shortcomings and potential improvements across policy and practice (Hossain *et al.*, 2025).

Finally, a critical dimension of cybersecurity awareness is stakeholder involvement, with educators, parents, and students playing central roles (Aaltonen *et al.*, 2024). Frequency of interactions, awareness program participation, and perceived responsibility in cybersecurity serve as survey measures of this construct (De Bruijn and Janssen, 2017). These theoretical constructs were clearly defined and operationalized in the research, enabling abstract concepts to be translated into empirical measures for effective data collection and robust statistical analysis, thereby enhancing the degree of reliability, validity and yielding recommendations supported by quantifiable data.

3.3 Research Purpose and Questions

Focused on high school education, this research aims to compare international and Indian cybersecurity initiatives to determine adaptable and scalable frameworks and actionable best practices for Indian educational setting (Mohanty *et al.*, 2024). The research not only reviews the structure of cybersecurity programs internationally but also evaluates their role in promoting student awareness, skills, and responsible internet usage (Shillair *et al.*, 2022). The assessment of global practices will serve as a basis for gauging weaknesses in Indian high school curricula and development of actionable, evidence-based, and locally relevant reforms.

Furthermore, the research highlights the need of stakeholder knowledge and involvement in the process of establishing cybersecurity education and awareness. The research investigation used a sample of high school students, parents, and educators across different states in the country to gather primary data, in an attempt to ascertain the sensitive

state of cybersecurity understanding as well as opinions among these important demographic groups. Combining these experimental findings with other comparable global outcomes supports the study's conclusion that interventions should be adopted at most levels, such as curriculum design, teacher preparation, policy support, and awareness-raising. Finally, the study aspires to reduce student susceptibility to online threats, enhance digital literacy, and equip policymakers and educators a structured roadmap for integrating cybersecurity education into schools.

Research Question(s)

1. **What** are the strengths and weaknesses of cybersecurity education programs in different countries, and how can these inform improvements in Indian high schools?
2. **Which** teaching methodologies, resources, and curriculum designs used internationally can be effectively adapted to the Indian context?
3. **What** role do government policies and regulations play in promoting cybersecurity education at the high school level in India?
4. **What** is the current level of cybersecurity awareness among high school students, parents, and educationalists across India?

3.4 Research Design

To explore the challenges of imparting cybersecurity education in high schools, the study employs a mixed-method strategy by blending qualitative insights with quantitative data (Beauchamp and Matusovich, 2022). This study adopts a mixed-methods approach since it enables the researcher to take the advantages of qualitative information and the power of quantitative analysis.

The qualitative dimension is achieved through a systematic review and content analysis of international and Indian literature including scholarly articles, policy

documents and reports of reputed bodies (Oranga and Matere, 2023). Through an analysis of international programs, this study was in a position to find best practices and lessons, evaluate curriculum designs, instructional practices, as well as policy reforms which can be implemented in the Indian educational system. Qualitative inquiry complemented numerical findings by addressing contextual issues and uncovering opportunities.

The quantitative dimension was achieved through primary data collection based on online questionnaire sent to the high school students, parents, and educationalists in India. The questionnaire consists of structured Likert-scale questions to identify the cybersecurity awareness, engagement, and perceptions (Ayyash *et al.*, 2024). The quantitative analysis provided measurable insights into stakeholder knowledge and behavior complementing the qualitative findings. The research achieved its extensive research scope by combining both qualitative and quantitative research methods. The study achieved depth and breadth, and provided three practical recommendations which included curriculum improvement, policy support, and stakeholder participation and these recommendations were backed by empirical data (Zhou *et al.*, 2024).

3.5 Population and Sample

The study drew its population from high school students, parents, and educationalists in India directly engaged in or impacted by cybersecurity education (Rahman *et al.*, 2020). Cybersecurity programs benefit school students as primary digital users, while educators ensure curriculum implementation, and parents reinforce safe practices; collectively shaping effective outcomes (Jerman Blažič and Jerman Blažič, 2022). The study presents an inclusive view of cybersecurity awareness, instructional practices and policy implementation across different states in India through the incorporation of these three stakeholder groups (Kivits and Sawang, 2021).

The study employed a non-probability convenience sampling approach to facilitate participation from the diverse stakeholder groups. The method was deemed suitable given the widespread geographical distribution of the target population across India and the exploratory objective of accessing cybersecurity awareness within the high school ecosystem. Convenience sampling allowed the researcher to engage with readily accessible respondents, thereby ensuring the survey reached a broad audience. To, maximize participation, the questionnaire was disseminated through multiple online platforms. While this enabled broad coverage and efficient data acquisition, it is important to acknowledge its limitations. Convenience sampling does not guarantee representativeness, and the findings may be subject to self-selection bias. As individuals with greater interest or access to digital platforms were more likely to respond. Nevertheless, given the exploratory nature of the research, the strategy was deemed sufficient to capture diverse perspectives and generate preliminary insights into the level of cybersecurity awareness among stakeholders in the high school context.

The correct number of respondents was estimated at 384 based on the Cochran formula. Considering confidence level of 95% with z-score of 1.96, estimated population proportion ($p = 0.5$ to maximize variability), and margin of error (desired precision) of $\pm 5\%$ into Cochran's formula (Ahmed, 2024):

$$\text{Necessary sample Size} = \frac{(Z\text{-Score})^2 * p * (1-p)}{(\text{Margin of Error})^2}$$

The estimated sample size stands at 384.

Respondents were contacted through social media and professional networks, across different geographic areas, and school boards to strengthen inclusivity of data and broaden representation. The sample size and sampling method provided sufficient statistical reliability for advance analyses, such as descriptive statistics, correlation and

regression tests, while ensuring that the findings are representative of the overall population of Indian high school stakeholders (Kaur *et al.*, 2018; Hossain *et al.*, 2024).

In this study, the sample was distributed into 3 categories based on the type of participants / respondents, which are listed in the following Table 3.1:

Note: There were 4 respondents who did not wish to participate in the survey and are excluded from the below table.

Table 3.1: Sample Size Distribution

Table 3.1: Sample Size Distribution

Category	Sample Size
Students	198
Parents	126
Teachers/Educators	121

Source: Primary data collected by author.

3.6 Participant Selection

This study engaged three key stakeholder groups to capture a holistic view of cybersecurity education in Indian high schools; namely the students, parents, and educationalists (Ayyash *et al.*, 2024). Students were included as primary beneficiaries whose knowledge and awareness reflects program effectiveness. Parents were considered as they were secondary influencers who reinforce safe digital practices at home. Educationalists, including teachers, school administrators, and curriculum planners were selected for their role in designing and implementing programs. Focusing on these three groups ensured the study addressed awareness levels, teaching practices, engagement patterns, and policy implementation challenges comprehensively.

Participants were engaged through non-probability convenience sampling method. The approach ensured that all individuals who met the eligibility criteria and expressed willingness to participate were offered to fill out the survey. The study targeted

stakeholders within the high school education sector, online learning institutions and professional social networks so as to spread the word about the poll. By disseminating the survey through these channels, the researcher was able to effectively engage students, parents, and educators across India. The strategy was particularly advantageous in overcoming geographical barriers and securing diverse perspectives from multiple regions. Responses were collected online on a voluntary basis, ensuring participants contributed freely and without coercion. Although convenience sampling does not ensure representativeness, it was considered a pragmatic choice for the exploratory study. The method facilitated efficient data collection and yielded informative insights into stakeholder perceptions, thereby supporting the broader objective of assessing cybersecurity awareness within the high school ecosystem.

Participants had to meet the eligibility criteria which included that the participants must be either current high school students, parents of high school students, or educationalists who actively participated in the high school education. The respondents' informed consent was secured beforehand, with the understanding that respondents' personal information (if any), would be treated with confidentiality and would only be used for this research study. This was done to eliminate any ethical concerns that could have arisen from the research. The chosen selection method guaranteed inclusivity, yielding practical knowledge to shape curriculum improvements, policy initiatives, and stakeholder engagement reforms (Kivits and Sawang, 2021).

3.7 Instrumentation

To gain a comprehensive understanding of cybersecurity awareness within the high school ecosystem, the study gathered information on the knowledge, attitudes, and practices of high school students, parents and educators through the use of standardized questionnaires. The questionnaire itself was thoroughly assembled on the basis of extensive

survey of international and Indian literature, international best practices, and policy issues connected with cybersecurity education (Arishi *et al.*, 2024; Kant, 2023; Raju *et al.*, 2022; Antunes *et al.*, 2021; Aljohani and Elfadil, 2020).

The questionnaire was carefully designed to guide participants through three stages. The first section established voluntary participation and collected demographic identifiers such as role, gender, age group and geographic location. Next, they were evaluated on their cybersecurity knowledge and practices, including awareness of online risks, safe internet use, and password management. Finally, the survey explored their attitude toward cybersecurity education, considering both personal views and the perspectives of schools and parents on integrating such education into the high school curriculum.

To measure the level of awareness and perception of participants, responses were recorded using a five-point Likert scale, where 1 indicated low awareness or strong disagreement and 5 represented high awareness or strong agreement. This approach facilitated the measurement of attitudes and perception regarding cybersecurity, allowing for robust statistical evaluation of stakeholder awareness (Joshi *et al.*, 2015). Open-ended questions were also incorporated to gather qualitative perspectives on challenges, experiences, and recommendations, supplementing the quantitative findings. The literature review served as the foundation for ensuring harmony across all aspects of the study, aligning its aims, conceptual framework, and the variables under investigation; and the questionnaire items were carefully developed in accordance with the literature review.

To ensure validity and reliability, a series of quality checks on the questionnaire were conducted. To begin, subject-matter experts examined the tool to ascertain content validity and relevant to the research objectives (Andersson *et al.*, 2024). Thereafter, pilot study was conducted on a small group of respondents, who represents the study population and their feedback was obtained to refine the wording, remove ambiguity questions and

simplify it to make it clearer and easier to comprehend. The questionnaire had gone through numerous stages of revision and check-up to make it short, relevant, and in line with the objectives of the research. The questions were also rephrased to avoid the possibility of interpretation so that all stakeholders including the parents, students, and educators, would find them easy to understand and respond to the survey. The survey was conducted using Google Forms, and the data collected was stored in local database to ensure confidentiality and integrity.

The reliability test statistics of this study survey is given in the following Table 3.2:

Table 3.2: Reliability Analysis of Study Survey

Table 3.2: Reliability Analysis (Cronbach's Alpha) for All Respondent Groups

Respondent Group	N	Items (N of Variables)	Cronbach's Alpha (α)	Reliability Level	Interpretation
Students	198	11	0.616	Moderate	Indicates acceptable internal consistency, though reliability can be improved by refining or removing weaker items.
Parents	126	16	0.828	Good	Reflects strong reliability; the items are consistent in measuring parental awareness and cybersecurity practices.
Administrators	121	15	0.808	Good	Demonstrates high internal consistency among variables

					assessing administrative perspectives on cybersecurity and safety.
--	--	--	--	--	--

Source: Data analysis by author.

The instruments structured nature enabled systematic data collection, and advanced statistical analysis with SPSS, including descriptive statistics, correlation, and Analysis of Variance (ANOVA) (Edelsbrunner *et al.*, 2025; Zemlyak *et al.*, 2022).

3.8 Data Collection Procedures

To achieve a thorough and impartial assessment of cybersecurity education and awareness in high schools, this study adopted a mixed-methods approach, integrating primary and secondary data (Schneider *et al.*, 2023). The study goals directly influenced the choice of data collection techniques. Following the study's criteria, qualitative content analysis of secondary data was used to address the first three objectives, which are to determine the strengths and weaknesses of international cybersecurity education programs, analyze the design of curriculum and teaching strategies, and provide insights into the function of policies and regulations. Quantitative analysis of survey responses addressed the fourth objective of gauging cybersecurity awareness among Indian educators, parents, and students.

Qualitative data

Secondary data for qualitative component was sourced from academic databases, research papers, policy studies, and publications of credible organizations including Verizon, Cloud SEK, the World Economic Forum Global Risk Report, and Fortinet's Global Cybersecurity Skills Gap Report. These databases were systematically searched for scholarly works on digital safety education covering trends, best practices, curricula,

teaching strategies, and policy interventions across varied geographic regions, which were subsequently filtered and critically examined. This content analysis provided the comparative framework to evaluate Indian high school cybersecurity education against global norms, fulfilling objectives one through three.

Preference was given to English-language publications, with research published between 2019 and 2025 to ensure contemporary relevance (Table 3.3).

Table 3.3: Literature Search and Selection Criteria

Table 3.3: Process of Selecting Past Studies

Search Journals	Keywords such as cyber awareness, cybersecurity, cyber education, cybercrime, school-based approach, and cybersecurity education in high schools in India.
Database Used	Google Scholar, Emerald, Scopus, EBSCO
Limit the studies	Cybersecurity education in schools, and cybersecurity awareness papers published during the period 2019 and 2025. Additionally, the research made use of secondary data published by CloudSEK, Verizon, World Economic Forum (WEF) – Global Risk Report, Fortinet’s 2024 Global Cybersecurity Skills Gap Report etc.

Source: Compiled by author.

Quantitative Data

The fourth objective i.e. assessing cybersecurity awareness among core stakeholders was achieved through online survey conducted by ensuring voluntary participation, informed consent and ethical safeguards (Kumari, 2024). The questionnaire contained standardized Likert-scale questions to measure cybersecurity knowledge, involvement, and attitudes. There were also the use of open-ended questions that would help to bring out more information about challenges and experiences (Takács and

Pogátsnik, 2024). Conducting the survey online facilitated broad participation, drawing respondents from several Indian states.

3.9 Data Analysis

By blending qualitative content analysis of secondary sources enriched by comparative insights from global publications, along with quantitative survey responses, the study delivered a comprehensive evaluation of high school cybersecurity education and awareness in India. The qualitative content analysis provided the context, explanations, and practical insights, whereas quantitative data provided measurable levels of awareness, involvement and perceptions (Grace *et al.*, 2023). The mixed-method approach uncovered training gaps, policy obstacles, and key factors shaping cybersecurity training effectiveness.

Qualitative Data Analysis

Secondary data from articles, policy reports, and international publications were subjected to content analysis to support the qualitative study (Vaismoradi *et al.*, 2013). Reviewing the secondary data provided global insights into curricula, policies, and best practices in cybersecurity education, that numerical data from quantitative measurement alone could not capture.

The qualitative analysis has provided evidence-based recommendations on how to improve cybersecurity education in India high schools, such as curriculum design, policy advocacy, awareness sensitization, and stakeholder involvement. Thorough content analysis strengthened the reliability, accuracy, and relevance of findings on improving cybersecurity education across India.

Quantitative Data Analysis

SPSS driven statistical analysis of online survey data provided insights into quantitative findings underpinning the research. This was done to verify reliability, spot patterns, and quantify change among the sets of stakeholders (Čaplová and Švábová, 2020).

- **Reliability Analysis:** “Cronbach's alpha” was used to test the internal consistency of the survey instrument. When dealing with Likert-scale questions that was used to measure cybersecurity knowledge, awareness, and engagement, the alpha coefficients have been calculated, and they indicated that the tool was perceived to be dependable and renders a consistent output (Nair and Meyyappan, 2024).
- **Descriptive Statistics:** To examine demographic variation, descriptive statistics were applied to stakeholder groups, assessing age, gender, and geographical representation. The measures included frequencies, percentages, means, and standard deviations, that gave a detailed picture of the sample population. This approach assisted to examine disparity in the attitudes, participation, and consciousness of cybersecurity among the students, parents, and educators (Rendón-Macías *et al.*, 2016).
- **Analysis of Variance (ANOVA):** The study used correlation analysis to determine relationships between demographics and cybersecurity awareness levels. This test was used to detect differences and areas where cybersecurity education and awareness programs needs improvement (Connelly, 2021).
- **Correlation Analysis:** The study used correlation analysis to examine relationships among study variables to clarify their impact on cybersecurity awareness and engagement (Senthilnathan, 2019).

3.10 Research Design Limitations

Even though the mixed-methods research design adopted in the current study provides a comprehensive overview of cybersecurity education in Indian high schools, certain limitations must be admitted. Firstly, given India's vast diversity in ethnicity, language, and socio-cultural contexts, the sample size may not fully capture the experiences of all students, parents, and educators. This limits the generalizability of the findings. More digitally literate, motivated, or technology-engaged respondents might be overrepresented, potentially bring a bias towards more digitally aware demographic. Also, the social desirability bias might affect the quality of the survey data, with respondents providing answers they perceived as favorable or positive rather than entirely accurate. Other factors that might influence the accuracy and reliability of the data collected can be variations in the honesty of respondents, their understanding of Likert-scale questions or differences in interpreting survey questions.

The other limitation is with regards to diverse educational settings in India with variations in curriculum, resources, teacher training, and policies across states that this study might not be able to capture as a whole. The study offers an insight into the awareness and perceptions at only one point in time, which does not allow tracking longitudinal changes and determining the effectiveness of cybersecurity awareness changes over a long period of time. In addition, although qualitative content analysis provides useful information about the experiences and views of the stakeholders, it is subjective and depends on interpretation of the researcher while categorizing, and find themes, which can bring bias. Future studies should include larger and more diverse groups, use multiple sources of data, and track changes over time to make the findings more reliable. Even with these limitations, the mixed-methods approach (using numbers and detailed opinions),

offers a strong picture and helps suggest ways to improve curriculum, policies, and stakeholder involvement.

3.11 Conclusion

This chapter outlined a mixed-methods approach to studying high school cybersecurity awareness in India, compared against global practices. Qualitative analysis of literature, policies, and curricula was paired with quantitative surveys of students, parents, and educationalists perceptions. The blending of theoretical and empirical methods enabled the study to provide strong foundation for evidence-based recommendations.

The study initially included 449 participants, but with 4 refusals (opting not to participate in the survey) the final sample size stood at 445, well above the 384 required by Cochran's formula. The respondents included 198 students (44.5 %), 126 parents (28.3 %), and 121 teachers/academicians (27.2 %). Ethical considerations, informed consent and confidentiality was maintained during the process of data collection and analysis.

CHAPTER IV:

RESULTS

4.1 Research Question One

What are the strengths and weaknesses of cybersecurity education programs in different countries, and how can these inform improvements in Indian high schools?

The increasing reliance on ICT has opened new avenues for cybercriminals to exploit states, organizations, and individuals. While cyberspace has become a driver of economic growth and global information exchange, escalating cyber threats threaten to undermine these advantages. Incidents of data breaches demonstrate the severe financial losses and reputational harm that cybercrimes can inflict. Within the education sector, schools have integrated technology for learning management systems, online assessments, and communication, and storing sensitive data such as personal details, academic records, and financial information of students, staff, and parents. This makes them prime targets for cyberattacks. Beyond institutional risks, students themselves are vulnerable to challenges like cyberbullying, online predators, and harmful digital content. With many parents' lacking awareness of their children's online behavior, embedding cybersecurity education into both school programs and family practices is essential to foster safe, responsible, and resilient digital engagement.

Strengths of Cybersecurity Education

Cybersecurity education enhances students' awareness of online risks and threats such as phishing, cyberbullying, and privacy breaches, while equipping them with self-protective skills like password management and threat recognition. As social media and online gaming usage grows, teaching children to safeguard personal data including names, addresses, and phone numbers helps prevent identity theft and exploitation. Digital safety awareness programs help prepare students to use technology responsibly and understand

the consequences of their online behavior (Quayyum *et al.*, 2021). The study by (Altarawneh *et al.*, 2025), emphasizes that legal literacy in areas like data privacy and cyberbullying is essential to help shape student's cybersecurity awareness and responsible online behavior.

In mainland China, digital awareness campaigns emphasize safe online behavior and good cyber hygiene and also encourages students interest in technical aspects to prepare them for future careers (Nieto *et al.*, 2025). Innovative curricular activities such as Capture the Flag competitions and simulation programs when included alongside classroom theoretical instructions further boosts engagement, critical thinking, and applied skills (Leune and Petrilli, 2017).

Table 4.1 summarizes the core strengths of cybersecurity education, as identified in multiple scholarly articles.

Table 4.1: Strength Analysis of Cybersecurity Education

Table 4.1: Strength Analysis of Cybersecurity Education

Paper / Author(s) (Year)	Focus / Topic	Strengths / Positive Findings
(Quayyum <i>et al.</i> , 2021)	Cybersecurity education and digital literacy for children	Increases awareness of online risks (phishing, cyberbullying, privacy breaches); teaches practical self-protection skills; fosters ethical online behavior.
(Altarawneh <i>et al.</i> , 2025)	Cyber threats among youth	Combines technical education with legal awareness to prepare learners for real-world online risks.
(Nieto <i>et al.</i> , 2025)	Cybersecurity awareness in China	Promotes safe online behavior, cyber hygiene, and interest in cybersecurity careers; helps address workforce gaps.
(Leune and Petrilli, 2017)	Innovative curriculum activities	Capture the Flag competitions and simulations enhance engagement, critical thinking, and applied cybersecurity skills.

Source: Compiled by author.

Weaknesses or limitations of cybersecurity education

Insights from the study by (Gorai *et al.*, 2025), reveals that the 2013 National Cyber Security Policy (NCSP) in India can be considered outdated, lacking clear objectives and timelines for implementation. It does not adequately address emerging threats posed by AI, IoT, and quantum computing, leaving critical gaps in preparedness. The study also highlights that there is absence of a centralized authority to coordinate initiatives across industries, leading to duplication of effort and jurisdiction among bodies such as NCIIPC and CERT-In.

- **Insufficient Infrastructure and Resources**

More and more people in the US are starting to pay attention to cybersecurity education. This is in reaction to the cyber landscape, which is particularly desolate due to the 750,000 unfilled cybersecurity jobs in the US and the severe scarcity of qualified candidates (Tierney, 2025). There have been 353 million data breaches in the US in the past year, which is a direct result of this catastrophe (Galletta *et al.*, 2024). U.S. losses due to cybercrime totaled \$320 billion in 2023. The projected increase in costs to \$1.8 trillion by 2028 is quite high (Cobos and Cakir, 2024). As cyber threats intensify, attacks on essential infrastructure like schools, water treatment plants, and power grids are becoming increasingly frequent, endangering the physical well-being of ordinary citizens.

As per the report by Boston Consulting Group (Global Cybersecurity Forum, 2024), there is a severe shortage of skilled cybersecurity professionals estimated at 2.8 million worldwide leaving organizations and nations vulnerable. In Indian context, businesses and individuals are easy targets for hackers due to the general public's ignorance of the importance of cybersecurity. Phishing, identity theft, and social engineering are all too common, yet there has been very little done to raise awareness and educate the public about them. Promoting cyber hygiene and safe online practices has been uneventful and narrowly focused endeavor (Khando *et al.*, 2021).

- **Inadequate Legal Framework**

With cyberattacks transcending national boundaries, international cooperation on cybersecurity laws and regulations is a major focus of global policy discussions in recent times (Ali, 2024). Unresolved issues such as attribution of attacks, jurisdictional conflicts, and the uneven application of international legal norms highlight the limitations of current frameworks (US Cybersecurity Act, EU’s GDPR, and India’s Information Technology Act). Differences in national legislation and legal definitions, sovereignty concerns, and resource disparities particularly in developing nations further complicates global cooperation. While efforts among nations have advanced, unresolved gaps call for strategies that balance sovereignty with international collaboration and strong privacy protections.

Several academics agree on critical limitations in cybersecurity education. Table 4.2 captures some of the core shortcomings.

Table 4.2: Weakness Analysis of Cybersecurity Education

Table 4.2: Weakness Analysis of Cybersecurity Education

Paper / Author(s) (Year)	Focus / Topic	Weaknesses / Challenges
(Altarawneh <i>et al.</i> , 2025)	Cyber threats among youth	A lack of cybersecurity awareness, coupled with high internet use, increases youth susceptibility to phishing, malware, and privacy risks.
(Gorai <i>et al.</i> , 2025)	Cybersecurity policy and strategy in India	Policy is outdated, lacks actionable objectives and timelines; does not cover emerging technologies; fragmented implementation due to multiple agencies.
(Bhangla and Tuli, 2021)	Legal framework and public awareness in India	Legal provisions are insufficient for modern cybercrimes; low user awareness contributes to harassment and cybercrime.

(Global Cybersecurity Forum, 2024)	Cybersecurity Workforce Report	Skill shortages and workforce gaps significantly weaken organizational defenses against cyberattacks.
(Khando <i>et al.</i> , 2021)	Public awareness & cyber hygiene in India	Limited reach of awareness campaigns, coupled with poor public awareness increases susceptibility to cyberattacks
(Chakraborty and Tiwari, 2025)	Cybersecurity infrastructure in India	Shortage of skilled professionals; SMEs lack resources; critical infrastructure vulnerable; over 60% of organizations experienced cyberattacks

Source: Compiled by author.

Some of the core strengths of cybersecurity education are that it equips students with awareness of online risks such as phishing, cyberbullying, and privacy breaches, while also fostering ethical digital behavior and practical self-defense skills. International programs, including those in China, combine technical training with cyber hygiene and career-focused initiatives, building student confidence for future roles in the field. Innovative methods like Capture the Flag competitions, simulations, and interdisciplinary curricula enhance engagement, critical thinking, and applied skills. Integrating technical knowledge with legal awareness further prepares learners to address real-world cybersecurity challenges responsibly (Altarawneh *et al.*, 2025; Quayyum *et al.*, 2021).

India's struggle with digital safety awareness highlights critical gaps in protecting its citizens in the cyber world. The outdated legal frameworks fail to address rising threats such as ransomware, cyberbullying, and privacy breaches. Schools often lack modern infrastructure, adequate resources, and trained teachers, leaving students unaware of the cyber risks. As noted by (Gupta and Gupta, 2025), to bridge the gaps, cybersecurity should be taught as a core subject complemented by instruction on digital ethics, teachers must receive specialized training, access to updated resources, and exposure to learning methods like simulations and competitions to build practical skills. Another strategy that schools

should adopt is to implement modern IT infrastructure and foster collaboration with industry and government, that can further raise awareness among students, educators, and parents. This will not only equip students to navigate the digital world safely but also inspire them to pursue higher education and careers in this rapidly growing field.

4.2 Research Question Two

Which teaching methodologies, resources, and curriculum designs used internationally can be effectively adapted to the Indian context?

The integration of cybersecurity and computer science into K-12 and higher education curricula has been widely studied. Investigations explore curriculum integration through general education, electives, minors, majors, and advisory programs; and examine issues and solutions in imparting cybersecurity education at different levels of schooling. The NICE K-12 Cybersecurity Education Conference in its two-day annual event brings together teachers and others interested in cybersecurity education. Attendees learn how to improve digital safety awareness, explore new teaching methods, and add cybersecurity to school programs. The conference also helps them design learning and career paths (Childers *et al.*, 2023). Such events contribute towards strengthening cybersecurity education and awareness by fostering collaboration among educators, promoting best practices, and equipping participants with the knowledge and tools necessary to prepare students for safe and responsible participation in the digital world.

Table 4.3 presents a summary and comparison of the latest cybersecurity curriculum approaches, emphasizing the primary focus of each paper and the practicality of the method.

Table 4.3: Comparison and Summary of Cybersecurity Curriculum Approaches

Table 4.3: Comparison and Summary of Cybersecurity Curriculum Approaches

Papers	Goal / Focus	Practicality	Audience
--------	--------------	--------------	----------

(Aoyama <i>et al.</i> , 2024)	Introduces a beginner-friendly cybersecurity education model that blends theoretical instruction with practical exercises to strengthen conceptual and applied understanding.	Applied	Students
(Su, 2024)	Develops Web-based Hands-On Learning Environment (WebHOLE), an online learning platform designed to teach web application security (WAS) through tailored exercises, online assessments, and interactive learning tools.	Applied	Students
(Rayavaram <i>et al.</i> , 2023)	Designs a visual and story-based cybersecurity curriculum utilizing the Scratch programming environment to create interactive stories, games, and animations and introduce core cybersecurity principles to K–12 learners.	Applied	Students
(Lasisi <i>et al.</i> , 2022)	Examines essential AI-related competencies for undergraduate cybersecurity programs and offers suggestions for updating curricula to prepare students for AI-integrated cybersecurity roles.	Proposal	Students
(Madathil <i>et al.</i> , 2023)	Presents an AI-powered smart learning platform that supports personalized education by monitoring learner progress and enhancing communication between educators and students.	Applied	Students, Teachers, and Parents
(Kaabi <i>et al.</i> , 2022)	Develops a gamified cybersecurity learning system featuring 11 interactive levels to promote engagement, creativity, problem-solving, and decision-making skills in learners.	Applied	General
(Affia <i>et al.</i> , 2022)	Investigates the integration of online hackathons in cybersecurity education to enhance teamwork, practical learning, and application of knowledge through real-world scenarios.	Applied	Students and Teachers

Source: Compiled by author.

These studies highlight that cybersecurity education programmes should be future ready, highlighting innovative curriculum designs such as ethical hacking, behavioral security, and integration of digital safety concepts into existing programs. Strategies include teacher awareness and training, aligning courses with industry standards, and

adopting active learning methods such as project-based learning, and hands-on labs. These efforts aim to broaden access, reaching K-12 students, organizations, and even first-time internet users.

Table 4.4 analyzes findings from international studies to identify best practices for cybersecurity education and their applicability to the Indian high school context. The analysis is organized across four dimensions: teaching methodologies, learning resources, curriculum design, and teacher professional development.

Table 4.4: Global Pedagogical Models with Applications for India

Table 4.4: Summary of Different Countries' Teaching Methodologies, Learning Resources, Curriculum Design, and Teacher Development with Recommendations for India

Dimension	International Best Practices & Evidence	Challenges Identified	Recommendations / Adaptation for the Indian Context
Teaching Methodologies	- Hands-on, experiential learning like Capture-the-Flag (CTF) competitions, gamified exercises, and simulations shown to improve engagement and skill acquisition (Prümmer <i>et al.</i>, 2024). - Cross-curricular integration of cybersecurity in social studies, ICT, and STEM subjects improves coverage and accessibility (Alotaibi <i>et al.</i>, 2025). - Scenario-driven and project-based learning helps connect theory to real-world applications	- Teacher knowledge gaps in topics such as ethical hacking, forensics, and encryption (Alotaibi <i>et al.</i>, 2025). - Time constraints in packed school curricula makes adding standalone cybersecurity courses difficult (Alotaibi <i>et al.</i>, 2025).	- Organize teacher training bootcamps and capacity-building workshops to improve teacher confidence. - Pilot after-school cybersecurity clubs, and summer bootcamps to give students hands-on exposure without overloading formal curricula.

	(Gkioulos and Chowdhury, 2021).		
Learning Resources	• Virtual labs, online platforms, and gamified tools (e.g., NCSC UK's <i>CyberFirst</i> and US NICE Cybersecurity Workforce Framework) make learning immersive (NIST NICE, 2022) • Centralized repositories of age-appropriate content are recommended for schools to reduce teacher burden (Alotaibi <i>et al.</i>, 2025). • Industry partnerships help keep materials updated and relevant (Beuran <i>et al.</i>, 2019).	• Challenges with digital literacy (limited computers, bandwidth, blocked content) especially in rural schools (Kumbhakar and Kumar, 2025). • Many open-source cybersecurity learning tools are discontinued or short-lived (Blažič and Blažič, 2024).	• Develop cloud-based cybersecurity learning environments accessible from low-end devices. • Build a national repository of lesson plans and virtual labs, maintained through public-private partnerships with Ed-Tech firms.
Curriculum Design	• Tiered curriculum design: start with cyber hygiene and phishing awareness, then proceed to advance topics like malware, encryption, and ethical hacking (Prümmer <i>et al.</i>, 2024). • Both standalone courses and integrated modules are used internationally, with flexibility based on school	• Curricula are fragmented and lack a clear progression framework for cybersecurity topics (Erickson and Kim, 2021). • No national consensus on whether cybersecurity should be a	• Create a National cybersecurity Education Framework aligned with Digital India, mapping age-appropriate competencies. • Use a modular approach: compulsory cyber hygiene modules

	resources (Alotaibi <i>et al.</i> , 2025). Frameworks such as NICE (USA) and NIST CS Framework ensure standardization of learning outcomes (NIST NICE, 2022).	separate subject or embedded into ICT classes (Kant, 2023).	and elective advanced cybersecurity topics for interested students.
Teacher Professional Development	Professional development programs with continuous training and practical exposure are recommended internationally (Alotaibi <i>et al.</i>, 2025; Shillair <i>et al.</i>, 2022).	Teachers report low confidence and lack of resources to teach cybersecurity (Alotaibi <i>et al.</i>, 2025).	Mandatory teacher certification, Continuing Professional Development (CPD) through MOOC, webinars, and industry engagement opportunities.

Source: Compiled by author.

The literature review of recommendations and policy practices in international frameworks indicates that successful cybersecurity education must integrate active learning methods, robust and updated learning resources, a structured and progressive curriculum design, and sustained teacher capacity-building efforts.

Global programs emphasize practical, hands-on learning, integrating capture-the-flag (CTF) exercises and gamified simulations to engage students and connect theory with real-world challenges (Prümmer *et al.*, 2024). Problem-based and project-based learning also serve as key strategies for integrating theoretical concepts with practical experience (Gkioulos and Chowdhury, 2021). Existing literature points towards gaps in teacher expertise in advanced topics such as encryption and ethical hacking, and time constraints of packed school timetables. In the case of India, the capacity-building strategies such as

boot camps, train-the-trainer workshops, and after-school cybersecurity clubs will offer practical ways to instill confidence and broaden academicians and students' exposure without overwhelming the formal curricula.

Effective cybersecurity education relies on strong resources, including virtual labs, gamified tools, and age-appropriate databases such as NCSC CyberFirst, NICE Cybersecurity Workforce Framework; that are widely adopted to enhance engagement and scalability (NIST NICE, 2022). Additionally, collaboration with industry specialists contributes to the relevance of these tools (Beuran *et al.*, 2019). In India, digital infrastructure barriers such as those in public schools and rural schools impede this, as do the lifespan of many open-source tools (Blažič and Blažič, 2024). To overcome these challenges, there is a need to invest in cloud-based and low-cost virtual laboratories and develop a national repository of lesson plans and practical exercises, and safe virtual environments through public-private collaborations.

The dimension of the curriculum is also very vital. Schools should adopt a tiered and modular approach starting with cyber hygiene and phishing awareness and moving on to specialized concepts such as malware, encryption, and ethical hacking (Prümmer *et al.*, 2024). Frameworks such as the NICE CS Workforce Framework and NIST CS Framework guarantee the presence of standard learning outcomes and career readiness (NIST NICE, 2022). However, in India, there has been no framework of progression, no agreement on whether cybersecurity should be offered as a separate subject or as part of ICT courses, which has led to fragmentation (Kant, 2023; Erickson and Kim, 2021). An appropriate national system of cybersecurity education to support Digital India, with distinct competency mapping and modular structure, can offer basic digital literacy and specialist technical options to the interested students.

The last pillar is teacher professional development, with global best practices suggesting ongoing professional growth that involves both theoretical knowledge and hands-on experience (Shillair *et al.*, 2022). India's education system struggles with limited resources (hardware, software, networking, labs), and low confidence among teachers to impart cybersecurity education. The introduction of obligatory certification of cybersecurity basics to teachers with the help of MOOCs, webinars and participation in hackathons, and collaboration with industry experts can significantly enhance teaching quality and strengthen teachers confidence (Alotaibi *et al.*, 2025).

Taken together, the findings suggest that tailoring international best practices to India's context may yield significant benefits, considering its infrastructure challenges, linguistic diversity, and policy needs. Government, academia, and industry collaboration is essential in cultivating a sustainable ecosystem of cybersecurity education. This collective effort aligns educational outcomes with workforce demands and strengthens national digital resilience.

4.3 Research Question Three

What role do government policies and regulations play in promoting cybersecurity education at the high school level in India?

As online threats intensify, schools must prepare students with both technical skills and risk awareness. Clear regulations and policies are essential to set objectives, ensure consistency, and align curricula with national priorities. The research examined the role of government policies and regulations in the field of cybersecurity education at high schools in India. It discovered that there is limited role of government policies and regulations in cybersecurity education sector in India. While some general digital skills programs have been introduced, there remains partial inclusion of cybersecurity concepts in school curricula (Kumar, 2024). The absence of harmonized policies in India has created

disparities in how schools deliver cybersecurity education; some have developed commendable programs, whereas others remain underprepared. To ensure equal access and consistent quality of cybersecurity education across schools, India requires strengthened policies with explicit objectives, structured assessment methods, and defined curricular content. The scholarly article by (Kant, 2023) also supports this view, noting that even though general digital skill initiatives exist, targeted policies and regulations are still lacking to effectively foster cybersecurity education at the high school level in India.

Students spend time online for both academic assignments and leisure activities such as social media, creating video blogs, and gaming. Unmonitored internet usage has become habitual, often leading to excessive screen time that harms mental health and reduced physical activities (Rahman *et al.*, 2020). As such, policy frameworks and regulations should ensure cyber hygiene practices among students, not by avoiding ICT, but by promoting its wise and responsible use. Such policies must integrate cybersecurity awareness by teaching the history of fraud and scams such as phishing and cyber theft, alongside knowledge of harmful software and secure practices on mobile devices and social media.

Table 4.5: Government Cybersecurity Policies: Indian and the World

Table 4.5: Analysis of Government Approaches to Cybersecurity Education in Indian High Schools Compared with Global Practices

Aspect	Current Situation in India (with Policy / Initiative Names where applicable)	International Comparison / Best Practices	Key Recommendations
Policy Clarity	Limited specific policies for cybersecurity in schools. Some inclusion under broader policies	Most countries have clear, structured plans for cybersecurity education in	Develop specific, well-organized policies with clear goals and measurable outcomes focused on

	like the National Education Policy (NEP) 2020, Digital India mission, and initiatives such as “Cyber Shikshaa” by Microsoft.	schools, with dedicated policies and legislative support.	cybersecurity education (e.g. obligations for schools, competency milestones).
Implementation Consistency	Implementation is uneven. Certain states (e.g. Karnataka government in collaboration with Meta has the “Digital Nagarik” programme) have proactive cyber awareness campaigns, while many other states and schools lag behind.	In many nations, centralized policy enables consistent rollout of curricula, teacher training, and resourcing across schools.	Standardize curriculum and program requirements across all schools; ensure alignment across states; monitor and support implementation regularly.
Multi-stakeholder Approach	Coordination between education departments, tech agencies, private sector is limited but growing. E.g. Karnataka’s partnership with Meta for awareness and teacher training.	Best practices show collaborations across ministries (education, ICT), industry, and NGOs to create sustainable programs.	Strengthen partnerships among government departments (Education, IT/BT), private sector (Ed-Tech, tech firms), and education institutions (schools, teacher training colleges).
Teacher Training & Lesson Oversight	Limited or no regulations mandate teacher training specific to cybersecurity. Some programs, such as “ET-CISO” in Karnataka state, and awareness programs by NGOs/Nasscom,	Best practices show teacher credentialing, regular professional development, and lesson plan review are required parts of policy.	Implement regular teacher training in cyber hygiene, threat awareness, and ethical hacking basics; exposure to online hands-on labs, institute oversight of lesson plans; make online

	provide training. Oversight of lesson content is minimal.		safety education mandatory.
Funding and Resources	Currently, resource allocation tends to focus on general ICT infrastructure. Cybersecurity specific labs, safe tools and materials are underfunded. Some state-level campaigns get budgeted.	Good practices include dedicated funding lines for cybersecurity education, equipment (labs), virtual tools, and digital platforms.	Allocate sufficient funds for lab infrastructure, cybersecurity educational tools, virtual labs and simulations; ensure rural and underprivileged schools are supported as well.
Integration with National Digital Strategy	Cybersecurity is recognized as a national concern, part of the Digital India mission. But school-level integration (in curricula, assessments) is patchy.	Internationally, school cybersecurity education is deeply embedded in national digital growth strategies; policy alignment ensures consistency from national to state to district and classroom level.	Connect school cybersecurity education policy directly with India's Digital India, National Mission on Education through ICT, NEP, etc.; embed cybersecurity in national education strategy and funding mechanisms.
Community & Sustainability Focus	Minimal involvement of parents, local communities, and influencers. Many programs are pilot or state-level without scale; long-term sustainability is not always planned. E.g.	Best practices include parent and community awareness programs, sustainable models (continuous funding, policy support) rather than one-off projects.	Engage parents and communities in digital safety awareness workshops; ensure programs are scalable and built for long-term sustainability (ongoing funding, policy embedding, feedback loops).

	“Cyber for YOUTh” in Madhya Pradesh.		
--	--------------------------------------	--	--

Source: Compiled by author.

Table 4.5 highlights significant disparities between India's current policy framework and globally recognized best practices for cybersecurity education. Programs like Cyber Shikshaa and the Digital Nagarik, National Education Policy (NEP) 2020 and various initiatives like the Digital India mission are all significant endeavors, but none of them provides a unified, standardized curriculum on cybersecurity education in schools (Datta and Mete, 2021; Kaur *et al.*, 2025). Global best practices recommend systems such as the NICE Cybersecurity Workforce Framework that have been embraced in nations such as the US, the UK, and Singapore, where competency milestones and curricular direction is offered through structured frameworks. Inconsistent application of digital safety practice by the different states and the lack of teacher training in India are still the critical challenges, consistent with findings by (Alotaibi *et al.*, 2025), that stress capacity-building of teachers as the key to program success. Practical learning suffers from inadequate funding and resources, compounded by limited cooperation among stakeholders and communities. International best practices emphasize parental involvement and public–private partnerships as essential for long-term effectiveness (Singh *et al.*, 2025). By introducing clear policies, uniform curricula, teacher training and certification, and targeted funding, India can bring its schools in line with global best practices and reinforce cyber-resilience.

The research indicates that India's current policies on cybersecurity education in high schools are vague and lag specificity, resulting in inconsistent implementation across institutions. Global successful stories point towards states having strong government involvement, well laid out strategies, and adequate funding to achieve more consistent and effective outcomes. In India, key shortcoming includes insufficient teacher training, weak

monitoring of lesson plans, and poor integration with broader digital plans. According to the findings presented by (Triplett, 2023), ensuring sustainable and high-quality cybersecurity education requires explicit policies, measurable objectives, standardized curricula, better collaboration among educational institutions, government and industry, adequate training and resources, and innovative strategies such as community engagement and game-based learning. A similar approach can be adopted in the context of India to align school programs with global best practices in cybersecurity education.

4.4 Research Question Four

What is the current level of cybersecurity awareness among high school students, parents, and educationalists across India?

This section presents the findings from a survey conducted among students, parents, and educationalists (teaching / non-teaching staff) in Indian high schools.

Findings of the survey among Students

There were 198 respondents from the student community, and this section includes the findings based on the survey.

Table 4.6: Demographic Details of Students

Table 4.6: Demographic Details of Students

Category	Sub-category	Frequency	Percent
Gender	Male	124	62.6
	Female	74	37.4
Age Group	<20 Years	198	100
State	Andhra Pradesh	4	2
	Arunachal Pradesh	3	1.5
	Assam	18	9.1
	Bihar	8	4
	Chhattisgarh	5	2.5
	Delhi	7	3.5
	Goa	1	0.5
	Gujarat	13	6.6

	Haryana	30	15.2
	Himachal Pradesh	5	2.5
	Jharkhand	8	4
	Karnataka	9	4.5
	Kerala	4	2
	Madhya Pradesh	18	9.1
	Maharashtra	14	7.1
	Manipur	7	3.5
	Meghalaya	6	3
	Punjab	2	1
	Rajasthan	10	5.1
	Tamil Nadu	8	4
	Uttar Pradesh	8	4
	Uttarakhand	6	3
	West Bengal	4	2
District	Kullu	1	0.5
	Agra	2	1
	Ahmedabad	3	1.5
	Ajmer	2	1
	Alappuzha	1	0.5
	Almora	1	0.5
	Alwar	1	0.5
	Ambala	5	2.5
	Amravati	1	0.5
	Amreli	1	0.5
	Anand	1	0.5
	Anantapuramu	1	0.5
	Anjaw	1	0.5
	Anuppur	2	1
	Araria	1	0.5
	Aravalli	1	0.5
	Arwal	1	0.5
	Aurangabad	4	2
	Bagalkot	1	0.5
	Baksa	6	3

Ballari	1	0.5
Balod	1	0.5
Balrampur	1	0.5
Banaskantha	1	0.5
Bangalore	2	1
Bangaluru	3	1.5
Bapatla	1	0.5
Barpeta	1	0.5
Bastar	1	0.5
Begusarai	1	0.5
Bemetara	1	0.5
Bhagalpur	1	0.5
Bhind	1	0.5
Bhiwani	1	0.5
Bhopal	2	1
Bicholim	1	0.5
Bikaner	2	1
Bilaspur	1	0.5
Bishnupur	2	1
Biswanath	1	0.5
Bokaro	1	0.5
Bongaigaon	1	0.5
Central Delhi	1	0.5
Chamarajanagar	1	0.5
Chamba	1	0.5
Chamoli	1	0.5
Champawat	1	0.5
Chandel	1	0.5
Changlang	1	0.5
Charkhi Dadri	1	0.5
Chatra	1	0.5
Chennai	6	3
Chittoor	1	0.5
Churachandpur	3	1.5
Dehradun	1	0.5

Delhi	4	2
Deoghar	1	0.5
Dhanbad	1	0.5
East Garo Hills	3	1.5
Faridabad	3	1.5
Guna	2	1
Gurgaon	1	0.5
Gwalior	4	2
Hamirpur	1	0.5
Haridwar	2	1
Indore	4	2
Jaipur	2	1
Jalgaon	1	0.5
Jamnagar	1	0.5
Jhansi	1	0.5
Jodhpur	1	0.5
Kakching	1	0.5
Kameng	1	0.5
Kamjong	1	0.5
Kamle	1	0.5
Kamrup Metro	3	1.5
Kamrup Rural	2	1
Kangra	1	0.5
Kinnaur	1	0.5
Kokrajhar	1	0.5
Kolhapur	1	0.5
Kolkata	4	2
Kollam	1	0.5
Kota	1	0.5
Lucknow	4	2
Mumbai	1	0.5
Murena	2	1
Mysuru	1	0.5
Nagpur	1	0.5
Nashik	1	0.5

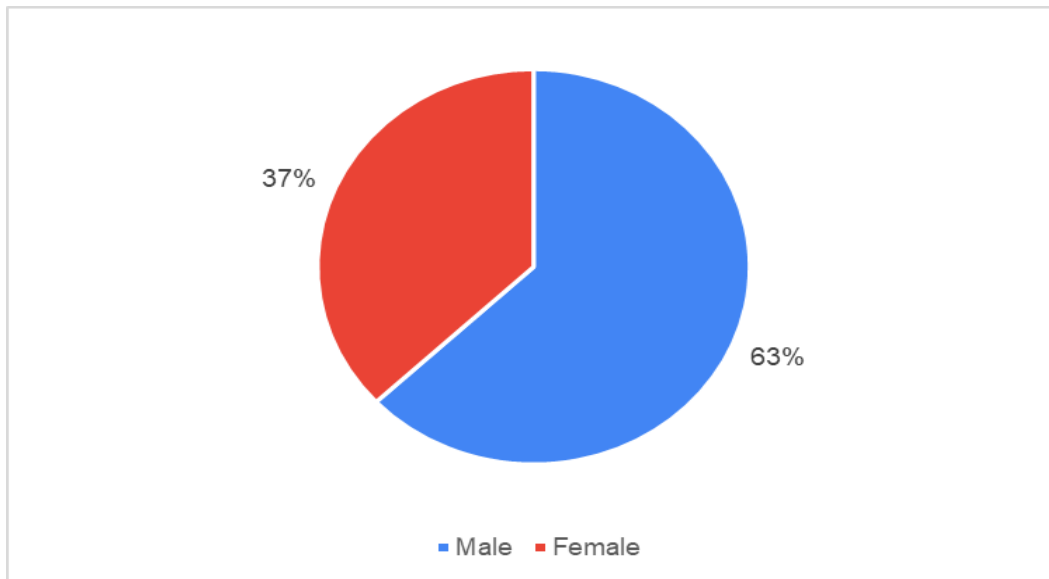
North Delhi	1	0.5
Orai	1	0.5
Palamu	1	0.5
Palwal	1	0.5
Panipat	4	2
Patiala	1	0.5
Patna	2	1
Pune	5	2.5
Rajkot	1	0.5
Ranchi	3	1.5
Ri Bhoi	1	0.5
Shivpuri	1	0.5
Sirsa	10	5.1
Solapur	1	0.5
Sonipat	6	3
South Delhi	1	0.5
South Garo Hills	1	0.5
Surat	1	0.5
Surendranagar	1	0.5
Tezpur	3	1.5
Thiruvananthapuram	2	1
Tiruchirappalli	2	1
Udaipur	1	0.5
Vadodara	1	0.5

Source: Data analysis by author.

The demographic profile of the respondents shows that they come from a wide range of genders, states, and districts in India. Of the total participants, 62.6% (124) were male and 37.4% (74) were female, which means that more male than female took part in the study. The entire sample (100%) consisted of individuals aged 20 and under, aligning with the study's focus on high school students. The respondents represented 23 Indian states, indicating a broad geographical distribution. Haryana had the most respondents (15.2%), followed by Assam and Madhya Pradesh (9.1% each) and Maharashtra (7.1%).

Goa, Punjab, and Arunachal Pradesh had the least representation, with less than 2% of the total. More than 100 districts were represented, and the most prevalent responses came from Sirsa (5.1%), Sonipat (3%), Chennai (3%), and Baksa (3%). This wide range of responses validate the study, aimed to collate opinions from people in India who speak different languages, come from different regions, and have distinct customs. The demographic data indicates that the student group is well-balanced and regionally diverse, providing a strong foundation for examining trends in cybersecurity education and awareness in India.

Fig 4.1: Student's Gender Distribution

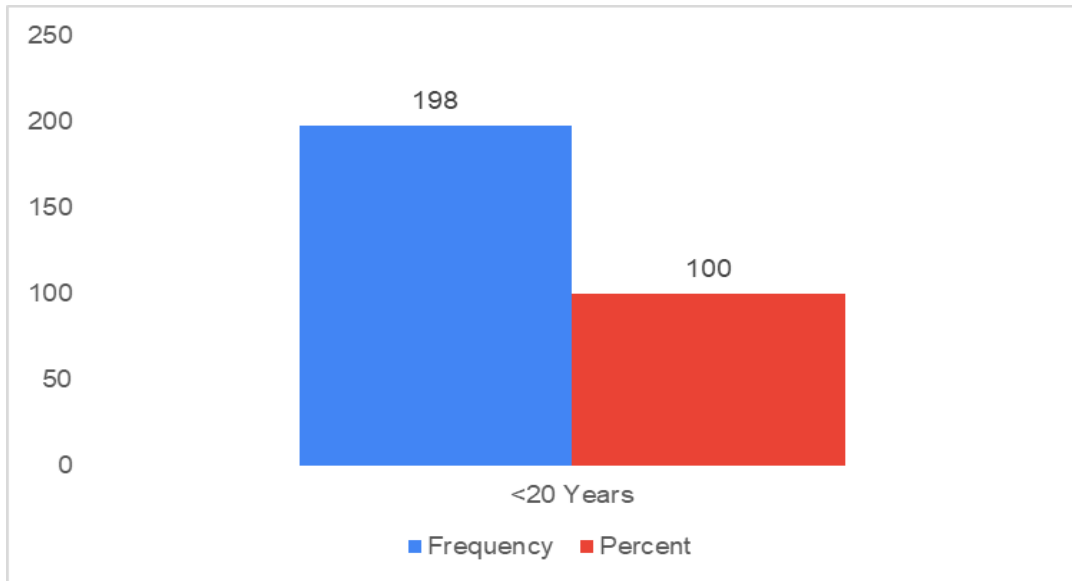


Source: Data analysis by author.

Figure 4.1: Gender

Figure 4.1 illustrates the gender distribution of the study participants. Of the 198 students who responded, 124 (62.6%) were male and 74 (37.4%) were female. This indicates that the sample contains more male than female, which may reflect the broader gender composition of the industry or context under study.

Fig 4.2: Student's Age Group



Source: Data analysis by author.

Figure 4.2: Age-Group

Figure 4.2 shows the age-group of the students who participated in the survey study. The data show that all 198 student respondents (100%) are under the age of 20. This shows that the whole sample is made up of young people aligning to this study objective targeting high school community, and captures the views, attitudes, and perspectives of this age group.

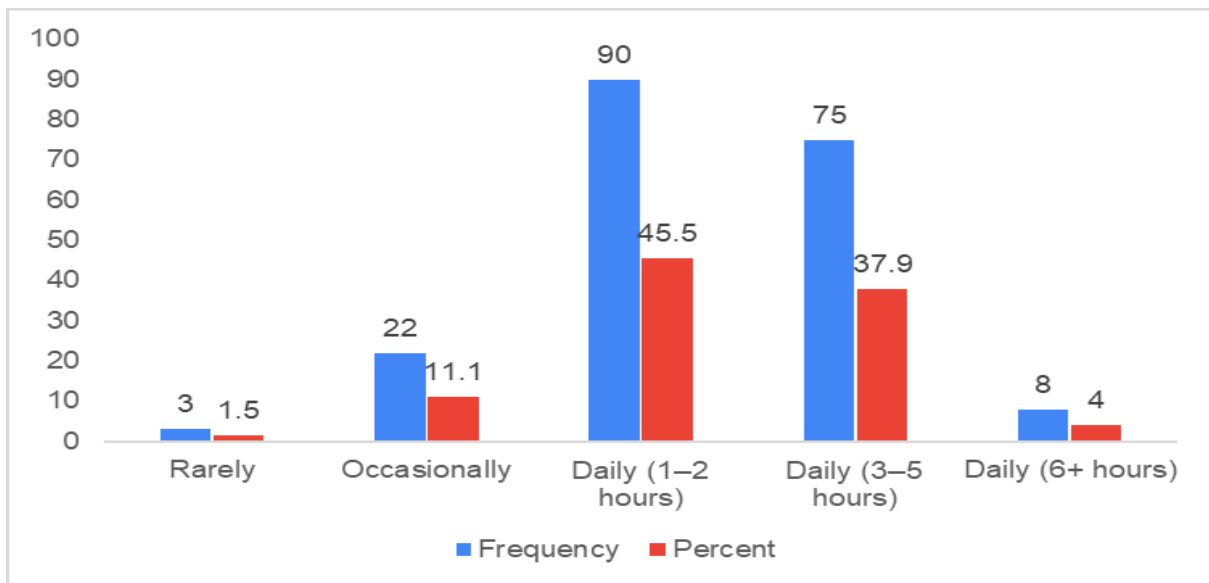
Table 4.7: Internet Usage Pattern Among Students

Table 4.7: How often do you use the internet for schoolwork or personal purposes?

	Frequency	Percent
Rarely	3	1.5
Occasionally	22	11.1
Daily (1–2 hours)	90	45.5
Daily (3–5 hours)	75	37.9
Daily (6+ hours)	8	4.0

Source: Data analysis by author.

Fig 4.3: Internet Usage Pattern Among Students



Source: Data analysis by author.

Figure 4.3: How often do you use the internet for schoolwork or personal purposes

Figure 4.3 and Table 4.7 show how often the student respondents of the survey used internet for schoolwork or personal reasons. The findings suggest that most of student's use the internet every day; with 45.5% having an internet usage time of 1–2 hours and 37.9% spending 3–5 hours on internet. Only 4.0% of the respondents mentioned they used the internet for more than 6 hours a day, while 11.1% mentioned they used the internet occasionally and 1.5% mentioned using is rarely. The survey results indicate that significant number of student participants access the internet daily, reflecting the growing reliance on digital resources for both academic and personal tasks.

Table 4.8: Devices Used by Students to Access Internet

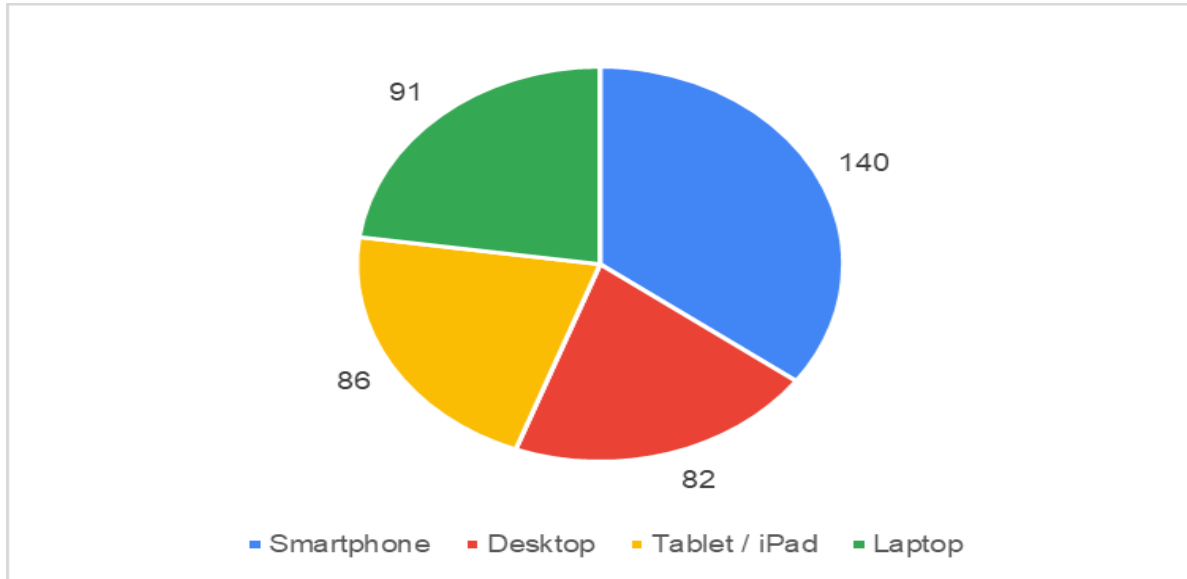
Table 4.8: Devices Most Frequently Used to Access the Internet

Device	Number of Times Chosen
Smartphone	140
Desktop	82
Tablet / iPad	86

Laptop	91
--------	----

Source: Data analysis by author.

Fig 4.4: Devices Used by Students to Access Internet



Source: Data analysis by author.

Figure 4.4: Which devices do you use most often to access the internet?

According to Figure 4.4 and Table 4.8, the most common devices to access internet by student participants were smartphones (140), followed by laptops (91), tablets/iPads (86), and Desktop (82). This reveals a clear preference for mobile technology, consistent with students' increasing reliance on cellphones for online activities and digital learning.

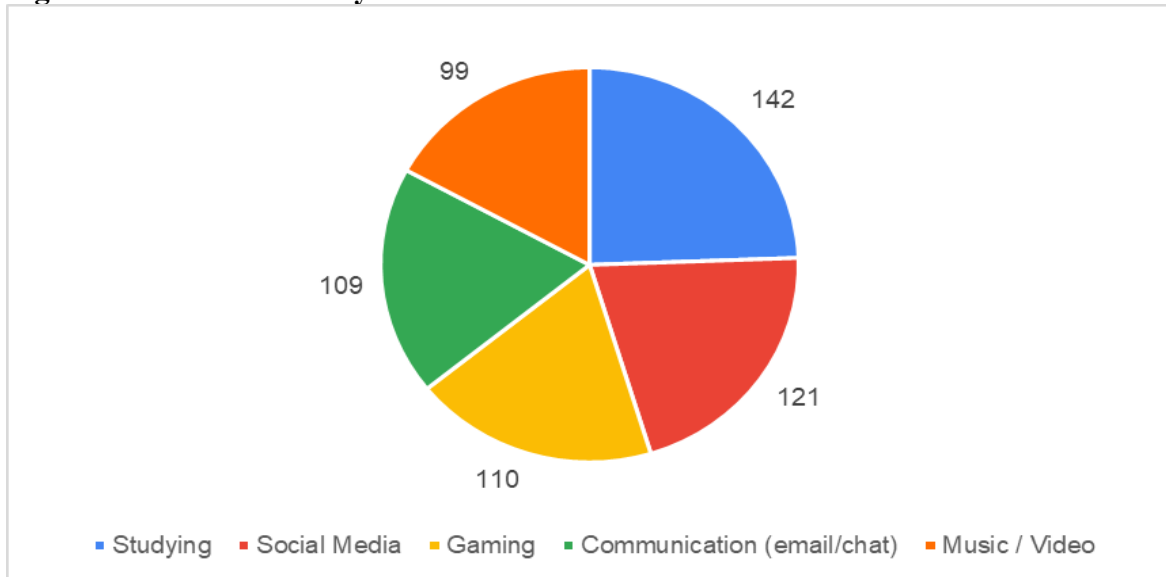
Table 4.9: Student's Primary Online Activities

Table 4.9: Primary Online Activities of Respondents

Category	Number of Times Chosen
Studying	142
Social Media	121
Gaming	110
Communication (email/chat)	109
Music / Video	99

Source: Data analysis by author.

Fig 4.5: Student's Primary Online Activities



Source: Data analysis by author.

Figure 4.5: What are your main purposes of using digital devices?

Figure 4.5 and Table 4.9 shows that most of the student respondents used digital devices for study (142), followed closely by social media (121) and gaming (110). Students also used these devices to converse with each other through email or chat (109) and watch or listen to music or videos (99). This trend demonstrates that students primarily use technology for academic purposes, although entertainment and socializing also remain prominent purposes.

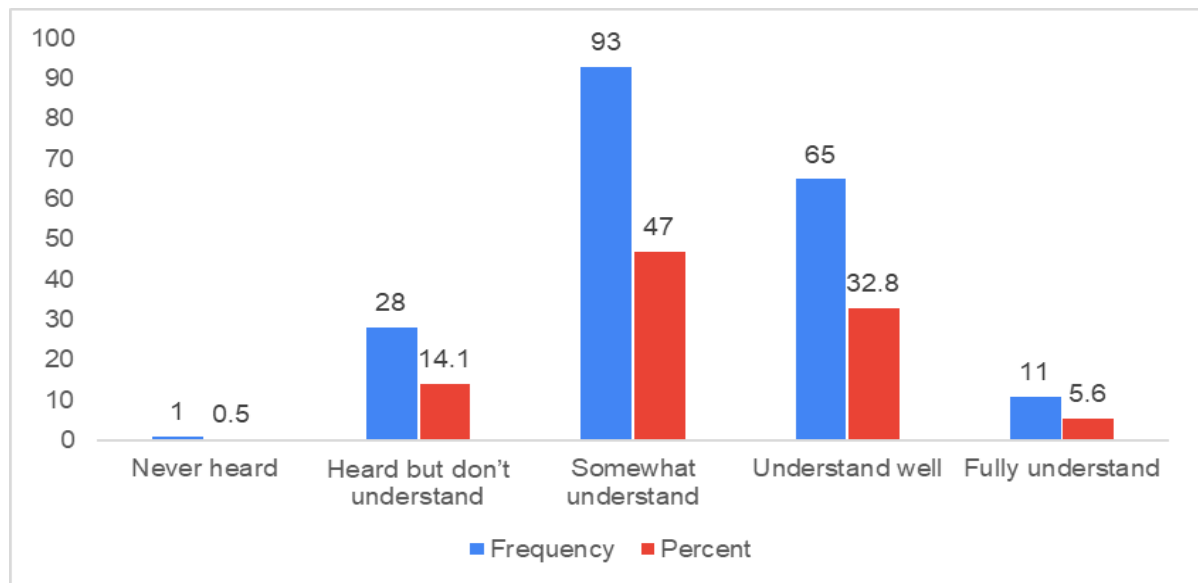
Table 4.10: Student's Understanding of Term Cybersecurity

Table 4.10: How well do you understand the term Cybersecurity?

Category	Frequency	Percent
Never heard	1	.5
Heard but don't understand	28	14.1
Somewhat understand	93	47.0
Understand well	65	32.8
Fully understand	11	5.6

Source: Data analysis by author.

Fig 4.6: Student's Understanding of Term Cybersecurity



Source: Data analysis by author.

Figure 4.6: How well do you understand the term Cybersecurity?

Figure 4.6 and Table 4.10 illustrate how well the student participants understood the term cybersecurity. The findings show that almost half of the respondents (47.0%) mentioned they partly grasp the idea of cybersecurity, and 32.8% understood it well. Only 5.6% fully understood cybersecurity, 14.1% of students had heard the term but didn't know what it meant, and only 0.5% had never heard of it. This distribution shows that most of the students who answered the question have a moderate to good comprehension of cybersecurity. Despite progress, the presence of many who struggle to grasp the concept, emphasizes the necessity of enhanced education and awareness around digital safety.

Table 4.11: Awareness Levels of Students on Different Cybersecurity Practices

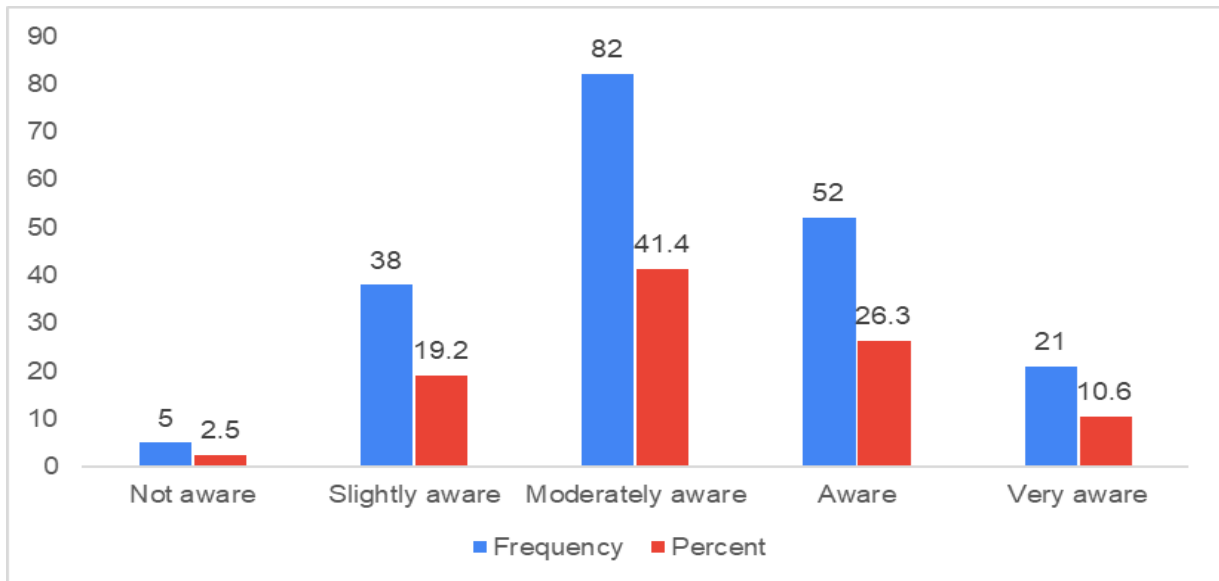
Table 4.11: Awareness Levels of Respondents on Different Cybersecurity Practices

Awareness Level	Distribution	Not aware	Slightly aware	Moderately aware	Aware	Very aware
Phishing Email	Frequency	5	38	82	52	21
	Percent	2.5	19.2	41.4	26.3	10.6
	Frequency	0	21	66	83	28

Strong Password Practices	Percent	0	10.6	33.3	41.9	14.1
Safe social media behavior	Frequency	0	26	93	69	10
	Percent	0	13.1	47	34.8	5.1
Cyberbullying	Frequency	14	42	69	47	26
	Percent	7.1	21.2	34.8	23.7	13.1
Reporting suspicious activity	Frequency	5	50	89	45	9
	Percent	2.5	25.3	44.9	22.7	4.5

Source: Data analysis by author.

Fig 4.7: Awareness Level of Students on Phising Email



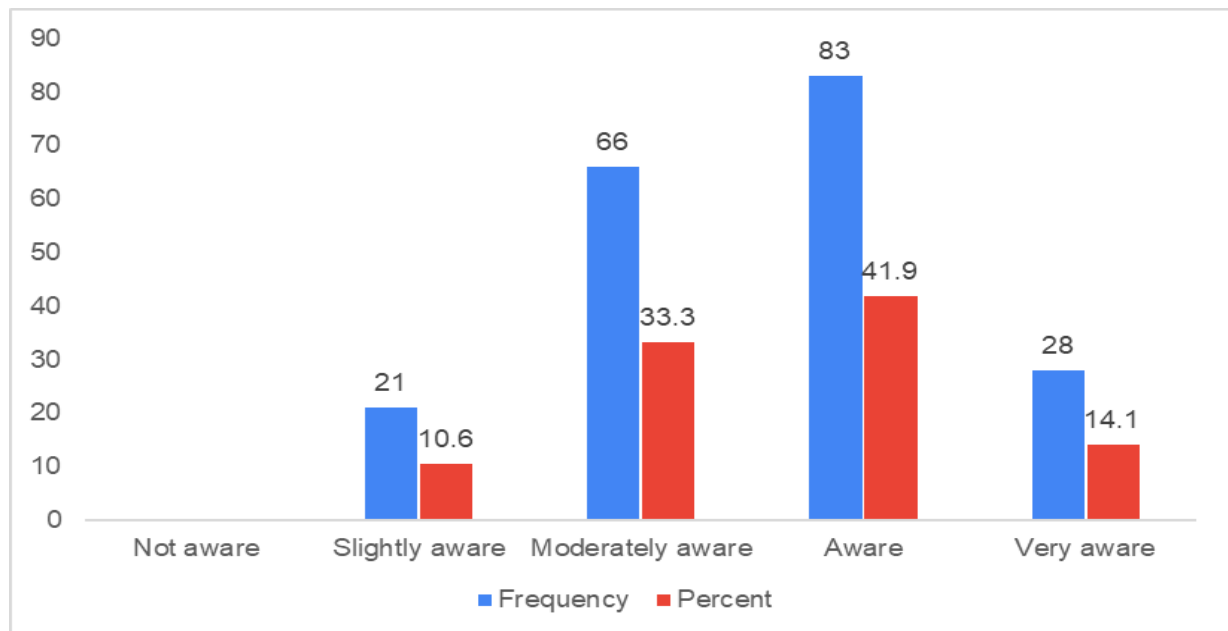
Source: Data analysis by author.

Figure 4.7: Phishing Email

Figure 4.7 and Table 4.11 show how much students were aware of Phishing emails. The findings reveal somewhat to extremely informed participants: 41.4% are moderately aware, 26.3% are aware, and 10.6% are highly aware. 19.2% mentioned, they were somewhat informed, and only 2.5% mentioned not being aware of phishing emails. The findings suggest that although the majority demonstrate adequate knowledge of phishing

emails, a minor portion may benefit from targeted awareness campaigns and structured cybersecurity education.

Fig 4.8: Awareness Level of Students on Password Practices

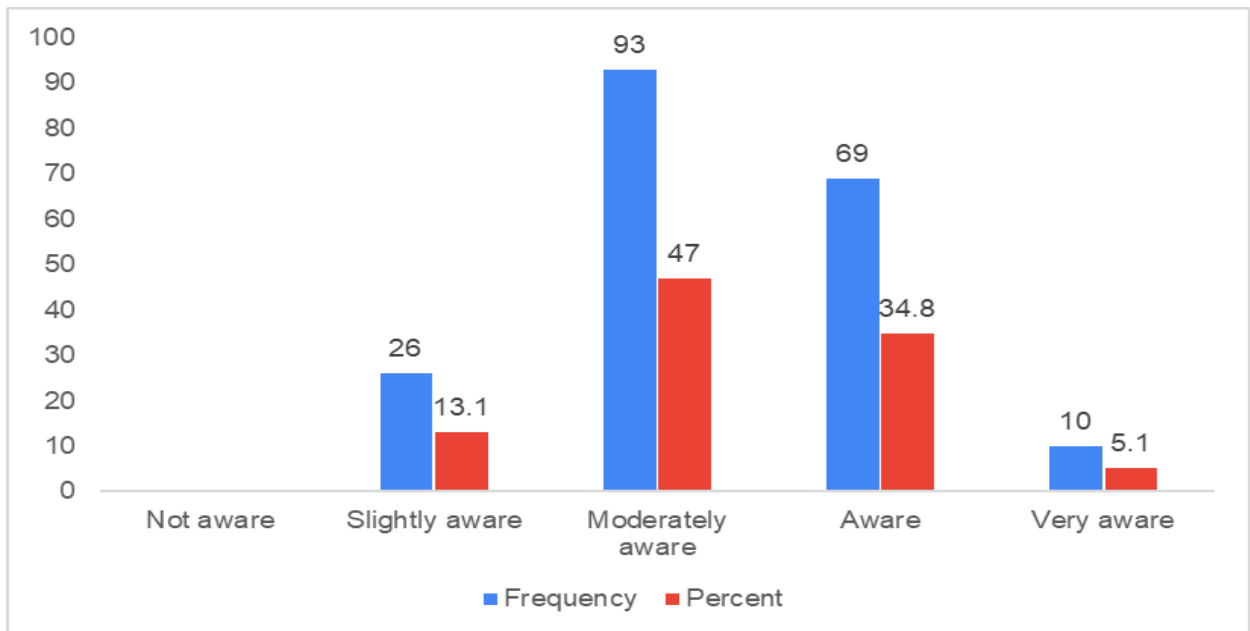


Source: Data analysis by author.

Figure 4.8: Strong Password Practices

Figure 4.8 and Table 4.11 illustrate how much the student participants were aware of strong password practices. The results indicate 41.9% having awareness and 14.1% indicating a high level of awareness regarding strong password practices. Also, 33.3% said they were somewhat aware, and a smaller group of 10.6% said they were slightly aware. The findings reveal that while strong password practices are widely understood, continuous awareness-raising is necessary to adapt to evolving risks, close knowledge gaps, and embed cybersecurity into everyday digital culture.

Fig 4.9: Awareness Level of Students on Safe Social Media Behavior

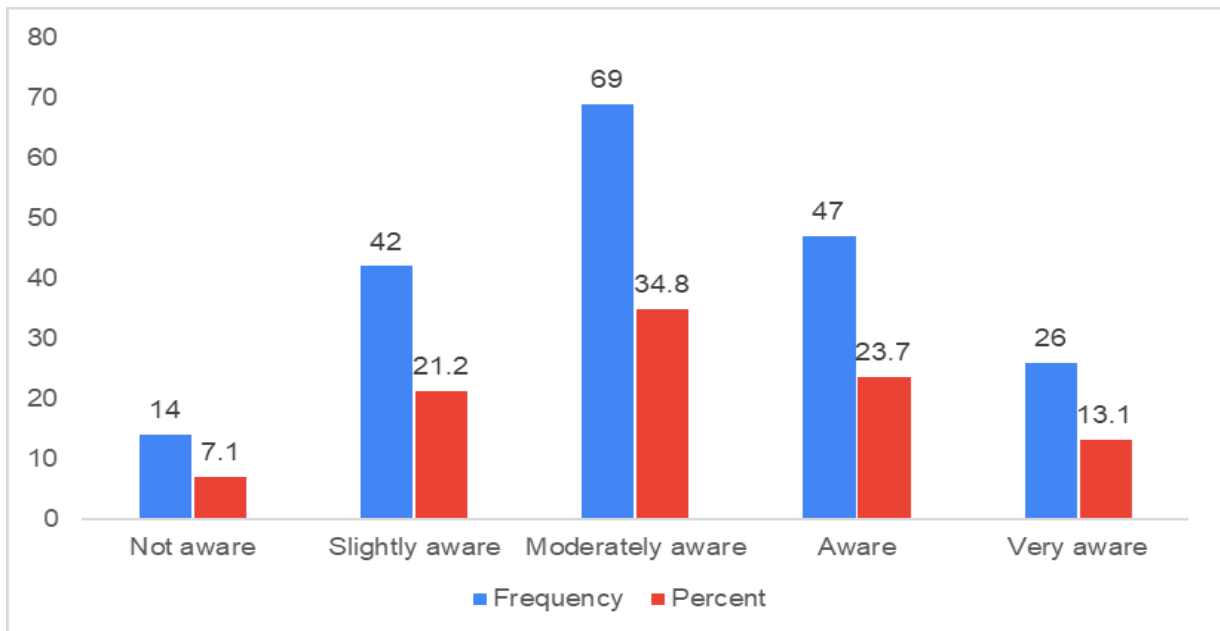


Source: Data analysis by author.

Figure 4.9: Safe social media behavior

Figure 4.9 and Table 4.11 illustrate how much the student respondents were aware of safe social media behavior. The numbers demonstrate that a significant student population: 47.0% are moderately aware and 34.8% are aware of safe social media behavior. At the same time, 13.1% of the respondents indicated they were slightly aware and 5.1% were very aware. This pattern suggests that the majority of student respondents recognize the importance of safe social media behavior. However, sustained education and targeted training programs are required to embed these behaviors deeply and prepare students for the challenges of an increasingly digital society.

Fig: 4.10: Awareness Level of Students on Cyberbullying

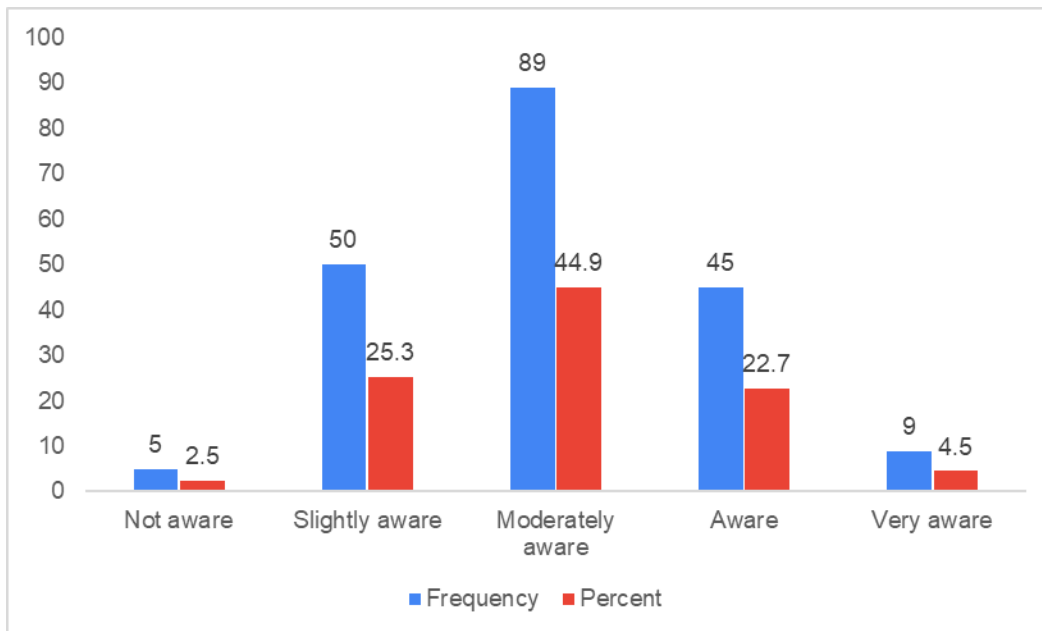


Source: Data analysis by author.

Figure 4.10: Cyberbullying

Figure 4.10 and Table 4.11 demonstrate how well student participants were aware of cyberbullying. The results indicate that most of the students possess moderate to high level of understanding on cyberbullying. 34.8% are moderately aware, 23.7% are aware, and 13.1% are very aware. Also worth noting, 21.2% are slightly aware, and 7.1% indicated not being aware of cyberbullying. The findings reveal that although awareness of cyberbullying is moderate to strong among many students, a significant portion remains underinformed (28.3%). This demonstrates the importance of teaching digital empathy, responsible online behavior, and reporting mechanisms.

Fig 4.11: Awareness Level of Students on Reporting Suspicious Activity



Source: Data analysis by author.

Figure 4.11: Reporting suspicious activity

Figure 4.11 and Table 4.11 show how aware student participants were with respect to reporting suspicious activity. The findings show that students are somewhat aware of reporting suspicious activity, with 44.9% being somewhat aware and 22.7% being aware. Also, 25.3% are slightly aware, 4.5% are highly informed, and only 2.5% mentioned being not aware. This indicates that most respondents know at least something about reporting suspicious activity and the related dangers, but more awareness is essential to close knowledge gaps and foster a culture of vigilance.

Table 4.12: Students response to receiving formal training / attending workshop on cybersecurity

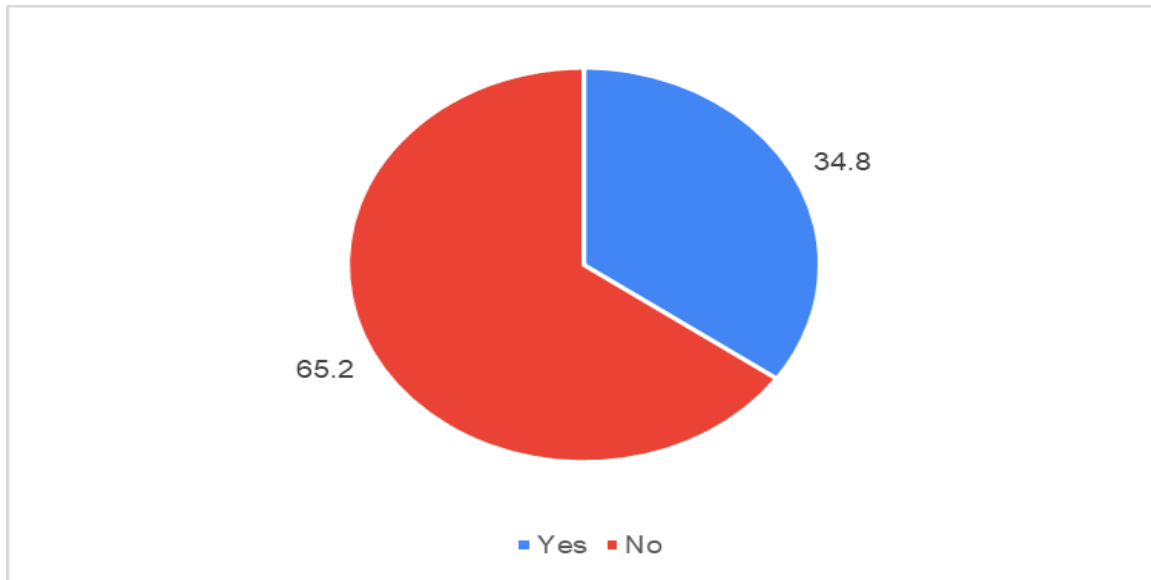
Table 4.12: Have you ever received any formal training/workshops on cybersecurity?

	Frequency	Percent
Yes	69	34.8
No	129	65.2

Total	198	100.0
-------	-----	-------

Source: Data analysis by author.

Fig 4.12: Students response to receiving formal training / attending workshop on cybersecurity



Source: Data analysis by author.

Figure 4.12: Have you ever received any formal training/workshops on Cybersecurity?

Figure 4.12 shows how many student respondents have taken part in any kind of cybersecurity training sessions or workshops. The results indicate that merely 34.8% of students had undergone such training, but a substantial majority of 65.2% have not participated in any official cybersecurity sessions. The findings reveal a clear shortfall in formal cybersecurity education among student respondents, underscoring the responsibility of schools and government to implement robust training initiatives that address knowledge gaps and foster a culture of digital safety.

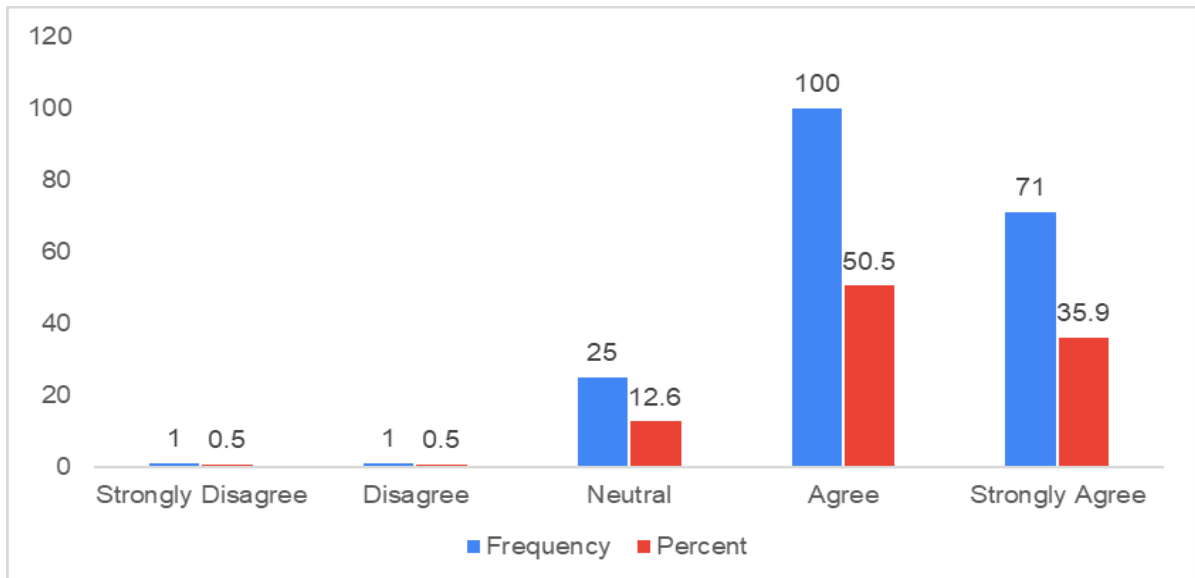
Table 4.13: Students Response to having Bilingual instructions to Enhance Awareness in ICT

Table 4.13: Would your awareness improve if Information and Communication Technologies (ICT) concepts were taught in the local language in addition to English?

	Frequency	Percent
Strongly Disagree	1	.5
Disagree	1	.5
Neutral	25	12.6
Agree	100	50.5
Strongly Agree	71	35.9
Total	198	100.0

Source: Data analysis by author.

Fig 4.13: Students Response to having Bilingual instructions to Enhance Awareness in ICT



Source: Data analysis by author.

Figure 4.13: Would your awareness improve if Information and Communication Technologies (ICT) concepts were taught in the local language in addition to English

Figure 4.13 shows what the student respondents thought regarding improved understanding, if Information and Communication Technologies (ICT) topics were taught in local languages, in addition to English. The numbers reveal that most of the respondents who filled out the survey agree with this viewpoint: 50.5% agree and 35.9% strongly agree. At the same time, 12.6% stayed neutral, while only 0.5% disagreed or strongly

disapproved. This suggests that teaching ICT and cybersecurity in local languages could greatly enhance digital learning, making it more accessible to a wider range of students and ensuring inclusivity across diverse linguistic backgrounds.

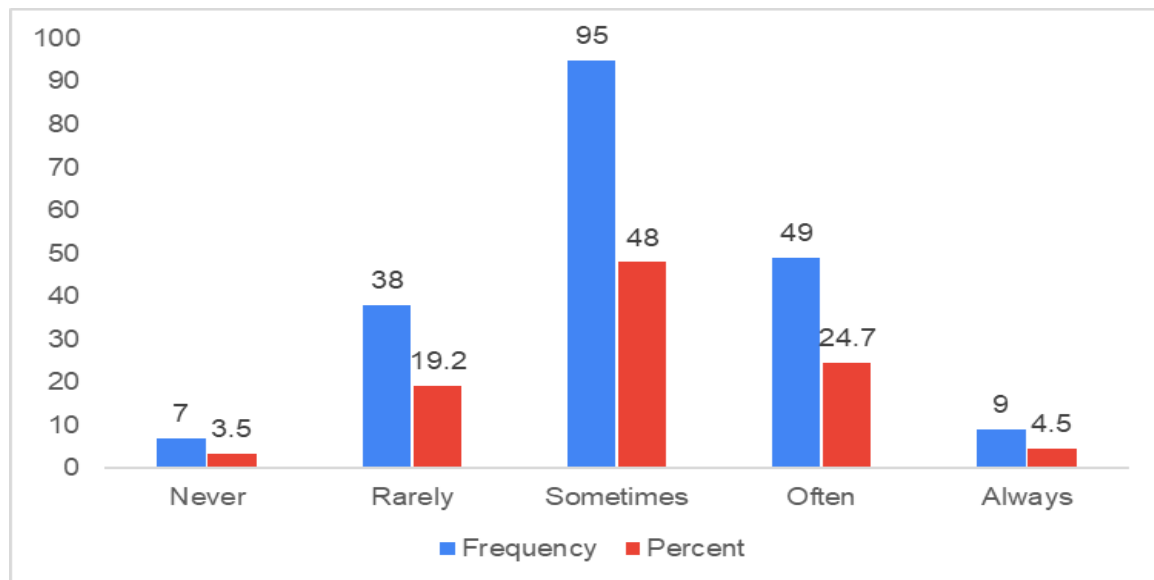
Table 4.14: Students Digital Behavior

Table 4.14: Usage of Online Techs

Statement	Category	Never	Rarely	Sometimes	Often	Always
Use the same passwords across multiple websites/apps	Frequency	7	38	95	49	9
	Percent	3.5	19.2	48	24.7	4.5
Use free public Wi-Fi for online payments or banking	Frequency	19	65	84	28	2
	Percent	9.6	32.8	42.4	14.1	1
Share. Your location on social media	Frequency	5	31	108	44	10
	Percent	2.5	15.7	54.5	22.2	5.1

Source: Data analysis by author.

Fig 4.14: Students Behavior on Reusing Passwords

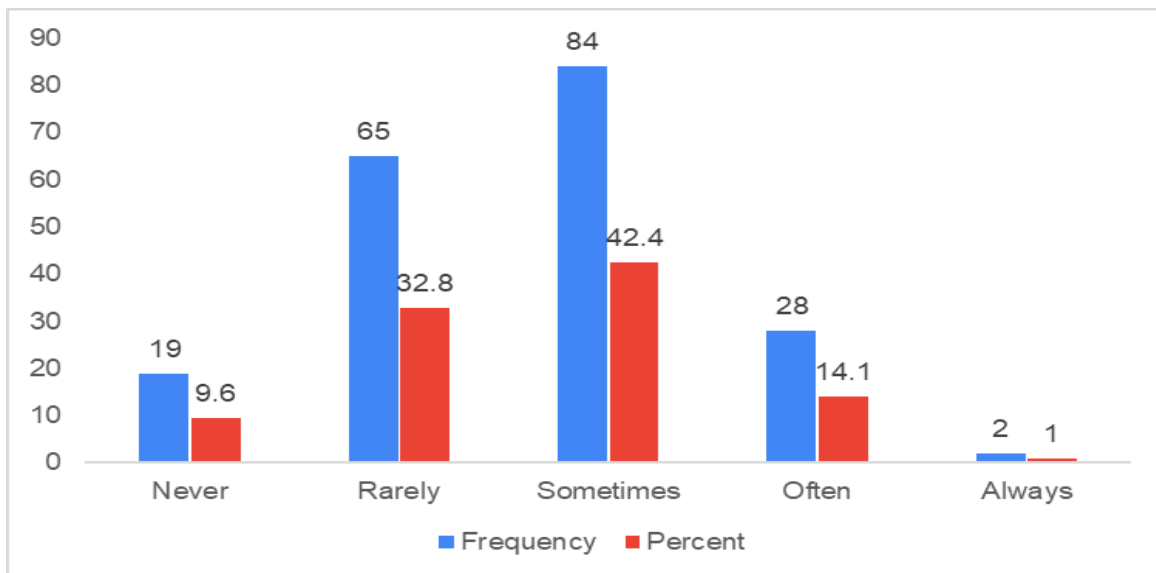


Source: Data analysis by author.

Figure 4.14: Use the same passwords across multiple websites/apps

Figure 4.14 shows survey participants responses on using the same password on more than one website or app. The results suggest that 48.0% of the people who took part in the study sometimes use the same password, 24.7% do so often, and 4.5% constantly reuse passwords. On the other side, 19.2% of people rarely use the same password again, while only 3.5% never re-used password. The survey results highlight that; a large portion of respondents are likely compromising their online security by reusing the same password across multiple accounts. This highlights the critical need to educate and encourage students for using unique and strong passwords; and to promote best practices in cybersecurity through awareness campaigns, training, and accessible tools such as password managers.

Fig 4.15: Students Behavior on Using Public Wi-Fi for Net-Banking



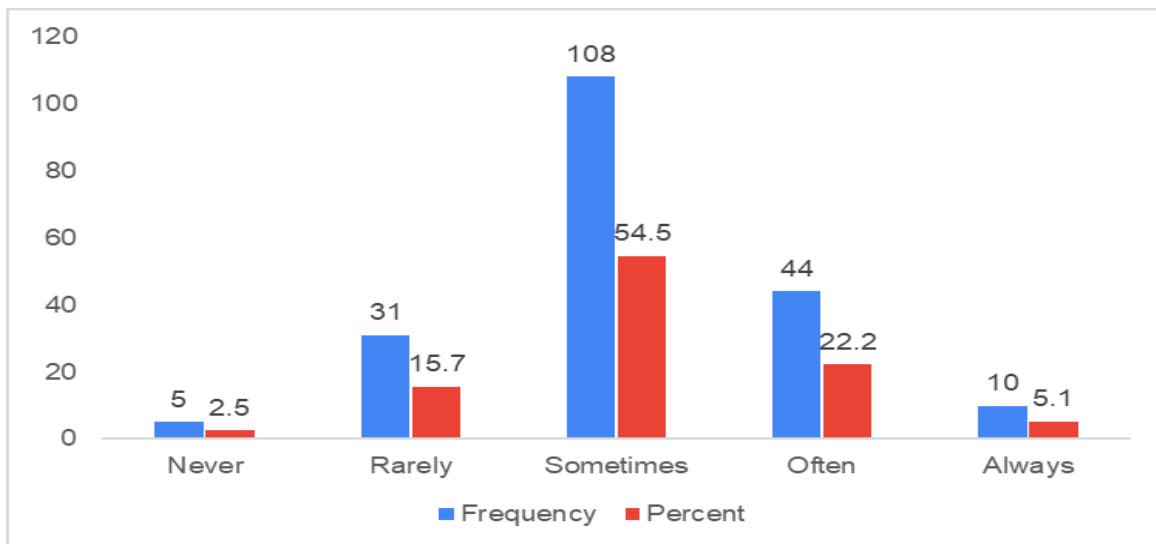
Source: Data analysis by author.

Figure 4.15: Use free public Wi-Fi for online payments or banking

Figure 4.15 illustrates student participants' responses regarding the use of free public Wi-Fi for paying bills or conducting online banking. The results suggest that 42.4% of the respondents sometimes use public Wi-Fi for these tasks, 32.8% do so rarely, and

14.1% do so regularly. A smaller minority of respondents (9.6%) said they never use public Wi-Fi for financial transactions, while only 1.0% said they always do. This illustrates that many individuals conduct online financial transactions using public Wi-Fi, a practice that can be highly risky. It highlights the urgent need to educate people about safe internet usage and the specific dangers associated with using public Wi-Fi, including data theft, financial frauds, phishing, and unauthorized access.

Fig 4.16: Students Behavior on Sharing Location Information

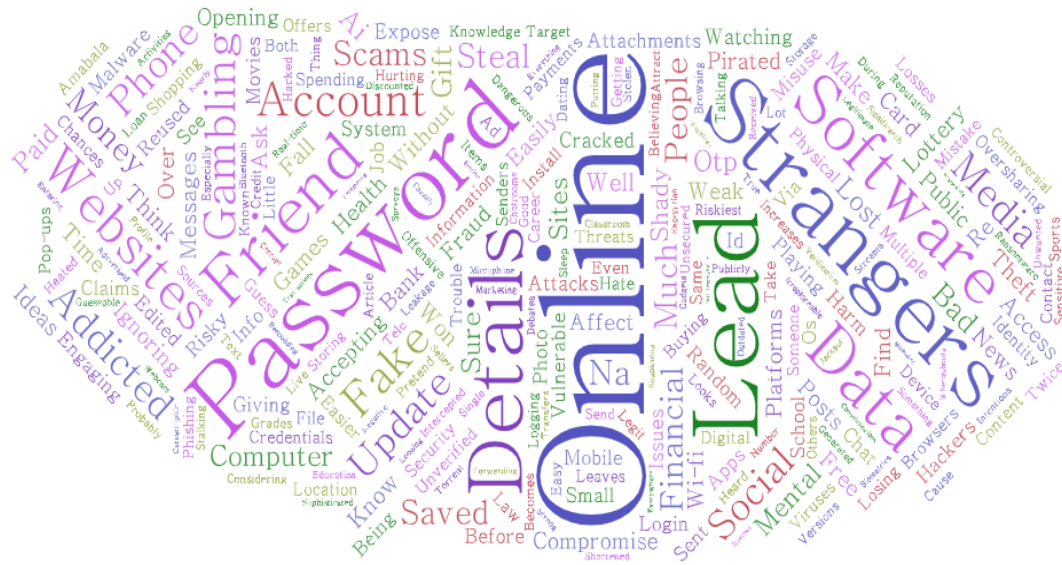


Source: Data analysis by author.

Figure 4.16: Share your location on social media

Figure 4.16 shows how student participants responded to the question on sharing their current location on social media. The data shows that 54.5% of people sometimes share their location, 22.2% do so often, and 5.1% do it all the time. But only 2.5% of people never share their location, and 15.7% do so only often. The findings show that a significant number of students disclose their location or check-ins over social media, exposing themselves to potential privacy threats. This emphasizes the importance of educating students about responsible social media usage and the consequences of sharing personal details publicly.

Fig 4.17: Perception of Students on Risky Online Behavior



Source: Data analysis by author.

Figure 4.17: Perceived Risky Online Activities Among Students

Figure 4.17 illustrates a word cloud consisting of the most prevalent words participants used when they talked about online safety and being aware of cybersecurity. The frequent use of terms such as “Password”, “Online”, “Strangers”, “Details”, “Software”, and “Friend” indicates that students were concerned with safeguarding their passwords, protecting personal data, avoiding risky interactions with strangers, and ensuring the security of their software. Students also expressed worries about the dangers of the digital environment, reflected in words like “Gambling”, “Fake”, “Update”, “Websites”, and “Phishing”. Similarly, references to “Saved”, “Account”, “Social Media”, and “Mobile” suggest that the central focus is on protecting personal information across multiple platforms. Overall, the responses from students’ reveal that most respondents are aware of critical digital safety concepts, underscoring the importance of adopting strong passwords, practicing caution when communicating online, and remaining vigilant against fraudulent websites, malicious software, and other evolving digital threats.

Table 4.15: Descriptive Statistics of the Students' Survey*Table 4.15: Descriptive Statistics of the Students' Survey*

	N	Mean		Std. Deviation
	Statistic	Statistic	Std. Error	Statistic
Gender	198	1.37	.034	.485
Age Group	198	1.00	.000	.000
State	198	11.60	.424	5.969
District	198	60.58	2.402	33.799
How often do you use the internet for schoolwork or personal purposes?	198	3.32	.056	.784
How well do you understand the term Cybersecurity?	198	3.29	.057	.795
Safe social media behavior	198	3.23	.069	.965
Cyberbullying	198	3.60	.061	.860
Reporting suspicious activity	198	3.32	.054	.764
Strong password practices	198	3.15	.079	1.115
Phishing email	198	3.02	.062	.875
Have you ever received any formal training/workshops on cybersecurity?	198	1.65	.034	.478
Would your awareness improve if Information and Communication Technologies (ICT) concepts were taught in the local language in addition to English?	198	4.21	.051	.714
How often do you use the same passwords across multiple websites/apps?	198	3.08	.062	.872

How often do you use free public Wi-Fi for online payments or banking?	198	2.64	.062	.877
How often do you share your location on social media?	198	3.12	.058	.820

Source: Data analysis by author.

Table 4.15 shows the descriptive statistics for the respondents' demographic traits and behaviors related to digital safety awareness. The statistics indicate that the average score for gender is 1.37 (SD = 0.485), signifying a greater percentage of male respondents. The average age of all participants is 1.00 (SD = 0.000), that implies all student respondents were under 20 years of age. The respondents come from different states and districts, with average values of 11.60 (SD = 5.969) and 60.58 (SD = 33.799), respectively. The average score for internet usage stands at 3.32 (SD = 0.784), which means that people often use the internet for schoolwork or personal reasons. Moderate levels of knowledge are shown by scores for safe social media behavior (M = 3.23, SD = 0.965), cyberbullying (M = 3.60, SD = 0.860), reporting suspicious activity (M = 3.32, SD = 0.764), strong password practices (M = 3.15, SD = 1.115), and phishing emails (M = 3.02, SD = 0.875). Only 34.8% of the student respondents had formal cybersecurity training (M = 1.65, SD = 0.478). Most of participants thought that teaching ICT ideas in their own languages will help them understanding better (M = 4.21, SD = 0.714). The average scores for password reuse (M = 3.08, SD = 0.872), utilizing public Wi-Fi for financial transactions (M = 2.64, SD = 0.877), and sharing location information on social media (M = 3.12, SD = 0.820) reveal that students are exposed to varied levels of online risks. The descriptive statistics outline the demographic distribution of student participants by age, gender and related attributes. It also highlights their familiarity with cybersecurity concepts and the degree to which they apply safe practices online.

Findings of the Parents' Survey

This section reports the findings based on the survey conducted among the parents of Indian high school students, with 126 participants providing responses.

Table 4.16: Demographic Profile of Surveyed Parents

Table 4.16: Demographic Details of Parents

Category		Frequency	Percent
Gender	Male	95	75.4
	Female	31	24.6
Age Group	20-29 Years	8	6.3
	30-39 Years	42	33.3
	40-49 Years	63	50
	50+ Years	13	10.3
State	Assam	10	7.9
	Chandigarh	2	1.6
	Chhattisgarh	5	4
	Delhi	4	3.2
	Goa	1	0.8
	Gujarat	5	4
	Haryana	12	9.5
	Himachal Pradesh	2	1.6
	Karnataka	13	10.3
	Kerala	2	1.6
	Madhya Pradesh	28	22.2
	Maharashtra	9	7.1
	Odisha	1	0.8
	Punjab	3	2.4
	Rajasthan	2	1.6
	Tamil Nadu	9	7.1
	Uttar Pradesh	18	14.3
District	Agra	4	3.2
	Ambala	1	0.8
	Amritsar	1	0.8
	Amroha	1	0.8

	Ballia	1	0.8
	Bangalore	10	7.9
	Barnala	1	0.8
	Bathinda	1	0.8
	Bengaluru	1	0.8
	Bharuch	1	0.8
	Bhavnagar	2	1.6
	Bhind	2	1.6
	Bhiwani	1	0.8
	Bhopal	1	0.8
	Bilaspur	2	1.6
	Chennai	3	2.4
	Chitrakoot	1	0.8
	Coimbatore	1	0.8
	Dabra	1	0.8
	Datia	1	0.8
	Delhi	3	2.4
	Devas	1	0.8
	Dharmapuri	1	0.8
	Dibrugarh	1	0.8
	Erode	2	1.6
	Etawah	1	0.8
	Faridabad	4	3.2
	Ganjam	1	0.8
	Gariaband	1	0.8
	Goa	1	0.8
	Guna	2	1.6
	Gwalior	10	7.9
	Hojai	1	0.8
	Indore	3	2.4
	Jaipur	1	0.8
	Jamnagar	1	0.8
	Jashpur	1	0.8
	Jhansi	2	1.6

	Kallakurichi	1	0.8
	Kanpur	9	7.1
	Korba	1	0.8
	Lucknow	4	3.2
	Mahoba	1	0.8
	Malappuram	1	0.8
	Mandi	1	0.8
	Morena	2	1.6
	Mumbai	2	1.6
	Nagpur	1	0.8
	Orai	1	0.8
	Panipat	1	0.8
	Pune	6	4.8
	Raipur	1	0.8
	Rohtak	1	0.8
	Sakti	1	0.8
	Salem	1	0.8
	Shimla	1	0.8
	Shivpuri	3	2.4
	Sirsa	4	3.2
	Solan	1	0.8
	Tiruvannamalai	1	0.8
	Trivandrum	1	0.8
	Tumkur	2	1.6
	Udaipur	1	0.8
	Ujjain	1	0.8
	Varanasi	1	0.8
	West Delhi	1	0.8

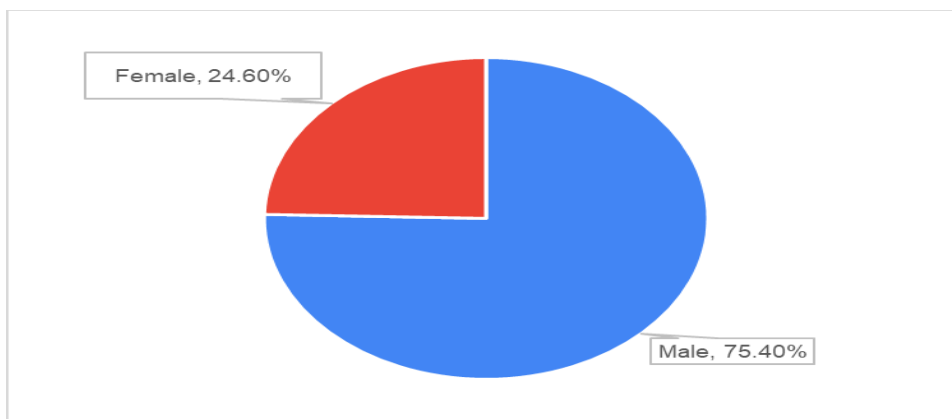
Source: Data analysis by author.

Table 4.16 details the demography of parents of high school students included in the sample survey and it represents a wide range of backgrounds, drawn from different states and districts across India. 24.6% of respondents were female and 75.4% were male. 50% of survey participants were between 40 and 49 years old, while 33.3% fell within the

30–39 age range. The data shows that middle-aged parents formed the predominant respondent group, which corresponds with the population most likely to have children in secondary education. The fact that only 6.3% of parents were aged 20–29 and 10.3% were 50 or older, suggest low participation rates among both younger and older parental groups.

The most represented Indian states among the respondents were Madhya Pradesh (22.2%), Uttar Pradesh (14.3%), Karnataka (10.3%), Haryana (9.5%), and Assam (7.9%). This indicates that a broad range of regions were covered by the survey. Smaller yet significant contributions from states like Tamil Nadu (7.1%), Maharashtra (7.1%), Chhattisgarh (4%), and Gujrat (4%) demonstrate how inclusive the survey was. This diversity is further underscored by district-level data, which capture parent participants from smaller regions alongside urban and semi-urban centers such as Bangalore (7.9%), Gwalior (7.9%), Kanpur (7.1%), Pune (4.8%), Lucknow (3.2%), and Chennai (2.4%); thereby offering a broad spectrum of perspectives. This demographic mix ensures that the researcher’s analysis of parental understanding and their active involvement in high school cybersecurity education reflects a wide range of socio-geographical contexts and age-related experiences.

Fig 4.19: Parents Gender

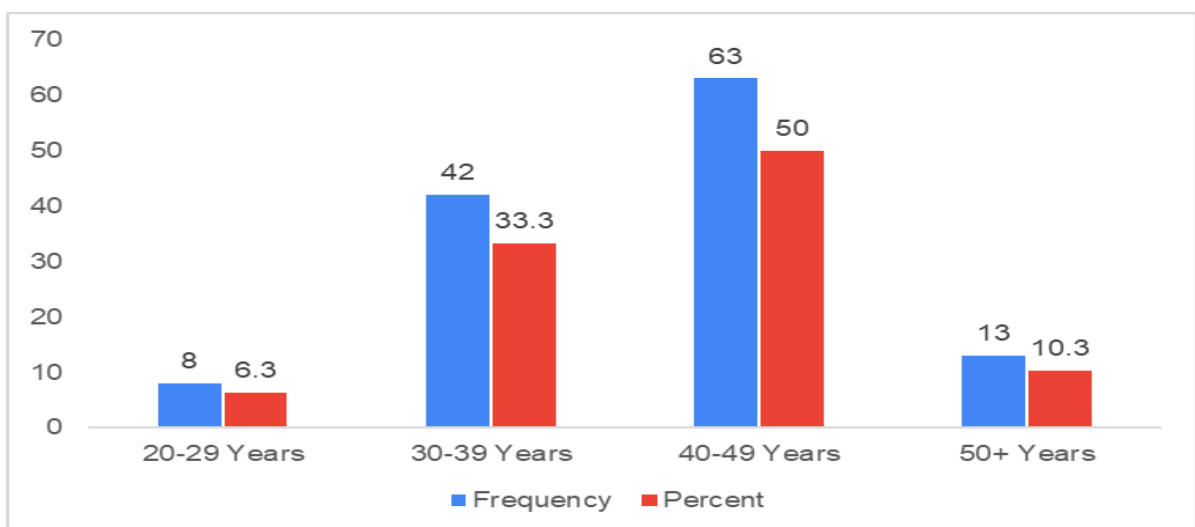


Source: Data analysis by author.

Figure 4.19: Gender

The number of male and female parents who participated in the survey is represented in Figure 4.19. Of the total 126 respondents, 31 (24.6%) were female, and 95 (75.4%) were male participants. The sample is largely composed of male respondents, which may result in over representative male perspectives compared to the other groups. Recognizing this gender gap is essential, as it has the potential to influence the interpretation of observed patterns and trends.

Fig 4.20: Parents Age-Group



Source: Data analysis by author.

Figure 4.20: Age Group

Figure 4.20 depicts the age distribution of the survey participants. 33.3% of the parents are in the age bracket of 30-39, and 50% are between the ages of 40-49. Only 10.3% of respondents are 50 years of age or older, while only 6.3% are between the ages of 20 and 29. This indicates that middle-aged individuals form the largest group, a factor that may affect viewpoints, experiences, and level of engagement with the study's aims.

Table 4.17: Parents Awareness of Childs Online Activities

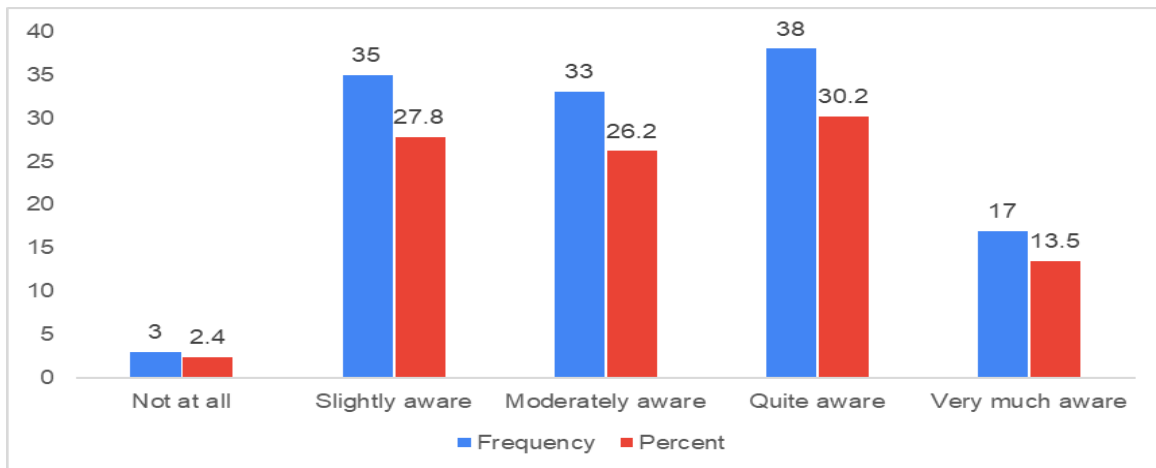
Table 4.17: How aware are you of your child's online activities?

	Frequency	Percent
Not at all	3	2.4

Slightly aware	35	27.8
Moderately aware	33	26.2
Quite aware	38	30.2
Very much aware	17	13.5
Total	126	100.0

Source: Data analysis by author.

Fig 4.21: Parents Awareness of Childs Online Activities



Source: Data analysis by author.

Figure 4.21: How aware are you of your child's online activities

Figure 4.21 shows how much the parents knew about their child online activities. The findings suggest that 30.2% of parents are highly knowledgeable, 26.2% are fairly aware, and 13.5% are very much aware. Also, 27.8% mentioned they were somewhat aware, and 2.4% were not at all aware regarding their children's internet activities. This shows that while most parents keep a reasonable level of oversight regarding their child's internet activities, a significant proportion do not. This lack of monitoring underscores the need for greater parental involvement to ensure responsible digital behavior among children, and reduce their exposure to potential risks such as cyberbullying, inappropriate content, and privacy breaches.

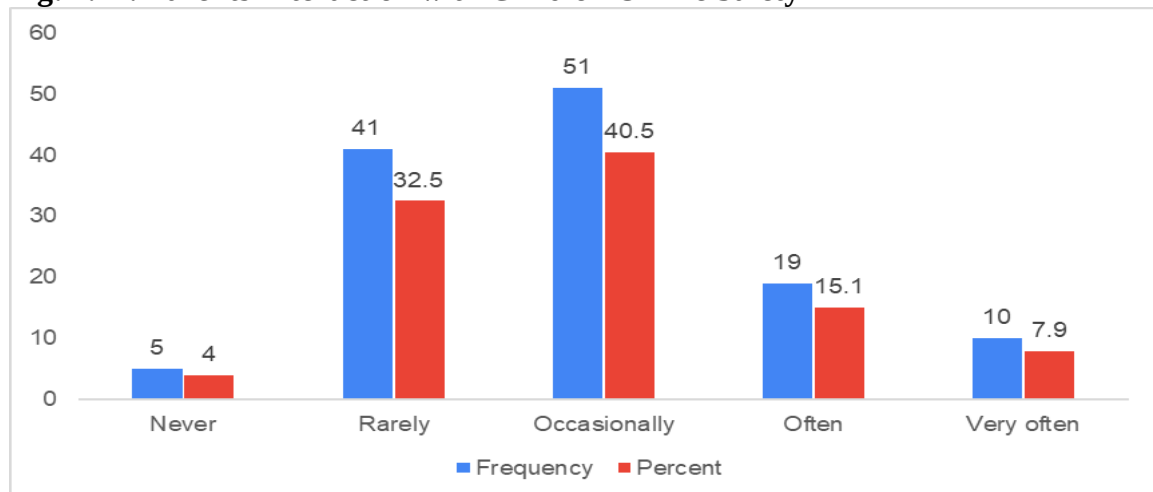
Table 4.18: Parents Interaction with Child on Online Safety

Table 4.18: How often do you talk to your child about online safety and responsible internet use?

	Frequency	Percent
Never	5	4.0
Rarely	41	32.5
Occasionally	51	40.5
Often	19	15.1
Very often	10	7.9
Total	126	100.0

Source: Data analysis by author.

Fig: 4.22: Parents Interaction with Child on Online Safety



Source: Data analysis by author.

Figure 4.22: How often do you talk to your child about online safety and responsible internet use

Figure 4.22 shows how often parents talk to their kids about online safety and how to use the internet responsibly. The results show that 40.5% of parents interact with their kids about safe digital practices occasionally, while 32.5% do so rarely. A relatively lesser percentage of parents talk about digital safety regularly (15.1%) or very often (7.9%), while 4.0% mentioned they never interacted with their children on this topic. This means that

even if some parents actively guide their kid’s online behavior, many do not do it very often. This highlights the need for greater parental awareness and frequent communication with children about responsible internet use, and the associated risks.

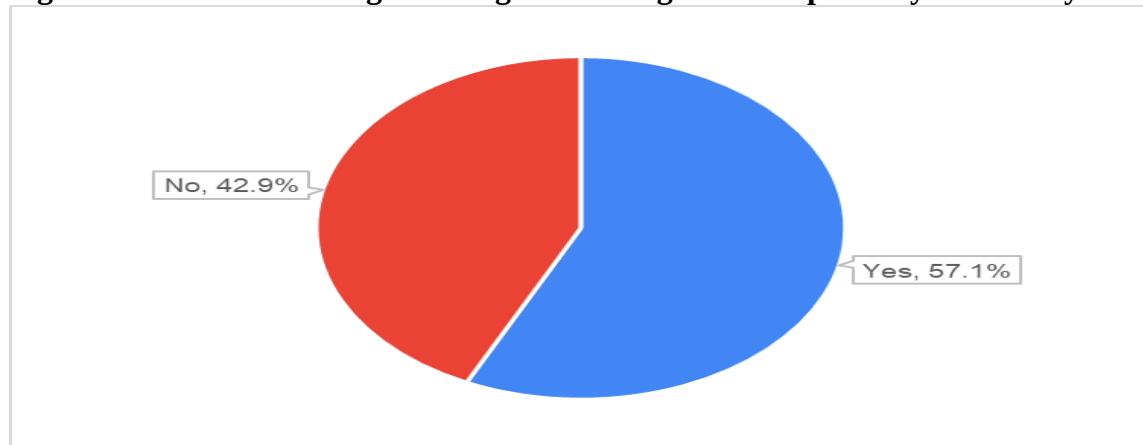
Table 4.19: Parents Receiving Training / Attending Workshops on Cybersecurity

Table 4.19: Have you ever received formal training/workshops on cybersecurity?

	Frequency	Percent
Yes	72	57.1
No	54	42.9

Source: Data analysis by author.

Fig 4.23: Parents Receiving Training / Attending Workshops on Cybersecurity



Source: Data analysis by author.

Figure 4.23: Have you ever received formal training/workshops on cybersecurity?

Figure 4.23 shows how many of the parents underwent some kind of training or workshops on cybersecurity. The statistics indicate that a majority of participants, 57.1%, have undergone formal training, whereas 42.9% have not participated in any such sessions. This means that more than half of the respondents are aware of cybersecurity concepts. The fact that a significant portion of parents reported not having formal training highlights the ongoing need to expand access to cybersecurity education. Strengthening such educational opportunities would enable more parents to develop the skills necessary to protect

themselves and their children's online activities, and contribute towards community awareness as well.

Table 4.20: Parents Awareness on Cybersecurity Practices

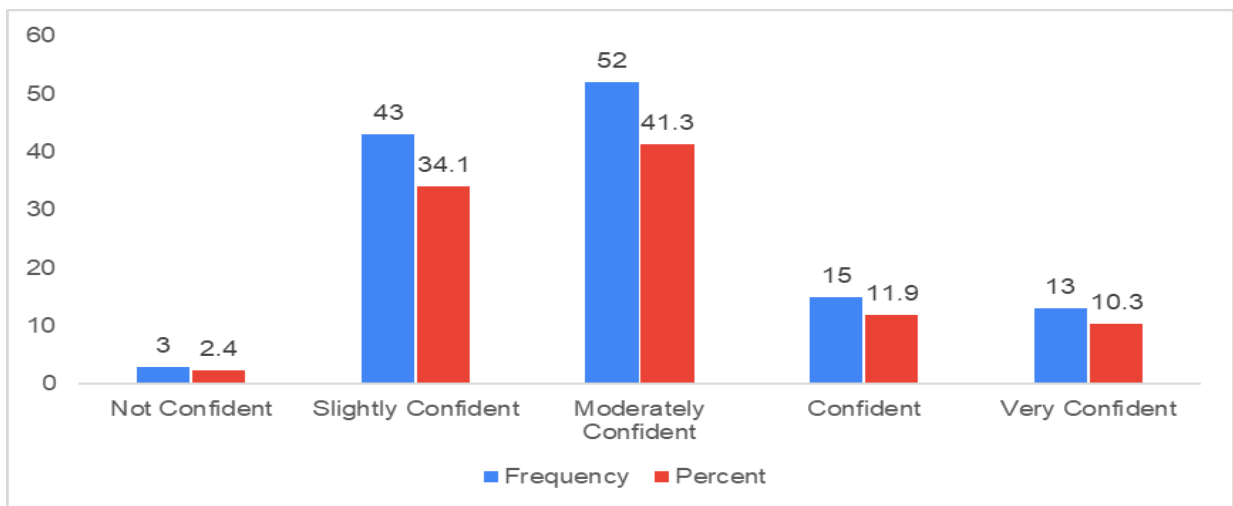
Table 4.20: Confidence Levels of Parents in Managing Cybersecurity Practices

Awareness / Confidence Level		Not Confident	Slightly Confident	Moderately Confident	Confident	Very Confident
Identifying online threats	Frequency	4	16	41	42	23
	Percent	3.2	12.7	32.5	33.3	18.3
Using parental controls on digital devices	Frequency	5	29	36	40	16
	Percent	4	23	28.6	31.7	12.7
Protecting personal data	Frequency	5	18	40	44	19
	Percent	4	14.3	31.7	34.9	15.1
Talking to children about cyber risks	Frequency	3	43	52	15	13
	Percent	2.4	34.1	41.3	11.9	10.3
Reporting Suspicious Activity	Frequency	2	25	40	39	20
	Percent	1.6	19.8	31.7	31	15.9
Recognizing phishing emails	Frequency	2	23	42	39	20
	Percent	1.6	18.3	33.3	31	15.9
Creating strong passwords	Frequency	0	12	43	41	30
	Percent	0	9.5	34.1	32.5	23.8
Promoting safe social	Frequency	7	32	32	32	23
	Percent	5.6	25.4	25.4	25.4	18.3

media behavior						
Monitoring screen time	Frequency	1	17	47	46	15
	Percent	0.8	13.5	37.3	36.5	11.9
Knowing Your Child's Online Friends	Frequency	12	24	37	33	20
	Percent	9.5	19	29.4	26.2	15.9

Source: Data analysis by author.

Fig 4.24: Parents Interaction with Child on Cyber Risks



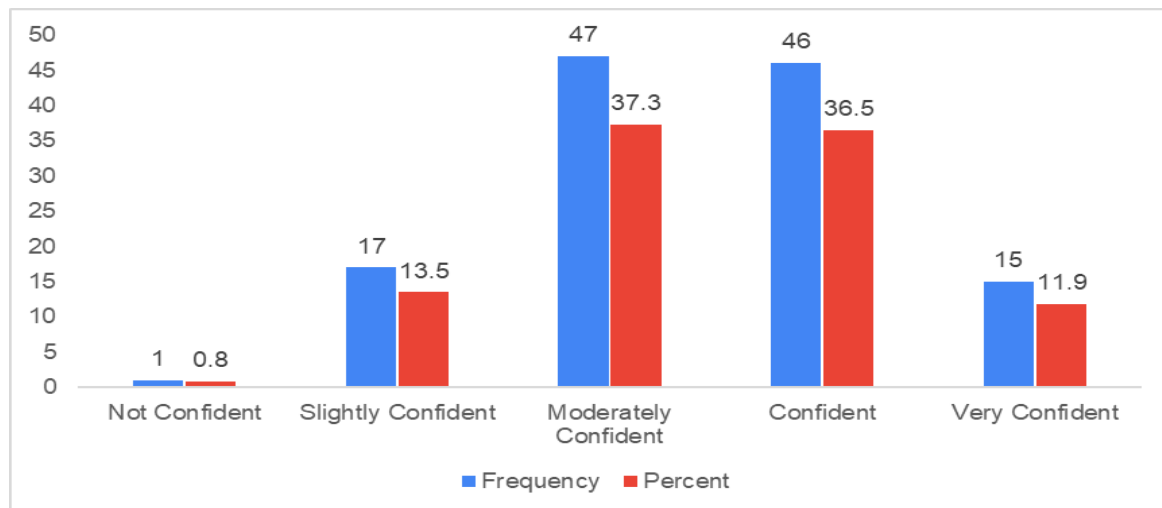
Source: Data analysis by author.

Figure 4.24: Talking to children about cyber risks

Figure 4.24 reports the confidence of parent participants when they talk to their kids about cyber hazards. The findings suggest that 11.9% of parents are confident, 41.3% are somewhat confident, and 10.3% are very confident. A large percentage of parents shared somewhat confidence (34.1%) or not confident (2.4%). The analysis indicates that only a small proportion of parents feel confident when discussing cyber risks with their children. A substantial segment of parents, however, lack this confidence and therefore require greater awareness and targeted training. Enhancing parental knowledge and skills in

cybersecurity is essential to ensure that children receive proper guidance, and develop safe online habits.

Fig 4.25: Parents Monitoring Childs Screen Time

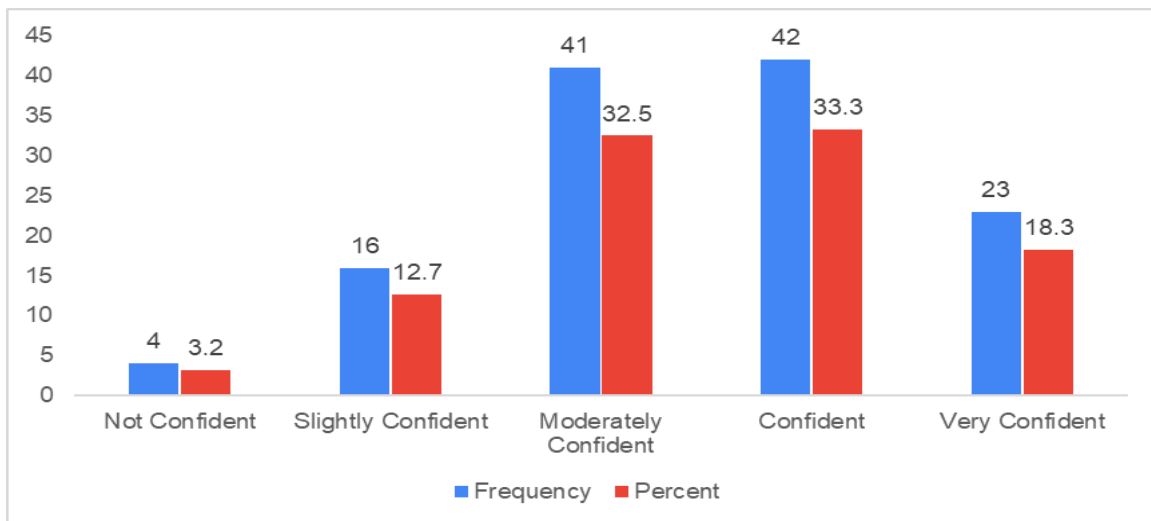


Source: Data analysis by author.

Figure 4.25: Monitoring screen time

Figure 4.25 shows how confident the parent participants were that they could keep an eye on their kids' screen time. The findings show that 36.5% of parents are sure they can handle screen time, 37.3% are somewhat sure, and 11.9% are extremely sure. Also, 13.5% mentioned they were somewhat confident, and 0.8% mentioned not being confident. The analysis suggests that most parents exercise moderate to low control over the amount of time their children spend on digital devices. As a result, they may benefit from guidance, resources, or practical strategies to strengthen their monitoring practices. Providing parents with effective tools and awareness programs can help them encourage healthier digital habits among the children. balance screen time, and reduce risks associated with excessive technology use, such as reduced physical activity, sleep disturbances, or exposure to harmful online content.

Fig 4.26: Parents Confidence on Identifying Online Threats

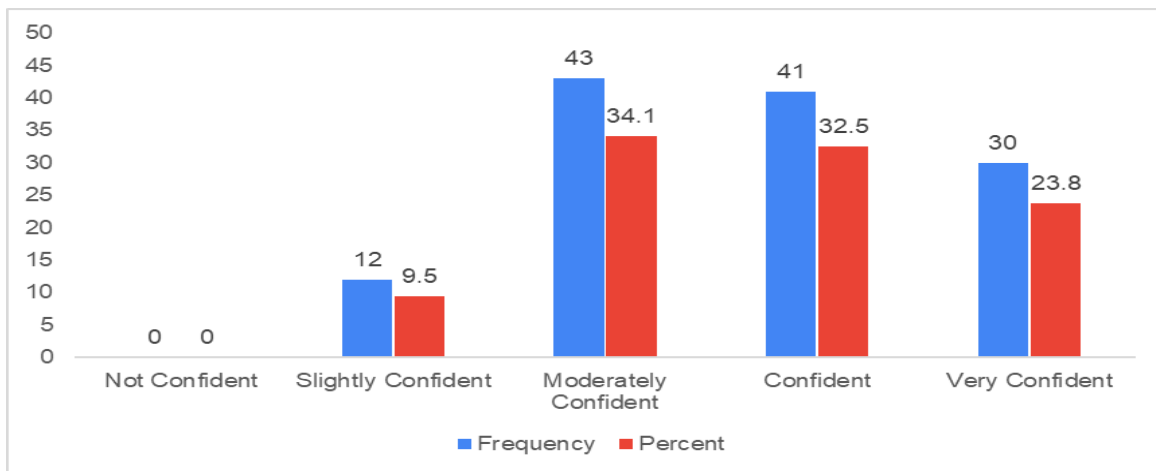


Source: Data analysis by author.

Figure 4.26: Identifying online threats

Figure 4.26 shows how sure parent participants were regarding their confidence on identifying internet threats. The study shows that 18.3% of parents were very confident, 33.3% are confident, and 3.2% are not at all confident in their ability to spot potential internet threats. At the same time, 12.7% said they were somewhat confident, and 32.5% said they were moderately confident. The findings suggest that, despite a large segment of parents being confident in their ability to recognize online threats, a notable portion of respondents demonstrated moderate to low confidence, and may need more guidance and training to get better at keeping themselves and their kids safe from digital threats.

Fig 4.27: Parents Awareness on Strong Password Practices

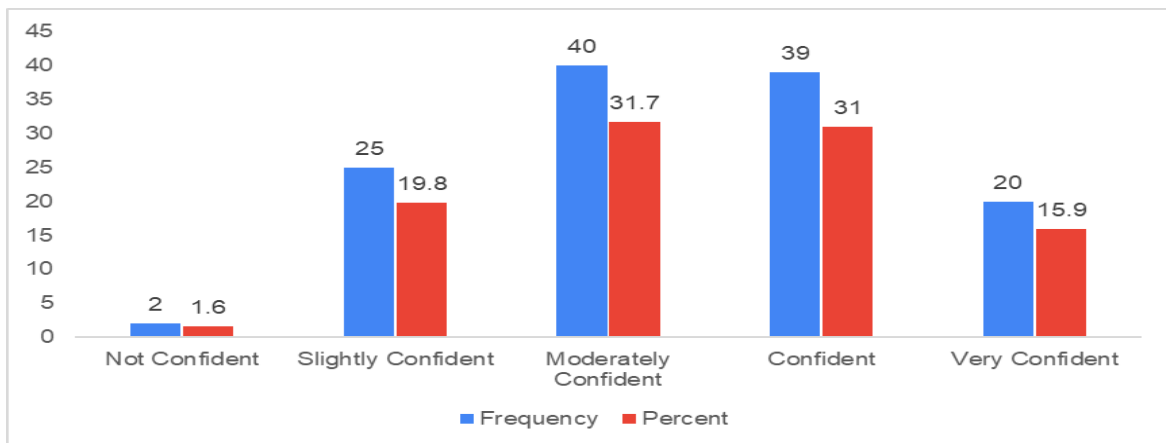


Source: Data analysis by author.

Figure 4.27: Creating strong passwords

Figure 4.27 shows confidence of parent respondents in creating and managing strong passwords. The findings show that 34.1% of parents are moderately confident, and 9.5% are slightly confident. Also, 32.5% mentioned they were confident, 23.8% said they were extremely confident, and 0.0% said they weren't confident at all. The findings indicate that although a majority of parents perceive themselves as competent in generating and maintaining strong passwords, a significant number express limited confidence. This highlights the need for training and awareness campaigns to strengthen password security practices among parents.

Fig 4.28: Parents Awareness on Reporting Suspicious Activities

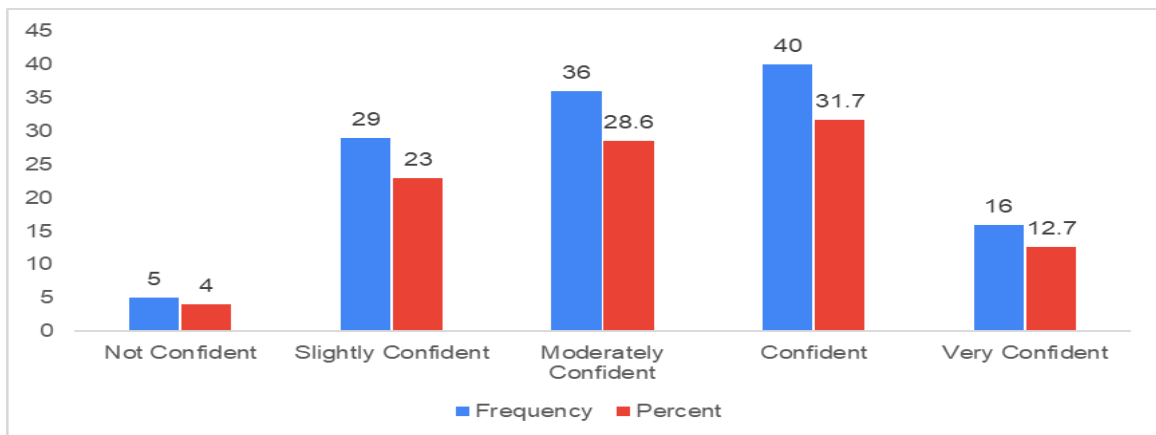


Source: Data analysis by author.

Figure 4.28: Reporting suspicious activity

Figure 4.28 shows confidence of parents in reporting suspicious activities. The findings suggest that 31.0% of parents are sure they can take the right steps, 31.7% are moderately sure, and 15.9% are very sure. Meanwhile, 19.8% mentioned they were less confident, and 1.6% mentioned not being sure at all. The findings suggest that although majority of parents express confidence in reporting suspicious online activity, a significant proportion demonstrate medium to low levels of confidence. This in essence calls for education and awareness programs aimed at strengthening parents' ability to recognize and respond effectively to potential cyber threats. Such initiatives would not only enhance parental vigilance but also contribute to safer online practices among their children.

Fig 4.29: Parents Awareness on Using Prenatal Controls on Digital Devices

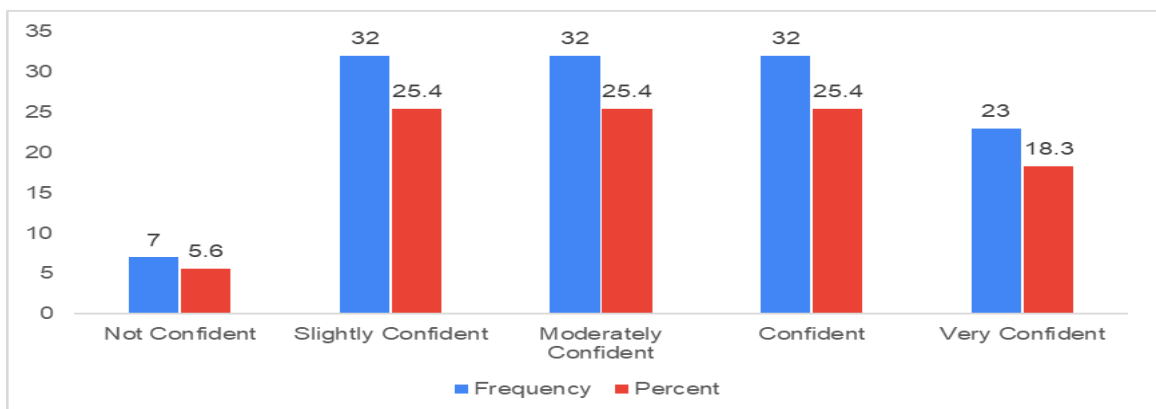


Source: Data analysis by author.

Figure 4.29: Using parental controls on digital devices

Figure 4.29 illustrates participants confidence on enabling parental controls on digital devices. The findings show that 28.6% of parents are moderately confident, 31.7% are confident, and 12.7% are very confident in using these controls. At the same time, 23% mentioned they were somewhat confident, and 4% mentioned not being confident at all. This indicates that although the majority of parents possess a satisfactory level of competency with parental control features, a significant segment may require further guidance and training on enabling digital safety measures.

Fig 4.30: Parents Confidence on Promoting Safe Social Media Behavior

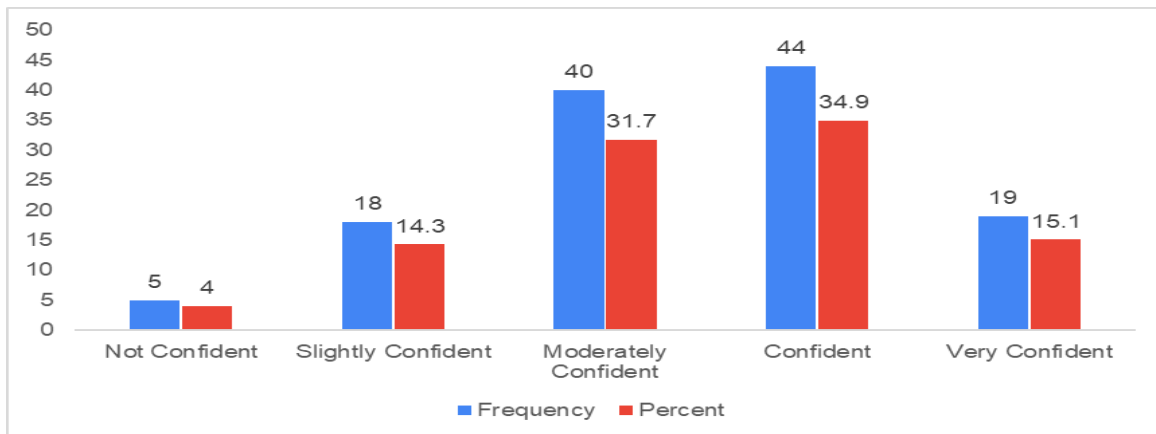


Source: Data analysis by author.

Figure 4.30: Promoting safe social media behavior

Figure 4.30 shows parents' ability to teach their kids on using social media safely. The findings suggest that 25.4% of parents are somewhat sure, 25.4% are sure, and 18.3% are very sure about how to help their kids stay safe online. 25.4% of the respondents also mentioned slight confidence and 5.6% mentioned being not confident. This shows that most parents think they can teach their kids how to use social media safely and responsibly, but others having moderate to low confidence may need more help in terms of training and tool awareness to increase cyber awareness. This will help parents to spread or promote safe practices among their children, friends and family members as well.

Fig 4.31: Parents Awareness on Protecting Personal Data

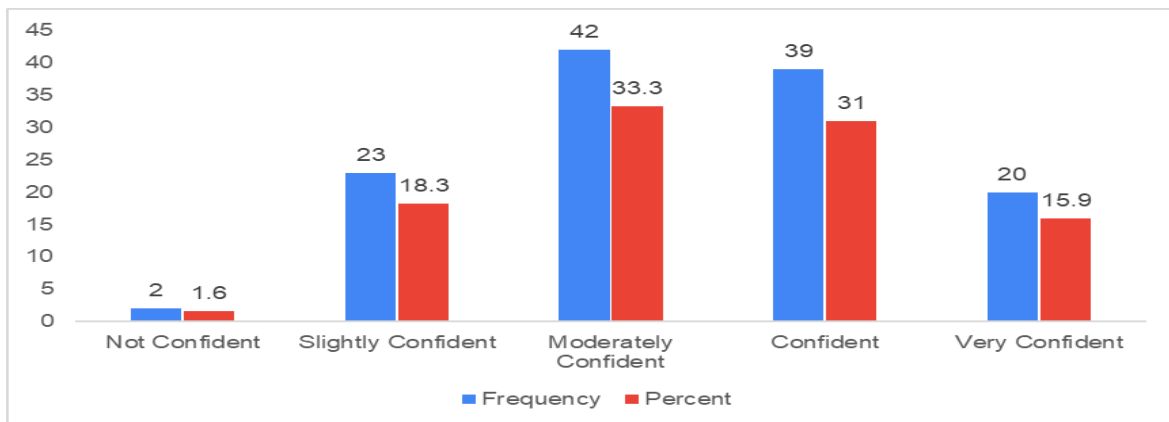


Source: Data analysis by author.

Figure 4.31: Protecting personal data

Figure 4.31 illustrates parent participants awareness on keeping personal information safe online. The statistics show that 31.7% of parents are moderately confident, 34.9% confident, and 15.1% very confident in keeping personal information protected. Also, 14.3% mentioned slight confidence and 4.0% were not confident in protecting personal data. This shows that a lot of parents display confidence in their ability to safeguard personal information, and there exists a significant proportion that doesn't have enough confidence. The findings underscore the need for targeted education and trainings to ensure data privacy awareness among parents.

Fig 4.32: Parents Confidence on Recognizing Phishing Emails

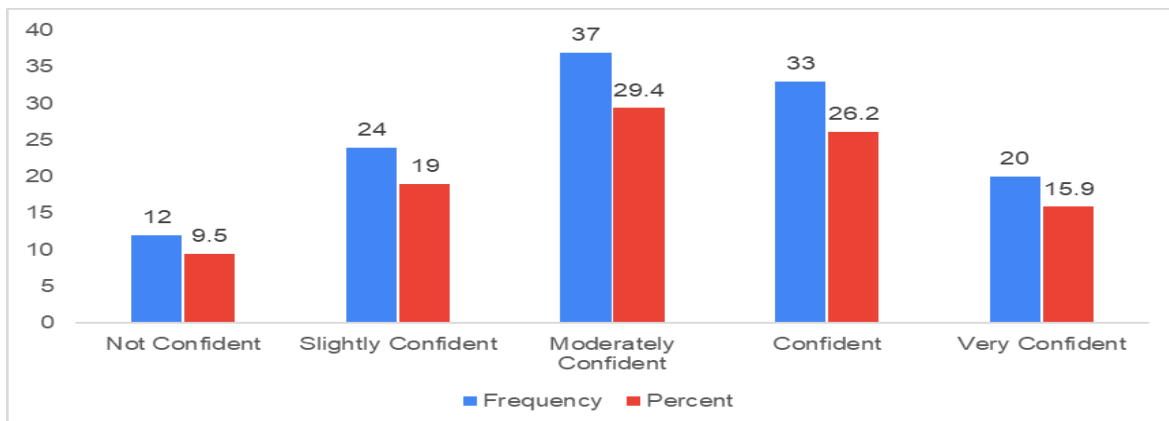


Source: Data analysis by author.

Figure 4.32: Recognizing phishing emails

Figure 4.32 illustrates parents' awareness to spot phishing emails. The statistics indicate that 33.3% of parents possess moderate confidence, while 31% exhibit confidence in recognizing phishing efforts. Also, 18.3% mentioned having slight confidence, 15.9% are very sure, and 1.6% reported not being confident at all. The findings indicate that although a majority of parents demonstrate skill in recognizing phishing emails, a significant subset conveyed limited confidence. This underscores the need for more involvement of parents in awareness programs and hands-on training.

Fig 4.33: Parents Awareness on Childs Online Friends



Source: Data analysis by author.

Figure 4.33: Knowing your child's online friends

Figure 4.33 shows how confident the parent respondents are about knowing their child's internet buddies. The results show that 29.4% of parents are moderately sure, 26.2% are sure, and 15.9% are extremely sure that they know who their child is talking to online. At the same time, 19.0% mentioned being somewhat confident, and 9.5% mentioned not being confident at all. This means that most parents keep a reasonable eye on their child's online activities, but a significant parent population may need assistance to keep an eye on their children to ensure safe digital relationships.

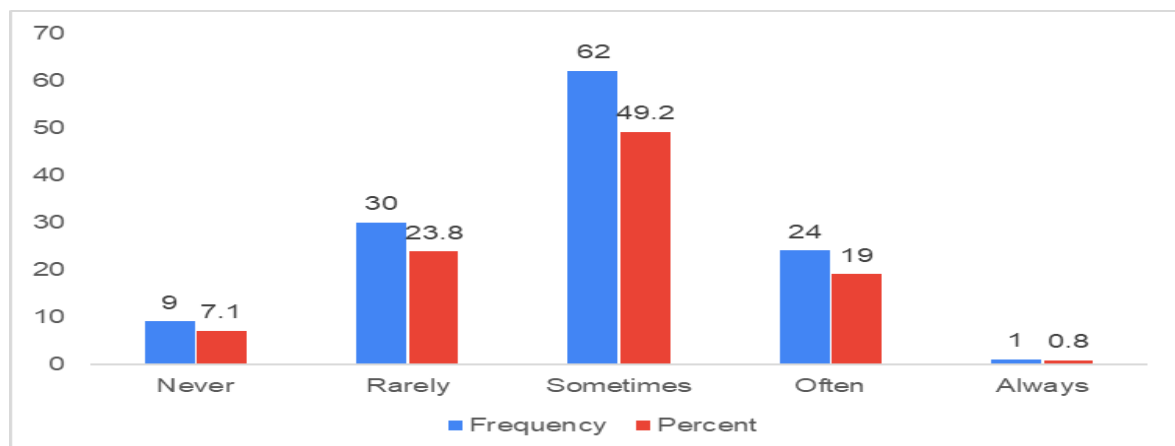
Table 4.21: Parents Behavior on Reusing Passwords

Table 4.21: How often do you use the same passwords across websites/apps?

	Frequency	Percent
Never	9	7.1
Rarely	30	23.8
Sometimes	62	49.2
Often	24	19.0
Always	1	.8
Total	126	100.0

Source: Data analysis by author.

Fig 4.34: Parents Behavior on Reusing Passwords



Source: Data analysis by author.

Figure 4.34: How often do you use the same passwords across websites/apps?

Figure 4.34 shows how often parents use the same passwords on one or more website or app. The results show that 49.2% of parents sometimes reuse password, 19.0% do so regularly, and 0.8% do it all the time. On the other hand, 23.8% said they rarely reuse passwords, while 7.1% said they never do. This indicates that many survey respondents compromise their online security by reusing the same password across multiple sites. Such practices significantly increase vulnerability to cyberattacks, as a single compromised account can expose several others. This underscores the importance of spreading awareness to parents about use of unique, complex passwords, password managers, and multi-factor authentication, to strengthen overall digital safety.

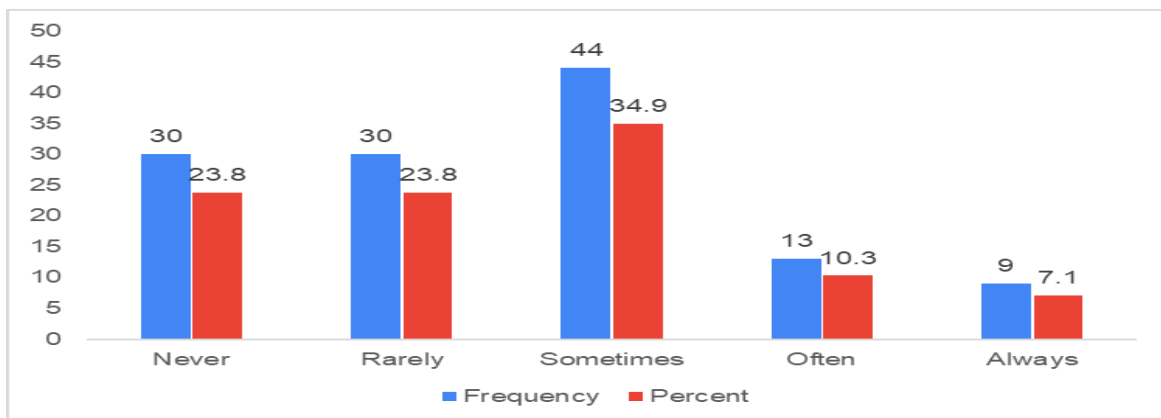
Table 4.22: Parents Behavior on Using Public Wi-Fi for Net-Banking

Table 4.22: How often do you use free public Wi-Fi for payments or banking?

	Frequency	Percent
Never	30	23.8
Rarely	30	23.8
Sometimes	44	34.9
Often	13	10.3
Always	9	7.1
Total	126	100.0

Source: Data analysis by author.

Fig 4.35: Parents Behavior on Using Public Wi-Fi for Net-Banking



Source: Data analysis by author.

Figure 4.35: How often do you use free public Wi-Fi for payments or banking?

Figure 4.35 presents data on how often parents utilize free public Wi-Fi to pay bills or performing online banking transactions. The results suggest that 34.9% of parents sometimes use public Wi-Fi for money transfers, while 23.8% mentioned they never or rarely do. Also, 10.3% of parents use public Wi-Fi often, and 7.1% always use them for online banking. This reveals that a lot of parent participants, place themselves at risk by conducting sensitive digital transactions on unprotected networks. Such practices increase the risk of cyberattacks, identity theft, and fraud, underscoring the need to promote safe internet use through secure connections, multi-factor authentication, and strong password practices among the parents.

Table 4.23: Parents Interest in Attending Cybersecurity Workshops Organized by Schools

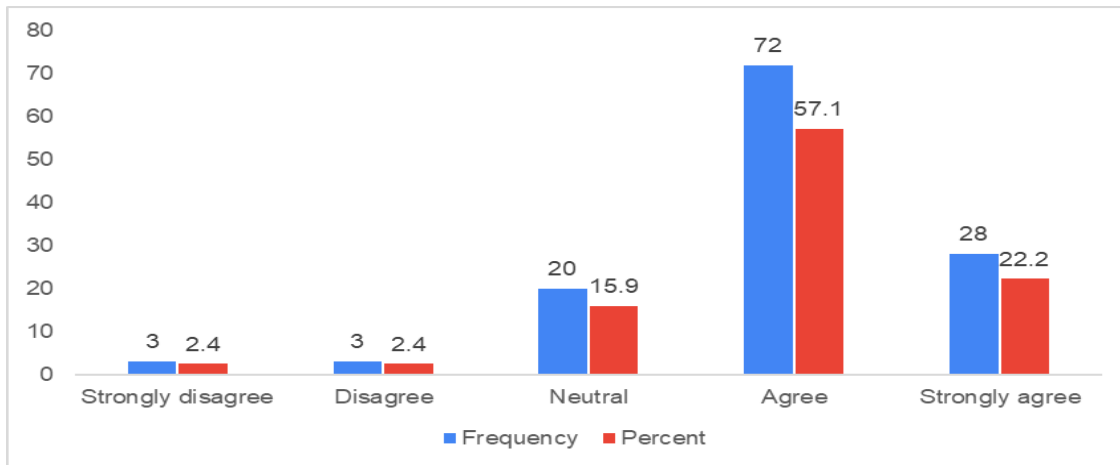
Table 4.23: Would you like schools to organize workshops on cybersecurity for parents?

	Frequency	Percent
Strongly disagree	3	2.4
Disagree	3	2.4
Neutral	20	15.9
Agree	72	57.1

Strongly agree	28	22.2
Total	126	100.0

Source: Data analysis by author.

Fig 4.36: Parents Interest in Attending Cybersecurity Workshops Organized by Schools



Source: Data analysis by author.

Figure 4.36: Would you like schools to organize workshops on cybersecurity for parents

Figure 4.36 depicts parents' interest and responses on schools conducting cybersecurity workshops for parents. According to the statistics, the majority of survey respondents (57.1% agree and 22.2% strongly agree) support this approach. Only 2.4% protested or strongly disapproved, while 15.9% remained neutral. This demonstrates that the majority of parents recognize the value of an organized cybersecurity sessions to educate parents about safe digital practices.

[illegible]

Figure 4.37: Biggest Concern About Child's Online Presence According to Parents

153

Fig 4.38: Parents Suggestion on Improving Schools Cybersecurity Awareness



Source: Data analysis by author.

Figure 4.38: Suggestions about improving cybersecurity awareness in schools

The word cloud in Figure 4.38 illustrates suggestions parents have regarding improving cybersecurity awareness in schools. The most often used terms, such as "safety", "awareness," "online," "school," and "exposure," suggests that parents are concerned about their children being exposed to inappropriate or harmful content on the internet which can be overcome via awareness and hands-on training exercises imparted through schools. Additional terms, like "competitions," "mental," "teach," and "strangers," indicate that parents are increasingly concerned about privacy, emotional distress, and communicating with strangers online. Advanced training that incorporates simulations, gamification, and competitive activities may contribute positively to skill development. This illustrates that parents view internet access and misinformation as serious safety risks, underscoring the need for digital literacy, proper technology use, and parental supervision.

Table 4.24: Descriptive Statistics of Parents' Survey*Table 4.24: Descriptive Statistics of Parents' Survey*

	N	Mean		Std. Deviation
	Statistic	Statistic	Std. Error	Statistic
Gender	126	1.25	.039	.432
Age Group	126	3.64	.067	.753
State	126	10.06	.432	4.848
District	126	32.18	1.639	18.403
How aware are you of your child's online activities?	126	3.25	.096	1.078
How often do you talk to your child about online safety and responsible internet use?	126	2.90	.087	.975
Have you ever received formal training/workshops on cybersecurity?	126	1.43	.044	.497
Talking to children about cyber risks	126	3.51	.092	1.033
Monitoring screen time	126	3.26	.096	1.075
Identifying online threats	126	3.43	.093	1.039
Creating strong passwords	126	2.94	.088	.986
Reporting suspicious activity	126	3.40	.092	1.028
Using parental controls on digital devices	126	3.41	.090	1.014
Promoting safe social media behavior	126	3.71	.084	.939
Protecting personal data	126	3.25	.106	1.186
Recognizing phishing emails	126	3.45	.080	.900
Knowing your child's online friends	126	3.20	.107	1.200
How often do you use the same passwords across websites/apps?	126	2.83	.076	.849
How often do you use free public Wi-Fi for payments or banking?	126	2.53	.104	1.171
Would you like schools to organize workshops on cybersecurity for parents?	126	3.94	.074	.832

Source: Data analysis by author.

Table 4.24 shows the descriptive statistics for parents' demographic information and their knowledge and behavior related to cybersecurity awareness. The average score for gender is 1.25 (SD = 0.432), implying that more male than female responded to the survey. The average score for age group is 3.64 (SD = 0.753), implying that most of the respondents were middle-aged adults. Respondents are spread out among different states (M = 10.06, SD = 4.848) and districts (M = 32.18, SD = 18.403). Parents are moderately aware of what their kids do online (M = 3.25, SD = 1.078), but they communicate less with their children about online safety and responsible internet use (M = 2.90, SD = 0.975). Only 57.1% of parents had received formal cybersecurity training or attended workshops (M = 1.43, SD = 0.497). Parents reported moderate confidence in talking to children about cyber risks (M = 3.51, SD = 1.033), monitoring screen time (M = 3.26, SD = 1.075), identifying online threats (M = 3.43, SD = 1.039), creating strong passwords (M = 2.94, SD = 0.986), and reporting suspicious activity (M = 3.40, SD = 1.028). Moderate proficiency is shown regarding use of parental controls on digital devices (M = 3.41, SD = 1.014) and the encouragement of safe social media behavior (M = 3.71, SD = 0.939). Protecting personal information (M = 3.25, SD = 1.186), spotting phishing emails (M = 3.45, SD = 0.900), and knowing who your kids' online pals are (M = 3.20, SD = 1.200) all illustrate moderate levels of knowledge. Additionally, parents reported engaging in moderately risky behaviors, such as reusing the same password across multiple sites (M = 2.83, SD = 0.849) and utilizing public Wi-Fi to make financial transactions (M = 2.53, SD = 1.171). In general, parents really wanted schools to hold cybersecurity workshops (M = 3.94, SD = 0.832). The findings reveal that though most parents are proactively driving online safety within families, there is a large section that lacks skills and awareness; underscoring the urgent need to equip them with practical tools, awareness programs, and digital literacy resources to build safer and more resilient online habits.

Findings of the Teacher/School Administrator's Survey

This section reports the outcomes of a survey carried out with academicians to assess cybersecurity awareness in Indian high schools.

Table 4.25: Demographic Profile of Academicians

Table 4.25: Demographic Profile of Teacher/School Administrator

Category	Subcategory	Frequency	Percent
Gender	Male	71	58.7
	Female	50	41.3
Age Group	20-29 Years	30	24.8
	30-39 Years	46	38
	40-49 Years	30	24.8
	50+ Years	15	12.4
State	Andaman And Nicobar Islands	1	0.8
	Andhra Pradesh	2	1.7
	Arunachal Pradesh	1	0.8
	Assam	11	9.1
	Bihar	3	2.5
	Chhattisgarh	1	0.8
	Delhi	5	4.1
	Goa	2	1.7
	Gujarat	7	5.8
	Haryana	5	4.1
	Himachal Pradesh	7	5.8
	Jammu And Kashmir	4	3.3
	Jharkhand	4	3.3
	Karnataka	7	5.8
	Kerala	5	4.1
	Ladakh	4	3.3
	Madhya Pradesh	3	2.5
	Maharashtra	4	3.3
	Manipur	5	4.1
	Meghalaya	4	3.3
	Mizoram	5	4.1

	Nagaland	3	2.5
	Odisha	3	2.5
	Punjab	3	2.5
	Rajasthan	4	3.3
	Sikkim	1	0.8
	Tamil Nadu	3	2.5
	Telangana	3	2.5
	Tripura	1	0.8
	Uttar Pradesh	5	4.1
	Uttarakhand	2	1.7
	West Bengal	3	2.5
District	Birbhum	1	0.8
	Dharmapuri	1	0.8
	Dindigul	1	0.8
	Kamjong	1	0.8
	Karimnagar	1	0.8
	Lunglei	1	0.8
	Narayanpet	1	0.8
	Nirmal	1	0.8
	Vadodara	1	0.8
	Agra	2	1.7
	Ahmedabad	1	0.8
	Aizawl	1	0.8
	Akola	1	0.8
	Alappuzha	1	0.8
	Aligarh	1	0.8
	Alirajpur	1	0.8
	Ambala	1	0.8
	Amritsar	2	1.7
	Anand	1	0.8
	Anantnag	1	0.8
	Araria	1	0.8
	Aurangabad	1	0.8
	Bagalkot	1	0.8

	Baghpat	1	0.8
	Bajali	1	0.8
	Baksa	3	2.5
	Balangir	2	1.7
	Balasore	1	0.8
	Ballari	1	0.8
	Bandipora	1	0.8
	Bangalore	3	2.5
	Bastar	1	0.8
	Bikaner	1	0.8
	Bilaspur	2	1.7
	Bishnupur	1	0.8
	Bokaro	1	0.8
	Chamba	1	0.8
	Champhai	1	0.8
	Chandel	1	0.8
	Chatra	1	0.8
	Chitradurga	1	0.8
	Cuddalore	1	0.8
	Darjeeling	1	0.8
	Delhi	2	1.7
	Dimapur	1	0.8
	Doda	1	0.8
	Dumka	1	0.8
	Ernakulam	1	0.8
	Faridabad	1	0.8
	Fatehabad	1	0.8
	Gandhi Nagar	1	0.8
	Gangtok	1	0.8
	Guntur	1	0.8
	Gurgaon	1	0.8
	Gurugram	1	0.8
	Hamirpur	2	1.7
	Haridwar	1	0.8

	Hojai	1	0.8
	Hooghly	1	0.8
	Indore	2	1.7
	Jaipur	1	0.8
	Jalandhar	1	0.8
	Jiribam	1	0.8
	Jodhpur	1	0.8
	Kamle	1	0.8
	Kamrup Metro	3	2.5
	Kamrup Rural	1	0.8
	Kanjhawala	1	0.8
	Kannur	1	0.8
	Karawal Nagar	1	0.8
	Kargil	1	0.8
	Kasaragod	1	0.8
	Kathua	1	0.8
	Kohima	1	0.8
	Kolasib	1	0.8
	Kolhapur	1	0.8
	Kollam	1	0.8
	Kunti	1	0.8
	Kutch	1	0.8
	Longleng	1	0.8
	Lucknow	1	0.8
	Mumbai	1	0.8
	Nainital	1	0.8
	Nashik	1	0.8
	Nellore	1	0.8
	Nicobar District	1	0.8
	Noney	1	0.8
	North East Delhi	1	0.8
	North Garo Hills	1	0.8
	North Goa	1	0.8
	Nubra	1	0.8

	Patna	1	0.8
	Ri Bhoi	1	0.8
	Serchhip	1	0.8
	Shimla	2	1.7
	South Goa	1	0.8
	Surat	2	1.7
	Tezpur	2	1.7
	Turtuk	1	0.8
	Udaipur	1	0.8
	Unakoti	1	0.8
	Vijayapura	1	0.8
	West Garo Hills	1	0.8
	West Khasi Hills	1	0.8
	Zaskar	1	0.8

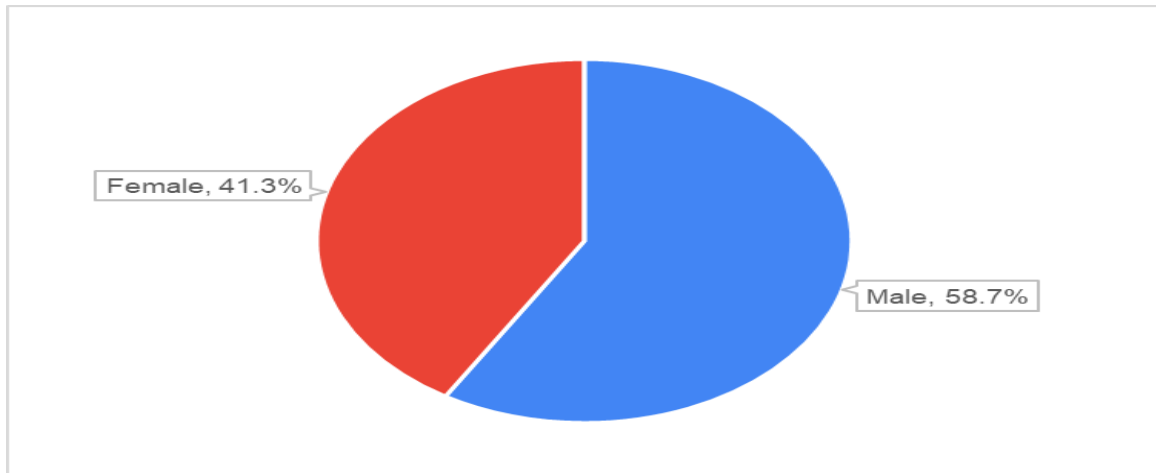
Source: Data analysis by author.

Table 4.25 presents a well-balanced and diverse representation of teachers and school administrators from across India. Survey participants consisted of 58.7% male and 41.3% female. The data reveals a moderate gender imbalance, but also highlights the substantial involvement of women in cybersecurity education. The majority of respondents (38%) were between the ages of 30 and 39, followed by 24.8% in the 20 to 29 and 40 to 49 age groups. Just 12.4% were over 50. With many educators still in their early or mid-career stages, they may be more open to learning new technologies like cybersecurity.

The responses were drawn from a wide range of Indian states and union territories, affirming the study's nationwide reach and enhancing the credibility of its conclusions by incorporating perspectives from varied geographic, cultural, and educational contexts. The highest percentage of academicians who undertook the survey came from Assam (9.1%), followed by Gujarat, Himachal Pradesh, and Karnataka (5.8% each). The survey's openness and thoroughness is demonstrated by the inclusion of remote regions like Sikkim, Ladakh, and the Andaman and Nicobar Islands. District-level data depicts that respondents

came from urban, semi-urban and rural settings, indicating a comparable range of involvement. Overall, the demographic distribution offers a wide and strong base for evaluating how Indian high school educators perceive cybersecurity awareness and practices.

Fig 4.29: Academicians Gender Distribution

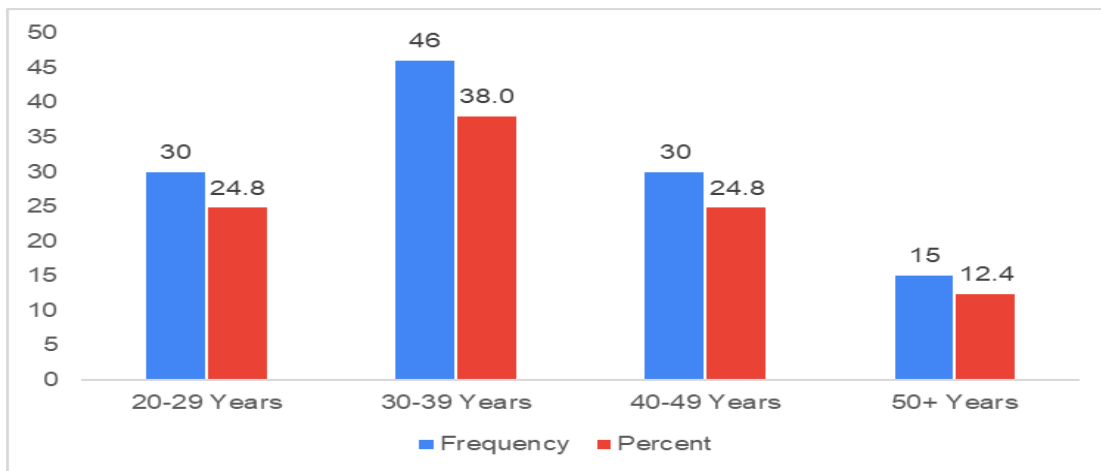


Source: Data analysis by author.

Figure 4.39: Gender

Figure 4.39 presents the gender distribution of academicians engaged in high school education who took part in the study. Of the 121 participants, 50 (41.3%) were female, and 71 (58.7%) were male. The survey findings indicate a higher proportion of male respondents, which may reflect existing gender imbalances in cybersecurity education and highlight the need for greater female participation to ensure inclusivity.

Fig 4.40: Academicians Age-Group Distribution



Source: Data analysis by author.

Figure 4.40 Age Group

Figure 4.40 presents the age group of survey participants. The data demonstrates that the age group 30-39 years (38.0%) has more representation, followed by 20-29 years (24.8%) and 40-49 years (24.8%). Only 12.4% of the respondents are 50 years of age or older. The predominance of young to middle-aged academicians reflects their digital skills, online habits, and cybersecurity views.

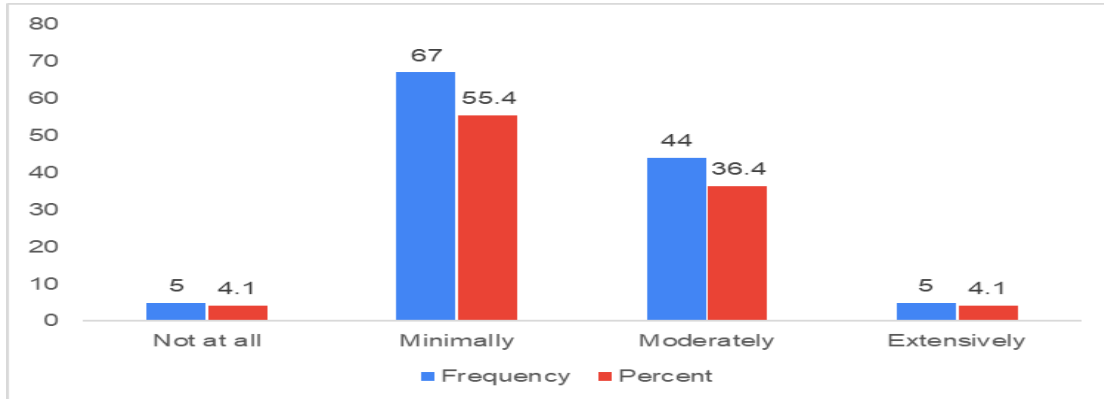
Table 4.26: Academicians Inclusion of Cybersecurity Topics in Curriculum / Discussions

Table 4.26: To what extent do you include cybersecurity topics in your curriculum/discussions?

	Frequency	Percent
Not at all	5	4.1
Minimally	67	55.4
Moderately	44	36.4
Extensively	5	4.1

Source: Data analysis by author.

Fig 4.41: Academicians Inclusion of Cybersecurity Topics in Curriculum / Discussions



Source: Data analysis by author.

Figure 4.41: To what extent do you include cybersecurity topics in your curriculum/discussions

Figure 4.41 illustrates the extent to which teachers incorporate cybersecurity topics into the curriculum or engage students in related discussions. The findings show that 55.4% participants, use cybersecurity topics minimally, and 36.4% use moderately. Just 4.1% of respondents indicated they cover cybersecurity lessons extensively in classroom settings, while another 4.1% stated, they never did. The fact that cybersecurity remains largely under-represented in educational discourse, even while being recognized as an essential domain, points to the necessity of implementing more extensive academic integration through policy initiatives, curriculum reforms, and targeted awareness programs.

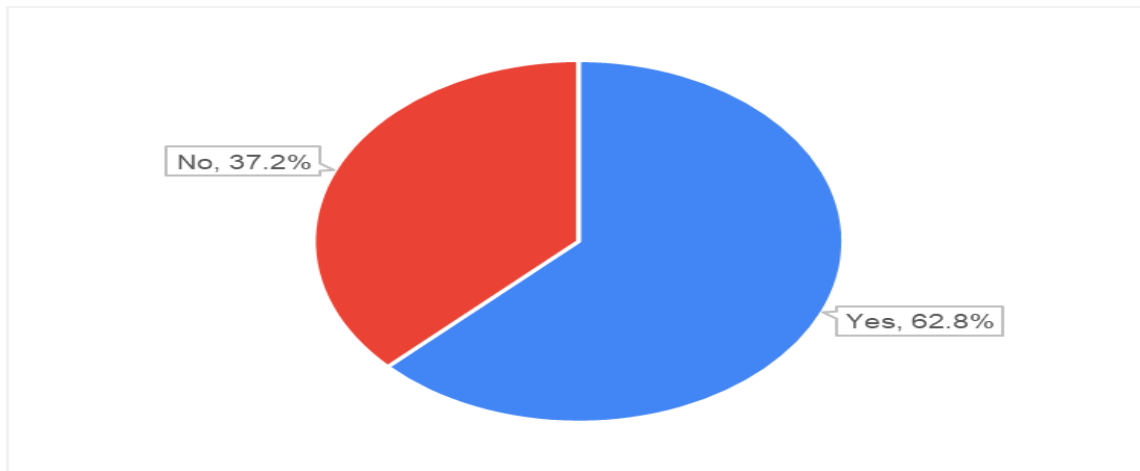
Table 4.27: Academicians Receiving Cybersecurity Training or Attending Workshops

Table 4.27: Have you ever received training/workshops on cybersecurity?

	Frequency	Percent
Yes	76	62.8
No	45	37.2

Source: Data analysis by author.

Fig 4.42: Academicians Receiving Cybersecurity Training or Attending Workshops



Source: Data analysis by author.

Figure 4.42: Have you ever received training/workshops on cybersecurity?

Figure 4.42 depicts the percentage of survey respondents that participated in any kind of cybersecurity seminars or training. According to the data, 37.2% of participants have not attended any sessions, while the majority, 62.8%, have received some kind of formal training. The findings suggest that most survey respondents possess knowledge of cybersecurity, reflecting the accessibility and use of training programs. However, significant population did not undergo any kind of cybersecurity trainings. The shortage of formal expertise emphasizes the importance of cybersecurity education to elevate digital safety across all sectors.

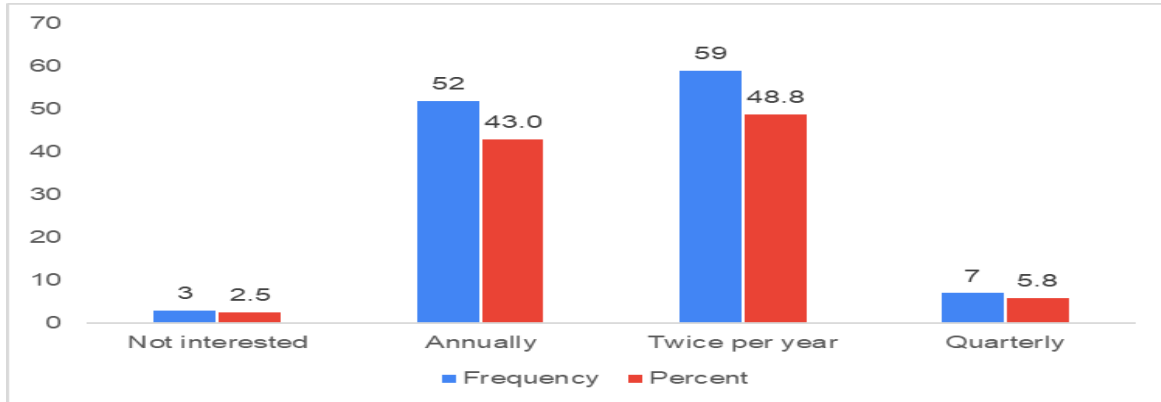
Table 4.28: Academicians interest in pursuing cybersecurity training and awareness sessions

Table 4.28: How often would you like to receive cybersecurity training?

	Frequency	Percent
Not interested	3	2.5
Annually	52	43.0
Twice per year	59	48.8
Quarterly	7	5.8

Source: Data analysis by author.

Fig 4.43: Academicians interest in pursuing cybersecurity training and awareness sessions



Source: Data analysis by author.

Figure 4.43: How often would you like to receive cybersecurity training?

Figure 4.43 shows how often respondents expressed interest in pursuing cybersecurity training and awareness sessions. The responses depict, 43.0% prefer training once a year, while 48.8% prefer pursuing twice a year. 2.5% academicians prefer not to attend any sessions, while 5.8% prefer training every three months. This illustrates the interest of a large number of respondents to participate in regular cybersecurity education sessions, underscoring the necessity of regular, and structured sessions alongside hands-on practical sessions designed to improve educators' familiarity of and preparedness for online threats.

Table 4.29: Academicians Perception to Barriers on Imparting Cybersecurity Awareness Programs in Schools

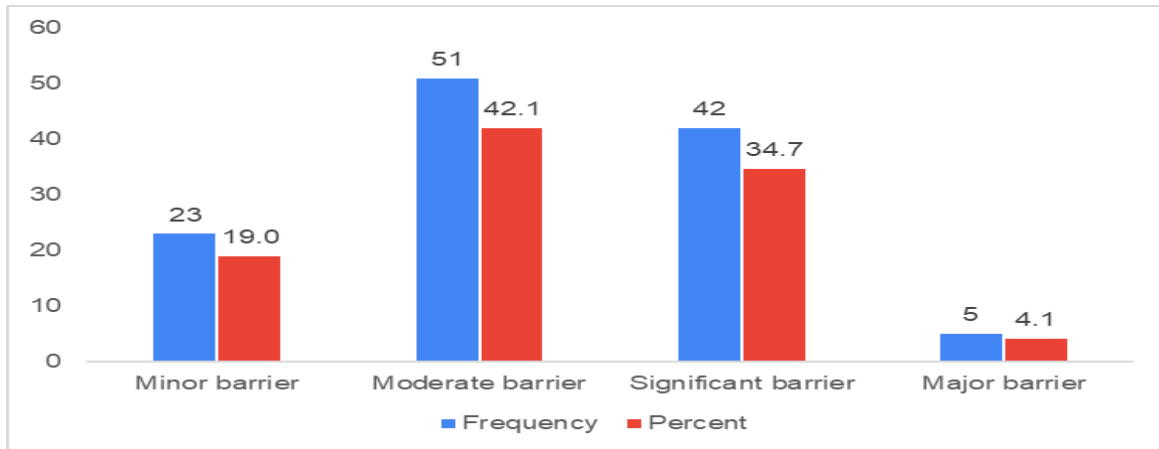
Table 4.29: To what extent are limited resources (funding, staff, technology, infrastructure) a barrier to implementing cyber-awareness programs in schools?

	Frequency	Percent
Minor barrier	23	19
Moderate barrier	51	42.1
Significant barrier	42	34.7

Major barrier	5	4.1
---------------	---	-----

Source: Data analysis by author.

Fig 4.44: Academicians Perception to Barriers on Imparting Cybersecurity Awareness Programs in Schools



Source: Data analysis by author.

Figure 4.44: To what extent are limited resources (funding, staff, technology, infrastructure) a barrier to implementing cyber-awareness programs in schools?

Figure 4.44 depicts respondents' opinions regarding the impact of inadequate funding, personnel, technology, and infrastructure on the effective implementation of cybersecurity awareness programs in educational institutions. The findings show that 42.1% of survey participants view these limitations as a moderate barrier, 34.7% view them as a significant obstacle, 19.0% view them as a minor barrier, and 4.1% view them as a major barrier. This finding highlights the significance of dedicated funding, institutional commitment, and strategic planning to advance curriculum design, laboratory setup and digital safety measures in the school environment.

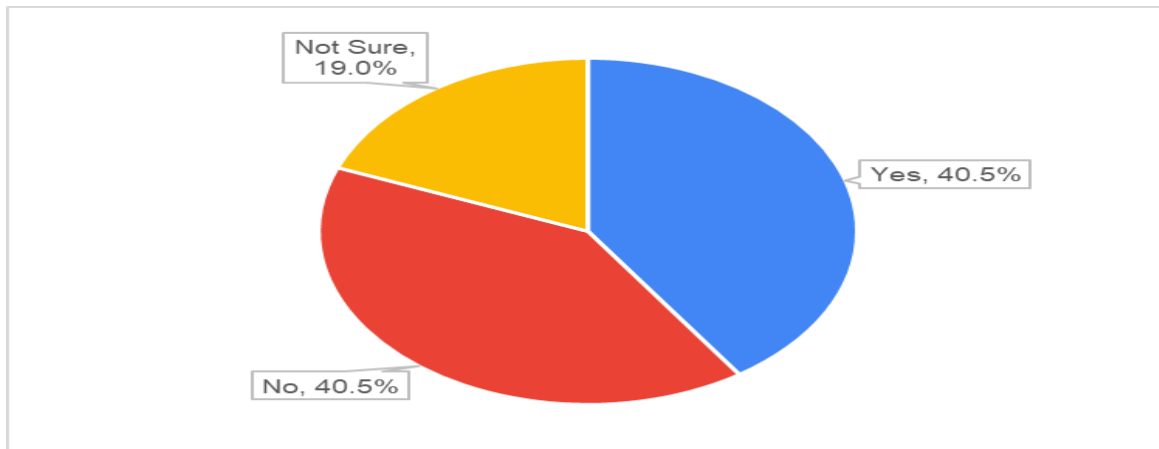
Table 4.30: Academicians Awareness in Installing Firewall / Antivirus in School Environment

Table 4.30: Have you installed a firewall/antivirus in school systems?

	Frequency	Percent
Yes	49	40.5
No	49	40.5
Not Sure	23	19.0

Source: Data analysis by author.

Fig 4.45: Academicians Awareness in Installing Firewall / Antivirus in School Environment



Source: Data analysis by author.

Figure 4.45: Have you installed firewall / antivirus in school systems?

Figure 4.45 depicts the survey participants response to setting up firewall or antivirus systems in school networks. The research shows that 40.5% of respondents have put in place these kinds of security measures, 40.5% have not, and 19.0% of respondents are not sure of such a setup. The survey findings suggest that some participants are aware of schools' initiatives to secure digital infrastructure, yet many lack clarity or engagement. This highlights the importance of schools enhancing threat awareness programs,

implement consistent cybersecurity standards, and pursue proactive measures to safeguard their infrastructure.

Table 4.31: Academicians Familiarity with Cybersecurity Concepts

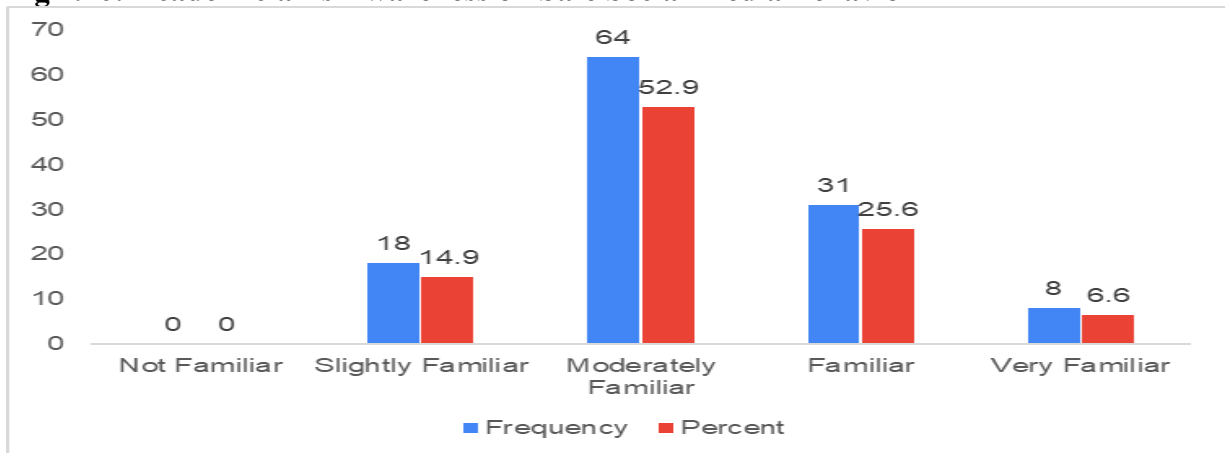
Table 4.31: Familiarity Levels of Teachers with Cybersecurity Concepts

Cybersecurity Area		Not Familiar	Slightly Familiar	Moderately Familiar	Familiar	Very Familiar
Safe Social Media Behavior	Frequency	0	18	64	31	8
	Percent	0	14.9	52.9	25.6	6.6
Understanding Data Privacy Laws	Frequency	30	42	38	10	1
	Percent	24.8	34.7	31.4	8.3	0.8
Identifying Online Threats	Frequency	2	33	57	20	9
	Percent	1.7	27.3	47.1	16.5	7.4
Student Data Protection	Frequency	6	34	51	22	8
	Percent	5.0	28.1	42.1	18.2	6.6
Talking to Students about Cyber Risks	Frequency	3	37	45	23	13
	Percent	2.5	30.6	37.2	19	10.7
Software / Hardware / Network Security	Frequency	19	42	47	10	3
	Percent	15.7	34.7	38.8	8.3	2.5
Reporting Suspicious Activity	Frequency	2	34	63	18	4
	Percent	1.7	28.1	52.1	14.9	3.3
Strong Password Practices	Frequency	0	4	42	52	23
	Percent	0	3.3	34.7	43	19
	Frequency	2	32	57	27	3

Cyber Hygiene Practices	Percent	1.7	26.4	47.1	22.3	2.5
Recognizing Phishing Emails	Frequency	1	19	57	28	16
	Percent	0.8	15.7	47.1	23.1	13.2

Source: Data analysis by author.

Fig 4.46: Academician's Awareness on Safe Social Media Behavior

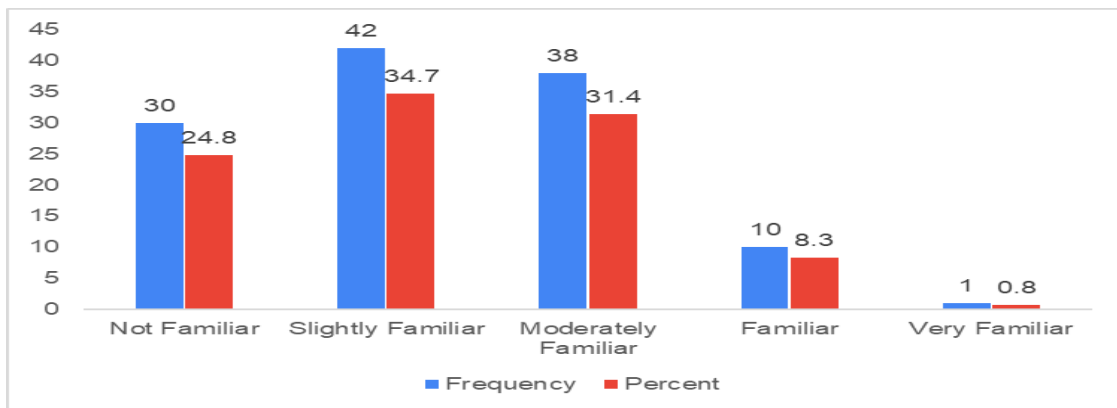


Source: Data analysis by author.

Figure 4.46: Safe social media behavior

Figure 4.46 shows familiarity of academicians regarding safe social media practices. The statistics show that 52.9% of the respondents are moderately familiar, 25.6% are familiar, and 14.9% are slightly familiar with how to use social media safely. Just 6.6% are extremely familiar. This indicates that the majority of respondents have a moderate to good understanding of safe social media behavior practices. However, the high proportion of respondents reporting only moderate or limited familiarity with safe social media practices is concerning; and points to the importance of implementing robust policies, expanding training opportunities, and embedding cybersecurity education within school curricula.

Fig 4.47: Academician's Understanding of Data Privacy Laws

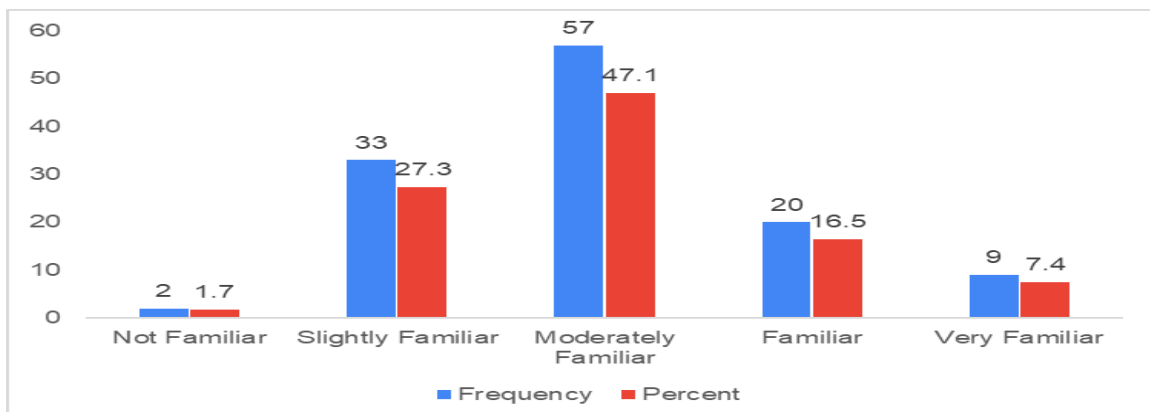


Source: Data analysis by author.

Figure 4.47: Understanding data privacy laws

Figure 4.47 depicts the level of awareness on data privacy laws among the survey participants. 31.4% of participants are moderately familiar with these laws, 34.7% are slightly familiar, and 24.8% are not at all familiar, according to the findings. Moreover, 8.3% are familiar and only 0.8% are very familiar with data privacy laws. The findings depict that most high school academicians have moderate to low familiarity regarding data privacy laws. This necessitates integrating data privacy concepts into the curricula to improve legal and regulatory awareness among teachers and students.

Fig 4.48: Academician's Awareness in Identifying Online Threats

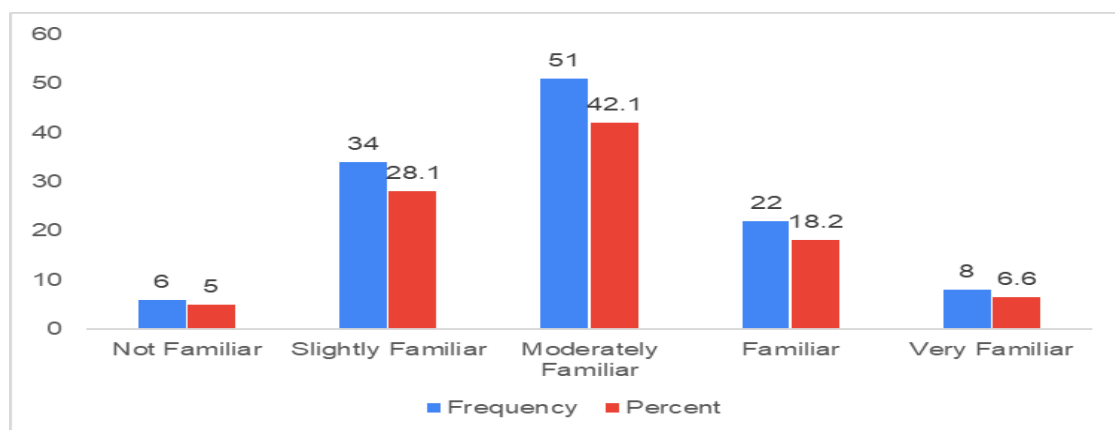


Source: Data analysis by author.

Figure 4.48: Identifying online threats

Figure 4.48 shows how aware the academicians were in spotting online risks. The research indicates that 47.1% of participants possess moderate familiarity, 27.3% exhibit minimal familiarity, and 1.7% demonstrate no familiarity. Also, 16.5% mentioned familiarity with identifying online threats and 7.4% mentioned being very familiar. This shows that a lot of respondents had a moderate to no grasp of possible online dangers. This underscores the need for more training and awareness programs among academicians to help recognize and respond to cyber threats.

Fig 4.49: Academician’s Familiarity in Protecting Students Data

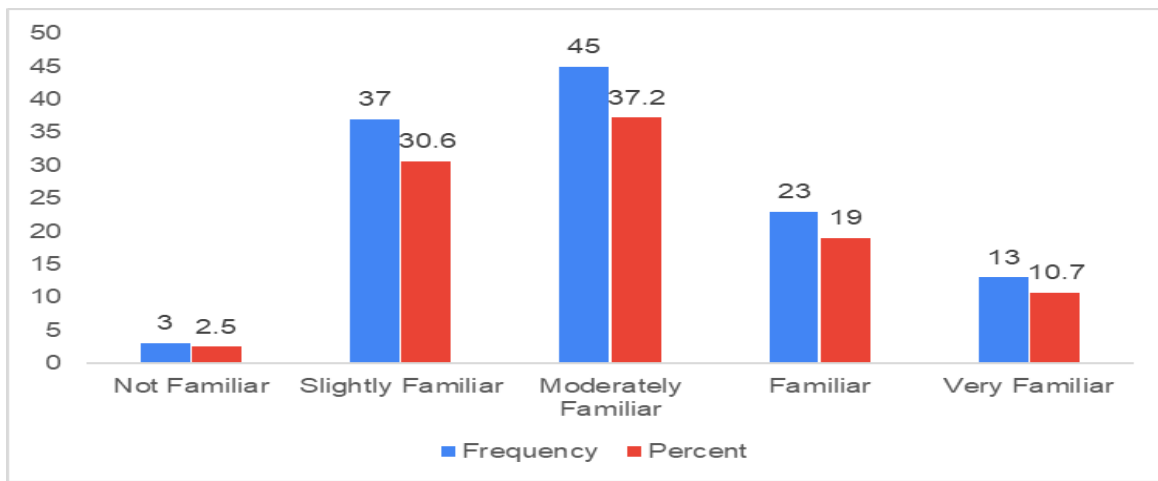


Source: Data analysis by author.

Figure 4.49: Student data protection

Figure 4.49 depicts familiarity of teacher participants in protecting student data. The statistics show that 42.1% participants are moderately aware about ways to protect student data, 28.1% are slightly aware, and 5% are not aware at all. Also, 18.2% are familiar, and 6.6% are very familiar on this subject. The findings reveal that participants demonstrate moderate to low awareness in handling student data, underscoring the need for enhanced training and awareness initiatives to ensure the secure handling of sensitive student information within educational settings.

Fig 4.50: Academician's Confidence in Talking to Students About Cyber Risks

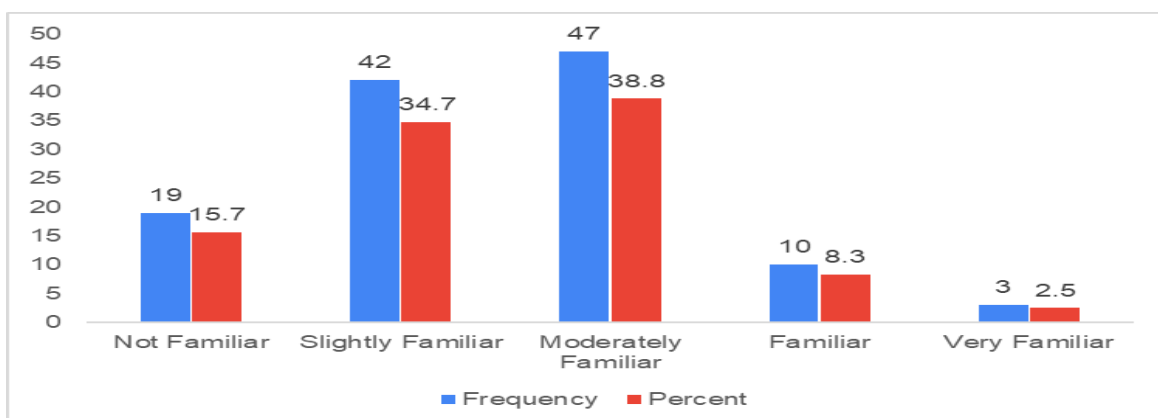


Source: Data analysis by author.

Figure 4.50: Talking to Students about cyber risks

Figure 4.50 depicts confidence of participants when interacting with students about cyber hazards. The statistics indicate that 37.2% of participants possess moderate familiarity, 30.6% exhibit modest familiarity, and 19.0% demonstrate familiarity with these discussions. Also, 10.7% show high confidence, and 2.5% are not familiar at all. While the survey reveals that many respondents contribute to raising awareness of cyber hazards among students, the data also highlights significant opportunities to strengthen their skills and confidence through trainings and supportive resources.

Fig 4.51: Academician's Familiarity with Software / Hardware / Network Security

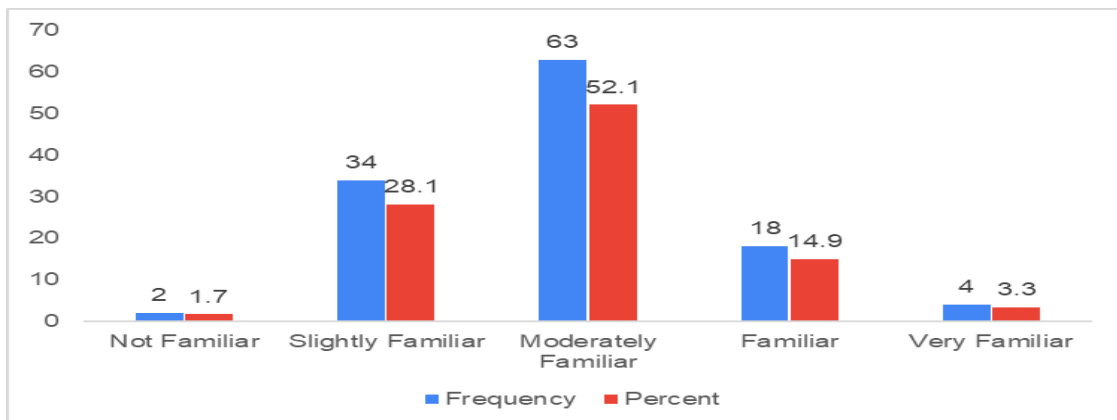


Source: Data analysis by author.

Figure 4.51: Software / Hardware / Network Security

Figure 4.51 shows the familiarity of participants with advanced concepts like software, hardware, and network security. The statistics show that 38.8% of the participants moderately know these security measures, 34.7% know them a little, and 15.7% know nothing about the subject. 8.3%, are familiar with the concepts, and only 2.5% are very familiar. The findings indicate that majority of respondents possess moderate to no knowledge of software, hardware, and network security, which necessitates the implementation of comprehensive training programs, curriculum integration, and institutional support to effectively address these gaps.

Fig 4.52: Academician's Awareness in Reporting Suspicious Activity



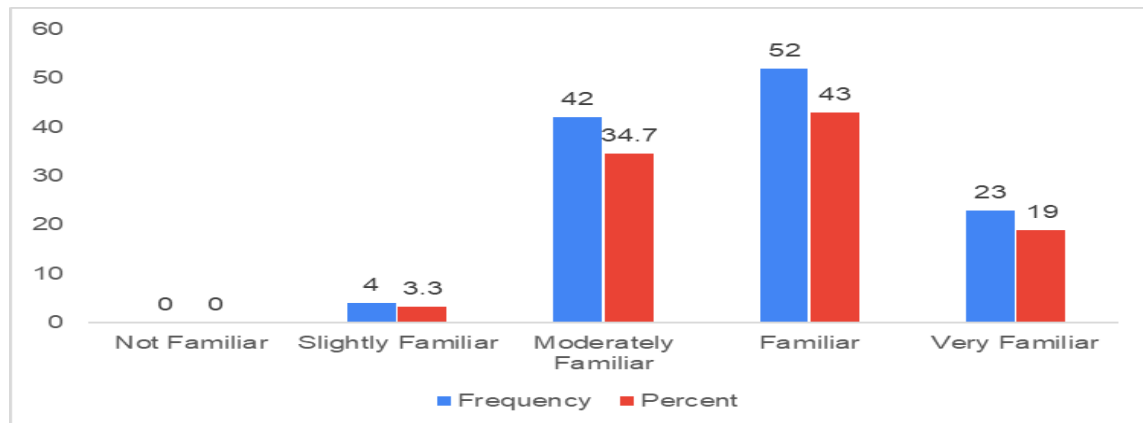
Source: Data analysis by author.

Figure 4.52: Reporting suspicious activity

Figure 4.52 illustrates how well the teacher respondents knew about reporting questionable online behavior. The numbers suggest that 52.1% of the participants are moderately familiar about reporting suspicious activity, 28.1% are slightly familiar, and 14.9% are familiar. Also, 3.3% are quite familiar in reporting suspicious activity, and 1.7% are not at all familiar. The findings indicate that majority of respondents possess moderate to minimal knowledge about reporting cybersecurity related suspicious activity. This underscores the need for targeted training and awareness campaigns to equip individuals

with the necessary skills and confidence to identify and escalate potential threats and foster a culture of vigilance and accountability.

Fig 4.53: Academician's Awareness in Strong Password Practices

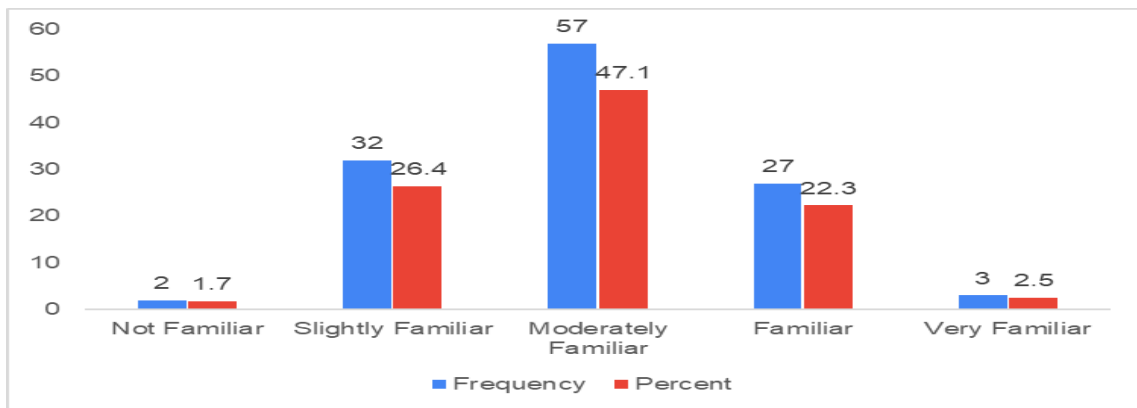


Source: Data analysis by author.

Figure 4.53: Strong password practices

Figure 4.53 demonstrates how well the teacher respondents knew about strong password practices. The numbers suggest that 43.0% of survey respondents are comfortable with creating and managing secure passwords, 34.7% are moderately familiar, 19.0% are very familiar, and 3.3% of the respondents being slightly familiar with the password practices. This means that most of the survey participants realize the importance of strong passwords practices. However, sustained efforts remain necessary to reinforce best practices for password creation and management, ensuring that individuals consistently adhere to established guidelines for secure password management.

Fig 4.54: Academician's Awareness in Cyber Hygiene Practices

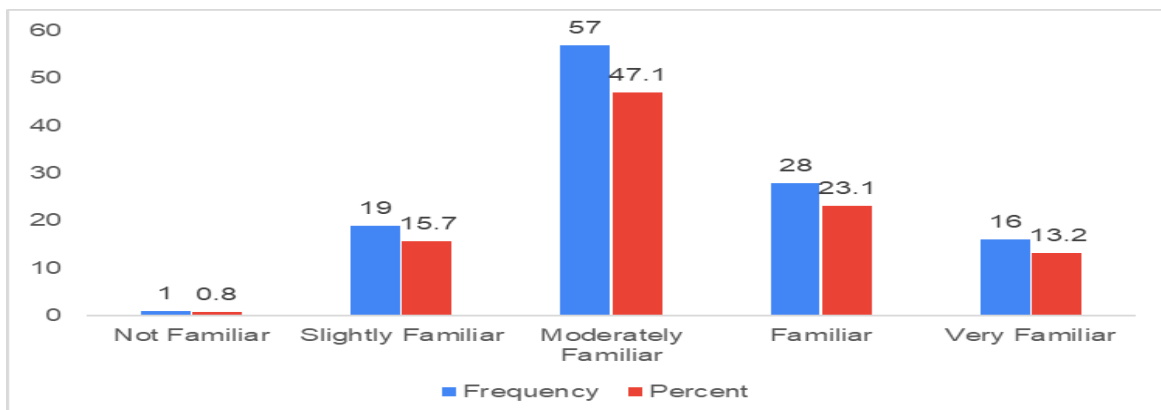


Source: Data analysis by author.

Figure 4.54: Cyber hygiene practices

Figure 4.54 shows survey respondents' familiarity about cyber hygiene. The statistics indicate that 47.1% of participants possess moderate familiarity, 26.4% are slightly familiar, and 22.3% are familiar with the principles of good cyber hygiene. Also, 2.5% are very familiar, and 1.7% are not at all familiar. This indicates that most academicians have a basic to moderate understanding of cyber hygiene. Nevertheless, additional training and awareness initiatives are required to ensure consistent adoption of secure online practices.

Fig 4.55: Academician's Competence in Recognizing Phishing Emails



Source: Data analysis by author.

Figure 4.55: Recognizing phishing emails

driven ideas, research, and helpful tools, with regular updates from the industry. Educators also need institutional support and lessons on digital ethics to stay safe online.

Table 4.32: Descriptive Statistics of the Teachers' Survey

Table 4.32: Descriptive Statistics of the Teachers' Survey

	N	Mean		Std. Deviation
	Statistic	Statistic	Std. Error	Statistic
Gender	121	1.41	.045	.494
Age Group	121	3.25	.088	.969
State	121	15.61	.764	8.399
District	121	52.48	2.742	30.162
To what extent do you include cybersecurity topics in your curriculum/discussions?	121	2.40	.058	.640
Have you ever received training/workshops on cybersecurity?	121	1.37	.044	.485
How often would you like to receive cybersecurity training?	121	2.58	.058	.642
To what extent are limited resources (funding, staff, technology, infrastructure) a barrier to implementing cyber-awareness programs in schools?	121	3.24	.073	.806
Have you installed firewall / antivirus in school systems?	121	1.79	.068	.744
Safe social media behavior	121	2.98	.074	.811
Understanding data privacy laws	121	2.93	.088	.964
Identifying online threats	121	2.47	.086	.941
Student data protection	121	3.01	.082	.899
Talking to Students about cyber risks	121	3.05	.092	1.015
Software / Hardware / Network Security	121	2.90	.072	.790
Reporting suspicious activity	121	3.32	.084	.924
Strong password practices	121	3.78	.072	.790
Cyber hygiene practices	121	3.24	.071	.786

Recognizing phishing emails	121	2.26	.087	.953
-----------------------------	-----	------	------	------

Source: Data analysis by author.

Table 4.32 presents the descriptive statistics on demographic data along with school administrators practices and views on cybersecurity. The gender distribution reveals a marginally greater percentage of male respondents ($M = 1.41$, $SD = 0.494$), whilst the mean age group of 3.25 ($SD = 0.969$) signifies that the majority of administrators are within the middle age range. Participants represent a wide geographical spread, encompassing different states ($M = 15.61$, $SD = 8.399$) and districts ($M = 52.48$, $SD = 30.162$). There is a moderate ($M = 2.40$, $SD = 0.640$) involvement of cybersecurity themes in the curriculum and conversations, however 62.8% of administrators said they have received cybersecurity training ($M = 1.37$, $SD = 0.485$). The ideal frequency for training is moderate ($M = 2.58$, $SD = 0.642$) which is annually or bi-annually. Participants are aware that not having enough funding, staff, technology, and infrastructure is a moderate obstacle to putting cyber-awareness initiatives into place ($M = 3.24$, $SD = 0.806$). Setting up firewall and antivirus systems demonstrates some compliance ($M = 1.79$, $SD = 0.744$). Moderate levels of awareness is shown in familiarity with safe social media behavior ($M = 2.98$, $SD = 0.811$), data privacy laws ($M = 2.93$, $SD = 0.964$), student data protection ($M = 3.01$, $SD = 0.899$), talking to students about cyber risks ($M = 3.05$, $SD = 1.015$), and software/hardware/network security ($M = 2.90$, $SD = 0.790$). Respondents are more likely to follow strong password practices ($M = 3.78$, $SD = 0.790$) than to recognize online risks ($M = 2.47$, $SD = 0.941$) or recognize phishing emails ($M = 2.26$, $SD = 0.953$). In general, reporting suspicious activity ($M = 3.32$, $SD = 0.924$) and exercising cyber hygiene ($M = 3.24$, $SD = 0.786$) indicate that educators demonstrate a moderate level of comfort with cybersecurity practices within the school environment.

Findings of Hypotheses Testing

This section includes the results obtained through hypothesis testing.

Hypothesis 1:

- **H₀₁:** There is no significant difference in cybersecurity awareness levels among students, parents, and educationalists in India.
- **H₁:** There is a significant difference in cybersecurity awareness levels among students, parents, and educationalists in India.

Table 4.33: ANOVA Test Statistics

Table 4.33: ANOVA Test Statistics

Cybersecurity Awareness Aspect	Group	Sum of Squares	df	Mean Square	F	Sig.
How well do you understand the term cybersecurity?	Students	0.001	1	0.001	0.001	0.979
	Parents	—	—	—	—	—
	Academicians	—	—	—	—	—
Safe social media behavior	Students	0.945	1	0.945	1.900	0.170
	Parents	8.417	1	8.417	10.178	0.002
	Academicians	0.049	1	0.049	0.064	0.800
Cyberbullying	Students	0.345	1	0.345	0.502	0.479
	Parents	—	—	—	—	—
	Academicians	—	—	—	—	—
Reporting suspicious activity	Students	0.748	1	0.748	0.994	0.320
	Parents	0.002	1	0.002	0.003	0.957
	Academicians	1.610	1	1.610	1.673	0.198
Strong password practices	Students	0.034	1	0.034	0.050	0.824
	Parents	0.017	1	0.017	0.027	0.870
	Academicians	2.420	1	2.420	2.362	0.127
Phishing email	Students	0.869	1	0.869	0.942	0.333

	Parents	1.465	1	1.465	2.157	0.146
	Academicians	0.273	1	0.273	0.254	0.615
Talking to children about cyber risks	Students	—	—	—	—	—
	Parents	2.886	1	2.886	7.060	0.009
	Academicians	0.033	1	0.033	0.036	0.850
Monitoring screen time	Students	—	—	—	—	—
	Parents	2.456	1	2.456	6.145	0.015
	Academicians	—	—	—	—	—
Identifying online threats	Students	—	—	—	—	—
	Parents	1.605	1	1.605	2.206	0.141
	Academicians	7.389	1	7.389	6.006	0.016
Using parental controls on digital devices	Students	—	—	—	—	—
	Parents	1.918	1	1.918	3.395	0.069
	Academicians	—	—	—	—	—
Promoting safe social media behavior	Students	0.945	1	0.945	1.900	0.170
	Parents	8.417	1	8.417	10.178	0.002
	Academicians	0.049	1	0.049	0.064	0.800
Protecting personal data	Students	—	—	—	—	—
	Parents	2.978	1	2.978	4.560	0.036
	Academicians	—	—	—	—	—
Knowing your child's online friends	Students	—	—	—	—	—
	Parents	1.446	1	1.446	2.410	0.124
	Academicians	—	—	—	—	—
Understanding data privacy laws	Students	—	—	—	—	—
	Parents	—	—	—	—	—
	Academicians	0.185	1	0.185	0.260	0.611
Student data protection	Students	—	—	—	—	—
	Parents	—	—	—	—	—

	Academicians	0.518	1	0.518	0.438	0.510
Software/Hardware/Network Security	Students	—	—	—	—	—
	Parents	—	—	—	—	—
	Academicians	4.325	1	4.325	3.919	0.050
Cyber hygiene practices	Students	—	—	—	—	—
	Parents	—	—	—	—	—
	Academicians	0.003	1	0.003	0.003	0.957

Source: Data analysis by author.

Table 4.33 presents the ANOVA findings for multiple cybersecurity awareness factors across three groups: students, parents, and academicians, using the significance value (Sig.) to determine if the differences observed are practically significant. A Sig. value that is lower than 0.05 means there is statistically significant difference, and the variation is most probably not due to random chance; whereas a value above 0.05 means no significant difference exists. The analysis reveals that for students, the evaluated factors comprising comprehension of cybersecurity, safe social media practices, cyberbullying, reporting suspicious activities, robust password practices, and phishing email identification did not show statistically significant differences ($p > 0.05$), which indicates that the awareness levels they have in different aspects of cybersecurity are the same and do not differ notably. The study fails to support the alternative hypotheses, and instead accepts the null hypothesis, meaning students share similar levels of awareness in these areas. For Parents, there were significant differences in "Talking to children about cyber risks" ($p = 0.009$), "Monitoring screen time" ($p = 0.015$), "Promoting safe social media behavior" ($p = 0.002$), and "Protecting personal data" ($p = 0.036$). This means that the alternative hypotheses for these variables are accepted, but the hypotheses for the other variables are not accepted because the p-values are not significant. Among Academicians, "Identifying online threats" ($p = 0.016$) and "Software/Hardware/Network Security" ($p = 0.050$)

exhibited significant differences, resulting in the acceptance of alternative hypotheses and indicates diverse levels of technical talent; whereas all other aspects were not accepted. In general, the results suggest that parents and academics display varying degrees of understanding in certain aspects of cybersecurity, while students had more uniform levels of awareness throughout the factors that were tested. Together, these findings highlight the need for a coordinated approach including but not limited to curriculum reform, parental engagement, and educator training to safeguard India's digital future.

Hypothesis 2:

- **H0₂:** Parents' engagement in digital safety practices do not positively affects students' cybersecurity awareness.
- **H₂:** Parents' engagement in digital safety practices positively affects students' cybersecurity awareness.

Table 4.34: Spearman's Rho Correlations

Table 4.34: Spearman's Rho Correlations of Cybersecurity Practices, Parental Awareness, and Training

S. No.	Variables	1	2	3	4	5	6	7	8
1	Safe Social Media Behavior	1.000	.603**	.619**	.673**	.628**	-.078	-.045	.073
2	Cyberbullying	.603**	1.000	.511**	.568**	.514**	-.008	.055	-.083
3	Reporting Suspicious Activity	.619**	.511**	1.000	.615**	.464**	-.136	.021	-.025
4	Strong Password Practices	.673**	.568**	.615**	1.000	.700**	-.063	-.041	-.057

5	Phishing Email Awareness	.628**	.514**	.464**	.700**	1.000	-.056	-.085	.018
6	Awareness of Child's Online Activities	-.078	-.008	-.136	-.063	-.056	1.000	.344**	-.157
7	Discussion about Online Safety	-.045	.055	.021	-.041	-.085	.344**	1.000	-.158
8	Formal Cybersecurity Training	.073	-.083	-.025	-.057	.018	-.157	-.158	1.000
N = 198 for variables 1–5; N = 126 for variables 6–8.									
Sig. (2-tailed): All coefficients marked ** with $p < 0.01$.									

Source: Data analysis by author.

Table 4.34 presents the Spearman's rank-order correlation results for H2, assessing the relationships between students' cybersecurity awareness dimensions and parental engagement variables; with coefficients marked ** denoting statistical significance at $p < 0.01$ (two-tailed). In other words, there is less than 1% chance that these relationships are due to random variation, and the findings are deemed reliable. The correlation strength is categorized as weak ($r \approx 0.10$ – 0.29), moderate ($r \approx 0.30$ – 0.59), and high ($r \geq 0.60$), which makes it easier to see the degree of connection between the variables.

The results indicate strong, positive, and statistically significant correlations among student-focused cybersecurity behaviors, including safe social media behavior, cyberbullying, reporting suspicious activity, strong password practices, and phishing email recognition (ranging from 0.464 to 0.700, $p < 0.01$), suggesting that these skills support each other and together help students become more aware and safer online. In contrast, parental awareness of their child's online activities and discussions about online safety were moderately correlated with each other ($r = 0.344$, $p < 0.01$). On the other hand, weak

and non-significant correlations are reported between formal cyber security training among parents and the majority of the other variables, indicating that conventional training by itself may not have a great impact on routine cyber security practices unless there are also opportunities for practical engagement and awareness efforts.

Parental practices are cohesive (monitoring and discussion), but they don't translate into measurable student awareness; association is mostly weak, non-significant (negative or near zero). Similarly, students' cybersecurity awareness cluster (safe behavior, passwords, phishing, reporting) is strongly interrelated, but independent of parental engagement. In Summary, Spearman Rho analysis shows no significant positive effect of parental engagement on student cybersecurity awareness. The null hypothesis stands. The findings suggest that while parents may foster dialogue and supervision, these efforts do not directly enhance students' technical or behavioral competencies in cybersecurity.

4.5 Summary of Findings

This research analyzed cybersecurity awareness in Indian high schools through a review of global practices and evaluation of survey responses from students, parents, and educationalists.

The findings of the first research question indicated that cybersecurity education significantly enhances awareness of online threats such as phishing, cyberbullying, and data breaches as well as providing students with practical skills such as managing strong passwords and understanding threats. While international programs blend technical skills, legal awareness, and engaging activities, India must overcome outdated rules, weak infrastructure, limited awareness, and teacher shortages by modernizing policies, investing in resources, partnerships with industry, and training educators to build resilient cybersecurity education.

The second research question revealed that effective international approaches rely on practical, experience learning assisted by innovative methods such as gamification, simulations, and project-based work. Cross-curricular integration ensures that gaps in cyber hygiene awareness are addressed, and business collaboration provides students with improved understanding, possibly inspiring students to continue higher education in this area. To ensure effective cybersecurity education, India requires unified national policies, modular curricula from basic to advanced concepts, teacher training boot camps, after-school clubs, and affordable cloud-based services adaptable to school environments having funding limitations.

Findings from the third research question indicate that government policies in India are marked by ambiguity, lack of standardization, and inconsistent implementation; while some states have initiated development programs in collaboration with industry partners, the absence of a nationwide policies and regulations limits their accessibility. Cybersecurity education worldwide succeeds through strong policies, standardized curricula, and cooperation; India must adopt explicit guidelines, allocate funds, prepare teachers, and integrate with digital policies to ensure sustainable growth.

Findings from the fourth research question revealed that the students are not fully aware of essential digital safety measures, particularly in areas such as reusing passwords across accounts, connecting to unsecured public Wi-Fi, and sharing their location information over social media. Parents and high school educators exhibit varying levels of knowledge and confidence in guiding children toward digital literacy, with many expressing the need for additional training and resources. Overall, the findings highlight the importance of a structured curriculum, parental involvement, clear policies, comprehensive teacher training, and active community involvement in strengthening cybersecurity education in India.

4.6 Conclusion

This chapter presents the findings of study on cybersecurity education in high schools, focusing on program strengths and weaknesses, current approaches, curriculum designs, teaching methodologies, regulatory frameworks, and awareness levels. The study reveals that India continues to face challenges due to weak regulations, poor implementation, and minimal teacher preparation, even as global models highlight experiential learning, structured curricula, and strong policy frameworks. Survey results indicated that students' awareness of unsafe digital behaviors was moderately high, yet such practices persist, while parents and educationalists showed varying confidence in guiding safe technology use and expressed interest in additional training and awareness programs. Overall, the findings underscore the urgent need for standardized curricula, teacher training, supportive policies, and community engagement to build a resilient cybersecurity education system to safeguard India's digital future and bridge existing gaps in cybersecurity workforce.

CHAPTER V:

DISCUSSION

5.1 Discussion of Results

This study sought to elucidate cybersecurity education and awareness at the high school level in India by examining the practices of other countries, the instructional approaches, the policies in place, and the level of awareness among key players. The investigation reveals that globally, nations have embraced well-organized cybersecurity programs that has been incorporated into the mainstream curriculum and combines technical skills with ethical, social, and behavioral understanding of cyber threats. This interdisciplinary method offers not only practical abilities but also critical thinking skills to students so that they can smoothly navigate the dangers of the digital world. In contrast, cybersecurity education in Indian high schools is mostly integrated in general computer literacy leading to disjointed and shallow learning. Digital safety programs in India should be enhanced through enriched curriculum and incorporation of international best practices, including interactive learning models, cross disciplinary studies, and age based developmental models.

These findings are in tandem with the likelihood of students within countries that have well established cybersecurity programs to be aware of the necessity of exercising precaution when using internet (Pencheva *et al.*, 2020). Cybersecurity education for children extends far beyond technical training. The social, ethical, and behavioral aspects of digital citizenship also need to be considered, and for that reason schools are adopting a multidisciplinary approach. The almost non-existent integration of cybersecurity awareness into the Indian high school curricula, in its turn, implies the absence of institutionalization and the underdeveloped curricular complexes as far as the cybersecurity

awareness is concerned. Therefore, integrating the curriculum and introducing systematic models may be crucial to raise awareness of cybersecurity among Indian students.

In the research study, pedagogues, equal distribution of resources and systematic curriculums were identified as some of the major factors that influenced successful cybersecurity training. International best practices identify experiential approaches, including virtual laboratories, gamification, competitions such as Capture-the-Flag experiences, and project-based learning, that can be especially useful in promoting active learning and development of applied skills.

Most schools in India, especially in rural areas struggle with limited access to updated online resources and adoption of practice-based methodologies. In addition, the Indian curriculum lacks clear and tiered progression unlike the global standards, which limits the systematic development of the cybersecurity skills from fundamental to advanced concepts. To resolve these gaps, India needs to invest in specialized teacher training, modernize educational resources, and modular curricula that strike a balance between cyber hygiene, technical education and ethical concerns. When we adapt such strategies to the socio-economic and infrastructural realities of India, we will be able to develop a dynamic and vibrant learning atmosphere that will contribute to both fundamental awareness and technical competence among students.

The final items that are highlighted in this report is that cybersecurity education thrives on synchronized policies, school and industry partnerships, and parental guidance. Unlike global models built on coordinated efforts, India's fragmented framework requires stable and clear regulations, teacher training, parental support, and regular program review to equip not only the teachers and students but the broader community for safe and responsible digital engagement and counter the threats in the face of ever changing and evolving cyber risks.

5.2 Discussion of Research Question One

The paper attempted to examine the strengths and weaknesses of cybersecurity education in various nations, aiming to suggest curricular reforms for Indian high schools. The findings indicate that in most countries, children acquire fundamental knowledge of cybersecurity concepts within the school setting. The study demonstrates the fact that these nations are advancing digital literacy and safety education with a long-term vision. Not only do they impart technological skills but also assist students to learn how to be responsible online, and develop the ability to distinguish between ethical and unethical actions. Although modest growth has been witnessed in Indian schools, but cybersecurity continues to occupy insignificant portion within the curriculum and budget allocation is insufficient (Teachcyber, 2021).

This finding is significant because, although the education system is increasingly becoming more digitized, cybersecurity education remains underrepresented in the secondary school curriculum in India. There is a possibility of students not being ready to deal with cyber threats as they are ever changing. The study concluded that the specifics of cybersecurity education are often outlined superficially (Mishra, 2024). The study emphasizes the critical role of instructors in delivering effective instructions and stresses their professional development to ensure long term sustainable results.

Numerous studies (Frusci, 2024; Rahman *et al.*, 2020), consistently highlight the reason for successful global teaching strategies lies in their interdisciplinary design. The study underscores the need that cybersecurity is taught alongside social science, civic education, and psychology. This interdisciplinary model will not only build technical skills but also equip students to tackle the ethical and social challenges of the digital age. To this end, Indian policymakers and educators must move beyond teaching the fundamentals of computers. This requires (i) including cybersecurity as part of core curriculum, not just an

add-on; (ii) integrate practical modules and labs; (iii) training and certifications for teachers; (iv) encourage safe internet practices at home; and (v) conduct frequent program reviews and adapt to international best practices. Such measures will help build a resilient and sustainable learning system.

The research also found out two fundamental elements that are essential to effectiveness of cybersecurity education; these are dedicated funding and resource allocation. Three main strategies have been discovered to be the best in addressing emerging cyber threats across the globe and this encompasses substantial investment on preparing instructors, modernizing of teaching materials, and continuous revision of course curricula to address new cyber challenges. Indian schools, by contrast, often lack adequately trained cybersecurity instructors and continue to rely on outdated resources. Another major issue in the context of India, is that the NCSP policy is obsolete and lacks specific goals and timelines. Additionally, it does not addresses emerging technologies such as artificial intelligence (AI) and Internet of Things (IoT) (Gorai *et al.*, 2025). India's cybersecurity education programs are weakened by policy gaps and poor collaboration among agencies. These findings highlight the importance of coordinated policy frameworks and institutional collaboration in ensuring effective implementation of cybersecurity education programs within school systems. To strengthen them, Indian schools need sustained support in teacher training, curriculum modernization and access to hands-on labs to help students, parents and educationalists to safeguard the educational institution and confront cyber threats (Tiwari and Dhiman, 2025).

Lastly, the findings reveal that the effectiveness and success of international cybersecurity programs largely stem from state support and close collaboration with industry. Indian schools need to adopt more effective measures to ensure the success of cybersecurity initiatives. Essential steps include establishing clear national standards,

fostering collaboration between schools and industry experts, and implementing programs that educate children, teachers, and parents on safe internet practices. India needs to do more than just get the word out; it needs to make sure that what kids learn in schools is relevant to the talents that employers are looking for. Limited funding, poor cyber hygiene awareness and inadequate IT infrastructure continue to obstruct the development of strong cybersecurity education. India should not wait for cyber incidents to happen. By adopting a comprehensive and forward-looking strategy, India can shift from reacting to cyber incidents to preventing them altogether, in essence, safeguarding the nation and preparing its citizens for the challenges of the digital future.

5.3 Discussion of Research Question Two

The study examined the pedagogical approaches, resources, and lesson structures employed by various countries to identify effective cybersecurity education strategies adaptable to Indian high schools. Findings show that leading global programs incorporate experiential learning, emphasizing hands-on learning through projects, simulations, and real-world problem solving. The experimental learning plans are very effective since, as the constructivist learning theory argues, students receive better insights through active problem solving and practical projects, as opposed to basic theoretical teaching. These methodologies can be used in cybersecurity education to allow students to sharpen their analytical and critical thinking abilities as they train their real-world responses to cyber dangers.

As per the study by (Beason *et al.*, 2021), such methodologies enable students think critically and gain practical understanding of how to use their learning beyond the classroom. The best practices provided by other countries also indicate that Capture-the-Flag competitions, gamified challenges, and problem-solving based on situations that are most effective at capturing the interest of students and relating concepts learned in

classrooms to the real-world cyber threats (Prümmer *et al.*, 2024). High school education in India, however, remain focused on book-based learning and basic ICT theory, which according to (Otoum *et al.*, 2025), restricts students from acquiring hands-on experience necessary to address evolving cybersecurity challenges.

Due to the overemphasis on theory on cybersecurity education, pupils in India's high schools may not be equipped with the practical skills employers want. Incorporating cybersecurity topics into ICT, STEM, and even social studies through cross-curricular initiatives benefits both instructors and students (Alotaibi *et al.*, 2025). Aside from enhancing digital abilities, this also encourages civic duty, ethical reasoning, and a societal understanding of technology's effects. One such approach may be to include cybersecurity instruction into the regular high school curricula in India. This should allow students to gain practical experience in the field while also learning how to utilize technology responsibly and ethically.

The study by (Citro *et al.*, 2024), notes the relevance of digital tools to raise cybersecurity awareness through storytelling approach. The study indicates that, though there is scarcity of free technologies, there remains a small yet promising set of digital tools and instructional resources like CyberSecurity Lab; INTERLAND; comicgen etc. accessible to the public for imparting cybersecurity education. Such tools that deliver cybersecurity awareness and training through storytelling can be adopted by the Indian education system to engage learners more effectively, simplify complex concepts, and instill ethical digital practices.

Evidence shows that, centralized repositories and cloud-based solutions, offering educators tailored resources such as CyberFirst in the UK and the NICE Cybersecurity Workforce Framework in the US, are effective in supporting cybersecurity education (NIST, 2023). In the Indian context, the challenges with respect to poor infrastructure,

unskilled educators or poorly trained teachers can be addressed through investment in reliable, cost effective and cloud-based laboratories and the development of a national repository of curated lesson plans and practice settings, that can be achieved through school-government-industry collaboration.

Curriculum design is one of the determining factors in effectiveness of cybersecurity education; and the most impactful approach is a balanced framework that covers both fundamental concepts of digital safety, such as malware and phishing, and the more intricate ones like data protection, encryption, and network security. The study by (Ismail *et al.*, 2024), proposes a step-by-step approach, suggesting students to start with general awareness and shift to advanced level of technical skills. On the contrary, cybersecurity education in India remains poorly organized, having a lot of loose ends. and there are no defined standards or clearly articulated benchmarks specifying the competencies students should acquire at each stage of schooling. International programs like NICE (USA) and NIST Cybersecurity Framework offer a clear pathway of tiered learning, beginning with basic cyber hygiene and gradually advancing to advanced competencies. Consistent with the goals of Digital India, the nation can implement a similar modular approach with basic cyber hygiene training mandatory for all students, and also offering optional advanced classes for students who wish to pursue advanced learning (Kant, 2023)

Lastly, the comparison reveals that while India can borrow ideas and learn good practices from other countries, it cannot merely mimic their methods. It should instead tailor them to ensure it can be carefully adapted to suit the domestic context. International best practices in cybersecurity advocate lifelong learning, professional credentialing, and alignment with industry guidelines (Shillair *et al.*, 2022). India may adopt a similar approach and enforce certification of teachers in cybersecurity basics, increase MOOCs

“massive open online courses” and webinars in local languages, and urge educators, students and parents to attend hackathons or locally organized workshops to develop confidence and competence. In order for schools to stay relevant, the study recommends training teachers to adopt student-centric methods and developing school programs aligned with national goals and international standards, and at the same time ensuring collaboration with technology companies to stay relevant with the emerging trends. These pedagogical shifts have the potential to strengthen the nation’s digital future, enhance cyber resilience, and significantly reduce cybersecurity workforce gap.

5.4 Discussion of Research Question Three

The research question addressed the government policies and regulations influence teaching cybersecurity in Indian high schools. (Kumar, 2024), notes that although India has introduced general programs to build digital skills, few targeted policies exist to guide cybersecurity instruction in schools. Successful countries worldwide follow effective policy frameworks maintain well-defined plans and regulations for integrating cybersecurity into school curricula, India’s ill framed policies lead to uneven implementation with some schools having strong programs, while others lag behind. For instance, states such as Karnataka have had proactive programmes such as the Digital Nagarik (Sridevi, 2020), while some other states continue to struggle and lack structured frameworks. In a bid to ensure that every school across the different states and districts are at the same level of cybersecurity awareness, efforts should be made to enhance the policies with concise objectives, methods of gauging achievement, and lessons to be taught in school syllabus.

Comprehensive study in this paper reveals that, strong government intervention using a multi-stakeholder model in which the education ministries, technology agencies, and corporations can join forces, to drive efficient cybersecurity awareness programs. The

research work produced by (Sharma, 2023), indicates that India has also advanced through the NEP 2020, Digital India mission, and Cyber Shikshaa; however, these remain broad digital initiatives aimed at harnessing technology to build a digitally empowered India, rather than structured school-based cybersecurity frameworks. Unlike the US NICE Cybersecurity Workforce Framework or the CyberFirst program in UK, India does not have a national framework that establishes competency milestones and curricular movement in the student population. The necessity for curriculum standardization led by legislation is underscored by the lack of such organized frameworks, which hinders schools' capacity to methodically cultivate cybersecurity capability among pupils. Such gaps call for a national framework, establishing clear guidelines and milestones for structured school-level programs that deliver cybersecurity lessons ranging from basic to advanced, impart training to upskill academicians, ensure awareness initiatives are implemented in multiple languages, engage community leaders and influencers to promote cyber hygiene, and allocate funding to setup labs. In order to ensure that schools are strengthened that supports a sustainable digital future, these initiatives should be implemented across all the states and districts of India and effectively engage students, teachers, and parents and the society at large.

Lastly, the paper emphasizes the urgency to embed cybersecurity education within India's general digital literacy programmes. As reliance on technology expands across education, finance, healthcare, and government sectors, it is an imperative that citizens are digitally literate and cognizant of cyber threats. To stay abreast of technological developments, policy changes must extend beyond classroom learning and new rules should be framed to provide opportunities to engage in competitions, hackathons, and collaborate with industry experts to stay current with advancements in emerging technologies. These frameworks cannot be sustained without the active participation of

parents, state and federal government, and community at large. India can build a robust cybersecurity education system by studying and incorporating successful international practices and adapting them to its unique socio-cultural context.

5.5 Discussion of Research Question Four

The research question was aimed at assessing the level of cybersecurity awareness among students, parents and educationalists in India. The findings indicate that although each group demonstrate having general familiarity with basic cybersecurity concepts, the level of awareness and the way they apply these principles in real world vary considerably. The findings indicate that while most students recognize common threats such as phishing and cyberbullying, this awareness rarely translate into preventive action; in other words, students seldom take any steps to protect themselves in the cyber world. It appears that being aware of the need of safe online habits is not enough to close the knowledge gap with actual behavior in action. To assist students to translate, what they have learnt in the classroom to real world cybersecurity scenarios, it is essential to incorporate more hands-on training, structured cyber ethics sessions, and practical learning activities may be required. Evidence of this gap is seen in practices such as reusing passwords, reliance on use of public Wi-Fi for banking, and oversharing location information on social media. As well noted by (Manalo and Gallardo, 2024), success of cybersecurity education program is reflected in students' capacity to stay safe online, identify prevalent threats, and proactively reporting suspicious incidents. Parental awareness of cybersecurity is evident in their efforts to monitor children's screen time and provide guidance on online activities. However, significant knowledge gaps remain when it comes to advanced cybersecurity practices. Educators possess technical understanding, but are unable to consistently translate into classroom application due to constraints such as limited opportunities, inadequate funding, scarce resources, and insufficient curriculum support. Additionally,

the study identifies that, both parents and educators expressed strong interest for receiving training in cybersecurity. This observation is consistent with the findings reported by (Sridevi, 2020; Corradini and Nardelli, 2020), that suggests structured training and awareness programs for each stakeholder groups to foster a safer digital environment.

The first hypothesis examined the possibility of significant variations in cybersecurity awareness among educationalists, parents, and students. The ANOVA results reveal distinct patterns across stakeholder groups. Findings indicate that despite the existing differences, especially in technical knowledge and interest in preventive measures, there is a moderate level of awareness of the groups (Ayyash *et al.*, 2024). For students none of the tested aspects including safe social media behavior, cyberbullying awareness, comprehension of cybersecurity, reporting suspicious activity, password practices, and phishing email identification showed statistically significant differences ($p > 0.05$), indicating that students awareness levels are relatively uniform. Parents on the other hand, demonstrated significant variation in proactive practices such as talking to children about cyber risks ($p = 0.009$), monitoring screen time ($p = 0.015$), promoting safe social media behavior ($p = 0.002$), and protecting personal data ($p = 0.036$). This highlights, parental guidance and formal education help to shape cybersecurity awareness among children. For academicians, significant differences emerged in technical competencies, particularly in identifying online threats ($p = 0.016$) and there was borderline significance for system/network security ($p = 0.05$), while general awareness practices remained largely consistent. To address the knowledge gap and empower teachers to promote responsible online behavior, teacher preparation programs should incorporate comprehensive cybersecurity instruction (Kumar, 2025). Together, these findings suggest that while student awareness is broadly uniform, it requires strengthening through curriculum reforms; parental approaches to cybersecurity vary considerably and need standardization

through awareness programs to ensure consistent digital safety at home; and academicians show gaps in technical expertise that can be addressed through professional development and standardized trainings. A strong cybersecurity education ecosystem in India can only be achieved via a concerted effort on the part of schools, parents, and teachers, backed by the government and business partners.

The second hypothesis was the parental involvement in the practice of digital safety and correlation with cybersecurity awareness of students. Findings indicate that there is a positive relationship between surveillance of online activities and discussion about online hazards. (Frank *et al.*, 2023) explains how learning institutions can use effective cybersecurity strategies and see how technologies (encryption, multi-factor authentication, and AI) can be used to protect their digital infrastructure. Findings indicate that when parents are actively involved in talking and watching over students, they develop better forms of protection and are more capable of identifying threats. Nonetheless, parents' overall engagement in relation to their child / student variables did not show significant relationship with the advanced skill such as good password practices or phishing awareness, indicating that structured parental training is important along with school-based intervention. Students' cybersecurity awareness cluster (safe behavior, passwords, phishing, reporting) is strongly interrelated, but independent of parental engagement. This suggests that formal awareness programs, peer influence, or direct training may be more impactful in addition to parental involvement. The findings indicate that a complex web of relationship exists, which impacts the cybersecurity awareness of students in India. The initial foundation is laid by parents and caregivers, technical and curricular information is taught by teachers and students apply the knowledge acquired in their everyday practice in the digital ecosystem. In order to support the ecosystem, schools need to have parental workshops, cybersecurity courses are to be offered as part of teacher training programs, the

curriculum needs to include not only technical training but also ethical conduct, critical thinking and risk mitigation skills.

Altogether, the results lead to the fact that there are three factors interacting with each other, and these are the pedagogical exposure, parental involvement, and institutional support impacting stakeholders in cybersecurity awareness of Indian high schools. Continuous adoption of secure digital behaviors by students still has room for improvement even though it seems that they have internalized the issues surrounding cybersecurity threats. The study's distinct contribution is its holistic vision integrating curriculum improvements, teacher professional development, and parental engagement to elevate cybersecurity awareness. This integrated model advances theoretical foundations, practical application, informed pedagogical practices, and shape policy directions for India's digital future.

Lastly, the general idea of this discussion is to emphasize the necessity of a multi-level intervention involving students, parents, and teachers so as to raise cybersecurity awareness in India. Although technical knowledge is the core, however, practical skills, ethical conduct and risk mitigation measures should also be addressed in the awareness campaigns (Frank *et al.*, 2023). Integrating formative curricula, interactive learning modules, and active parental engagement will contribute towards improving both awareness and practical application of cybersecurity principles. Moreover, the results underscore the need for ongoing evaluation and revision of programs to address new threats and technological changes. Strengthening the home-school policy framework will enable India to foster a culture of cybersecurity awareness and equip high school students to operate securely and responsibly in the digital sphere.

CHAPTER VI: SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1 Summary

Based on the current laws and practices to past researches and the recommendations of stakeholders and world analysts, the paper discussed cybersecurity education in high schools of India in all conceivable angles. According to the available information, the best global programs feature cybersecurity education as part of their elementary education system combining technical expertise with moral, social and behavioral aspect of online safety. Indian high schools, on the other hand, lacked a coherent curriculum, and largely emphasized on basic computer literacy, resulting in a fragmented understanding and limited practical experience. To encourage engagement and applied competencies, the findings underscore the relevance of multidisciplinary approaches and learning strategies such as virtual labs, gamified modules, and the use of modern digital tools. We can only imagine that India needs to act promptly to develop a cybersecurity education system that considers every detail, broaden its curriculum, modernize and strengthen instructional resources, and adopt international best practices to build a comprehensive and sustainable cybersecurity education framework.

It also explored the possible directions of boosting cybersecurity awareness, parental engagement, and regulation. The study reveals that Indian policy frameworks remain fragmented and weakly enforced, unlike international models that are able to incorporate companies, schools, and government. Formal education through parental involvement can be considered as an extension of formal education and enhances knowledge among children. The study further affirms that educators possess technical expertise that must be effectively translated into practical teaching methods.

Overall, the study concludes that building a resilient culture of cybersecurity requires an interactive, multi-layered approach anchored in clear rules and regulations, structured curricula, teacher training, family participation, and effective industry collaboration. Once this comprehensive framework is implemented, Indian high school students will be able to engage with digital environment more effectively, fostering competence, responsibility, and confidence. In parallel, it will contribute to strengthening the nation's digital infrastructure, contribute to the workforce and enhancing its overall security.

6.2 Research contributions of the study

The research contributes to the existing information in the field of cybersecurity education as it captures information on the effectiveness of cybersecurity programs, challenges in implementing them, and possible advantages to the students in Indian high schools. This study could be useful to theory, practice, and policy formulation; offering a multi-dimensional analysis that bridges international best practices with India's education context.

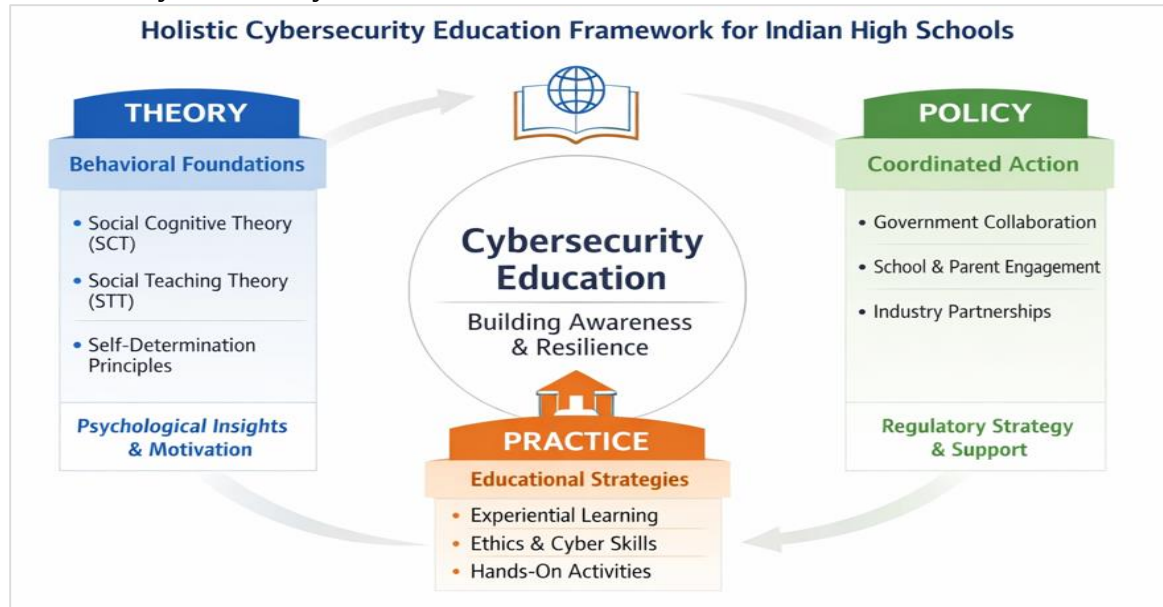
- **Theoretical Foundations:** The work is theoretically established by ensuring that cybersecurity curricula incorporate Social Cognitive Theory (SCT), Space Transition Theory (STT), and principles of Self-Determination. Besides contributing to the existing body of theoretical knowledge, this study illustrates how school-based cybersecurity education can be enhanced with the involvement of stakeholders, educational exposure, and awareness.
- **Comparative Analysis and Benchmarking:** Unlike prior studies, this study points out important techniques and transferable practices that can be adapted to Indian high schools, by systematically evaluating strengths and weaknesses of cybersecurity education across multiple countries. The research concluded that high

schools in India may improve their cybersecurity education by using tactics such as experiential learning, curricular integration, and hands-on cybersecurity education. This information was derived from research on instructional techniques, instructional design, and pedagogical resources used in different countries.

- **Stakeholder Collaboration:** A novel contribution lies in the assessment of multi stakeholders including students, educationalists, and parents. All of the identified stakeholders may benefit from putting this study's findings into action by filling up important gaps in cybersecurity understanding. When it comes to creating a successful school cybersecurity culture, the findings stress the need for stakeholder collaboration. In the light of this, the report provides policy makers, educators, and school administrators with actionable guidance for enhancing children's cybersecurity and online safety.
- **Policy-Level Implications:** The study explores the impact of government policies and regulatory frameworks affecting cybersecurity education programs across multiple nation, identifying gaps and offering policy-level refinements tailored to India's socio-cultural and infrastructural realities. Formal cybersecurity education systems that can contribute to long-term national cyber resilience require improved cooperation across government organizations, educational institutions, and industry partners, according to the research.
- **Holistic Framework Proposal:** The study proposes theoretical framework for improving cybersecurity education in Indian high schools by encouraging stakeholder awareness, policy backing, curricular modifications, and educator training. Additionally, there is a holistic perspective that it will serve as a springboard for the establishment of more organized and long-lasting cybersecurity initiatives in India.

The below image illustrates contribution of this research paper – a three-pillar framework for cybersecurity education in Indian high schools.

Fig 6.1: Holistic Cybersecurity Education Framework



Source: Created by author.

Figure 6.1: Holistic Cybersecurity Education Framework for High School Curriculum

The diagram is not just a set of recommendations, but a conceptual model that integrates theory, practice, and policy; with Cybersecurity Education: Building Awareness & Resilience at its center; showing how these three pillars converge into a holistic framework to safeguard India's future. The model underscores behavioral foundations, coordinated policy, and experiential learning actions to build awareness and resilience among high school students.

Theory: Builds behavioral foundations (STT, SCT, and Self-Determination principles), motivation, ethical awareness, and provides a psychologically grounded approach for digital safety.

Practice: Education strategies (Experiential Learning, Hands-On Activities, Ethics & Cyber Skills) in turn translates, classroom knowledge into real-world competence and responsible online behavior.

Policy: Structured policies (Government Collaboration, School & parent Engagement, Industry Partnerships) provide strategic support, sustainability and national cyber resilience.

Ultimately, the study contributes to our knowledge of theory, practice, and policy by demonstrating the possible advantages of incorporating cybersecurity education into India's high school curricula. Drawing on global best practices, it provides a roadmap for triangulated stakeholder collaboration and raising a generation of students who are digitally competent, ethically responsible, and more wary of and attentive to the dangers posed by technological advancements.

6.3 Implications

The results of this study have important implications for enhancing education policies in India. The fact that cybersecurity is not well integrated in high school curricula underscores need for major changes in planning and implementation. By following a clear, consistent, and multi-faceted approaches such as storytelling, simulations and gamification; decision-makers can help students learn not just technical skills but also to pave the way for how to think critically and understand ethical issues. Aligning curricula with global best practices, while adapting to local contexts and cultural settings, will ensure reforms are practical, effective, and sustainable. Implementing these changes will also enable India to develop a digitally skilled workforce capable of safeguarding against online threats.

An equally important consideration is the training of teachers and the provision of adequate resources. The study demonstrates that without proper training and access to

modern digital tools, even well-designed lesson plans fail to achieve their intended purpose. Continuous professional development empowers educators with confidence and equips them to design and recommend effective course content. Therefore, it is essential for the government, industry leaders, and schools to invest time and resources in sustained teacher training programs that strengthen instructional competence in delivering effective cybersecurity education.

The paper emphasizes the critical role of parental involvement in shaping children's digital safety awareness, noting that primary education begins at home and that children often mirror the behaviors of their parents and caregivers. By designing programs that involve parents through workshops, awareness campaigns, and home-based activities can strengthen their understanding of cybersecurity. Positioning parents as active partners in digital education ensures a supportive environment that helps students navigate cyber risks responsibly.

Finally, the study underscores that strengthening cybersecurity education is vital for India's digital future. Equipping students with real-world skills fosters responsible online behavior, reduces cybercrime, and builds national resilience. Achieving this requires collective action from government, educators, parents, and industry experts working together to create a secure and sustainable digital community.

6.4 Recommendations for Future Research

Based on the analysis and findings, future research should pursue projects aligned with the following recommendations to improve cybersecurity education in Indian high schools:

- Examine how integrating cybersecurity concepts into various social science subjects such as psychology, sociology, and ethics enhances students' critical thinking skills, and shapes their understanding of responsible online behavior.

- Assess the impact of cybersecurity workshops by comparing educators' and parents' awareness levels before and after participation.
- Evaluate the effectiveness of government led cybersecurity education efforts through district-level micro analysis, with subsequent comparisons across states.
- Evaluate how using games and hands-on learning helps high school students to acquire practical cybersecurity competencies.
- Investigate the partnerships between schools, subject experts, and tech firms in delivering real-world cybersecurity learning opportunities to students.

Further studies could examine how international models of cybersecurity education can be tailored to India's educational structures and cultural background, and use long-term research to track growth in students' cybersafety awareness. Such studies would offer valuable insights for policymakers, educators, and stakeholders by producing empirical data to help shape stronger policies, design more effective programs, and guide their implementation. This would ensure that Indian high school students acquire the skills, knowledge, and understanding of ethics necessary to navigate the complex digital world.

6.5 Conclusion

In today's digital landscape, safeguarding information has become indispensable due to the growing frequency of privacy breaches, data losses, and the substantial financial costs incurred to restore compromised systems; often accompanied by diminished customer trust. In addition, the study identifies substantial shortages in skilled cybersecurity professionals. Educational institutions, including schools, are not exempt from cyber risks, as they manage sensitive personally identifiable information (PII) such as student / parent / educator names, contact details, addresses, SSN, academic grades, and even unpublished research work. While the term cybersecurity may resonate with

professionals, it is often less relatable or age-appropriate for younger audiences, particularly K-12 students. Research suggests that alternative expressions such as digital safety, digital awareness, or digital hygiene are more effective in fostering understanding and engagement among school learners.

This study investigated cybersecurity education in Indian high schools, benchmarking it against practices in other nations. It assessed teaching methods, government policies, and student / teacher / parent awareness. Evidence shows that many countries have embedded cybersecurity into school curricula, teaching not only technical skills but also ethical principles and responsible online conduct. In India, cybersecurity instruction remains limited, centered on basic ICT theory. The study recommends linking cybersecurity with subjects such as psychology, civics, and social studies to help students think critically and understand the ethics of safe usage.

The study highlights that curriculum design, accessibility of resources, and dedicated funding are critical factors in advancing cybersecurity education. In India, however, teachers often lack sufficient preparation to deliver these lessons effectively. Structured teacher training, leveraging expertise from industry professionals, continuous learning and development, modernized teaching infrastructure, and systematic curricula designed progressively from basic to advanced concepts are essential, as they equip educators with the confidence and competence needed to deliver cybersecurity knowledge in formats appropriate for school children's level of comprehension. Additional approaches may include employing innovative methods such as storytelling, simulations, and gamification to engage students. These approaches will not only strengthen teachers and students' foundational knowledge but also spark interest in higher learning, ultimately helping to address global cybersecurity workforce gaps and fostering a stronger, safer generation prepared to navigate the digital world responsibly.

The study also explores the critical role of parental involvement in instilling safe digital practices. A child's early education begins at home under the guidance of family and caregivers, and when combined with school-based instruction, can significantly enhance children's cybersecurity awareness. To support this, the government must establish clear rules and policies and ensure a standardized curriculum across all schools. Teacher training, parental guidance, and accessible resources together create a strong foundation for digital safety education. Such an approach will enable India to establish a strong, collaborative framework that advances cybersecurity education, enhances digital safety, and remains culturally and infrastructurally appropriate while aligning with international best practices.

Ultimately, a forward-looking revolutionary and sustainable transformation in India's cybersecurity education is essential, combining curriculum innovation, teacher training, and stakeholder involvement. This will not only equip students with essential skills but also strengthen national security and digital trust.

REFERENCES

- AAG., 2024. *The Latest Cyber Crime Statistics (updated October 2024)* | AAG IT Support.
<https://aag-it.com/the-latest-cyber-crime-statistics/>
- Aaltonen, K., Derakhshan, R., Di Maddaloni, F. and Turner, R., 2024. Stakeholder engagement: Theoretical and methodological directions for project scholarship. *International Journal of Project Management*, 42(7), 102649.
<https://doi.org/10.1016/j.ijproman.2024.102649>
- Abela, R., 2017. *How do consumers protect themselves from cyber attacks? Invicti*. Available at: <https://www.invicti.com/blog/news/consumers-web-applications-most-risk-hacked/> (Accessed: 23 Jul. 2025)
- Abrahams, T., Ewuga, S., Dawodu, S., Adegbite, A., and Hassan, A., 2024. A Review of Cybersecurity Strategies in Modern Organizations: Examining The Evolution and Effectiveness of Cybersecurity Measures for Data Protection. *Computer Science & IT Research Journal*, 5, 1–25. <https://doi.org/10.51594/csitrj.v5i1.699>
- Adejumo, A. and Ogburie, C., 2025. The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, 25(3), 1542–1556.
<https://doi.org/10.30574/wjarr.2025.25.3.0909>
- Admass, W.S., Munaye, Y.Y. and Diro, A.A., 2024. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, 100031.
<https://doi.org/10.1016/j.csa.2023.100031>
- Affia, A. O., Nolte, A. and Matulevičius, R., 2022. *Integrating hackathons into an online cybersecurity course*. <https://doi.org/10.1145/3510456.3514151>
- Afzal, A., Khan, S., Daud, S., Ahmad, Z. and Butt, A., 2023. Addressing the Digital Divide: Access and Use of Technology in Education. *Journal of Social Sciences Review*, 3(2), 883–895. <https://doi.org/10.54183/jssr.v3i2.326>

- Ahmed, S.K., 2024. How to choose a sampling technique and determine sample size for research: A simplified guide for researchers. *Oral Oncology Reports*, 12, p.100662.
- Ahn, G., Jang, J., Choi, S. and Shin, D., 2024. Research on Improving Cyber Resilience by Integrating the Zero Trust security model with the MITRE ATT&CK matrix. *IEEE Access*, 12, 89291–89309. <https://doi.org/10.1109/ACCESS.2024.3417182>
- AICTE, n.d. *AICTE Cyber Security Strategy for Higher Education Institutes*. Available at: <https://www.aicte-india.org/sites/default/files/cyber/AICTE%20Cyber%20Security%20Strategy%20for%20Higher%20Education%20Institutes.pdf> (Accessed: 22 December 2024).
- Aksoy, C., 2024. Building A Cyber Security Culture for Resilient Organizations Against Cyber Attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), 96–110. <https://doi.org/10.33416/baybem.1374001>
- Al-Sharhan, A., Alsaber, A., Al Khasham, Y., Al Kandari, A., Nafea, R. and Setiya, P., 2024. The influence of governmental support on cyber-security adoption and performance: the mediation of cyber security and technological readiness. *International Journal of Business Data Communications and Networking (IJBDCN)*, 19(1), 1–16. <https://doi.org/10.4018/IJBDCN.341264>
- Alam, M.S., 2022. Need of Cyber Security in Higher Education in Present Era. *International Journal of Creative Research Thoughts (IJCRT)*, 10(3).
- AlDaajeh, S., Saleous, H., Alrabae, S., Barka, E., Breiting, F. and Choo, K.K.R., 2022. The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119, p.102754.
- Ali, M.D.J., 2024. Cybercrime and Cybersecurity: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms. *Bharati International Journal of Multidisciplinary Research and Development*, 2(8), pp.137-154.

- Aljohani, W. and Elfadil, N., 2020. Measuring cyber security awareness of students: A case study at fahad bin sultan university. *International Journal of Computer Science and Mobile Computing*, 9(6), pp.141-155.
- Alnajim, A.M., Habib, S., Islam, M., AlRawashdeh, H.S. and Wasim, M., 2023. Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry*, 15(12), 2175. <https://doi.org/10.3390/sym15122175>
- Alotaibi, M., Cherdantseva, Y., Rana, O. and Teehan, C., 2025. Empowering Youth in The Digital Age with Cyber Security Education. *Journal of The Colloquium for Information Systems Security Education*, 12(1), 8. <https://doi.org/10.53735/cisse.v12i1.203>
- Alqurashi, F. and Ahmad, I., 2024. A data-driven multi-perspective approach to cybersecurity knowledge discovery through topic modelling. *Alexandria Engineering Journal*, 107, 374–389. <https://doi.org/10.1016/j.aej.2024.07.044>
- Altarawneh, M.H.M., Althunibat, A., Almajali, M.H., Alzriqat, N. and Alazzam, S., 2025. Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps. *International Journal of Innovative Research and Scientific Studies*, 8(1), 1516–1529. <https://doi.org/10.53894/ijirss.v8i1.4696>
- Althibyani, H.A. and Al-Zahrani, A.M., 2023. Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability*, 15(15), 11512. <https://doi.org/10.3390/su151511512>
- Amankwa, E., 2021. Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, 12(04), 233–249. <https://doi.org/10.4236/jis.2021.124013>
- American Psychological Association (APA), 2012. *DART Toolkit II: Legal Issues* —

- FERPA Overview*. Available at: <https://www.apa.org/pi/disability/dart/legal/ferpa> (Accessed: 28 Jul. 2025).
- Andersson, M., Boateng, K. and Abos, P., 2024. Validity and Reliability: The extent to which your research findings are accurate and consistent. *ResearchGate, September*, 1–7.
- Antunes, M., Silva, C. and Marques, F., 2021. An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. *Applied Sciences*, 11(23), p.11269.
- Aoyama, D., Yonemura, K. and Shiraki, A., 2024. Effective Methods in Cybersecurity Education for Beginners. *2024 12th International Conference on Information and Education Technology (ICIET)*, 372–375. <https://doi.org/10.1109/ICIET60671.2024.10542828>
- Arishi, A.A., Kamarudin, N.H., Bakar, K.A.A., Shukur, Z.B. and Hasan, M.K., 2024. Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences. *International Journal of Advanced Computer Science and Applications*, 15(12), 467–478. <https://doi.org/10.14569/IJACSA.2024.0151249>
- Armas, R. and Taherdoost, H., 2025. Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm. *Information*, 16(5), 336. <https://doi.org/10.3390/info16050336>
- Askew, M., Rhodes, V., Brown, M., Wiliam, D., and Johnson, D., 1997. *Effective teachers of numeracy: final report*.
- Asrifan, A., Vivekanantharasa, R., and Aini, N., 2025. Enhancing Cybersecurity Skills Through Gamified Learning. In *Gamification Learning Framework for Cybersecurity Education* (pp. 37–64). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3373-0477-9.ch002>

- Ayeyemi, M., 2023. A Systematic Review of Cybersecurity Education in K-12 Context. *Supervisors of the Master's Thesis: M.Sc. Ismaila Sanusi*.
- Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S. and Parkinson, S., 2024. Cybersecurity Education and Awareness Among Parents and Teachers: A Survey of Bahrain. *IEEE Access*, 12, 86596–86617. <https://doi.org/10.1109/ACCESS.2024.3416045>
- AZUBUIKE, C.F., 2023. Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. *Nnamdi Azikiwe Journal of Political Science*, 8(3), 101–114.
- Manalo, M. and Gallardo, R.D., 2024. Cyber Security Awareness and Educational Outcomes of Grade 4 Learners. *International Journal of Innovative Science and Research Technology (IJISRT)*, 9(4), 1390–1422. <https://doi.org/10.38124/ijisrt/ijisrt24apr1261>
- Bada, M. and Nurse, J.R., 2020. The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 73–92). Elsevier. <https://doi.org/10.1016/B978-0-12-816203-3.00004-6>
- Beason, R., Phelan, M. and Devine, S., 2021. *Evaluation of Hands-On Cybersecurity Skills Development*. September, 1–18.
- Beauchamp, C., Matusovich, H., 2022. A Mixed-Method Study of Significant Learning Experiences with Cyber Ranges in Cybersecurity Education. *Proceedings of the EDSIG Conference ISSN*, 5728.
- Beuran, R., Tang, D., Tan, Z., Hasegawa, S., Tan, Y. and Shinoda, Y., 2019. Supporting cybersecurity education and training via LMS integration: CyLMS. *Education and Information Technologies*, 24(6), 3619–3643. <https://doi.org/10.1007/s10639-019-09942-y>

- Bhangla, A. and Tuli, J., 2021. A study on cyber crime and its legal framework in India. *Issue 2 Int'l JL Mgmt. & Human.*, 4, p.493.
- Bishop, M., Burley, D., Buck, S., Ekstrom, J.J., Fitcher, L., Gibson, D., Hawthorne, E.K., Kaza, S., Levy, Y., Mattord, H. and Parrish, A., 2017. Cybersecurity curricular guidelines. In *IFIP world conference on information security education* (pp. 3-13). Cham: Springer International Publishing.
- Blažič, A. J. and Blažič, B. J., 2024. Toward effective learning of cybersecurity: new curriculum agenda and learning methods. *Journal of Cybersecurity*, 10(1). <https://doi.org/10.1093/cybsec/tyae018>
- Blažič, B.J., 2022. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?. *Education and information technologies*, 27(3), pp.3011-3036.
- Bolun, I., Bulai, R., and Ciorbă, D., 2021. Support of Education in Cybersecurity. *Pro Publico Bono - Magyar Közigazgatás*, 9(1), 128–147. <https://doi.org/10.32575/ppb.2021.1.8>
- Brooks., 2021. *More alarming cybersecurity stats for 2021*.
- Burov, O.Y., Butnik-Siversky, O.B., Orliuk, O. and Horska, K.A., 2020. Cybersecurity and innovative digital educational environment. *Information Technologies and Learning Tools*, 80(6), 414–430.
- Business World, 2022. *Cybersecurity In 2022: Awareness The Key*. Available at: <https://www.businessworld.in/article/cybersecurity-in-2022-awareness-the-key-450686> (Accessed: 11 May 2025).
- Cabaj, K., Domingos, D., Kotulski, Z. and Respício, A., 2018. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, 75, 24–35. <https://doi.org/10.1016/j.cose.2018.01.015>

- Čaplová, Z. and Švábová, P., 2020. IBM SPSS statistics. In *Statistics and Probability in Forensic Anthropology*. <https://doi.org/10.1016/B978-0-12-815764-0.00027-7>
- Catota, F.E., Morgan, M.G. and Sicker, D.C., 2019. Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, 5(1), 1–19. <https://doi.org/10.1093/cybsec/tyz001>
- Caulkins, B., Marlowe, T. and Reardon, A., 2018, June. Cybersecurity skills to address today's threats. In *International Conference on Applied Human Factors and Ergonomics* (pp. 187-192). Cham: Springer International Publishing.
- Chakraborty, A. and Tiwari, S., 2025. An analytical study on challenges and gaps in India's cyber security framework. *International Journal of Criminal Common and Statutory Law*, 5(1), p.4.
- Chase, J., Uppuluri, P., Denny, E., Patterson, B., Eller, J., Lane, D., Edwards, B. and Onuskanich, R., 2020. STEAM powered K-12 cybersecurity education. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 7, No. 1, pp. 8-8).
- Chatlani, S., 2017. Cost of education data breaches averages \$245 per record. *Education Dive*. <https://www.educationdive.com/news/cost-of-education-data-breaches-averages-245-per-record/447376>.
- Chen, W., He, Y., Tian, X. and He, W., 2021. Exploring cybersecurity education at the K-12 level. In *SITE Interactive Conference* (pp. 108-114). Association for the Advancement of Computing in Education (AACE).
- Chen, W.B. and Gregory, A., 2009. Parental Involvement as a Protective Factor During the Transition to High School. *The Journal of Educational Research*, 103(1), 53–62. <https://doi.org/10.1080/00220670903231250>
- Cheung, R.S., Cohen, J.P., Lo, H.Z. and Elia, F., 2011. Challenge-based learning in cybersecurity education. In *Proceedings of the International Conference on Security*

- and Management (SAM)*, p.1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)
- Childers, G., Linsky, C.L., Payne, B., Byers, J. and Baker, D., 2023. K-12 educators' self-confidence in designing and implementing cybersecurity lessons. *Computers and Education Open*, 4, 100119. <https://doi.org/10.1016/j.caeo.2022.100119>
- Chiou, Y.M., Barnes, T., Jelenewicz, S.M., Mouza, C. and Shen, C.C., 2021. Teacher views on storytelling-based cybersecurity education with social robots. *In Proceedings of the 20th Annual ACM Interaction Design and Children Conference* (pp. 508-512).
- Ciabo, A. B. T. and Labadan, C.B., 2025. Students' Awareness on Safety and Security in Digital Communication and Their Online Behavior. *Global Scientific Journal*.
- Citro, T., Palmieri, G. and Pellegrino, M.A., 2024. Digital Tools, Approaches and Assessment for Cybersecurity Education via Storytelling: a Systematic Literature Review. *CEUR Workshop Proceedings*, 3700.
- Clark, M., 2022. The social consequences of the information civilization: Cyber risks to youth in the digital age. *Journal of Policy Options*, 5(2), 20-27., 5(2), 20-27. <https://doi.org/https://resdojournals.com/index.php/jpo/article/view/267>
- Cobos, E. V. and Cakir, S., 2024. *A Review of the Economic Costs of Cyber Incidents*.
- Connelly, L.M., 2021. Introduction to Analysis of Variance (ANOVA). *MEDSURG Nursing*. <https://doi.org/10.62116/msj.2021.30.3.218>
- Corradini, I. and Nardelli, E., 2020. Developing digital awareness at school: a fundamental step for cybersecurity education. *In International Conference on Applied Human Factors and Ergonomics* (pp. 102-110). Cham: Springer International Publishing.
- CSA SINGAPORE., 2024. Cybersecurity education and learning guidebook. CSA SINGAPORE.
- Cutas, F., Chatzopoulous, A., Athanatos, M. and Antonakaki, D., 2023. *CONCORDIA*

- Governance model for a European Education Ecosystem for Cybersecurity.* CONCORDIA. Available at: https://www.concordia-h2020.eu/wp-content/uploads/2023/02/CONCORDIA_Governance_model_for_EEEEC.pdf (Accessed: 28 Jul. 2025).
- Cyberlite., 2023. *Cyber Safety Education in India.* Cyberlite.
- Danquah, P. and Longe, O.B., 2011. An Empirical Test of The Space Transition Theory of Cyber Criminality: Investigating Cybercrime Causation Factors in Ghana. *African Journal of Computing & ICT*, 2(1), 37–48.
- Dar, S.A. and Lone, N.A., 2020. Cyber Crime In India. *Sambodhi*, 43(04 (VIII)).
- Darshini, S., Thrisha, A., Navya Sree, M., Varshitha, G. and Thippanna, G., 2025. Dark Sides of Cyber Attacks: Protection from the Assorted Cyber Attacks. *Journal of Cyber Security, Privacy Issues and Challenges*, 4(1), 14–21. <https://doi.org/10.46610/JCSPIC.2025.v04i01.002>
- Datta, R. and Mete, J., 2021. Digital Initiatives of New Education Policy 2020 on Higher Education in India. *Asian Journal of Electrical Sciences*. <https://doi.org/10.51983/ajes-2021.10.2.3169>
- De Bruijn, H. and Janssen, M., 2017. Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1–7. <https://doi.org/10.1016/j.giq.2017.02.007>
- Deaconu, S.M., Olah, R. and Haj, C.M., 2020. Assessing students’ perspective on teaching and learning: The case of national students’ surveys. In *European Higher Education Area: Challenges for a New Decade*. https://doi.org/10.1007/978-3-030-56316-5_22
- Deci, E.L. and Ryan, R.M., 2013. *Intrinsic motivation and self-determination in human behavior*. Springer Science & Business Media.
- Deshpande, A., 2023. Internationalization of Education: Significance, Challenges,

Strategies and Potential Benefits for Higher Education Sector in India. *Education and Society/UGC CARE*, 1(1), 37–42.

Dobos, O. and Cs1szar1k-kocs1r, A., 2022. The Role of Project Management in Cyber Warfare with the Support of Artificial Intelligence. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, 17, 26–37. <https://doi.org/10.55549/epstem.1175898>

Dudley, A., Braman, J., and Vincenti, G., 2024. *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices: Issues, Impacts and Practices*. 10(January), 343.

Edelsbrunner, P.A., Simonsmeier, B.A. and Schneider, M., 2025. The Reliability, But Not the Cronbach's Alpha, of Knowledge Tests Matters: Response to Zitzmann and Orona (2025). *Educational Psychology Review*, 37(2), 1–5. <https://doi.org/10.1007/s10648-025-10023-5>

Eling, M., Elvedi, M. and Falco, G., 2023. The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*, 27(3), pp.429-443.

Erickson, M. and Kim, P., 2021. Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning. *Issues in Information Systems*. https://doi.org/10.48009/4_iis_2021_9-21

Ervural, B. C. and Ervural, B., 2018. Overview of Cyber Security in the Industry 4.0 Era. In *Springer Series in Advanced Manufacturing*. https://doi.org/10.1007/978-3-319-57870-5_16

European Commission, 2017. Joint Communication To The European Parliament And The Council. *European Commission*.

Fan, X. and Chen, M., 2001. Parental Involvement and Students' Academic Achievement: A Meta-Analysis. *Educational Psychology Review*, 13(1), 1–22. <https://doi.org/10.1023/A:1009048817385>

- FBI - Internet Crime Complaint Center., 2023. *Annual Reports—Internet Crime Complaint Center (IC3)*. <https://www.ic3.gov/AnnualReport/Reports>
- Francis, S.P., Kolil, V.K., Pavithran, V., Ray, I. and Achuthan, K., 2024. Exploring gender dynamics in cybersecurity education: a self-determination theory and social cognitive theory perspective. *Computers & Security*, 144, p.103968.
- Frank, E., Ok, E., and Enoch, O., 2023. *Cybersecurity in Education Protecting Students and Staff*.
- Frusci, J., 2024. Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training. *Journal of Cybersecurity Education, Research and Practice*, 2024(1). <https://doi.org/10.62915/2472-2707.1209>
- Galletta, D.F., Moody, G.D., Lowry, P.B., Willison, R., Boss, S., Chen, Y., Luo, X., Pienta, D.A., Polak, P., Schuetze, S. and Thatcher, J., 2024. Balancing Fear and Confidence: A Strategic Approach to Mitigating Human Risk in Cybersecurity. *MIS Quarterly Executive*, 2024. <https://doi.org/10.17705/2msqe.00108>
- Garzotto, F., Paolini, P. and Sabiescu, A., 2010. Interactive storytelling for children. In *Proceedings of the 9th international conference on interaction design and children* (pp. 356-359).
- Gaur, B.P., 2023. Cybersecurity awareness education in schools: A review. *International Journal of Applied Research*, 9(6).
- Gkioulos, V. and Chowdhury, N., 2021. Cyber security training for critical infrastructure protection: A literature review. In *Computer Science Review*. <https://doi.org/10.1016/j.cosrev.2021.100361>
- Global Cybersecurity Forum, 2024. *Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap*. Available at: <https://gcforum.org/en/research->

publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap/ (Accessed: 24 December 2025).

Gorai, S. K., Behra, S. and Kumar, M., 2025. Issues and Challenges of Cyber Security in India. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 11(1), 159–166. <https://doi.org/10.32628/CSEIT251112>

Goud, N., 2020. Texas School District experiences DDoS Cyber Attack. *Cybersecurity Insiders*. Available at: <https://www.cybersecurity-insiders.com/texas-school-district-experiences-ddos-cyber-attack/> (Accessed: 28 Jul. 2025).

Grace, H., Banson, K. and Saraf, A., 2023. Mixed-methods research. In *Translational Radiation Oncology*. <https://doi.org/10.1016/B978-0-323-88423-5.00029-7>

Grimus, M., 2020. Emerging technologies: Impacting learning, pedagogy and curriculum development. *Emerging technologies and pedagogies in the curriculum*, pp.127-151.

Gupta, M. and Gupta, A., 2025. Cyber Security Legal Framework in India – Overlaps, Problems and Challenges. *Journal of Business Management and Information Systems*, 12(1), 11–20. <https://doi.org/10.48001/jbmis.1201002>

Halder, D. and Jaishankar, K., 2011. Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders*, 6(4), pp.386-398.

Harris, J.A., Carins, J. and Rundle-Thiele, S., 2021. Can Social Cognitive Theory Influence Breakfast Frequency in an Institutional Context: A Qualitative Study. *International Journal of Environmental Research and Public Health*, 18(21), 11270. <https://doi.org/10.3390/ijerph182111270>

Hartikainen, H., Iivari, N. and Kinnula, M., 2016. Should we design for control, trust or involvement? A discourses survey about children's online safety. In *Proceedings of*

the The 15th International Conference on Interaction Design and Children (pp. 367-378).

Hassan, L., Dias, A. and Hamari, J., 2019. How motivational feedback increases user's benefits and continued use: A study on gamification, quantified-self and social networking. *International Journal of Information Management*, 46, 151–162. <https://doi.org/10.1016/j.ijinfomgt.2018.12.004>

Hero, J. L., 2020. Teachers' Preparedness and Acceptance of Information and Communications Technology (ICT) Integration and Its Effect on their ICT Integration Practices. *Puissant A Multidisciplinary Journal*, 1(November), 59–76.

Hossain, R., Ghose, P., Chowdhury, T.M., Hossen, M.D., Hasan, M.N. and Mani, L., 2024. Ownership Structures and Firm Performance: A Correlation and Regression Analysis of Financial Institutions in Bangladesh. *Pakistan Journal of Life and Social Sciences*, 22(2), 6278–6295. <https://doi.org/10.57239/PJLSS-2024-22.2.00473>

Hossain, S.T., Yigitcanlar, T., Nguyen, K. and Xu, Y., 2025. Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Governance*, 5(1), 1–19. <https://doi.org/10.1016/j.ugj.2024.12.010>

Hyseni, V., 2024. Cybersecurity awareness — its importance and impact. *PECB*. Available at: <https://pecb.com/article/cybersecurity-awareness--its-importance-and-impact> (Accessed: 19 Jul. 2025).

IBM, 2024. *Cost of a data breach 2024: Financial industry*. IBM Think Insights. Available at: <https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry> (Accessed 22 November 2025).

Iclg., 2024. *Cybersecurity Laws and Regulations India 2025*. Iclg.

Ige, O.A., 2020. School-based cybersecurity education programme for schoolchildren in South Africa! A timely call from Bloemfontein. *Universal Journal of Educational*

Research, 8(6), pp.2710-2716.

India Today., 2024. *Cybersecurity in education: Protecting student data in the digital world.* India Today. <https://www.indiatoday.in/education-today/featurephilia/story/cybersecurity-in-education-protecting-student-data-in-the-digital-world-2490262-2024-01-18>

Ioannidi, V., 2025. Reducing the Gap in Inclusive Practice. Using School and Family Collaboration To Increase Student Achievement. *European Journal of Special Education Research*, 11(1). <https://doi.org/10.46827/ejse.v11i1.5876>

Ismail, M., Madathil, N.T., Alalawi, M., Alrabae, S., Al Bataineh, M., Melhem, S. and Mouheb, D., 2024. Cybersecurity activities for education and curriculum design: A survey. *Computers in Human Behavior Reports*, 16, 100501. <https://doi.org/10.1016/j.chbr.2024.100501>

Jacob, S., 2015. Towards a Comparative Subnational Perspective on India. *Studies in Indian Politics*, 3(2), 229–246. <https://doi.org/10.1177/2321023015601744>

Jaishankar, K., 2007. Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, 1(7), 7–9.

Jawaid, S. A., 2023. Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity. *International Journal of Data Science and Big Data Analytics*, 2(2). <https://doi.org/10.51483/IJDSBDA.2.2.2022.11-17>

Jayaraman, K., 2022. *Is India Under An Illusion Of Cybersecurity?* <https://www.dqindia.com/is-india-under-an-illusion-of-cybersecurity/>

Jerman Blažič, B. and Jerman Blažič, A., 2022. Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability*, 14(8), 4763. <https://doi.org/10.3390/su14084763>

- Johnson, N.F., Ibrahim, A., Sikos, L. and McKee, M., 2023. *Going beyond: Cyber security curriculum in Western Australian primary and secondary schools*. Final Report.
- Johnson, N., Ibrahim, A., Sikos, L. and Glowrey, C., 2022. *Cyber security curriculum in Western Australian primary and secondary schools: Interim report: Curriculum mapping*.
- Joshi, A., Kale, S., Chandel, S. and Pal, D.K., 2015. Likert Scale: Explored and Explained. *British Journal of Applied Science & Technology*.
<https://doi.org/10.9734/bjast/2015/14975>
- Kaabi, L. Al, Ketbi, W. Al, Khoori, A. Al, Shamsi, M. Al and Alrabaee, S., 2022. Safe: Cryptographic Algorithms and Security Principles Gamification. *IEEE Global Engineering Education Conference, EDUCON*.
<https://doi.org/10.1109/EDUCON52537.2022.9766526>
- Kant, R., 2023. Cyber-Security Awareness In India: How Much Students of Higher Education Are Aware?. *Education Sciences & Psychology*, 67(2).
- Karuppannan, J., 2008. *Space Transition Theory of Cyber Crimes* (pp. 283–301).
- Kaur, M., Dutta, N., Singh, A., Sudhir, M. and Rajput, S., 2025. NEP 2020 in Reference to AI and Cyber Threats: An Analytical Study. *African Journal of Biomedical Research*, 2500–2508. <https://doi.org/10.53555/AJBR.v28i1S.6716>
- Kaur, P., Stoltzfus, J. and Yellapu, V., 2018. Descriptive statistics. *International Journal of Academic Medicine*, 4(1), 60. https://doi.org/10.4103/IJAM.IJAM_7_18
- Kaur, R., Gabrijelčič, D., & Klobučar, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*.
<https://doi.org/10.1016/j.inffus.2023.101804>
- Kemp, S., 2024. *Digital 2024: India*. *DataReportal – Global Digital Insights*.
<https://datareportal.com/reports/digital-2024-india> (Accessed: 21 Jul. 2025).

- Kesavardhanan, J., 2022. *Is India Under An Illusion Of Cybersecurity?* DQIndia., Available at: <https://www.dqindia.com/is-india-under-an-illusion-of-cybersecurity/> (Accessed: 8th July 2023).
- Khando, K., Gao, S., Islam, S. M., and Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, 102267. <https://doi.org/10.1016/j.cose.2021.102267>
- Kim, E.B., 2013. Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective*, 22(4), pp.171-179.
- Kivits, R. and Sawang, S., 2021. *Stakeholder Engagement* (pp. 9–17). https://doi.org/10.1007/978-3-030-70428-5_2
- Knapp, K.J., Maurer, C. and Plachkinova, M., 2017. Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education*, 28(2).
- Kumar, A., 2025. Cyber Crime Awareness from the Perspective of Educators: A Conceptual Study. *Seejph*, 26(s2), 4348–4359.
- Kumar, N., 2024. *India 'S Cyber Security Policies and the Road Ahead*. October.
- Kumar, P., Vitak, J., Chetty, M., Clegg, T.L., Yang, J., McNally, B. and Bonsignore, E., 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM conference on interaction design and children* (pp. 67-79).
- Kumari, K., 2024. ETHICAL CONSIDERATIONS IN EDUCATIONAL RESEARCH: SAFEGUARDING PARTICIPANTS AND DATA. *SSRN Electronic Journal*, 5, 6349–6351. <https://doi.org/10.2139/ssrn.4991412>
- Kumbhakar, M.M. and Kumar, N., 2025. Cyber Security Awareness Among Higher

- Education Students. *National Journal of Education*, 23(1), pp.335-349.
- Kwilinski, A. and Trushkina, N., 2024. Impact of Cyber Risks and Threats on the Critical Infrastructure Development: Visualization of Scientific Research. *Proceedings of International Conference on Applied Innovation in IT*, 12(2), 107–119.
- Lasisi, R. O., Menia, M., Farr, Z. and Jones, C., 2022. Exploration of AI-enabled Contents for Undergraduate Cyber Security Programs. *Proceedings of the International Florida Artificial Intelligence Research Society Conference, FLAIRS*. <https://doi.org/10.32473/flairs.v35i.130615>
- Lauricella, A.R., Barr, R. and Calvert, S.L., 2014. Parent–child interactions during traditional and computer storybook reading for children’s comprehension: Implications for electronic storybook design. *International Journal of Child-Computer Interaction*, 2(1), pp.17-25.
- Leat, D. and Higgins, S., 2002. The role of powerful pedagogical strategies in curriculum development. *The Curriculum Journal*, 13(1), 71–85. <https://doi.org/10.1080/09585170110115286>
- Leune, K. and Petrilli, S. J., 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. *Proceedings of the 18th Annual Conference on Information Technology Education*, 47–52. <https://doi.org/10.1145/3125659.3125686>
- Leung, E. and Pluskwik, E., 2018. Effectiveness of gamification activities in a project-based learning classroom. *ASEE Annual Conference and Exposition, Conference Proceedings, 2018-June(April)*. <https://doi.org/10.18260/1-2--30361>
- Levinson, M., 2012. *Are you at risk? What cybercriminals do with your personal data*. CIO. Available at: <https://www.cio.com/article/284563/security0-are-you-at-risk-what-cybercriminals-do-with-your-personal-data.html> (Accessed: 28 Jul. 2025).
- Li, Y. and Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber

- security; Emerging trends and recent developments. *Energy Reports*.
<https://doi.org/10.1016/j.egyr.2021.08.126>
- Luna, R., 2021. Stranger danger!: How hackers break into school databases to steal student data, and what legislatures should do about it. *Texas Tech Law Review*, 54, p.381.
- Madathil, N. T., Abula, W., Alaboolan, S., Almadhaani, M. and Alrabae, S., 2023. PESS: Progress Enhancing Student Support. *2023 International Conference on Smart Applications, Communications and Networking, SmartNets 2023*.
<https://doi.org/10.1109/SmartNets58706.2023.10216155>
- Manzil, H. H. R. and Manohar Naik, S., 2023. Android malware category detection using a novel feature vector-based machine learning model. *Cybersecurity*, 6(1), 6.
<https://doi.org/10.1186/s42400-023-00139-y>
- Martínez-Domínguez, M. and Fierros-González, I., 2022. Determinants of internet use by school-age children: The challenges for Mexico during the COVID-19 pandemic. *Telecommunications Policy*, 46(1), 102241.
<https://doi.org/10.1016/j.telpol.2021.102241>
- MassMediaLink India LLP SecurityLink India, 2024. *Fortinet Annual Skills Gap Report Reveals Growing Connection Between Cybersecurity Breaches and Skills Shortages in India*. Available at: <https://www.securitylinkindia.com/latest/14/fortinet-annual-skills-gap-report-reveals-growing-connection-between-cybersecurity-breaches-and-skills-shortages-in-india/> (Accessed: 11 May 2025).
- Merayo, N. and Ayuso, A., 2023. Analysis of barriers, supports and gender gap in the choice of STEM studies in secondary education. *International Journal of Technology and Design Education*, 33(4), pp.1471-1498.
- Minocha, S., Hristov, D. and Leahy-Harland, S., 2018. Developing a future-ready global workforce: A case study from a leading UK university. *The International Journal of*

- Management Education*, 16(2), 245–255. <https://doi.org/10.1016/j.ijme.2018.03.002>
- Mishra, S., 2024. *Integrating Cybersecurity Education into the Curriculum: Best Practices and Implementation Challenges*.
- Mohanty, S.N., Singh, T., Goel, R., Baral, S.K. and Kumar, R., 2024. A study on building awareness in cyber security for educational system in India using interpretive structural modellings. *International Journal of System Assurance Engineering and Management*, 15(6), 2518–2528. <https://doi.org/10.1007/s13198-024-02273-3>
- Morandini, S., Fraboni, F., De Angelis, M., Puzzo, G., Giusino, D. and Pietrantoni, L., 2023. The Impact of Artificial Intelligence on Workers' Skills: Upskilling and Reskilling in Organisations. *Informing Science: The International Journal of an Emerging Transdiscipline*, 26, 039–068. <https://doi.org/10.28945/5078>
- Mouheb, D., Abbas, S., and Merabti, M., 2019. Cybersecurity Curriculum Design: A Survey. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11345 LNCS(October), 93–107. https://doi.org/10.1007/978-3-662-59351-6_9
- Mukherjee, M., Le, N.T., Chow, Y.W. and Susilo, W., 2024. Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information (Switzerland)*, 15(2). <https://doi.org/10.3390/info15020117>
- Muthuppalaniappan, M. and Stevenson, K., 2021. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, 33(1). <https://doi.org/10.1093/intqhc/mzaa117>
- Nair, S.S. and Meyyappan, P.L., 2024. Reliability analysis of benchmark water distribution system. *Communications - Scientific Letters of the University of Žilina*. <https://doi.org/10.26552/com.C.2024.005>
- Nardelli, E. and Corradini, I., 2019. Informatics Education in School: A Multi-Year Large-

Scale Study on Female Participation and Teachers' Beliefs. In *International Conference on Informatics in Schools: Situation, Evolution, and Perspectives* (pp. 53-67). Cham: Springer International Publishing.

National Association of Criminal Defense Lawyers (NACDL), n.d. *Computer Fraud and Abuse Act (CFAA)*. Available at: <https://www.nacdl.org/Landing/ComputerFraudandAbuseAct> (Accessed: 28 Jul. 2025).

National Cyber Security Centre., 2022. *CyberFirst overview*. National Cyber Security Centre.

National Initiative for Cybersecurity Careers and Studies., 2024. *Cybersecurity for Students*. Available at: <https://niccs.cisa.gov/education-training/cybersecurity-students> (Accessed: 28 Jul. 2025).

National Institute of Standards and Technology (NIST), 2023. *NICE Strategic Plan (2021–2025)*. Available at: <https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan> (Accessed: 28 Jul. 2025).

Nieto, B. F., Romanini, D., and Zhu, Y., 2025. Cybersecurity Education Showdown: A Comparative Analysis of K-12 Education Systems in the United States, the European Union and China. *CEUR Workshop Proceedings*, 3962.

NIST., 2023. NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence. *NIST*.

NIST NICE., 2022. *NICE Cybersecurity Apprenticeship Program Finder*. National Institute of Science and Technology (NIST).

Nunes, C., Oliveira, T., Castelli, M. and Cruz-Jesus, F., 2023. Determinants of academic achievement: How parents and teachers influence high school students' performance. *Heliyon*, 9(2), e13335. <https://doi.org/10.1016/j.heliyon.2023.e13335>

- Nygaard, K., Chowdhury, M., Kambhampaty, K. and Kotala, P., 2018, April. Cybersecurity materials for K-12 education. In *The Midwest Instruction and Computing Symposium 2018*.
- Odo, C., 2024. Strengthening Cybersecurity Resilience: the Importance of Education, Training, and Risk Management. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4779289>
- OECD, 2020. *OECD Digital Economy Outlook 2020*. OECD Publishing, Paris. Available at: https://www.oecd.org/en/publications/oecd-digital-economy-outlook-2020_bb167041-en.html (Accessed: 11 May 2025).
- Ojha, E., and Chattopadhyay, K. N., 2025. CYBERSECURITY EDUCATION AND AWARENESS: A FRAMEWORK-BASED APPROACH FOR DIGITAL LITERACY. *EPRA International Journal of Multidisciplinary Research (IJMR)*, 796–801. <https://doi.org/10.36713/epra22511>
- Okeke, D.C., 2024. *Taxonomies and models of adversarial behavior in cybersecurity: A literature review on motivations, attack vectors, and attribution challenges*. University of Gloucestershire, School of Business, Computing and Social Sciences. Available at: https://www.academia.edu/126909254/AdversaryBehaviour_DarlingtonOkekeCT7074_S (Accessed: 9 Nov. 2025).
- Olmstead, K. and Smith, A., 2017. *Americans and cybersecurity*. Pew Research Center, 26(311-27).
- Onyema, E.M., Edeh, C.D., Gregory, U.S., Edmond, V.U., Charles, A.C. and Richard-Nnabu, N.E., 2021. Cybersecurity awareness among undergraduate students in Enugu Nigeria. *International Journal of Information Security, Privacy and Digital Forensics*, 5(1), pp.34-42.

- Oranga, J. and Matere, A., 2023. Qualitative Research: Essence, Types and Advantages. *OALib*, 10(12), 1–9. <https://doi.org/10.4236/oalib.1111001>
- Otoun, N., Al Maqousi, A., Alauthman, M. and Almomani, A., 2025. Remote Labs in Cybersecurity Education: Analyzing Software Requirements and Challenges. *International Journal of Cloud Applications and Computing*, 15(1), 1–27. <https://doi.org/10.4018/IJCAC.383300>
- Oyewole, A.T., Okoye, C.C., Ofodile, O.C. and Ugochukwu, C.E., 2024. Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, 21(3), 625–643. <https://doi.org/10.30574/wjarr.2024.21.3.0707>
- Padmaja, N., Leela, D., Bharathi, M. and Begam, Y., 2019. Innovative Methods of Effective Teaching and Learning. In *Innovative Teaching Practices for 4G Students* (Issue September). <https://doi.org/10.34256/iorip1914>
- Pal, A., 2022. *Why cybersecurity is education sector's very own Achilles' heel*. Available at: <https://www.financialexpress.com/jobs-career/education-why-cybersecurity-is-education-sectors-very-own-achilles-heel-nbsp-2705368/> (Accessed: 11 May 2025).
- Panjani, H. and Mudgal, A., 2025. A Study of Cyber Safety Awareness among Students and Educational Initiatives. *Indian Journal of Educational Technology*, 7(II), pp.246-256.
- Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar, M.R., Jøsang, A., Pereira, T. and Stavrou, E., 2018. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, 36–54. <https://doi.org/10.1145/3293881.3295778>

- Payne, B.K., He, W., Wang, C., Wittkower, D.E. and Wu, H., 2021. Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course. *Journal of Information Systems Education*, 32(2).
- Pencheva, D., Hallett, J. and Rashid, A., 2020. Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security & Privacy*, 18(2), 68–74. <https://doi.org/10.1109/MSEC.2020.2969409>
- PHDCCI and Grant Thornton Bharat, 2022. *Technology and cyber trends in the Indian education sector*. Available at: <https://www.grantthornton.in/globalassets/1.-member-firms/india/assets/pdfs/technology-and-cyber-trends-in-the-indian-education-sector.pdf> (Accessed: 8th July 2023).
- Pranggono, B. and Arabo, A., 2021. COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, 4(2). <https://doi.org/10.1002/itl2.247>
- Prümmer, J., van Steen, T. and van den Berg, B., 2024. A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585. <https://doi.org/10.1016/j.cose.2023.103585>
- Pusey, P. and Sadara, W.A., 2011. Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, 28(2), pp.82-85.
- Quayyum, F., 2024. Co-designing cybersecurity-related stories with children: Perceptions on cybersecurity risks and parental involvement, *Entertainment Computing* 52 (2025). URL [https://www.sciencedirect.com/science/article/pii S](https://www.sciencedirect.com/science/article/pii/S).
- Quayyum, F., Cruzes, D.S. and Jaccheri, L., 2021. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343. <https://doi.org/10.1016/j.ijcci.2021.100343>
- Rahman, M. J. A., Hamzah, M. I., Yasin, M. H. M., Tahar, M. M., Haron, Z. and Ensima, M.

- N. K. E., 2019. The UKM Students Perception towards Cyber Security. *Creative Education*, 10(12), 2850–2858. <https://doi.org/10.4236/ce.2019.1012211>
- Rahman, N.A.A., Sairi, I.H., Zizi, N.A.M. and Khalid, F., 2020. The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, 10(5), pp.378-382. <https://doi.org/10.18178/ijiet.2020.10.5.1393>
- Raju, R., Abd Rahman, N.H. and Ahmad, A., 2022. Cyber security awareness in using digital platforms among students in a higher learning institution. *Asian Journal of University Education (AJUE)*, 18(3), pp.756-766.
- Rattanabunno, S., Werapun, W., Suaboot, J., Karode, T. and Puongmanee, M., 2023. An EOA Identity Tracing System (AITS) on Ethereum Blockchain. In *2023 8th International Conference on Information and Network Technologies (ICINT)*, pp.61-65. IEEE.
- Rayavaram, P., Jagadeesha, A., Narain, S. and Lee, C. S., 2023. Designing a Visual Cryptography Curriculum for K-12 Education. *SIGCSE 2023 - Proceedings of the 54th ACM Technical Symposium on Computer Science Education*. <https://doi.org/10.1145/3545947.3576266>
- Reginald, G., 2023. Teaching and learning using virtual labs: Investigating the effects on students' self-regulation. *Cogent Education*, 10(1). <https://doi.org/10.1080/2331186X.2023.2172308>
- Reisinger, D., 2016. *Here's how much your Social Security number is worth on the dark web*. Fortune. Available at: <https://fortune.com/2016/08/03/social-security-dark-web/> (Accessed: 21 Jun. 2025).
- Rendón-Macías, M.E., Villasís-Keever, M.Á. and Miranda-Novales, M.G., 2016. Descriptive statistics. *Revista Alergia Mexico*.

<https://doi.org/10.29262/ram.v63i4.230>

- Ricci, J., Breiting, F. and Baggili, I., 2019. Survey results on adults and cybersecurity education. *Education and Information Technologies*, 24(1), pp.231-249.
- Roksa, J. and Kinsley, P., 2019. The Role of Family Support in Facilitating Academic Success of Low-Income Students. *Research in Higher Education*, 60(4), 415–436. <https://doi.org/10.1007/s11162-018-9517-z>
- Saarsar, P., 2018. Exploring the constructivist approach in education: Theory, practice, and implications. *International Journal of Research and Analytical Reviews*, 5(2), pp.716-724.
- Safitra, M.F., Lubis, M. and Fakhurroja, H., 2023. Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, 15(18), p.13369.
- Sağlam, R.B., Miller, V. and Franqueira, V.N., 2023. A Systematic Literature Review on Cyber Security Education for Children. *IEEE Transactions on Education*, 66(3), 274–286. <https://doi.org/10.1109/TE.2022.3231019>
- Santos, H., Pereira, T. and Mendes, I., 2017. Challenges and reflections in designing Cyber security curriculum. *2017 IEEE World Engineering Education Conference (EDUNINE)*, 47–51. <https://doi.org/10.1109/EDUNINE.2017.7918179>
- Saxena, H. and Mittal, A., 2022. *Unprecedented increase in cyber attacks targeting government entities in 2022*. Available at: <https://cloudsek.com/whitepapers-reports/unprecedentedincrease-in-cyber-attacks-targeting-government-entities-in-2022> (Accessed: 11 May 2025).
- Saxena, P., Kotiyal, B. and Goudar, R.H., 2012. A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India. *International Journal of Information and Education Technology*, 2(2).
- Schneider, A., Wagenknecht, A., Sydow, H., Riedlinger, D., Holzinger, F., Figura, A.,

- Deutschbein, J., Reinhold, T., Pigorsch, M., Stasun, U., Schenk, L. and Möckel, M., 2023. Primary and secondary data in emergency medicine health services research – a comparative analysis in a regional research network on multimorbid patients. *BMC Medical Research Methodology*, 23(1), 34. <https://doi.org/10.1186/s12874-023-01855-2>
- Senthilnathan, S., 2019. Usefulness of Correlation Analysis. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3416918>
- Sharma, P. and Gupta, H., 2024. Emerging Cyber Security Threats and Security Applications in Digital Era. 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 1–6. <https://doi.org/10.1109/ICRITO61523.2024.10522181>
- Sharma, S., 2023. *Ensuring Cyber Security in Digital India in the Context of NEP 2020*.
- Shillair, R., Esteve-González, P., Dutton, W.H., Creese, S., Nagyfejeo, E. and von Solms, B., 2022. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 119, 102756. <https://doi.org/10.1016/j.cose.2022.102756>
- Simola, J. and Leppänen, T., 2025. Identification of the Emerging Sources of Cybersecurity Threats. *European Conference on Cyber Warfare and Security*, 24(1), 794–802. <https://doi.org/10.34190/eccws.24.1.3569>
- Singh, K., Chatterjee, S., Mariani, M. and Wamba, S.F., 2025. Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. *Technovation*, 143, 103219. <https://doi.org/10.1016/j.technovation.2025.103219>
- Sridevi, K.V., 2020. Cyber security Awareness among In-service secondary school teachers of Karnataka. *Indian Journal of Educational Technology*, 2(2), 82–94.

- Statista., 2024. *Number of smartphone users in 2024, by country (in millions)*, Available at: <https://www.statista.com/forecasts/1146962/smartphone-user-by-country> (Accessed: 20 July 2025).
- Statti, A. and Torres, K.M., 2020. Digital Literacy: The Need for Technology Integration and Its Impact on Learning and Engagement in Community School Environments. *Peabody Journal of Education*, 95(1), 90–100. <https://doi.org/10.1080/0161956X.2019.1702426>
- Straková, J., Simonová, J. and Greger, D., 2018. Improving mathematics results: does teachers' academic optimism matter? A study of lower secondary schools. *School Effectiveness and School Improvement*, 29(3), 446–463. <https://doi.org/10.1080/09243453.2018.1446449>
- Su, J.M., 2024. WebHOLE: Developing a web-based hands-on learning environment to assist beginners in learning web application security. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-023-12090-z>
- Sunita., 2024. Digital frontlines: Cyber threats and India's national security imperatives. *International Journal of Sociology and Humanities*, 6(2), 229–235. <https://doi.org/10.33545/26648679.2024.v6.i2c.151>
- Švábenský, V., Čeleda, P., Vykopal, J. and Brišáková, S., 2021. Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers and Security*, 102, 1–32. <https://doi.org/10.1016/j.cose.2020.102154>
- Santhosh, T. and Thiyagu, K., 2024. Fostering Responsible Behavior Online- Relevance of Cyber Ethics Education. *Malaysian Online Journal of Educational Technology*, 12(1), 32–38. <https://doi.org/10.52380/mojet.2024.12.1.428>
- Tabe, H.T., 2023. Teacher quality as a defining factor of student academic performance in schools : The case of a district in South Africa. *African Perspectives of Research in*

Teaching and Learning, 7(3), 487–502.

- Taherdoost, H., 2024. A Critical Review on Cybersecurity Awareness Frameworks and Training Models. *Procedia Computer Science*, 235, 1649–1663. <https://doi.org/10.1016/j.procs.2024.04.156>
- Takács, J. M. and Pogátsnik, M., 2024. A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education. *Acta Polytechnica Hungarica*, 21(10 Special Issue), 533–552. <https://doi.org/10.12700/aph.21.10.2024.10.32>
- Taylor, R.W., Fritsch, E.J. and Liederbach, J., 2014. *Digital crime and digital terrorism*. Prentice Hall Press.
- Tchernykh, A., Schwiegelsohn, U., Talbi, E.G. and Babenko, M., 2019. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, 36, 100581. <https://doi.org/10.1016/j.jocs.2016.11.011>
- Teachcyber., 2021. High School Cybersecurity Curriculum Guidelines & Glossary. *Teachcyber*.
- Thakur, M. K., 2023. A Comparative Study of Cybersecurity Laws in India and Other Countries. *Interantional Journal of Scientific Research in Engineering and Management*, 07(04). <https://doi.org/10.55041/IJSREM18920>
- Tierney, A., 2025. *U.S. ratio of cybersecurity positions 2024*.
- Tiwari, P. K., and Dhiman, V., 2025. Integrating Cybersecurity Awareness into Teacher Training Programs: A New Frontier in Educational Policy. *International Journal of Research Publication and Reviews*, 6(5), 6246–6253. <https://doi.org/10.55248/gengpi.6.0525.1781>
- Translators without Borders, 2020. *Language data for India*. Available at:

- <https://translatorswithoutborders.org/language-data-for-india/> (Accessed: 28 Jul. 2025).
- Triplett, W.J., 2023. Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability*, 3(1), 47–67. <https://doi.org/10.53889/ijses.v3i1.132>
- Tsado, L., 2019. Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach. *Journal of Cybersecurity Education, Research and Practice*, 2019(1), p.4.
- Turkanović, M., Welzer, T. and Hölbl, M., 2019, September. An example of a cybersecurity education model. In *2019 29th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE)* (pp. 1-4). IEEE.
- Untawale, T., 2021. Importance of Cyber Security in Digital Era. *International Journal for Research in Applied Science and Engineering Technology*, 9(8), 963–966. <https://doi.org/10.22214/ijraset.2021.37519>
- Vaismoradi, M., Turunen, H. and Bondas, T., 2013. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. In *Nursing and Health Sciences*. <https://doi.org/10.1111/nhs.12048>
- Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boekee, S., Koppen, L., van den Berg, B., de Bos, A. and van der Lubbe, J.C.A., 2015. On (the emergence of) cyber security science and its challenges for cyber security education. In *Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium, Tallinn, Estonia, October 13; 14 2014. Winner of the BEST PAPER AWARD*. NATO Science and Technology Organization.
- Venter, I., Blignaut, R., Renaud, K. and Venter, M., 2019. Cyber Security Education Is as

- Essential as “The Three R’s”. *Heliyon*, 5, e02855 [online]. Available at: <https://doi.org/10.1016/j.heliyon.2019.e02855> (Accessed: 21 July 2025).
- Verizon, 2022. *Data Breach Investigations Report 2022*. Available at: <https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf> (Accessed: 11 May 2025).
- Verma, V. and Pawar, J., 2024. Assessment Of Students Cybersecurity Awareness And Strategies To Safeguard Against Cyber Threats. *Journal of Advanced Zoology*, 82–89. <https://doi.org/10.53555/jaz.v45iS4.4156>
- Vigneswari, T., Pramila, S., Gomathi, M. V, and Madhumitha, M., 2025. Enhancing Cybersecurity in Educational Institutions: Challenges and Strategies. *Eureka Publications, February*, 32.
- Vikasconcept., 2025. *Cybersecurity Education for Middle and High School Students*. Vikasconcept.
- Volante, L., Jerrim, J., Klinger, D.A. and Schnepf, S.V., 2019. Socioeconomic inequality and student outcomes across education systems. In *Socioeconomic inequality and student outcomes: Cross-national trends, policies, and practices* (pp. 3-16). Singapore: Springer Singapore.
- Waldock, K.E., Miller, V., Li, S. and Franqueira, V.N., 2022, February. Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people. *Global Forum on Cyber Expertise*.
- Wilson, E., 2019. *The worrying trend of children’s data being sold on the dark web*. Available at: <https://thenextweb.com/news/children-data-sold-the-dark-web> (Accessed: 21 June 2025).
- World Economic Forum - GCO, 2024. *Global Cybersecurity Outlook 2024*. In collaboration with Accenture. World Economic Forum, Geneva. Available at:

<https://www.weforum.org/publications/global-cybersecurity-outlook-2024/>

(Accessed: 11 May 2025).

World Economic Forum - GRR, 2024. *Global Risks Report 2024*. In collaboration with Marsh McLennan and Zurich Insurance Group. World Economic Forum, Geneva. Available at: <https://www.weforum.org/publications/global-cybersecurity-outlook-2024/> (Accessed: 11 May 2025).

World Population Review, 2025. *Total Population by Country 2025*. Available at: <https://worldpopulationreview.com/countries> (Accessed: 11 May 2025)

Xu, X., 2024. Internationalisation of higher education: What does it mean in the Chinese context?. In *Critical Intercultural Perspectives on Higher Education* (pp. 27–49). Routledge. <https://doi.org/10.4324/9781003567950-3>

Yaacob, M.N., Idrus, S.Z.S. and Idris, M., 2023. Managing Cybersecurity Risks in Emerging Technologies. *International Journal of Business and Technopreneurship (IJBT)*, 13(3), 253–270. <https://doi.org/10.58915/ijbt.v13i3.297>

Yadav, N.. 2024. The Impact of Digital Learning on Education. *International Journal of Multidisciplinary Research in Arts, Science and Technology*, 2(1), 24–34. <https://doi.org/10.61778/ijmrast.v2i1.34>

Yan, Z., Xue, Y. and Lou, Y., 2021. Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior*, 121, p.106791.

Yashwant, L.P., 2021. Need of Cyber Security Education in School. *International Journal of Innovative Research in Technology*, 8(2), pp.199–203.

Zemlyak, S., Gusarova, O. and Khromenkova, G., 2022. Tools for Correlation and Regression Analyses in Estimating a Functional Relationship of Digitalization Factors. *Mathematics*, 10(3), 429. <https://doi.org/10.3390/math10030429>

- Zhadan, A., 2022. *World Economic Forum finds that 95% of cybersecurity incidents occur due to human error*. Cybernews.
- Zhang-Kennedy, L. and Chiasson, S., 2021. A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, 54(1), pp.1-39.
- Zhou, Y., Zhou, Y. and Machtmes, K., 2024. Mixed methods integration strategies used in education: A systematic review. *Methodological Innovations*, 17(1), 41–49. <https://doi.org/10.1177/20597991231217937>
- Zote, H.V.L.N., Roy, T.S. and Longkumer, O., 2023. A Study of Cybersecurity Awareness Among Faculty and Students At Assam Don Bosco University, Guwahati. *International Journal of Creative Research Thoughts (IJCRT)*. Available at: <https://ijcrt.org/papers/IJCRT2302072.pdf> (Accessed: 11 May 2025).
- Zurkarnain, S.M.B. and Abdulsahib, A.A., 2023. Investigating The Correlation between The Five Major Personality Traits and a Student's Online Habits. *Asia-Pacific Journal of Information Technology and Multimedia*, 12(01), 57–69. <https://doi.org/10.17576/apjitm-2023-1201-04>

APPENDIX A: DATASET

[illegible]