Report On

Developing a Cybersecurity Awareness Program: A Qualitative Study Based on Internship Experience at Jamroll Design Studio

By

Arafat Hussain
23164036

An internship report submitted to the BRAC Business School in partial fulfillment of the requirements for the degree of
Master of Business Administration

BRAC Business School
BRAC University
May 2025

Declaration

It is hereby declared that

1. The internship report submitted is my/our own original work while completing degree at BRAC University.
2. The report does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The report does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I/We have acknowledged all main sources of help.

Student's Full Name & Signature:

Arafat Hussain

23164036

Supervisor's Full Name & Signature:

Najmul Hasan

Assistant Professor, BRAC Business School

BRAC University

Letter of Transmittal

Najmul Hasan
Assistant Professor,
BRAC Business School
BRAC University
Kha 224 Pragati Sarani, Merul Badda, Dhaka 1212

Subject: Submission of Internship Report

Dear Sir,

It is with great pleasure that I submit my internship report titled "**Developing a Cybersecurity Awareness Program: A Qualitative Study Based on Internship Experience at Jamroll Design Studio**" completed during my internship tenure from January to May 2025. This report is submitted as partial fulfillment of my MBA degree in Information Technology Management at BRAC University.

The experience at Jamroll Design Studio has been instrumental in shaping my understanding of how cybersecurity awareness integrates with everyday business IT operations. I hope this report meets your expectations and accurately reflects the practical and academic aspects of my work.

Sincerely yours,

Arafat Hussain
23164036
MBA, Information Technology Management
BRAC Business School
BRAC University
Date: 14th May 2025

Non-Disclosure Agreement

This agreement is made and entered into by and between Jamroll and the undersigned student at BRAC University, Arafat Hussain, Student ID: 23164036.

Acknowledgement

I would like to express my deepest gratitude to my academic supervisor and the faculty of BRAC Business School for their continuous support. I am especially thankful to Mr. Najmul Hasan, Assistant Professor at BRAC University, for providing me with the opportunity to intern and supporting my learning process.

My sincere thanks also go to the team at Jamroll Design Studio who supported my work and allowed me to learn from real-life challenges. I also appreciate the valuable insights provided by the individuals I interviewed during my research.

This experience would not have been possible without the guidance of my professors in courses such as MIS, Digital Transformation, Information Security, and Business Intelligence, which laid the groundwork for this report.

Dedication

In the name of Allah, the Most Gracious, the Most Merciful, I express my heartfelt gratitude for the guidance, patience, and strength that sustained me throughout my academic and professional journey.

I dedicate this report to my beloved parents, whose endless support, encouragement, and belief in me have been the driving force behind all my endeavors. Their sacrifices and unwavering faith have shaped who I am today.

I also dedicate this work to Jamroll Design Studio, where I had the privilege to work as a Flutter Developer and simultaneously explore the wider organizational environment, including the critical area of cybersecurity awareness among employees. This internship gave me the unique opportunity to apply my technical skills while also engaging with the human side of digital security — an experience that broadened my understanding and appreciation of IT in a real-world business context.

To my mentors, colleagues, and everyone who contributed to this journey with their time, knowledge, and insights — thank you. This report stands as a reflection of all that I have learned and experienced during this formative phase.

Executive Summary

This report presents the outcomes of a five-month internship at Jamroll Design Studio, where I worked as a Flutter Developer on the "Inkam" mobile application using Flutter and Riverpod. While contributing to the app's development and release on the Play Store, I also conducted a qualitative analysis on employee cybersecurity awareness. Through interviews and observation, I found inconsistencies in staff understanding of security practices, a lack of formal policies, and a general underestimation of cyber risks. These gaps highlighted the need for structured onboarding, ongoing training, and behavioral reinforcement. The internship allowed me to apply academic knowledge in mobile development, cybersecurity, and IT management to a real-world environment. It broadened my perspective on how organizational culture and informal practices impact digital safety. The experience not only sharpened my technical and analytical skills but also underscored the importance of cybersecurity awareness in agile, fast-growing tech firms.

Keywords: Cybersecurity; Information Security Policy; Awareness Program; Employee Behavior; Digital Transformation

Table of Contents

Chapter 1

Overview of Internship

1.1 Student Information

I am Arafat Hussain, enrolled in the program of Master of Business Administration (MBA), I am majoring in Information Technology Management (ITM) from BRAC University. My Student ID is 23164036 and I have my masters back in the semester of Spring 2023. Although I have completed my under-graduation in Computer Science Engineering, that too from BRAC University, I have chosen to go with masters in business to widen my vision.

1.2 Internship Information

1.2.1 Period, Company Name, Department/Division, Address

From January to May 2025, I worked as an intern at Jamroll Design Studio, which is located in H: 654, R: 09, Ave: 04, Mirpur DOHS, Dhaka 1216. I was a member of the Mobile Application Development team in the IT department.

1.2.2 Internship Company Supervisor's Information: Name and Position

Nur Mohammad Kawser, the Lead Frontend Developer at Jamroll Design Studio, monitored my internship. He gave me constant direction and technical mentorship during the internship, which really improved my educational experience. I was able to learn the nuances of app deployment, hone my practical Flutter and Riverpod skills, and acquire knowledge of real-world project management under his guidance. His personable leadership style and eagerness to impart information contributed to the development of a positive learning atmosphere. Additionally, he supported my interest in cybersecurity

awareness and provided insightful criticism when I planned and carried out my qualitative study. In addition to improving my technical skills, his helpful criticism helped me better grasp workplace dynamics and digital accountability in a tech-driven company.

1.2.3 Job Scope – Job Description/Duties/Responsibilities

One of my duties was to work on the "Inkam" mobile application project as a Flutter Developer. For front-end programming and state management, I used Flutter and Riverpod. In March 2025, I helped launch the app to the Google Play Store by working with my teammates on feature design, implementation, and testing. Additionally, I used observations and interviews to perform an independent examination of staff cybersecurity awareness.

1.3 Internship Outcomes

1.3.1 Student’s contribution to the company

I actively participated in the development, debugging, and optimization of the "Inkam" mobile application project, playing a crucial development role. Additionally, I started a qualitative investigation on employees' awareness of cybersecurity and offered unofficial suggestions for enhancing online safety.

1.3.2 Benefits to the student

Through this internship, I was able to learn about the end-to-end mobile app deployment process, expand my understanding of corporate cybersecurity policies, and obtain hands-on experience with Flutter development utilizing Riverpod. My ability to communicate and think critically was also improved.

1.3.3 Problems/Difficulties (faced during the internship period)

One major challenge was the eventual removal of the app from the Play Store due to internal organizational issues. I also faced limitations in accessing formal cybersecurity documentation and observed varied levels of awareness among employees.

1.3.4 Recommendations (to the company on future internships)

I recommend Jamroll Design Studio to put in place an organized, ongoing cybersecurity awareness program that is suited to the requirements of its technical and creative staff. Mandatory onboarding seminars that thoroughly explain appropriate usage guidelines, digital safety procedures, and typical cyberthreat examples should be part of this. These trainings will guarantee that all staff members, irrespective of their technical expertise, begin with a solid foundation in cybersecurity. The business should also update and disseminate digital policy documents on a regular basis to take into account new threats and technological advancements. Jamroll will be able to maintain innovation while upholding operational security if it continues to invest in mobile development infrastructure, which includes safe coding techniques and deployment methods. When taken as a whole, these initiatives will support a robust corporate culture that honors innovation and conformity.

Chapter 2

Organization Part

2.1 Introduction, Objectives, Scope, Methodology, Significance, Limitations

This chapter provides an in-depth overview of Jamroll Design Studio and places the internship in the context of the company. This chapter's goal is to analyze the business's managerial, financial, marketing, and operational procedures while relating them to the internship's results. This analysis's scope encompasses a number of internal factors, such as the organization's structure, management style, human capital, marketing channels, financial and accounting procedures, and information system utilization. This section's methodology is based on observations, casual conversations with staff members and managers, and hands-on involvement in projects. This chapter is important because it provides insights into actual organizational dynamics by bridging the gap between theoretical academic learning and real-world workplace exposure. A notable limitation was the lack of access to detailed financial reports and formal documentation related to cybersecurity policies, which restricted the depth of certain analyses.

2.2 Overview of the Company

Based in Dhaka, Bangladesh, Jamroll Limited is a private design company committed to assisting businesses, nonprofits, and startups in creating and growing digital products that have a good impact. The studio focuses on digital strategy, branding, web development, and UI/UX design. With design sprints that give user research, prototyping, and testing top priority, Jamroll thrives on the Human-Centered Design (HCD) ethos. With a robust portfolio spanning education, public health, financial technology, sustainable fashion, and

other areas, the company serves both startups and major enterprises. Every solution they provide fosters trust, creativity, and innovation thanks to their nimble structure and collaborative culture.

2.3 Management Practices

The management style of Jamroll Design Studio is casual and engaging. Flexible working arrangements and employee input are encouraged by the leadership. Instead of using regular HR procedures, skill assessments and portfolio reviews are used for recruitment and selection. Although the company does not have a structured incentive structure, compensation is competitive in the industry. Instead of formal learning programs, on-the-job training and mentoring are the main ways that employees are developed. Peer reviews and the accomplishment of project milestones serve as the foundation for informal performance reviews. These procedures are indicative of a startup-like atmosphere that encourages innovation but may impede risk reduction and scalability.

2.4 Marketing Practices

In addition to client referrals and Behance portfolio exposure, Jamroll has collaborated with globally recognized brands and nonprofits, including Yunus Environment Hub, Powwater, Trust Axiata Pay (TAP), and Give2Asia. These collaborations serve as organic marketing drivers. Despite strong project output, Jamroll does not yet employ structured SEO, paid ads, or targeted content strategies—limiting proactive lead generation.

2.5 Financial Performance and Accounting Practices

A low degree of financial transparency is maintained by Jamroll Design Studio due to its size and status as a privately held company. The company manages daily transactions with

software like QuickBooks and adheres to accrual accounting rules. The straight-line approach is used to compute depreciation. The general accounting cycle is kept up to date, although the public can only examine a small portion of the documents. Comprehensive financial analysis is hampered by the lack of formal disclosures and audited financial statements. This implies that stronger financial management and reporting procedures must be put in place, especially if the business wants to grow or draw in investment.

2.6 Operations Management and Information System Practices

Depending on the project, Jamroll uses a contemporary technology stack that includes serverless architecture, Vue.js, Next.js, Flutter, Node.js, Express.js, and MongoDB. User research, wireframing, prototyping, user testing, and delivery are all intricate steps in their process. The workflow is enhanced by platforms such as Notion, GitHub, and Airtable, each of which is designed for optimal user experience. However, formalization of QA and cybersecurity awareness are still lacking.

2.7 Industry and Competitive Analysis

The digital services industry in Bangladesh is highly competitive, with low barriers to entry and rapid technological change. Porter's Five Forces study indicates that the availability of digital technologies makes the danger of new competitors moderate. Because there are numerous service providers available to clients, buyer power is still strong. Because there are too many independent contractors and talented developers, supplier power is low. Substitutes provide a small but increasing hazard as automation techniques advance. There is fierce competition in the industry, especially in the design and development sector. According to a SWOT analysis, Jamroll's responsive workforce and design expertise are its strongest points, but its unstructured procedures and poor internet marketing are its

weaknesses. Threats include cyber dangers and rivalry from more established organizations, while opportunities include the growing need for digital transformation.

2.8 Summary and Conclusions

In conclusion, Jamroll Design Studio functions well in a very adaptable and imaginative manner, exhibiting noteworthy prowess in project management and teamwork. The lack of established procedures in marketing, cybersecurity, and financial reporting, however, presents difficulties for the business. Its ability to grow may be constrained by these gaps, which also leave it open to security risks and operational inefficiencies. Although innovation is encouraged by the company's casual attitude, formalizing important procedures would improve risk management and promote sustainable growth.

2.9 Recommendations/Implications

Jamroll Design Studio should apply standard operating procedures (SOPs) in all departments, especially in cybersecurity, onboarding, and quality assurance, to improve its internal resilience and competitive posture. Funds should be set aside for organized staff training courses that emphasize both behavioral and technical skills. To increase brand awareness, the business should also spend money on SEO tactics, digital marketing tools, and content-driven interaction. Lastly, in order to facilitate future investment opportunities, scalability, and transparency, financial procedures should be codified.

Chapter 3

Project Part

3.1 Introduction

Cybersecurity has progressively grown as a serious managerial concern for organizations of all sizes, especially in the age of digital transformation. Small and Medium size Enterprises (SMEs) continue to be especially vulnerable, even though large firms frequently possess the resources necessary to put in place thorough security procedures. Under the government's "Digital Bangladesh" strategy, the ICT sector in Bangladesh is growing quickly, and SMEs in this country confront particular difficulties in safeguarding digital assets, customer data, and intellectual property. Their exposure to cyber dangers is made worse by a combination of low staff awareness, budgetary restrictions, and a lack of formalized cybersecurity policies.

Jamroll Design Studio, a Dhaka-based creative IT company, exhibits this issue. Despite handling sensitive client data and providing live digital apps, the organization lacks formal cybersecurity onboarding or ongoing training methods. Employees frequently learn informally through peer mentoring or own initiative, resulting in variances in practices like password management, phishing detection, and device safety. This organizational setting shows the interaction of technology infrastructure and human behavior, emphasizing the need for a cultural shift in how cybersecurity is perceived and implemented in SMEs.

The project I worked on during my internship addresses these shortcomings by conducting a qualitative survey of Jamroll workers' cybersecurity awareness. Through interviews and observations, the study investigates the behavioral patterns, perceptual gaps, and cultural dynamics that impact employee attitudes about digital safety. The final goal is to present a

framework for a structured, context-specific cybersecurity awareness program that is manageable for resource-constrained organizations while adhering to worldwide best practices.

3.1.1 Background and Problem Statement

Globally, cybersecurity breaches are increasing at an alarming rate. According to IBM's 2024 Cost of a Data Breach Report, the global average cost of a breach was USD 4.45 million, with SMEs frequently facing disproportionate consequences due to their limited recovery capabilities. In Bangladesh, the Bangladesh Computer Council (BCC) recorded a 35% increase in cyber incidents in 2024, with many of them targeting small businesses without strong defense measures. Despite these threats, the majority of SMEs still view cybersecurity as an afterthought, frequently underestimating the likelihood or severity of assaults. Bangladesh was also top six destinations face the threat of DDoS attacks in the APAC region according to the report published by CTI Unit of BGD e-GOV CIRT in 2022. The CTI Unit of BGD e-GOV CIRT identified 602 exploited vulnerabilities from global feeds over the year, impacting an average of 905 IP addresses per day in Bangladesh, underscoring the extensive prevalence of unpatched systems as of 2024.

Top DDoS prone countries in APAC, 2022	
Country	**Percentage**
South Korea	81.46%
China	14.44%
Australia	0.91%
Singapore	0.73%
Hongkong	0.68%
Bangladesh	0.41%

Jamroll's start-up mentality exacerbates these challenges. Despite being very innovative and flexible, the lack of explicit standards and specific security training has resulted in uneven behaviour among staff. While some people adopt security procedures based on existing knowledge, others rely on shortcuts or outmoded approaches, hence raising risks. During my internship, I noticed password sharing, the installation of untested software, and sporadic system updates.

The problem statement is so formulated as follows: Jamroll Design Studio lacks a defined cybersecurity awareness and training framework, leading to uneven staff practices, poor risk perception, and increased vulnerability to cyber threats.

3.1.2 Objectives

The project aims to achieve the following objectives:

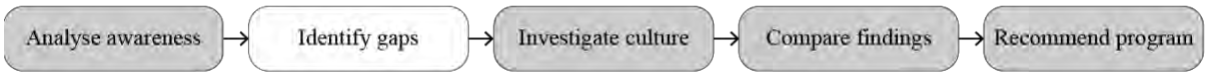
1. To analyze Jamroll workers' current cybersecurity awareness levels.

2. To uncover behavioral and perceptual gaps that affect digital safety behaviors.

3. To investigate how company culture influences cybersecurity behaviors in a creative IT context.

4. To compare findings to existing national and international research on SME cybersecurity awareness.

5. To recommend a planned, realistic, and scalable awareness program for Bangladesh's SMEs.



3.1.3 Significance

The value of this study stems from its twin contributions. Academically, it contributes to the literature on cybersecurity by contextualizing awareness difficulties among SMEs in Bangladesh, a relatively underexplored area. In practice, it gives Jamroll Design Studio with actionable insights regarding its organizational vulnerabilities and a road map for executing low-cost, behaviorally based treatments.

Furthermore, the study is consistent with the national Digital Bangladesh strategy, emphasizing the importance of secure digital practices in ICT-led development. By addressing human-centric aspects of cybersecurity, the initiative helps to build a cyber-aware workforce capable of protecting organizational resilience, client trust, and national digital assets.

3.1.4 Scope of the Study

This project's scope is purposely narrow to allow for in-depth analysis. It focuses on:

Employee attitudes, habits, and informal learning techniques about cybersecurity.

Internal organizational culture and its impact on risk perception.

Gaps in policy communication and onboarding procedures.

The study specifically excludes:

Technical infrastructure audits (such as penetration testing).

Client-side security practices.

Risk assessments are conducted for vendors and other parties.

This breadth assures practicality within the internship duration while also providing valuable insights for SMEs.

3.2 Literature Review

Existing literature consistently reinforces the central role of human factors in cybersecurity. While firewalls, encryption, and intrusion detection systems are necessary, their effectiveness diminishes if employees remain unaware of or indifferent to secure practices. Herath and Rao (2009) argue that employee non-compliance is one of the greatest risks to organizational security. Behaviors such as password reuse, delayed software updates, and susceptibility to phishing attacks are often rooted in convenience-seeking or lack of knowledge. More recent studies by Ifinedo (2023) show that awareness interventions significantly improve compliance, but only when reinforced regularly. This highlights that awareness must be treated as an ongoing process rather than a one-off event.

Small and medium-sized enterprises (SMEs) face particular constraints compared to large corporations. Abukari and Bankas (2022) found that SMEs in developing economies often

lack budgets for security specialists, relying instead on generalist IT staff. This leads to uneven enforcement of security protocols and weakens resilience against attacks. In Bangladesh, Azad et al. (2025) documented low awareness among digitally active youth, suggesting that workplace training cannot be assumed based on digital literacy alone. Furthermore, studies show that SME employees often underestimate risks, assuming hackers target only larger organizations, which further reduces vigilance.

Training has been identified as a crucial but underdeveloped element of cybersecurity practice. Oroni et al. (2025) emphasized that policy enforcement alone is insufficient; employees must be engaged through dynamic awareness programs. Gamified training platforms such as CyberSAFE have demonstrated positive outcomes by making learning interactive and memorable. Puhakainen and Siponen (2010) argue that embedding training into organizational culture, rather than treating it as a compliance checkbox, ensures longer-term behavioral change. Gamification has also been linked to higher retention of concepts in younger demographics, making it particularly relevant for creative IT SMEs that employ large numbers of recent graduates.

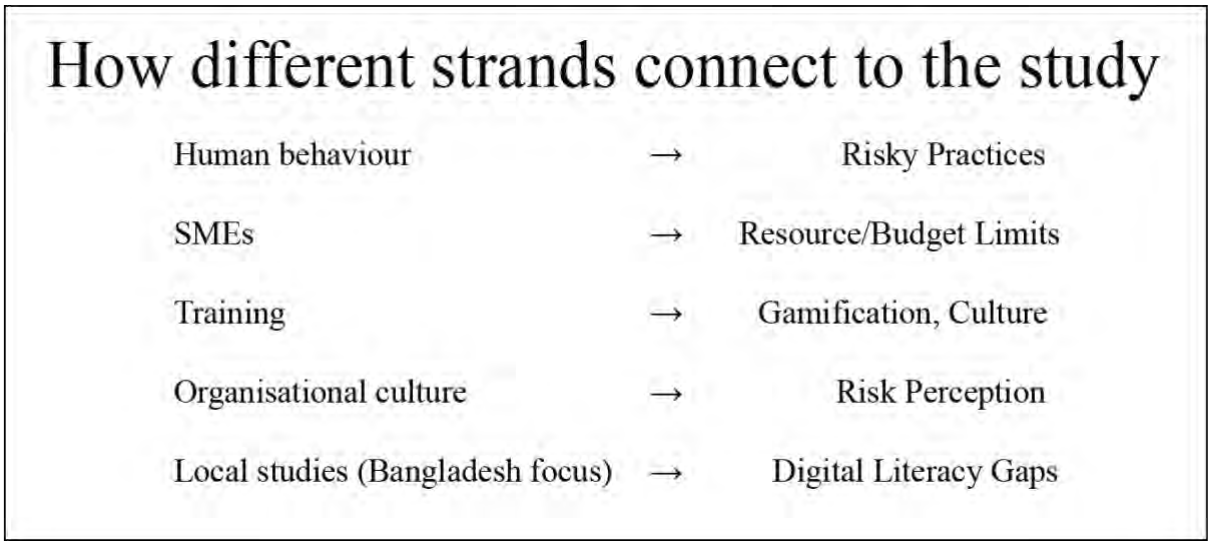
Organizational culture strongly influences employee security behavior. A relaxed workplace that prioritizes innovation and rapid delivery may inadvertently downplay security protocols. Romke (2025) noted that Bangladesh's uneven national cybersecurity infrastructure is mirrored in its SMEs, where informal learning often substitutes for structured awareness initiatives. This cultural dimension affects how seriously employees perceive risks. Studies in educational contexts show that experiential learning, such as directly encountering minor cyber incidents, often heightens risk perception and encourages proactive adoption of security measures.

Recent localized research provides further evidence of gaps in cybersecurity awareness. A large-scale study of Bangladeshi women across high school, university, and professional groups (n=1,202) revealed that exposure to cyber threats is not solely linked to lack of knowledge but also behavioral tendencies and situational vulnerabilities, stated by Islam et al. (2023). Findings showed frequent use of weak passwords, poor incident reporting habits, and inconsistent malware detection practices. Crucially, the study highlighted that women often underestimated risks, assumed they were unlikely targets, and displayed hesitation in acting upon security warnings. Such insights underline the importance of contextualizing training by demographic factors such as gender, education, and professional background.

Complementary evidence comes from Hasan et al. (2025), who examined cybersecurity awareness among university students in Bangladesh. Their data-driven approach revealed inconsistent practices in password management, browser security, and social media use. For example, while many students acknowledged the importance of password complexity, a large proportion admitted to reusing passwords or neglecting two-factor authentication. The study also showed that more than half of respondents had beginner-level computer skills despite being active digital users, illustrating that exposure to technology does not automatically translate to secure practices. These results reinforce the idea that awareness campaigns must be tailored, not generic, and should focus on application of knowledge rather than just information delivery.

Other empirical evidence indicates that Bangladesh remains highly vulnerable to cyber threats due to systemic and cultural shortcomings. Studies note that phishing, malware, and spam remain among the country's most pressing threats, with Bangladesh ranked 18th globally as a spam source. Weak organizational responses and lack of enforcement of cyber

laws exacerbate these issues, as demonstrated by incidents such as the Bangladesh Bank heist and the mass data leak from the Birth and Death Registration Information System. These failures reveal that awareness initiatives must be embedded within stronger institutional frameworks to create a sustainable culture of security.



What emerges from the literature is a set of consistent themes. First, human behavior is central to cybersecurity outcomes, with non-compliance and risky decision-making posing major threats even in technologically equipped environments. Second, SMEs and developing country contexts, such as Bangladesh, face unique challenges of limited resources, uneven training, and informal learning cultures. Third, demographic dimensions such as gender, age, and skill levels further shape awareness and vulnerability. Finally, while awareness campaigns are expanding, gaps remain in ensuring that training translates into long-term secure practices. This study therefore fills an important gap by contextualizing awareness challenges in a creative IT SME in Bangladesh, where design, innovation, and rapid delivery often overshadow formal security planning.

3.3 Methodology

This study adopted a qualitative research design; a methodological choice well aligned with the exploratory objectives of the project. Since the aim was to understand how employees at Jamroll Design Studio perceive, learn, and practice cybersecurity, a qualitative approach allowed for an in-depth exploration of behaviors, attitudes, and cultural influences that cannot be easily captured through numerical data alone. Unlike quantitative surveys that priorities breadth of responses, qualitative inquiry emphasizes depth and richness of information, thereby providing valuable insights into the lived experiences of participants within their organizational context.

Data collection was carried out using two complementary methods: semi-structured interviews and direct observations. The semi-structured interviews were conducted with six employees drawn from both the IT and design departments, ensuring representation across diverse functional roles and levels of seniority. Participants included junior developers, mid-level designers, and senior technical staff. This diversity allowed the study to capture perspectives from individuals with varying levels of exposure to cybersecurity issues. The interview guide consisted of open-ended questions covering themes such as awareness of company policies, daily digital practices, incident response behaviors, and perceptions of cyber risks. The semi-structured format provided flexibility, enabling probing questions and follow-ups based on participants' responses, which ensured richer and more nuanced data.

Direct observation was employed to complement the interviews and reduce the risk of self-reporting bias. Over the course of the internship, everyday practices were carefully noted, particularly in relation to device use, password management, software installation, and methods of information sharing. Observational data revealed discrepancies between what

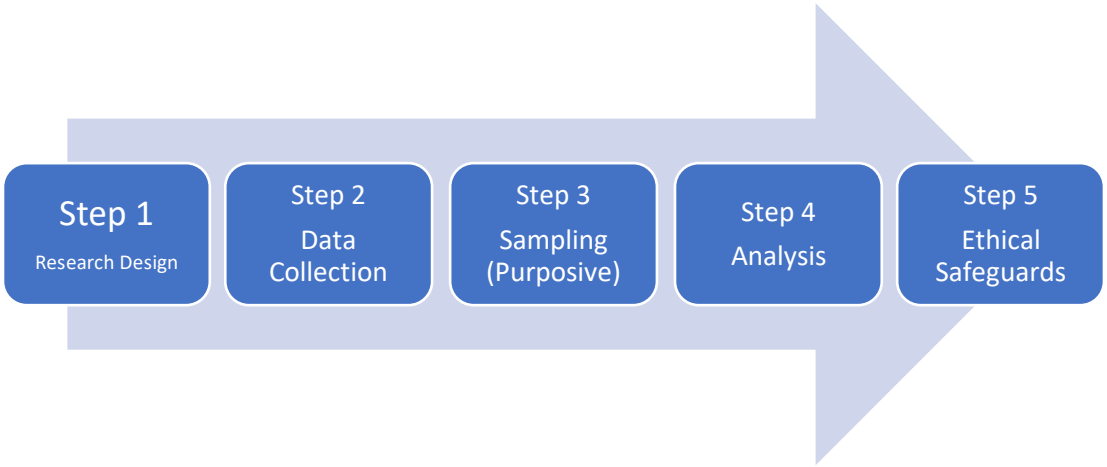
participants reported and what was actually practiced, thereby strengthening the validity of the findings. For instance, while several employees expressed confidence in their ability to identify phishing attempts, observations revealed instances where suspicious links were not scrutinized or flagged.

Purposive sampling was applied to select participants most relevant to the research objectives. This non-probability sampling technique was considered appropriate because the focus was not on generalizing results to all employees but on generating insights from those directly engaged with digital tools and client data. Although the sample size of six may appear limited, qualitative research prioritizes depth over breadth, and the concept of *thematic saturation*—the point at which no new themes emerge—was considered sufficient to validate the sample size.

The collected data were analyzed using thematic coding, a systematic process of categorizing qualitative responses into meaningful themes. Initial codes such as "policy awareness," "risky behavior," and "cultural attitudes" were generated from the raw data. These were gradually refined into higher-level categories that reflected broader organizational patterns. Manual coding was performed due to the small dataset, ensuring close engagement with the material. However, it is worth noting that in larger studies, software such as NVivo or Atlas.ti could be utilized to enhance efficiency and reliability. The coding process allowed for both convergence and divergence of themes, highlighting not only the dominant practices but also the inconsistencies across different employee groups.

Ethical considerations were carefully observed throughout the research process. All participants were informed in advance about the study’s objectives, the voluntary nature of

their involvement, and the measures taken to protect their confidentiality. Informed consent was obtained verbally before interviews commenced. To ensure anonymity, no personal identifiers were recorded in transcripts, and findings are presented in aggregated form. All data were securely stored on password-protected devices and used strictly for academic purposes in line with the ethical standards of BRAC University.



Overall, the chosen methodology enabled a comprehensive exploration of cybersecurity awareness within Jamroll Design Studio. The combination of interviews and observations provided triangulation of data sources, thereby enhancing the reliability of the findings. By situating individual practices within the wider organizational culture, the methodology effectively captured the behavioral, perceptual, and structural dimensions of cybersecurity awareness in a small but dynamic SME environment.

3.4 Findings and Analysis

The findings of this study are based on both semi-structured interviews and direct observations conducted during the internship at Jamroll Design Studio. The results reveal significant discrepancies in employee knowledge, behaviors, and perceptions of cybersecurity, underscoring the role of organizational culture in shaping digital safety practices. Four central themes emerged from the analysis: awareness gaps, behavioral insights, organizational culture, and risk perception.

3.4.1 Awareness Gaps

Employees demonstrated uneven levels of awareness regarding cybersecurity practices. While most participants were able to identify basic external threats such as phishing emails, malware, or suspicious attachments, their knowledge of formal organizational procedures was limited. For example, several employees reported uncertainty about the process of escalating incidents to supervisors or IT leads. One employee candidly stated, *"I know I should not click suspicious links, but I don't remember any formal rules about reporting such incidents."* This highlights a disconnect between individual knowledge of common threats and structured organizational response mechanisms.

The absence of a formal onboarding program or documented security guidelines further amplified these gaps. Instead, employees often relied on verbal instructions from peers, which resulted in inconsistent practices across teams. Some individuals assumed that "common sense" was sufficient for secure digital behavior, while others admitted they were not sure whether certain actions, such as downloading external tools, were permitted. This reliance on informal, unverified knowledge created confusion and left employees vulnerable to social engineering attacks. In the absence of clear policy communication, the

workforce struggled to maintain a unified approach to cybersecurity, increasing the organization's exposure to both external and insider risks.

Practice Observed	Count (out of 6)	% of Employees
Reused weak passwords	4	67%
Ignored system/software updates	3	50%
Installed unverified plugins/apps	2	33%
Used personal email for file sharing	2	33%
Used password manager / 2FA	1	17%

3.4.2 Behavioral Insights

Direct observations revealed multiple risky behaviors that contradicted best practices for digital safety. Common habits included downloading and installing unverified plugins from unofficial sources, postponing or ignoring regular system updates, and reusing simple passwords across multiple accounts. These practices not only increased the likelihood of malware infection but also heightened vulnerability to credential theft. In one instance, employees were found sharing files over personal email accounts or messaging platforms instead of secured channels, inadvertently exposing sensitive client data.

Although a minority of staff exhibited stronger practices, such as adopting password managers or enabling two-factor authentication (2FA), these individuals were exceptions rather than the norm. Interestingly, those who followed secure practices often did so out of personal interest or prior experience, rather than due to any organizational requirement. This finding mirrors the arguments of Herath and Rao (2009), who suggest that secure behavior in many organizations relies heavily on individual initiative in the absence of institutional enforcement mechanisms. The inconsistency in behaviors across the team points to a lack of systematic reinforcement of security practices. Without structured training or regular audits, employees tended to prioritize convenience and efficiency over security, a trend also echoed in global SME contexts.

3.4.3 Organizational Culture

Jamroll's organizational culture plays a critical role in shaping cybersecurity behaviors. The company's flat hierarchy, emphasis on collaboration, and informal learning environment foster innovation and creativity but simultaneously weaken the enforcement of security standards. New employees, for instance, often received little to no formal cybersecurity orientation. Instead, they were introduced to organizational practices through ad-hoc conversations with colleagues or by observing existing habits. This peer-dependent learning process reinforced inconsistencies and normalized risky behaviors.

While the culture promotes openness and flexibility, it inadvertently deprioritizes compliance and risk management. Employees viewed cybersecurity as peripheral to their creative and technical responsibilities, often considering it a "secondary concern." In the absence of accountability mechanisms such as performance metrics or periodic policy reviews, many employees continued to overlook security guidelines even when they were aware of them. This aligns with Romke's (2025) assertion that informal, innovation-driven

work cultures often deprioritize cybersecurity in favor of rapid delivery and experimentation. Such cultural attitudes make it difficult to sustain long-term behavioral change, especially when security is not seen as integral to the organization's success.

3.4.4 Risk Perception

A recurring theme in the interviews was the belief that small organizations like Jamroll are unlikely to be targeted by cybercriminals. One respondent openly remarked, *"Why would hackers come after us? We are small compared to banks or telecoms."* This sense of complacency is a significant risk factor, as research demonstrates that SMEs are frequently targeted precisely because of their weaker security postures (Abukari & Bankas, 2022). Such perceptions can lead to underinvestment in security measures and a tendency to dismiss potential threats as irrelevant.

Interestingly, risk perception varied noticeably among employees who had personally encountered cyber incidents. Those who had experienced data loss, unauthorized account access, or malware infections in the past demonstrated heightened awareness and were more cautious in their practices. For example, one participant explained how losing important project files in a past incident had prompted them to regularly back up data and verify suspicious emails more carefully. This suggests that experiential learning plays a powerful role in shaping cybersecurity behavior, reinforcing the importance of incident-based training or simulation exercises in awareness programs.

Collectively, the findings illustrate a misalignment between employee awareness, behaviors, and perceptions at Jamroll Design Studio. The lack of formal structures, combined with complacent attitudes and an overreliance on peer-driven learning, creates vulnerabilities that could have serious implications for both the organization and its clients.

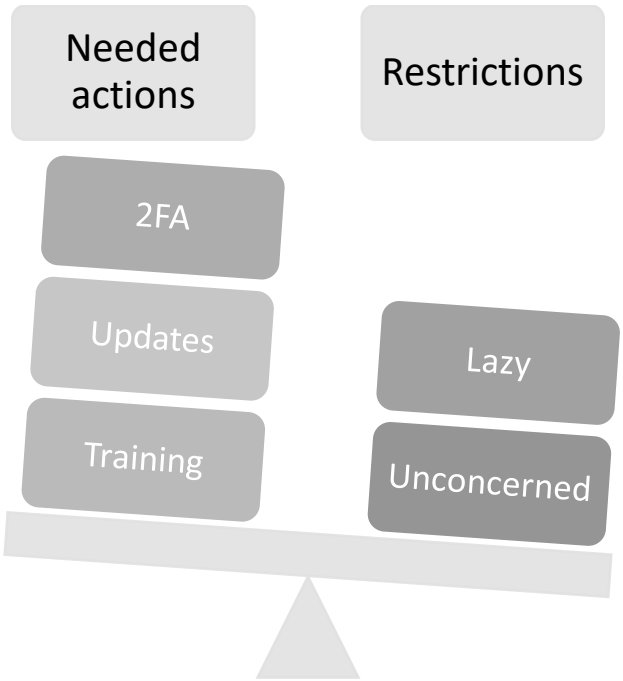
Theme	Key Observations from Interviews/Observation	Example Quote/Behavior
Awareness Gaps	Limited knowledge of reporting process; reliance on informal peer learning	"I know I should not click links, but I don't recall rules for reporting."
Risky Behaviors	Password reuse, ignoring updates, use of unverified plugins	Observed employees downloading free design plugins without IT approval
Organizational Culture	Flat structure, no formal onboarding, reliance on ad-hoc advice	New hires said they learned practices from colleagues, not training
Risk Perception	Employees assume SMEs are not hacker targets; vigilance only after incidents	"Why would hackers come after us? We're small compared to banks."

3.5 Summary and Conclusions

The findings of this study demonstrate that Jamroll Design Studio's cybersecurity challenges are rooted more in human and cultural shortcomings than in technological deficiencies. While the company employs modern development tools and has capable staff, its lack of structured policies, consistent training, and a cyber-aware culture weakens its overall security posture. The analysis revealed clear awareness gaps, with employees uncertain about formal reporting mechanisms and often dependent on peer-driven learning rather than official guidance. Behavioral insights further highlighted risky practices, such

as installing unverified plugins, postponing updates, and reusing weak passwords, which collectively heighten the likelihood of breaches.

Organizational culture emerged as a double-edged sword: the flat hierarchy and informal learning environment fostered creativity and flexibility, yet simultaneously hindered enforcement of security standards. The absence of formal onboarding or refresher training left new hires particularly vulnerable. Risk perception was another critical concern. Many employees assumed that small organizations were unlikely targets for cyberattacks, a misconception that is both dangerous and widespread in SMEs. Interestingly, those who had personally experienced cyber incidents showed higher levels of caution, suggesting that experiential learning plays a pivotal role in shaping attitudes toward digital safety.



Taken together, these findings mirror broader trends across SMEs in Bangladesh, where limited resources, informal knowledge-sharing, and complacency about cyber threats dominate workplace practices. The study therefore concludes that creating a secure digital environment in such contexts requires more than technical tools; it requires behavioral

interventions that reshape attitudes, embed secure habits into everyday practices, and make cybersecurity an organizational priority. For Jamroll, as with other SMEs, building a cyber-conscious workplace will involve sustained investment in both human capital and policy frameworks. Effective cybersecurity must be affordable, practical, and culturally embedded, ensuring that awareness translates into consistent, secure action across the workforce.

3.6 Recommendations/Implications

Based on the findings, several recommendations can be made to strengthen Jamroll Design Studio's cybersecurity posture and provide broader implications for SMEs in similar contexts. The first step is to address awareness and behavior at the individual level. Employees should be provided with mandatory onboarding modules that introduce core cybersecurity concepts such as password hygiene, phishing awareness, and safe data-handling practices. These training sessions should not be limited to one-time events but reinforced regularly through reminders, refreshers, and updates. Providing access to simple tools, such as password managers, and encouraging the adoption of multi-factor authentication will further reduce reliance on insecure practices.

At the organizational level, Jamroll must formalize its approach to cybersecurity by developing a written policy that is easily accessible and clearly communicated to all employees. This should outline expectations for secure behavior, reporting mechanisms, and the consequences of non-compliance. Training initiatives should move beyond lectures to interactive formats such as case studies, role-play simulations, and gamified quizzes, which have been shown to increase engagement and retention. Quarterly workshops can be introduced to ensure that knowledge is consistently refreshed and adapted to new threats. Additionally, the company could appoint cybersecurity "champions" within teams,

individuals tasked with promoting good practices and supporting peers. This peer-driven reinforcement would complement formal policies by embedding security into daily routines. Regular integration of policy reminders into team meetings, Slack channels, or Notion dashboards would further normalize discussions of digital safety, creating a culture of accountability and vigilance.

Beyond the boundaries of the organization, SMEs like Jamroll should seek to leverage national and industry-level initiatives. The Bangladesh Computer Council (BCC) and other government bodies frequently run training programs that can provide cost-effective resources for small companies. Participation in such programs would allow Jamroll to benefit from expert-led guidance without bearing the full financial burden. Industry associations, too, could play a critical role by developing shared cybersecurity awareness resources tailored to SMEs, enabling smaller firms to adopt best practices collectively. By tapping into these broader initiatives, Jamroll could strengthen its resilience while contributing to a wider culture of cybersecurity in the Bangladeshi SME ecosystem.

The long-term implications of implementing these measures are significant. Moving from a reactive to a proactive cybersecurity stance will not only protect Jamroll's internal operations but also enhance client confidence and trust. In an industry where data protection is paramount, demonstrating strong security practices could become a competitive advantage, attracting clients who prioritize safe handling of their digital assets. Proactive awareness initiatives would also reduce reputational and financial risks associated with breaches, which can be devastating for SMEs. More broadly, aligning the organization's practices with international frameworks such as ISO 27001 or the NIST Cybersecurity Framework would position Jamroll as a forward-looking SME, capable of balancing innovation with responsibility.

Recommendation	Practical Action	Expected Impact
Onboarding	Training module	Improved awareness
Policy	Written guidelines	Consistency
National programs	BCC initiatives	SME resilience

In conclusion, the recommendations offered here are not merely technical fixes but strategic steps toward cultural transformation. For Jamroll, adopting them will mean embedding cybersecurity into the fabric of everyday operations. For the SME sector in Bangladesh more generally, these insights emphasize that affordable, engaging, and culturally embedded interventions are essential for creating digitally resilient organizations in an era of escalating cyber threats.

References

[1] Azad, R. U., Tasmim, S., & Atikuzzaman, M. (2025). Investigating students' awareness of online privacy and cybersecurity: An empirical study with effective cybersecurity training framework. *Global Knowledge, Memory and Communication*. https://doi.org/10.1108/GKMC-01-2025-0013

[2] Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Enhancing cyber safety in e-learning environments through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis. *Computers & Security, 150*, 104276. https://doi.org/10.1016/j.cose.2024.104276

[3] Romke, R. A. (2025). Navigating the socio-economic impact of Digital Bangladesh: An overview. *International Journal of Research and Scientific Innovation (IJRSI)*. https://doi.org/10.51244/IJRSI.2025.12030004

[4] Hasan, M., Sampa, M. A., & Mahmud, M. K. (2025). Understanding cybersecurity awareness among students in Bangladesh: A data-driven approach. Society & Sustainability, 7(1), 67–76. Research & Innovation Initiative Inc. https://doi.org/10.38157/ss.v7i1.682

[5] Islam, S., Chowdhury, S., Shamsi, A., & Rahman, M. (2023). Cybersecurity awareness of Bangladeshi women in the digital era: An empirical study. International Journal of Computer Science and Engineering (CSE), 11(2), 45–61. https://doi.org/10.5281/zenodo.8101432

Appendix A. Sample Interview Questions

1. Are you aware of the company's cybersecurity policies?
2. What practices do you follow to protect your devices?
3. Have you received any training regarding information security?
4. Do you understand the consequences of not following policy guidelines?
5. What would make you more interested in learning about cybersecurity?