CYBERSECURITY FOR SMES IN BANGLADESH: REVIEW OF ATTACK AND AWARENESS STRATEGY

By
Tasnim Binte Zahir
20304022

A thesis submitted to the department of BRAC Business School in partial fulfillment of the requirements for the degree of Bachelor of business administration

Bachelor of Business Administration
BRAC University

24th December, 2023

Declaration

It is hereby declared that

1. The thesis submitted is my own original work while completing degree at Brac University.
2. The thesis 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 thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I have acknowledged all main sources of help.

Student's full name and signature:

Tasnim Binte Zahir
20304022

Approval:

The thesis titled "**CYBERSECURITY FOR SMES IN BANGLADESH: AN INTEGRATIVE REVIEW OF CYBER ATTACK AND AWARENESS STRATEGY"** submitted by Tasnim Binte Zahir (20304022) of [Fall semester], [2023] has been accepted as satisfactory in partial fulfillment of the requirement for the degree of BBA] on [24th of December].

Examining Committee:

Supervisor

_____

Dr. Md Shamimul Islam
Assistant Professor,
BRAC Business School
BRAC University

Acknowledgement:

First and foremost, I would like to thank Almighty Allah, the Most Gracious and Merciful, for enabling me to conduct a thorough investigation in a proper manner and effectively prepare the report. Additionally, I would like to thank my Supervisor and Co-supervisor, for the guidance and oversight. I am indebted to him for his astute advice and resolute assistance.

Abstract:

Purpose: The goal of this study is to examine cybersecurity strategies and defense mechanisms employed by organizations in order to target small and medium-sized businesses with cybersecurity education and awareness campaigns.

Design/methodology/approach: A comprehensive assessment of the literature on cybersecurity strategy and awareness, specifically for SMEs, was done in order to organize this study. An integrative review was used to supplement this theoretical study.

Findings: Although the literature can be useful in directing strategy, defense mechanisms, and awareness campaigns, it might not always apply to actual campaigns. Existing programs, like the one this study examined, have a lot of potential, but they can yet be improved. For the benefit of the academic and practitioner communities, knowledge from each of these fields may and ought to be merged.

Keywords: Cybersecurity, education program, awareness, strategy, mechanism.

Table of contents:

Declaration…….……..….02

Approval…….……...…...….03

Acknowledgement…….……..……..…04

Abstract…….…….05

Chapter: 01 Introduction……...….……...09-15

Chapter: 02 literature review…….…….....15

2.1 Cybersecurity and SMEs:.....15-20

2.2. ISF Standard of Good Practice for Information Security……21

2.3 COBIT……...…22

2.4. NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF).....22

2.5: Emerging Cyber Threats…….……..23

2.6: SMEs in Bangladesh…….24

2.7 Cyber threats and defense mechanisms for SMEs in Bangladesh……26-28

Chapter 03 Methodology……29

3.1 Identify Keywords and Search Terms……..29

3.2 Search Strategy…….....29

3.3 Inclusion Criteria……...30

3.4. Exclusion Criteria…….31

3.5 Screening Process……...32

3.6 Data Extraction…….33

3.7 Quality Appraisal……..….34

3.8. Synthesis of Findings……35

3.9. Questionnaire Analysis……36

Chapter 04 Findings……...……..…..36

4.1. Cybersecurity Adoption in SMEs……37

4.2. Cyber-attacks specific to SMEs in Bangladesh:……..…….38

4.3. Cybersecurity Challenges and Trends in Bangladesh's SME Sector……..…44

4.5. Impact on Business Operations and Data Security……45

4.6. The existing cybersecurity awareness strategies of SMEs in Bangladesh……..……46

4.7. Defense Mechanisms for SMEs in Bangladesh……..……..…48

4.8. Programs for educating and raising awareness of cybersecurity among SMEs in Bangladesh……49

4.9. Data analysis of the questionnaire……...……..……..…52

Chapter 05 Discussions……..…..55

5.1. Cybersecurity for SMEs in Bangladesh……...…….……..…55

5.2. Global Cybersecurity Trends for SMEs……...…….……..……...…55

Chapter 06 Conclusions……..…….59

Chapter 07 Recommendations…….…....60

References…….…….…..…61-67

Appendix……..68

List of Acronyms:

ISF Information Security Forum

SoGP The standard of good practice

COBIT Control Objectives for Information and Related Technologies.

NIST National Institute of Standards and Technology

CSF Cybersecurity Framework

Chapter: 01 Introduction:

Cybersecurity has become a critical issue in the context of the global digital transition, especially for (SMEs). These businesses' susceptibility to cyberattacks puts not only their information security but also Bangladesh's larger economic fabric at risk as they traverse the digital environment. SMEs form the foundation of Bangladesh's national economy. This industry is essential to the growth of our nation's economy. The SMEs sector has a significant role in reducing poverty in the nation as well. SMEs businesses are especially well-suited for densely populated nations like Bangladesh, where the SME sector can create a lot of jobs with a lot less capital. They are anticipated to boost the economy, eliminate poverty, and produce jobs. According to the International Monetary Fund's (IMF) 2012 Country Report, SMEs in Bangladesh constituted over 99% of private sector manufacturing companies and provided employment for 70–80% of the country's other than agriculture working population (Alauddin & Chowdhury, 2015).

Cybersecurity risks such as login attacks, phishing, pharming, and website vandalism have fostered mistrust in the industry and made it extremely difficult for SMEs online service providers (SMEs) to compete with established virtual and brick-and-mortar service providers (Sharma et al., 2009).

Numerous suggestions have been made to support the security of SMEs, particularly in the areas of awareness, education, and training. Through various procedures, training programs, and other ways, they aim to explicitly provide cybersecurity support for small and medium-sized enterprises (SMEs). But despite these suggestions, SMEs continue to face the problem of cybercrime.

The SME sector's share of GDP is projected by the Bangladesh Bureau of Statistics (BBS) to be 21.36 percent in FY17, 21.98 percent in FY18, and 22.86 percent in FY19. But because of the pandemic in FY20, this sector's contribution fell to 22.40 percent (Luthfe et al., n.d.).

For economic growth and employment creation SMEs are important to Bangladesh. If we do not understand the importance of SME, it will have negative effects. According to the World Bank, Bangladesh's almost 10 million SMEs account for 25% of the country's labor force, 80% of jobs in the industry sector, and 23% of the country's GDP. The global bank, which oversaw several programs to assist small enterprises, claims that MSMEs are the main driver of the creation of non-farm jobs in Bangladesh (*Critical Motors of Growth and Job Creation: How the Rest of the World Views SMEs*, 2023).

Even though cybersecurity is becoming more and more important, there is still a significant research gap in Bangladesh, especially when it comes to how effective current cybersecurity measures are for SMEs. The majority of the material that is currently available concentrates on more general or worldwide cybersecurity issues, frequently ignoring the particular difficulties that SMEs in developing nations face. The lack of a thorough examination of recent cyberattack instances that targeted SMEs in Bangladesh is one obvious shortcoming. Developing focused and efficient cybersecurity policies for the SME sector requires a close analysis of the different types of attacks, how often they occur, and the strategies that cybercriminals use.

In addition, although several researches recognize the significance of cybersecurity knowledge and instruction, a thorough examination of the current awareness tactics employed by SMEs enterprises in Bangladesh is lacking. Building a resilient cybersecurity framework for SMEs requires an understanding of the effectiveness of current awareness initiatives, the identification of knowledge gaps among SME owners and staff, and an assessment of the variables impacting the adoption of cybersecurity best practices. For example, Wallang (2022) discussed the aspects of cybersecurity in (SMEs), exploring both positive and negative elements. Arroyabe (2022) discussed using machine learning to assess the impact and extent of cyberattacks on SMEs.

Moreover, Bangladesh is a developing nation going through an ICT revolution right now. Bangladesh is currently embracing technology and rapidly increasing its usage of the Internet and other electronic devices. They have great expectations for their investment to pay off, but they haven't yet experienced any benefits. Developing technological nations exist in this region, and their online communities are growing. This paper's investigation demonstrated that the nation's officials require additional direction about the security of its cyberspace. It is necessary to gain a deeper awareness of the cyber security concerns facing this country. To decide how to best overcome the challenges and pinpoint areas that need further research, the difficulties at hand must be made more apparent and the conditions looked into.

An in-depth and thorough comprehension of a given issue is sought after by the integrative review, a comprehensive research synthesis process that synthesizes evidence from a variety of sources, including both theoretical and empirical literature (Whittemore & Knafl, 2005). An integrative review method is essential for this paper. Because to get the information about cyberattacks and

awareness strategies and to have a comprehensive analysis integrative review is a must. By doing this method, multiple trends and insights can be found which would help to get the understanding of cyber threats impact on SMES in Bangladesh.

SMEs face a wide range of cybersecurity threats, so it's important to comprehend how these threats affect particular industries like e-commerce. The literature makes clear that because to their perceived advantageous risk-to-reward ratio and their desirable targets due to their supply chain connections with larger firms, SMEs are frequently targeted by cybercriminals (Cybersecurity for SMEs - Challenges and Recommendations, 2021). E-commerce must, however, be more subtly incorporated into the conversation in relation to the current research vacuum. Notably, there is a knowledge vacuum about the precise ways in which cyberattacks impact e-commerce in the context of small and medium-sized enterprises. By exploring the nuances of cyber threats encountered by SMEs in the e-commerce industry and, in particular, by examining vulnerabilities in cloud-based systems, this study aims to close this gap. In doing so, this study aims to advance knowledge of the particular cybersecurity difficulties that SMEs have in the e-commerce environment. The paper provided information about how cyberattacks may affect e-commerce and analyze its cloud vulnerabilities.

This study seeks to address these gaps by focusing on two primary research questions:

1. What are the types of cyber-attacks faced by SMEs (E-commerce) in Bangladesh?
2. How effective are the existing cybersecurity awareness strategies of SMEs in Bangladesh in mitigating prevalent cyber threats?

3. What recommendations can we draw for the practitioners and policy makers from the study?

4. To what extent Bangladeshi students are concerned about the impact of cyber-attacks on SMEs in Bangladesh?

The objectives of this research are: to summarize the attacks and defence

1. To identify and understand the cybersecurity awareness and education initiatives for Bangladeshi SMEs.

2. To identify the cybersecurity impact on business operations and data security

3. To derive actionable recommendations for practitioners and policymakers in the field of cybersecurity for (SMEs).

4. To find out the Bangladeshi university students' familiarity with cybersecurity and their involvement in cybersecurity seminars or workshops, and their knowledge of successful tactics for promoting awareness among SMEs in Bangladesh.

Given the sector's significance to Bangladesh's economy, it is imperative to comprehend the cybersecurity landscape for SMEs in that country. SMEs are more vulnerable to cyberattacks due to the explosive rise of digital commerce and their growing reliance on technology. These attacks can have significant effects on SMEs' ability to survive and expand. With the purpose of

illuminating the present cybersecurity situation among Bangladeshi SMEs, this study highlights about the impact of cyber threats on SMEs.

Chapter 02: Literature Review:

2.1: Cybersecurity and SMEs:

"Cybersecurity describes a broad range of guidelines, conventions, and technological developments aimed at protecting computer systems, networks, and data against harm, illegal access, and cyberattacks" (Whitman & Mattord, 2018). SMEs are those that employ fewer staff members, have a smaller physical presence, and have fewer financial resources. Within the framework of this research, SMEs enterprises are those that fit the predetermined parameters for size, which are frequently based on variables like annual turnover, staff size, and income. SMEs are acknowledged for their adaptability, creativity, and notable contributions to regional economies; nonetheless, they frequently encounter distinct obstacles, such as limited resources, when it comes to putting strong cybersecurity measures in place (European Commission, 2005).

The paper will make references to the inputs from current research studies that concentrate on the numerous cybersecurity-related issues encountered by SMEs while referencing the body of existing literature. Understanding the synopsis of a few typical cyber-threats encountered by SMEs will also be helpful to readers.

Security-related standards and requirements, as the ISO 27000 series, ISF SOGP, NIST 800 series, SOX, and Risk IT, primarily focus on security issues (Taherdoost, 2022). Developed by the

International Electro Technical Commission (IEC) and the International Organization for Standardization (ISO), SO/IEC 27000 focuses on cybersecurity in information systems management (ISM) (Arora, n.d.). The series of ISO/IEC 27000 standards was once known as BS7799 and was subsequently added to the ISMS standards by the ISO, at which point it was introduced as ISO standards (Koza, 2022).

With a focus on data transfer and communication methods, the comprehensive guidelines and standards provided in ISO 27001 address how to implement information security in an organization in a way that is dependable and safe (Koza, 2022).

Table: 01 Related papers of cybersecurity attacks and strategy awareness:

Authors	Year	Focus of study	Methodology	Key findings	Title
Shekhar Ashok Pawar, Hemant Palivela	2023	Cyber-attacks have become a major problem for SMEs, which is having an immediate effect on the world business.	Through the use of efficient research surveys and immediate input from SMEs, this study has gathered the most recent observations.	(SMEs) face challenges in adopting cybersecurity guidelines and structures due to their restricted finances and differing company goals on cybersecurity management application.	A framework for least cybersecurity controls to be implemented for (SMEs)

Alireza Shojaifar, Samuel A. Fricker	2023	The purpose is to describe the assessment of a self-paced tool called CyberSecurity Coach (CYSEC) and to talk about how (SMEs) may enhance their cybersecurity capabilities by using CYSEC.	The foundation of this investigation is a qualitative method. (CEOs) and (CISOs) participated in nine organized interviews with the research team after it initially completed a survey study.	The results indicate that there was significant variation in the tool's adoption. The key determinants of CYSEC adoption are four: customized features; CEOs' or CISOs' knowledge level; the extent to which they have experience in IT and cybersecurity; and their relationship to cybercrime experience.	Design and evaluation of a self-paced cybersecurity tool
The Business Standard	2023	Bangladesh is vulnerable to cyberattacks because of a shortage of knowledgeable workers and understanding.	Interview and observation-based analysis.	Draws attention to Bangladesh's lack of widespread knowledge and its scarcity of qualified cybersecurity personnel. demands ongoing action to counter escalating	Bangladesh at risk of cyber attacks for lack of awareness and expertise

				attacks	
BGD e-GOV CIRT	2022	Bangladesh's government's pledge to improve the country's cybersecurity.	To identify the steps involved in putting the cybersecurity plan into action, collected data from government meetings.	Cybersecurity is now seen by the Bangladeshi government as a major economic and national security concern. The developed approach backs up the four pillars of the Digital Bangladesh project.	To help and improve the cybersecurity landscape of Bangladesh.
Inspira Advisory and Consulting Ltd	2022	Assessing Bangladeshi MSMEs' understanding of cybersecurity.	Evaluation employing quantitative and qualitative data collection techniques in seven Bangladeshi areas, with an emphasis on MSME owners.	Found that MSMEs poor understanding and expertise about cybersecurity. Companies with fewer than 100 employees were the target of 55% of ransomware attacks. Among Bangladeshi MSMEs, there is a clear need for increased cybersecurity education and awareness.	SARDI Cybersecurity Awareness Campaign For MSMEs In Bangladesh

Karen Renaud, Jacques Ophoff	2021	(SMEs) appear to be more susceptible because of the result of smaller companies not having the means to put security controls and procedures in place or not having sufficient situational knowledge to make wise decisions in this area.	361 SMEs in the UK participated in an online survey to gather empirical data	How well SMEs adopt cyber controls and procedures is significantly impacted by increased situational awareness and the availability of resources.	A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs
Maria Bada, Jason R.C. Nurse	2019	Cybersecurity knowledge and strategy program that can be applied to (SMEs/SMBs) in a given city.	Case study and considering a continuous, creative program that aims to collaborate with these companies to greatly improve their security posture.	Even though the literature can be useful in directing awareness and education campaigns, it might not always make it to actual campaigns. Existing programs, like the one this study examined,	Developing cybersecurity education and awareness programmes for (SMEs)

				have a lot of potential, but they can yet be improved.	
Mehdi Panjwani, Marko Jantti, Juuso Sormunen	2016	Stress the need of user-specific information security (IS), physical information security, control over entry and rights, and information security state tracking in SMEs.	Action research and case study.	SMEs face various information security obstacles.	IT Service Management from a Perspective of SMEs

2.2. ISF Standard of Good Practice for Information Security

An international organization with workers in New York City and headquarters in London, the Information Security Forum (ISF), first released the standard of good practice (SoGP) in 1996. The Information Security Forum (ISF) is a separate, non-profit organization that focuses on benchmarking and the creation of best practices for safeguarding data (Karie et al., 2021).

On an annual basis, the cyber security best practices standard is updated to reflect the latest information security best practices. The standard focuses largely on six areas: configuring devices, putting in place essential company procedures, managing connectivity and safety developing mechanisms, and safeguarding customer surroundings (Syafrizal et al., 2020).

2.3 COBIT (Control Objectives for Information and Related Technologies)

Businesses are depending more and more on the use of technology and communication, they are significantly more vulnerable to cyber threats from inside as well as outside sources. (Karie et al., 2021). When COBIT was first published in 1996, it was intended to assist users and decision-makers in IT systems by creating and refining a set of widely recognized and authoritative information technology control objectives. As a result, they may develop the necessary level of control and security to safeguard the assets of their businesses by (Karie et al., 2021).

2.4. NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF)

NIST created the "cybersecurity framework" subsequent to President Obama's 2014 signing of the executive order. The Cybersecurity Enhancement Act of 2014 (CEA), which aims to address the discovery and implementation of cybersecurity risk frameworks for critical infrastructure operators and owners, also revised the NIST's role. This framework addresses current corporate operations and cybersecurity issues. As a result, it can be thought of as the basis for a new cybersecurity program or mechanism that enhances an already-existing one, which businesses or the private sector can use as best practices to safeguard their own vital enterprises (Karie et al., 2021)

The NIST cyber security framework (CSF) helps organizations to increase their cybersecurity measures and provides an integrated organizing structure for different approaches in cybersecurity through collecting best practices, standards, and recommendations. In other words, a framework

providing a means of expressing cybersecurity requirements can be effective to point out gaps in the cybersecurity practices of an organization.

2.5: Emerging Cyber Threats:

Security dangers are increasing tremendously in cyberspace as Internet usage has skyrocketed. According to two bank insiders informed on the situation, investigators believe that unidentified hackers planted malware in the computer systems of the central bank of Bangladesh and observed, perhaps for weeks, how to take money out of the institution's U.S. account. Cyber security specialists are attempting to determine how the hackers gained entrance to Bangladesh Bank's systems more than a month after they attempted to steal about $1 billion from the bank's account at the Federal Reserve Bank of New York. The credentials of Bangladesh Bank for the SWIFT messaging system, which banks all over the world use for secure financial communication, looked to have been obtained by the hackers (“Rise of Ransomware and the Readiness of Bangladesh, 2017).

The number of incidents reported by the government-run Bangladesh e-Government Computer Incident Response Team (BGD e-Gov. CIRT), which is housed under the Ministry of Posts, Telecommunications, and Information Technology, increased to 870 in 2018 from 683 in 2017.19 379 was the number in 2016. 63.2% of attacks, 5.7% of hacking or attacks, 22.5% of harmful code, 4.5% of offensive material, and the other percentages coming from fraud, attempted invasion, requests for services, identity security, and other sources are all related to vulnerabilities (Mamun, 2022).

The authorities seldom recovered even a small portion of the 81 million dollars that the hackers known as the "three boys" had taken just a few months prior, causing a significant blow to our nation's economy. Our national bank's hacking is the only example of how vulnerable our cyber security is (“Rise of Ransomware and the Readiness of Bangladesh, 2017). Ransomware assaults have escalated recently in Bangladesh. Nobody is immune to this malware—not even individuals or organizations. Malware- and phishing-based attacks are also becoming more frequent. Malware without files will rule the next era. We must thus exercise greater caution and awareness (*“Bangladesh at Risk of Cyber Attacks for Lack of Awareness and Expertise,”* 2023).

There is insufficient legislation pertaining to ICT security in Bangladesh. There is some legislation that addresses specific areas of cybercrime. Although the National Cyber Security Strategy has been partially implemented, it does not offer specific guidelines that cybersecurity stakeholders can follow (Security, 2018).

2.6: SMEs in Bangladesh:

(SMEs) are crucial for reducing poverty and accelerating industrialization in emerging countries like Bangladesh. SMEs, are essential to Bangladesh's economy and are seen as the foundation of the nation's industrial development (Miraz & Habib, 2016).

SME definitions vary among nations and organizations. SME groups are divided into two main categories by the Bangladeshi government: manufacturing enterprises and non-manufacturing activities.

Two categories apply to manufacturing enterprises:

Small enterprise: A business would be considered small if, at current market prices, the replacement cost of its land and buildings, as well as its equipment, fixtures, support utilities, and related technical services through capitalized costs (such as turn-key consulting services), totaled up to Tk. 15 million;

Medium enterprise: A business would be classified as medium if, at current market prices, the replacement cost of its land and buildings, as well as its equipment, fixtures, support utilities, and related technical services through capitalized costs (such as turn-key consulting services), totaled up to Tk. 100 million.

Activities not related to production (like trading or other services)

Two types of non-manufacturing activity can be distinguished;

- Tiny business: a company is considered tiny if its full-time equivalent workforce is less than 25;
- Medium-sized business: If a company employs 25 to 100 people, it is considered small.

Miah (2007) found in a study about the SME sector in Bangladesh that the main obstacles facing SMEs are: a lack of modern technology; a high interest rate on bank loans; irregular or insufficient power supply; poor physical infrastructure and high transportation costs; a lack of skilled technicians and workers; a lack of facilities for research and development; fierce competition; the absence of an efficient and transparent legal system; credit constraints; low access to business services; a constraint on the quality of human resources; low awareness; low lobbying capacity.

According to BSCIC estimates, there are presently 511,612 cottage industries—that is, industries other than handlooms—and 55,916 minor industries. The number of cottage units soars to 600,000 units when handlooms are included, demonstrating the prevalence of small and cottage industries (SCIs) in Bangladesh. According to the most recent private sector survey, MSMEs account for between 20 and 25 percent of the GDP (Islam, Khan, Obaidullah , Alam,2010).

SME development is an extremely economical path to industrial development for LDCs like Bangladesh. The manufacturing sector makes up the largest portion of the GDP—38%. Additionally, it is noted that the retail and wholesale agriculture industries account for more than 22% of Bangladesh's GDP (Chowdhury & Ahmed, n.d.).

2.7 Cyber threats and defense mechanisms for SMEs in Bangladesh:

As Bangladesh becomes more conscious of its cybersecurity risks, (SMEs) must comprehend cyber dangers and put defense mechanisms in place. Bangladesh's vulnerability to cyber dangers was brought to light by a notable cyberbank heist in 2016, in which $101 million was taken from the Bangladesh Bank's New York Federal Reserve Bank account (*Cybersecurity: A National Priority for Bangladesh*, 2021).

This incident underscores the importance of robust cybersecurity policies and practices, especially for SMEs that may lack the resources and skilled manpower to adequately protect their digital infrastructure.

The involvement of key institutions like the Ministry of Science and Information & Technology, as well as non-state actors, plays a significant role in combating cyber threats. These entities contribute to policy formulation, awareness building, and implementation of cybersecurity measures (*Cybersecurity: A National Priority for Bangladesh*, 2021).

The Ministry of Posts, Telecommunications, and Information Technology oversees the state-run Bangladesh e-Government Computer Incident Response Team (BGD e-Gov. CIRT), and it reports that the number of events the team records increased to 870 in 2018 from 683 in 2017.19 379 was the number in 2016. 63.2% of attacks, 5.7% of hacking or attacks, 22.5% of harmful code, 4.5% of offensive material, and the other percentages from fraud, attempted invasion of privacy, requests for services, identity security, and other sources are all related to vulnerabilities (*Cybersecurity: A National Priority for Bangladesh*, 2021).

Despite several safety precautions, the frequency of cyberattacks against commercial and service-oriented establishments nationwide keeps rising. In the age of digital technology, the nation has made great strides, especially in the socioeconomic arena, but the number of cyber-related occurrences is rising along with it. The increase of information technology-related crimes has made cyber security a major worry for the majority of significant public and commercial entities (*Cybersecurity: A National Priority for Bangladesh*, 2021).

Chapter 03. Methodology: Integrative Review

3.1 Identify Keywords and Search Terms

- Keywords: “Cybersecurity”, “SMEs in Bangladesh”, “Cyber Attacks”, “Awareness Strategies”, "Cybersecurity in Bangladeshi SMEs", "Cyber attack trends in Bangladesh", "Awareness strategies for cybersecurity in SMEs".

3.2 Search Strategy

- Databases and Sources: Utilized IEEE Xplore, ScienceDirect, Google Scholar, newspapers, and journal reports.
- Query Approach: Combined keywords in various formats to ensure comprehensive coverage. For example, searching "Cybersecurity AND SMEs AND Bangladesh" in one instance and "Cyber attacks in Bangladeshi SMEs" in another.

3.3 Inclusion Criteria

Time Frame: Focus on studies published within the last ten years, such as "Cybersecurity: A National Priority for Bangladesh" (Ebrary, n.d.) and "92% MSME Entrepreneurs Unaware of Cyber Security: Study" (2022).

Content Relevance: Included articles discussing both cyber attacks and awareness strategies, like the "SARDI Cybersecurity Awareness Campaign for MSMEs in Bangladesh" (Inspira Advisory and Consulting Ltd, n.d.).

Geographical Relevance: The research must be explicitly related to Bangladesh, ensuring the context is directly applicable to the country's SME sector.Emphasize studies specifically related to Bangladesh, evident in sources like "The Computer Incident Response Team for Bangladesh e-Government" (n.d.).

- Focus on studies published within the last ten years addressing cybersecurity in SMEs in Bangladesh, like "Cybersecurity: A National Priority for Bangladesh" (Ebrary, n.d.), "SMEs and Cybersecurity Threats in E-Commerce" (Sharma et al., 2009), and "The Computer Incident Response Team for Bangladesh e-Government" (n.d.).

- Renaud & Weir (2016): A comprehensive study on cybersecurity challenges and strategies.

Articles and Case Studies: Recognized institutions' papers and in-depth case studies provide real-world information and valuable perspectives. As an illustration:

- The SARDI Cybersecurity Awareness Campaign is a program that emphasizes doable strategies for increasing knowledge about cybersecurity among Bangladeshi MSMEs.

- Bebshay Digital Shurokkha: A campaign centered on online safety that offered helpful advice on how to put safety precautions into practice.

3.4. Exclusion Criteria

Location Irrelevance: Main focus of our paper is to concentrate on cybersecurity on SMEs of Bangladesh. This is why the paper which is not based on Bangladesh is being excluded. For example: "Cybersecurity in Small States: Obstacles and goals for Small emerging countries". This paper has not discussed about Bangladesh.

Non-SME Focus: Articles that do not specifically address SMEs are excluded from the research because the main objective is to understand cybersecurity in the context of SMEs. For example,

the article "Cybersecurity: Problems and Opportunities in Emerging States" was dismissed since it did not specifically target SMEs in its analysis.

Non-Relevance to Cybersecurity and Awareness Strategy: Sources with no information about cyberattacks or education programs that were pertinent to Bangladesh's SMEs were excluded. The sources must unambiguously contribute to the SME sector's understanding of cybersecurity threats and awareness initiatives. The paper "Cybersecurity Risk Management: Are We Making Enough Efforts??" was eliminated because it was based on the broad range of cybersecurity but not on specific in SMEs in Bangladesh

The inclusion criteria helped to find out the most relatable paper for cybersecurity awareness strategies in SMEs in Bangladesh and exclusion criteria helped to eliminate those papers which do not meet the requirements.

3.5 Screening Process

Initial Screening

- The titles and abstracts of the retrieved articles are carefully examined as part of the first screening process. This phase is essential to determine whether the paper is associated with the research question. Looked through publications like "Youth Entrepreneurship through SMEs Can Change Bangladesh’s Economic Landscape" to see if they address cybersecurity in SMEs. Sources like "SARDI Cybersecurity Awareness Campaign for MSMEs in Bangladesh" (Inspira Advisory and Consulting Ltd, n.d.), "92% MSME

Entrepreneurs Unaware of Cyber Security: Study" (2022), and "Rise of Ransomware and the Readiness of Bangladesh" (2017) should have both their titles and their abstracts looked over for relevancy.

- **Relevance Check:** During this stage, It has confirmed whether the studies relate to cybersecurity, SMEs, and specifically the context of Bangladesh. In-depth analysis of articles like Sharma et al. (2009) "SMEs and Cybersecurity Threats in E-Commerce" to confirm relevance and depth of content.

Detailed Screening

- Full-Text Review: Articles that make it past the first round of screening undergo a full-text review. This comprehensive analysis guarantees that the papers are directly relevant to the study objectives and meet all inclusion criteria.

- Conducted a full-text assessment of the shortlisted publications, such as those by Renaud & Weir (2016), Alauddin & Chowdhury (2015), and Mamun (2022), to confirm their depth and relevance.

3.6 Data Extraction

Created a template (Authors name, key findings, methodology) and standardized the process of extracting data to make it easier to compare and contrast different studies.

Template that were created to gather data from publications like Renaud & Weir (2016), " The Intolerable and Safety online of Unpredictability," underlining the focus, the year the study was published, the author, and the primary conclusions. "2022 Cybersecurity Annual Report" (n.d.),

"Hasan et al. (2019), Mahmud et al. (2020), and "Bangladesh at Risk of Cyber Attacks for Lack of Awareness and Expertise" (2023) are a few examples.

3.7 Quality Appraisal

Evaluation Metrics

Source Credibility: Assessed the impact factor of the journals in which the articles are published. Higher impact factors generally indicate a higher standard of research and most cited paper. For example: Renaud, K., & Weir, G. R. S. (2016). "Cybersecurity and the Unbearability of Uncertainty." Cybersecurity and Cyberforensics Conference.

- Assessment: This paper was presented at a reputable conference, indicating a level of peer-review and scholarly recognition. While conferences typically do not have an impact factor like journals, their credibility can be ascertained by the reputation of the conference and the organization behind it.

Author Expertise: Considered the expertise and background of the authors to gauge the reliability of the findings. SARDI Cybersecurity Awareness Campaign for MSMEs in Bangladesh" by Inspira Advisory and Consulting Ltd

- Assessment: This report is authored by a consulting firm known for its work in advisory and consulting, which adds to the credibility of the findings. The firm's analysis and suggestions are supported by its domain experience, particularly in relation to the Bangladeshi setting.

Methodological Robustness: Assess the studies' approaches for rigor, applicability, and thoroughness in answering the research issue. Singh, A., Sharma, V. P., and Sharma, K. (2009). "SMEs and Cybersecurity Threats in E-Commerce." EDPACS.

Assessment: This article most likely uses the structured research methodology that is standard for peer-reviewed journal publications. The methodology's level of robustness would be assessed based on the paper's explanation of the research design, analysis techniques, and data collection procedures.

Impact Factor and Expertise: Using sources like Alauddin & Chowdhury (2015) and Luthfe et al. (n.d.), analyze the impact factors of journals and the experience levels of authors.

3.8. Synthesis of Findings

- Identifying Themes: Determine the main topics from the literature, including the kinds of cyberattacks that Bangladeshi SMEs have to deal with, the public's understanding of cybersecurity, the efficacy of defenses, and the gaps in the tactics that exist today. For instance, "Cyber Security Awareness in Bangladesh: An Overview of Problems and Approaches" (2022) as well as "Rising of Ransomware and the Preparedness of Bangladesh" (2017).
- Key Themes: Aggregated information from various sources, with an emphasis on the different kinds of cyberattacks, the degree of knowledge, and defensive strategies, like in Mamun (2022) and "Rise of Ransomware and the Readiness of Bangladesh" (2017). "SMEs may assist Youth Entrepreneurial Enhance Bangladesh's Gdp" (n.d.). "Critical

Motors of Growth and Job Creation: How the Rest of the World Views SMEs" (2023).Included information from additional sources, such as "Bangladesh at Risk of Cyber Attacks for Lack of Awareness and Expertise" (2023) and the "2022 Cybersecurity Annual Report" (n.d.), to guarantee a thorough and knowledgeable viewpoint.

- Arranged information from many sources into categories. Like "Youth Entrepreneurs through SMEs Might Revolutionize Bangladesh's Financial Landscape" (n.d.) as well as "Critical Motors of Growth and Job Creation: How the remainder of the Global Perceives SMEs" (2023). By ensuring that the study is grounded in multiple points of view, this approach contributes to a thorough understanding of the subject.

3.9 Questionnaire:

In addition, by using a questionnaire survey to gather primary and raw data, 92 Bangladeshi university students—private or public—were included. In order to get additional understanding and produce a study result free of bias.

Online social media channels were largely used for conducting the interviews. A questionnaire that was created using the research's original questions may be found in the report's Appendices section. The questions were not derived from any prior research. Every survey response was noted and is included in the appendices section as well.

Also, the primary data were appropriately verified. All personal information of the participants was kept private, along with any other information they deemed private.

Chapter 04: Findings:

4.1 Cybersecurity Adoption in SMEs:

Even though Bangladesh is ranked 11th in the world for cyber security preparation, experts and academics recently noted at a seminar in Bangladesh that cybercrimes increased at an alarming rate along with the rapid rise in both individual and institutional Internet users (Bhuiyan et al., 2016). Bangladesh remains vulnerable to cyber-attacks because traditional cyber defences such as anti-virus software and firewalls are ineffective against new threat vectors such as zero-day malware and Advanced Persistent Threats (APT) (Mahmud et al., 2020).

More than 92% of micro, SMEs are unaware of cyber security despite around 40% of them having directly or indirectly been victims of cyberattacks, according to a study by Inspira – a management and consulting research farm". "Of the entrepreneurs, 82% think that cyber security is not relevant for them at all, according to the findings. As a result, they often fall prey to various cyber threats and incur significant business losses (*92% MSME Entrepreneurs Unaware of Cyber Security: Study*, 2022)

Many developing countries, such as Bangladesh, have restrictions on access to information, and access to it is not cost- effective in terms of the insufficiency of existing infrastructure and the lack of appropriate education (Mamun, 2022).

The "Bebshay Digital Shurokkha" Campaign aims to improve the cybersecurity awareness of business owners in Bangladesh. The campaign is funded by the U.S. Agency for International

Development (USAID), and is a part of the South Asia Regional Digital Initiative (SARDI) initiative, which is being implemented by DAI Inc (*Bebshay Digital Shurokkha*, 2022).

Programs to raise awareness are available, however they are very haphazard and do not have specific target groups in mind. As a component of BCC, the BGD e-GOV CIRT creates awareness campaigns, has modified some Stop.Think.Connect materials, and posts content online. However, it was unclear from the discussions whether these efforts are directed toward particular target audiences or if any metrics were used. An integrated National Cybersecurity Education Framework is still lacking, and the government is still unaware of the NCS's action item. The number of cybersecurity experts and cybersecurity qualification programs remain extremely low, even though the government has taken several steps to address these issues (Cybersecurity, 2018).

4.2 Cyber-attacks specific to SMEs in Bangladesh:

As Internet has grown in our country, the need has been felt to enact the appropriate cyber laws, which are indispensable to legalize and regulate Internet in Bangladesh. The existing laws of Bangladesh, even with the most generous and moderate interpretation, could not be interpreted the light of the promising cyberspace, to consist of all aspect relating to different activities in cyberspace. There are no existing laws (Siddique, n.d.).

The E- commerce business growth has been aided by better internet connections and a rise in the number of individuals with access to the internet during the past few years. In 2016, 50 million dollars was consumed in the E- commerce market of Bangladesh. 10 million of that total came from FDI. In the year 2017, the retail market generated BDT 1335.71 billion. On

the other hand, the B2C market for E- commerce business was 110-115 million dollars (BDT 9.0 billion (Islam et al., 2022).

E-commerce and online marketplaces in Bangladesh started without any kind of legal structure. The government of Bangladesh has made some steps to provide a legal framework for online commerce. In Bangladesh, there is no specific legislation governing online commerce. These rules can aid in regulating and ensuring the protection of e-commerce customers if a seller on an e-commerce site commits any act that is punishable by law (Rahman, M, 2023).

According to a Statista survey, 90% of global online consumers have at least one major concern regarding data privacy (*11 Disastrous Cyberattacks to Warn Your E-Commerce Business*, n.d.). Personal information of 57 million customers was exposed, and the company attempted to cover up the breach by paying the hackers (*11 Disastrous Cyberattacks to Warn Your E-Commerce Business*, n.d.)

The e-commerce sector in Bangladesh faced a challenging year in 2021 due to a number of e-commerce scams, which resulted in the loss of trust of the public in the sector. The fraudulent activities led to the closure of some e-commerce businesses and government interventions to regulate the sector. As a result, the e-commerce business suffered a setback in the second half of the year, with transactions through formal banking channels dropping sharply due to customers' trust deficit (Rahman, M, 2023).

A real-life example of a cyber-attack on an SME is the incident involving Evaly, a prominent e-commerce platform. In September 2021, Evaly faced severe allegations of financial fraud and embezzlement. While this case primarily involved financial irregularities, it also raised significant concerns about cybersecurity and data protection, as the platform handled a large amount of customer and transaction data. This incident highlighted the vulnerabilities in the e-commerce sector and underscored the need for better cybersecurity measures to protect both financial assets and sensitive data (Prothom Alo, 2021).

The youth, who are new to e-commerce, mostly jumped up to social media tools to open their shops. But there are some issues like spamming, phishing, email, scam, and spy apps, which can be used by malicious actors to get crucial security information. In addition to that, the e-payment system in our country is not also developed as effectively as needed to grow successful e-commerce. Fraudulent poor customer servicing, mismanagement, loopholes in apps, and many other vulnerabilities are found in our research that indicate the riskiest area of the e-commerce industry (Islam et al., 2022).

Table: 02 Cyber threats and crimes related to e-commerce:

Crime Name	**Description**	**Source**	**Title**
Card Testing Fraud	Illegitimate access to credit card numbers for fraudulent transactions.	(*Versapay*, 2023)	Digital payment Fraud Prevention

Friendly Fraud	Similar to charge-back fraud, where a customer falsely claims a transaction as invalid, leading to a charge-back.	(*Stripe*, 2023).	Three types of chargebacks and how to prevent them
Fraud of Refund	Using a stolen credit card to make a purchase and then requesting a refund for an unintended overpayment.	(Decorte,2023b)	Credit Card Refund Schemes
Account Takeover Fraud	Unauthorized access to a customer's account on an e-commerce site, leading to identity theft and other issues.	(Hasson, 2021)	Prevent Account Takeover Fraud
Interception Fraud	Placing orders on an e-commerce site using stolen credit card information, intercepting the delivery for personal gain.	(Hasson, 2021).	E-Commerce Fraud Prevention: 6 Worst Scams & How To Avoid Them
Triangulation Fraud	Legitimate purchases on third-party marketplaces using fraudulently obtained merchandise	(Fletcher, 2022)	**What Is Triangulation Fraud?**

	from another retailer's website.		
Supply Chain Attacks	Attacks on the software supply chain, compromising legitimate requests and introducing malicious code into the system.	(CrowdStrike , 2023)	**What is a supply chain attack?**
Malware Attack	Deployment of malicious software, such as viruses, worms, trojans, spyware, and ransomware, to compromise systems.	(*Rapid7*, 2023)	Malware Attacks
Social Engineering Attack	Deceptive tactics to trick users into providing sensitive information or unknowingly installing malware on their devices.	(Hasson, 2023)	What is Social Engineering?
Man-in-the-Middle Attack	Intercepting communications between two points to gather sensitive information or manipulate the	(Magnusson, 2023)	Man-in-the-Middle (MITM) Attack: Definition, Examples & More

	communication.		
Denial-of-Service (DoS) Attack	Overloading the target system with traffic to disrupt normal functioning, with Distributed Denial-of-Service (DDoS) attacks involving multiple devices.	(Frankenfield , 2023)	Denial-of-Service (DoS) Attack: Examples and Common
Injection Attacks	Exploiting vulnerabilities to insert malicious inputs into online applications, including SQL injection and cross-site scripting.	(*What Is SQL Injection (SQLi) and How to Prevent Attacks*, 2022)	What is SQL Injection (SQLi) and How to Prevent It
Phishing and Spear-Phishing	Deceptive emails or communications aimed at individuals or organizations to install malware or steal sensitive data.	(Valimail & Valimail, 2023)	Spear Phishing vs Phishing: The Differences and Examples
Spoofing	Deceiving someone by appearing as something or someone else,	(*What Is Spoofing?*, 2023)	What is spoofing attack?

	including URL spoofing, email spoofing, and caller ID spoofing		

Case study: Distributed Denial of Service (DDoS) Attack on an E-commerce SME:

An e-commerce SME faced a DDoS attack that overwhelmed its website, resulting in significant downtime and loss of revenue. The company had not implemented effective DDoS mitigation measures. To prevent future DDoS attacks, the company employed the services of a cloud-based DDoS protection provider, implemented traffic filtering and rate limiting solutions, and established incident response procedures to minimize the impact of future attacks (*Cybersecurity for Small and Medium-Sized Enterprises (SMEs): Challenges and Solutions*, n.d.)

4.3 Cybersecurity Challenges and Trends in Bangladesh's SME Sector: An Analysis of National Strategies and Vulnerabilities

National Cybersecurity Strategy: An examination of the 'National Cybersecurity Strategy of Bangladesh' through research offers valuable insights into the official cybersecurity protocols used in the nation. This plan probably takes into account the larger context in which SMEs function as well as the cybersecurity regulations that they must adhere to (Uddin,2017).

Cybersecurity Risk Management Challenges: Another paper discussed the need for changing technological safety standards, which is a major barrier for (SMEs) wishing to implement new

technology. This suggests that SMEs' inability to swiftly adjust to changing cyber-threats is a result of inflexible or antiquated security requirements (Duncan, 2020)

Cyber Attack Trends in the Financial Sector: To determine the patterns and reasons behind cyber heists, a review of recent cyberattacks, particularly those that targeted the financial industry, was undertaken. A review of Bangladesh's current legal system for handling cybercrimes was part of this. This suggests that financial SMEs should have a robust legal and regulatory framework since they may be especially vulnerable to cyberattacks (*Cyber Crime Trend in Bangladesh, an Analysis and Ways out to Combat the Threat | IEEE Conference Publication | IEEE Xplore*, n.d.)

These results make it clear that cyber dangers to SMEs in Bangladesh, especially those in the e-commerce industry, are varied and complex. The findings highlight the necessity of effective risk management techniques, strong cybersecurity measures, and knowledge of the particular patterns and techniques of cyberattacks that impact SMEs in Bangladesh.

Notably, e-Gov CIRT found eight phishing websites particularly made in the names of the aforementioned institutions out of a total of eighteen websites targeting these organizations. These websites, which included bkashagent.com, corona-bd.com, and others, were made to look like trustworthy platforms in order to trick users and collect private data, including consumers' National ID card numbers. It was urged that the Bangladesh Telecommunication Regulatory Commission take down these phony websites (Dhaka Tribune, 2023).

4.4 Impact on Business Operations and Data Security:

Financial and Reputational Costs: SMEs often lack the financial resources to recover from cyber-attacks, with the average cost of an attack easily exceeding $200,000. This includes direct costs like IT support and legal fees, and indirect costs such as lost productivity and revenue. For many SMEs, this can lead to bankruptcy (Gondek, n.d.)

Supply Chain Vulnerabilities: SMEs often rely on a network of suppliers, partners, and contractors. A cyber-attack on any of these partners can have a ripple effect throughout the entire supply chain, exacerbating the damage (Gondek, n.d.)

Global Economic Threat: Cybercrime, predominantly targeting SMEs, has become a major global economic threat. With SMEs often unable to afford adequate cybersecurity systems, cybercriminals exploit their online and network vulnerabilities. The financial losses due to cybercrime could significantly increase the operational costs for SMEs and limit their productivity, potentially leading to business closures and job losses (Awal, 2022)

In Bangladesh, the e-commerce sector, still nascent, has to contend with underdeveloped organizational structures and the smooth running of online businesses. Bangladesh is an emerging country, hence its e-commerce websites are not as organized. as in more developed countries, which may contribute to vulnerabilities to cyber-attacks (*A Study to Analyse Bangladeshi Consumers' E-Commerce Security and Privacy Satisfactions in Small to Mid-Sized Enterprises*, n.d.).

4.5 The existing cybersecurity awareness strategies of SMEs in Bangladesh:

SMEs in Bangladesh, significant contributors to the GDP, have faced increasing cyber threats with the rise of digitalization, after the COVID-19 forced many to adopt digital tools. The lack of robust information security frameworks makes them susceptible to cyber-crime.

Despite the government taking different initiatives to introduce cyber security qualification programs and to increase the number of cyber security experts, both are still very limited. The need for training professionals in cyber security has been documented in the current NCS. However, there was also no evidence from the consultations to the extent initiatives were implemented (Rahaman, 2022)

People use mostly free antivirus which is a major security flaw. Also people use paid antivirus, firewall, authentication, encryption and others. In terms of cybersecurity practices, there are some good security practices. 61% people always aware, 29% people are sometimes aware and 10% people are never aware about the legitimacy of a website. 74% people are always aware, 21% people are sometimes aware and 4% people are never aware about the danger when clicking on banners, advertisements or pop-up screens that appear when surfing the Internet (Ahmed,2022).

Overall cyber-security situation in Bangladesh: In 2015, Bhuiyan, Alam, and Farah performed a statistical analysis on the state of a few well-known cyber vulnerabilities that were found in Bangladeshi web apps. They sampled 2500 web apps, including those from the public and commercial sectors as well as those for education, banking, healthcare, and e-commerce. 400 of the 600 online apps were discovered to be weak points. Bangladesh's main web apps were all still in their early stages of development. They examined online applications that were susceptible to

even the most elementary cyberattacks. Bangladesh was not as cyber robust as the experts had anticipated. The researchers contend that in order to guarantee the security of web applications, the government must establish regulations for online security that must be adhered to and inform the public about cyber-threats.

4.6 Defense Mechanisms for SMEs in Bangladesh: Bangladesh is responding to these increasing cyber-threats by implementing a comprehensive cybersecurity plan. Under the direction of the Digital Security Agency and the Information and Communication Technology (ICT) Division, this plan aims to bolster the nation's cyber resilience. The strategy outlines several steps to address cyber dangers, including giving all ministries access to specialist software and skilled labor, focusing on 10 key areas, and improving cybersecurity incident response and defense. Most significantly, this plan places a high priority on education and aims to produce a sizable number of cybersecurity graduates and postgraduates annually. This effort reflects a broader grasp of Bangladesh's digital hazards (Molla, 2021).

4.7 Programs for educating and raising awareness of cybersecurity among SMEs in Bangladesh:

Building a strong cybersecurity culture is essential because it can address a multitude of behavioral issues that are the root cause of security breaches. Additionally, the organization's business needs must be supported by awareness and training programs that are relevant to the organization's culture and that address important subjects like threats and the harms caused by cyberattacks (Santos-Olmo et al., 2016; Agrafiotis et al., 2018; ENISA, 2019).

One of the most difficult issues facing organizations today is raising employee knowledge of cybersecurity. SME/SMBs confront similar challenges to large organizations in terms of worker education and training, but they have far fewer resources at their disposal (Bada &Nurse, 2019).

Sadly, there is a lack of knowledge regarding the most effective ways to promote security-aware behavior. Such actions would have to take into account the ways that cybercriminals target people, which are always changing (Nurse, 2018; Iuga et al., 2016). Secondly, it would need to last for an extended period of time. Due to this, some SMEs have stopped doing security training, or those that have are unsure of how to continue without running the risk of problems like security weariness (Furnell and Thomson, 2009; InfoSecurity, 2017). Organization, work procedures, and human elements should all be considered (ENISA, 2019). Moreover, people are acknowledging the importance of cybersecurity. Incidentally, With support from the United Nations Development Programme (UNDP) in Bangladesh, the Bangladesh Hi-Tech Park Authority and the ICT Division's Digital Security Agency are leading the inaugural "Bangabandhu International Cyber Security Awareness Award" initiative (The Business Standard, 2022).

The competition's cyber security awareness and education award went to Tamjid Rahman, a teenage Bangladeshi. With the tagline "Janle Ain, Safe Online," he is attempting to raise awareness of online safety (The Business Standard, 2022).

State Minister Junaid Ahmed Palak saidiIn his remarks at the function, he listed four critical components for ensuring cyber security. First, awareness. It's critical to guarantee awareness at all levels in order to assure cyber security. Development of technology comes in second. The Framework for Development Policy is the Third, International Cross-Border Collaboration is the Fourth (The Business Standard, 2022). To develop effective cybersecurity programs for SMEs in

Bangladesh, the approach recommended by Bada, M., and Nurse, J.R.C. (2019) includes engaging SMEs through targeted events, building a strong cybersecurity culture, conducting regular security assessments, providing accessible resources and support, and maintaining ongoing communication. This strategy should be adapted to the specific context and needs of Bangladeshi SMEs, balancing technical and non-technical aspects of cybersecurity (The Business Standard, 2022).

Effective engagement is achieved by visiting SMEs at their workplaces, establishing a presence at local events, conducting SME-focused events, and building relationships with industry and trade bodies. This approach emphasizes the importance of direct, relevant communication to help SMEs understand cybersecurity and implement effective security practices (The Business Standard, 2022).

The strategy uses tools like the Scorecard for technical security assessments and broadens the focus to include cybersecurity education and awareness because it recognizes the significance of both technical and non-technical factors. This will address the behavioral problems that frequently result in security lapses, and each SME will receive training customized to the unique cyber-threats they face (The Business Standard, 2022).

Essential resources such as tools, materials, and training programs need to be regularly updated and aligned with audit outputs. The recommendation includes maintaining a vetted list of security practice and awareness materials, and conducting events and workshops tailored to SMEs. This addresses the common issue of limited resources and expertise in cybersecurity among SMEs (The Business Standard, 2022).

Cyber security awareness courses in Bangladesh:

- Cybersecurity Fundamentals. Introduction to Cybersecurity. The evolution of Cybersecurity.
- Cybersecurity Concepts. Risk. Approaches to Cybersecurity. ...
- Security Architecture Principles. Overview of security architecture. ...
- Security of Networks, Systems, Applications, & Data.

Another course by Skilllogic of cybersecurity. The goal of the SKILLOGIC cybersecurity certification programme is to meet the market's demand for seasoned professionals with the required skills and competence as well as the desires of those professionals to further their careers in the sector and increase their value to employers. Topics and curricula are carefully chosen to have the greatest positive impact (SkillLogic, n.d.).

4.8 Data analysis of the questionnaire:

a) Preparing the data:

I have chosen Bangladesh based students from private or public universities and created a standard questionnaire that can be used by any of them. This questionnaire covers Bangladeshi university students' awareness of cybersecurity and their involvement in cybersecurity seminars or workshops, and their knowledge of successful tactics for promoting awareness among SMEs in Bangladesh

b) Analysis:

The questionnaire has been added to the appendix section. When the students were asked about their awareness of cybersecurity, their participation in cybersecurity seminars or workshops, and their knowledge of effective strategies for raising awareness among SMEs in Bangladesh, it was discovered that they had given a variety of answers. The answers of respondents are given below:

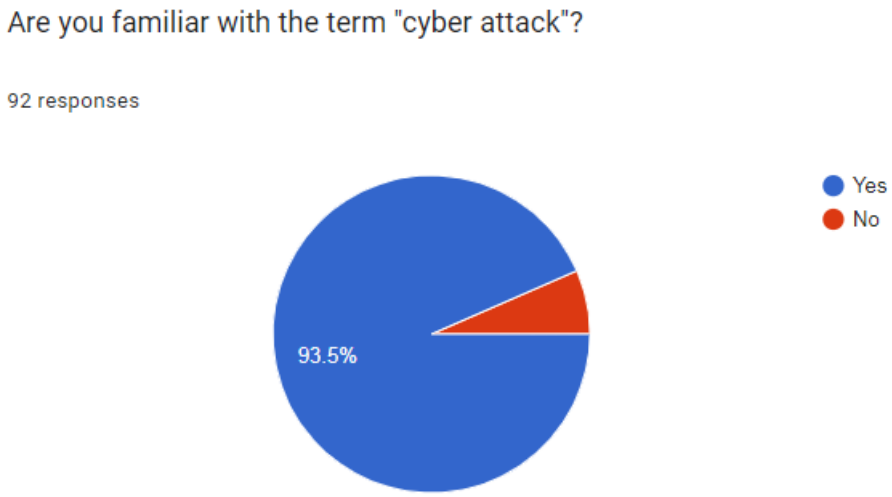


Figure: 01: Familiarities with the term of Cyber-Attack

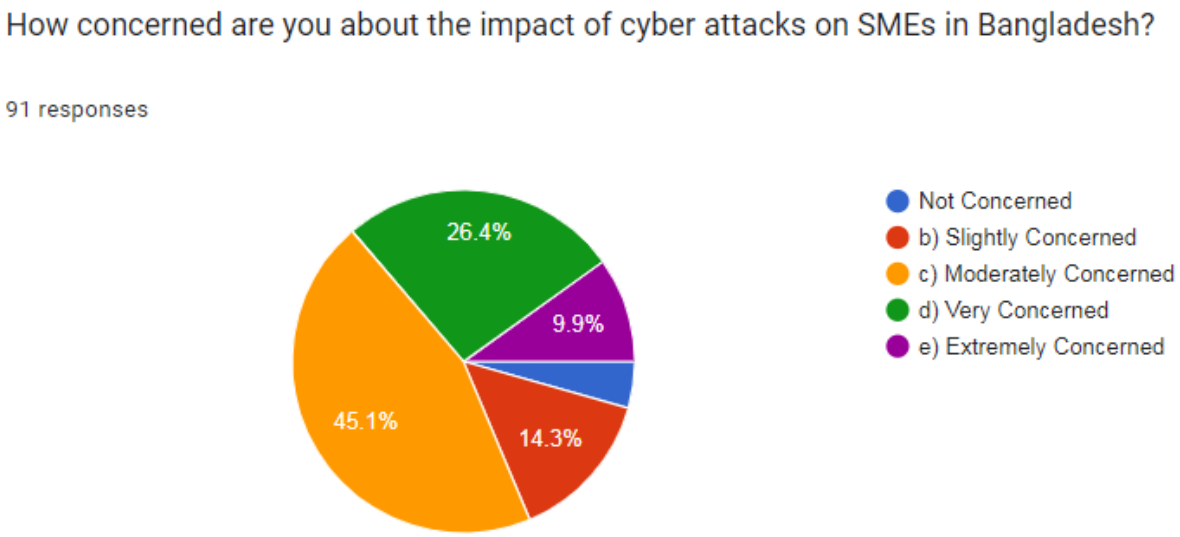


Figure: 02 Students' concern regarding the impact of cyber-attacks on SMEs in Bangladesh

Familiarity with cyber-attacks**:** Majority (93.5%) of the university students have heard about the term of cyber-attacks nonetheless only 6.5% have not heard about the cyber-attacks. Furthermore, A large majority of the people are moderately concerned about the cyber-attacks on SMEs in Bangladesh. However, only 4.4% are not concerned about the impact of cyber-attacks on SMEs in Bangladesh. In addition to that, 26.4% group of students are very concerned about the impact of cyber-attacks on SMEs in Bangladesh whereas less than 15% people are extremely concerned about the impact of cyber-attacks on SMEs in Bangladesh. However, when the university students have been asked about their opinions of effective ways to raise awareness about cybersecurity among SMEs in Bangladesh their answers are given as illustrations:

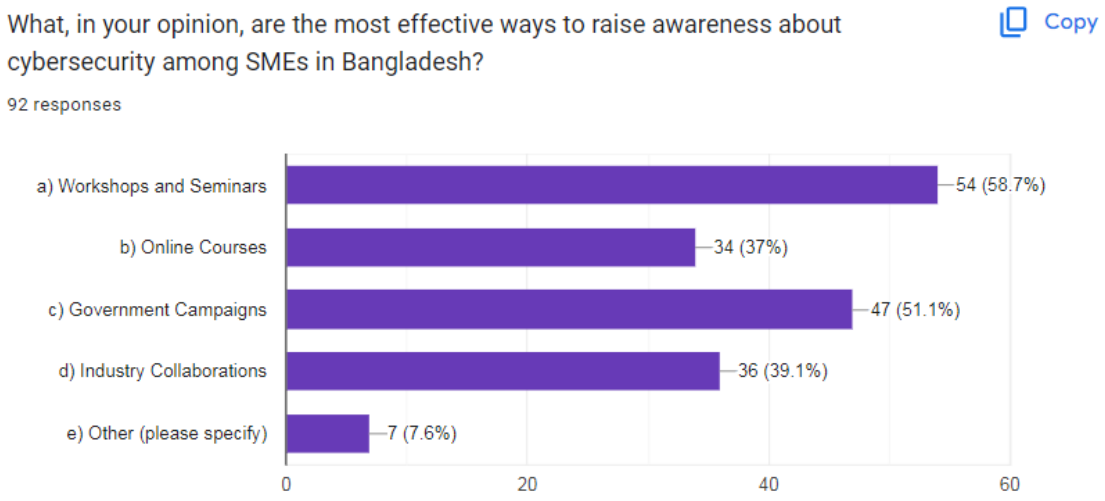


Figure: 03: The most effective ways to raise awareness about the cybersecurity among SMEs in Bangladesh

Majority (58.7%) of the students gave their opinion for workshops and seminars to raise awareness about cybersecurity among SMEs in Bangladesh. But only 7.6% students specified other options to raise awareness. In addition, second effective way for raising the awareness is government campaigns. And rest of the students voted for the industry collaboration (39.1%) and online courses (37%).

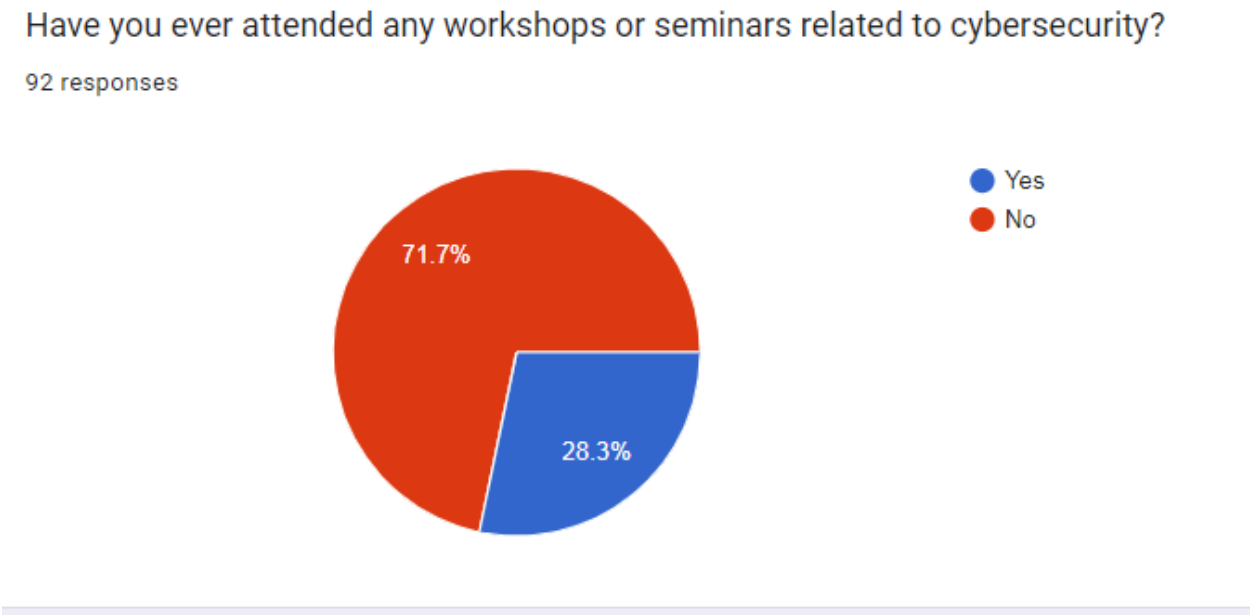


Figure: 04 Percentage of students attending workshops/seminars related to cybersecurity

Lastly, majority of the students (71.7%) have not attended any workshops or seminars related to the cybersecurity and only 28.3% have attended the workshops.

Chapter 05 Discussions:

5.1 Cybersecurity for SMEs in Bangladesh

- Understanding and Awareness: A major issue in Bangladesh is the lack of cybersecurity understanding at the board level. Only 52% of Bangladeshi companies believe their board genuinely understands cybersecurity, despite increasing cybersecurity expenditures and self-assessed maturity in South Asia and Pacific organizations (Ahmed, 2022).
- Primary Threats: The key cybersecurity challenges for Bangladeshi organizations include ransomware, phishing, and data breaches. These threats are consistent with global trends, including the surge in ransomware attacks worldwide (Ahmed, 2022).

- Budget and Skill Shortages: The biggest obstacle to improving cybersecurity in Bangladesh is a lack of budget. Additionally, a lack of skilled workers and support from management also poses significant challenges. About 51% of Bangladeshi IT companies expect difficulty in finding cybersecurity workers in the next 24 months, indicating a significant skills shortage (Ahmed, 2022).
- Frustrations of Cybersecurity Professionals: Professionals in Bangladesh face frustrations such as cybersecurity being a low priority, insufficient budgets, and a perception that cybersecurity is easier than it is or that threats are exaggerated (Ahmed, 2022).
- Education and Training: There's a need for focused cybersecurity education at all levels, including executive and board level, to prioritize critical information and systems protection, and basic cybersecurity education for all staff (Ahmed, 2022).
- Cloud Maturity: A majority of Bangladeshi enterprises are not mature in cloud adoption, which is crucial for improving user experience and security (Ahmed, 2022).
- Regulatory Environment: The National CIRT and the central bank of Bangladesh have released revised IT security guidelines, emphasizing the development of an actionable cybersecurity roadmap (Ahmed, 2022).

5.2 Global Cybersecurity Trends for SMEs

Rising Cybercrime: Cybercrime is expected to increase significantly, costing globally $11.5 trillion in 2023. SMEs are particularly vulnerable, with 43% of attacks targeting them and 60% of affected small businesses going out of business within six months. For instance, in 2020, 55% of SMEs experienced a cyberattack, including ransomware, social-engineering attacks, and malicious insider activity. This vulnerability is due to inadequate cybersecurity systems in many SMEs (“What Is the Impact of Cybercrime on SMEs?,” 2022).

Ransomware and Phishing: Ransomware remains the most common threat globally, with sophisticated phishing attacks being a primary method for cybercriminals. These attacks are increasingly targeting small to mid-size institutions. “SamSam ransomware, operated by BOSS SPIDER, used unpatched server-side software for attacks, including the notable 2018 attack on the city of Atlanta, Georgia, affecting city services and employee computers (*15 Ransomware Examples from Recent Attacks | CrowdStrike*, n.d.)

Business Email Compromise (BEC): BEC attacks are on the rise, often coordinated with phishing. They are spreading beyond email to cloud-based mobile apps.

Fraud and Identity Theft: Significant financial losses are incurred due to fraud and identity theft, with cybercriminals employing a variety of tactics.. Kenneth Gibson, an IT professional in Nevada, opened 8,000 fraudulent accounts and withdrew cash using debit cards, resulting in approximately $3.5 million in losses between 2012 and 2017 (Gareth, 2022).

Cloud Security: Cloud security is the fastest-growing segment in IT security, with increased demand for cloud solutions and rising threats.

Open Source Vulnerabilities: A significant number of codebases contain open-source vulnerabilities, which are exploited by cybercriminals.

Data Breaches: Data breaches are becoming more common, with hackers finding ways to breach even multi-factor authentication technologies.

DDoS Attacks: The frequency and intensity of DDoS assaults have increased significantly, affecting companies of all kinds, including SMEs.

Supply Chain Attacks: Supply chain attacks and self-propagating malware are on the rise, requiring a holistic cybersecurity strategy.

The analysis of the survey findings indicates that while respondents were generally aware of cyberattacks, their levels of concern varied. The term "cyber-attack" is recognizable to most, showing that the idea is well understood. There is a great deal of concern in Bangladesh regarding cyberattacks on (SMEs), as seen by the large number of respondents who expressed extreme or very high concern. Furthermore, based on respondents' preferences and the high attendance rate in workshops and seminars are thought to be the most successful way to increase cybersecurity awareness. This indicates that students respect and attend interactive and collaborative instructional programs, indicating a proactive approach to cybersecurity challenges among the general public.

In conclusion, although though Bangladesh shares many of the same cybersecurity concerns and trends as the rest of the globe, its special context in the cybersecurity landscape is underlined by distinctive issues like board-level understanding, cloud maturity, and regulatory activity.

Chapter 06 Conclusion:

The main findings emphasize how frequently these firms are targeted by cyberthreats and how effective the existing cybersecurity awareness campaigns are.

Main Findings:

- SMEs in Bangladesh's e-commerce industry are vulnerable to a various of cyberattacks, such as supply chain intrusions, malware assaults and account takeover fraud.

- National Cybersecurity Strategy Analysis: Despite of having national cybersecurity strategy of Bangladesh it is blur to SMEs
- Difficulties in Cybersecurity Risk Management: SMEs in Bangladesh faces obstacles in terms of cyber threats and changing IT regulations.
- Financial and Operational Impact: Cyberattacks have a significant negative influence on SMEs, often outpacing their capacity for financial recovery, upsetting supply chains, and posing a severe threat to global economic stability.

Significance of Comprehending Cyber threats and Formulating Awareness Plans:

- It is imperative for (SMEs) in Bangladesh to acknowledge the diverse and dynamic character of cyber dangers, particularly in the rapidly growing e-commerce domain.

Chapter 7: Recommendations

- For Practitioners (SMEs): Adopt stringent cybersecurity protocols, including frequent security assessments, thorough employee education initiatives, and the purchase of cutting-edge security equipment (Siddique, n.d). Developing and enforcing legislation is the first step toward bolstering our cyber security. Governments require appropriate legislative permission in order to make this feasible. One example of this is the creation of cyber security groups (The National Cyber Security Council, 2021).
- For Researchers: Evaluate the efficacy of the cybersecurity procedures in place and consider how technological advances might improve the safety record of SMEs. This could

aid in the creation of creative and practical cybersecurity approaches suitable for Bangladeshi SMEs (Siddique, n.d).

Limitations and Future Research:

- The majority of publications talk about cyber dangers in general rather than concentrating on Bangladesh's SMEs' e-commerce sector. For the future research, research can go into deep analysis of SMEs cyber security awareness strategies. Addressing the unique cybersecurity needs of Bangladesh's (SMEs), particularly those involved in e-commerce, is crucial despite all of the obstacles. This strategy advances the general security and economic stability of the country while simultaneously safeguarding specific enterprises. The conclusions and suggestions of the report emphasize how urgently different stakeholders must work together to enhance Bangladesh's cyber security environment for SMEs.

References:

1. *A Study to Analyse Bangladeshi Consumers' E-Commerce Security and Privacy Satisfactions in Small to Mid-Sized Enterprises*. (n.d.). Docslib. Retrieved November 27, 2023, from https://docslib.org/doc/2089274/a-study-to-analyse-bangladeshi-consumers-e-commerce-security-and-privacy-satisfactions-in-small-to-mid-sized-enterprises

2. Ahmed, T. (2022, August 5). *The Future issues of Cybersecurity in Bangladesh*. Fintech Magazine. https://fintechbd.com/the-future-issues-of-cybersecurity-in-bangladesh/

3. Ashok, S. (2023, May). https://www.emerald.com/insight/content/doi/10.1108/S1569-37592023000110B002/full/html

4. Awal, M. (2022, June 27). *What is the impact of cybercrime on SMEs?* The Business & Financial Times. https://thebftonline.com/2022/06/27/what-is-the-impact-of-cybercrime-on-smes/

5. Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ics-07-2018-0080

6. Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access*, *8*, 174200–174221. https://doi.org/10.1109/access.2020.3026063

7. CrowdStrike. (2023, September 27). *What is a supply chain attack? - CrowdStrike*. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/#:~:text=Software%20supply%20chain%20attacks%20inject,components%20for%20the%20same%20purpose.

8. Correspondent, S. (2021, February 25). *Central bank to investigate Evaly's financial mismanagement*. Prothomalo. https://en.prothomalo.com/business/local/central-bank-to-investigate-evalys-financial-mismanagement#:~:text=If%20a%20product%20is%20not

9. *Cybersecurity for Small and Medium-sized Enterprises (SMEs): Challenges and Solutions*. (n.d.). https://www.linkedin.com/pulse/cybersecurity-small-medium-sized-enterprises-smes-challenges/

10. *Cyber crime trend in Bangladesh, an analysis and ways out to combat the threat | IEEE Conference Publication | IEEE Xplore*. (n.d.). Ieeexplore.ieee.org. Retrieved November 27, 2023, from https://ieeexplore.ieee.org/document/8323800

11. *Cybersecurity for SMEs - Challenges and recommendations*. (2021, June 28). ENISA. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

12. *Cybersecurity: a national priority for Bangladesh*. (n.d.). Ebrary. https://ebrary.net/173519/political_science/cybersecurity_national_priority_bangladesh

13. Decorte, D. (2023b, July 31). *Overpayment Scams: Can Accommodating Buyers be WRONG?* Chargebacks911. https://chargebacks911.com/overpayment-scams/

14. *Disastrous Cyberattacks To Warn Your E-commerce Business*. (n.d.). Www.autogrow.co. https://www.autogrow.co/recent-cyber-attacks-on-companies/

15. Fletcher, D. (2022, September 13). What is triangulation fraud? *ClearSale*. https://blog.clear.sale/what-is-triangulation-fraud

16. Frankenfield, J. (2023, May 24). *Denial-of-Service (DOS) attack: Examples and common targets*. Investopedia. https://www.investopedia.com/terms/d/denial-service-attack-dos.asp#:~:text=In%20a%20DoS%20attack%2C%20rapid,online%20requests%2C%20blocking%20legitimate%20access.

17. Gondek, C. (n.d.). *The Impact of Cyber Attacks on SMEs*. Originstamp.com. https://originstamp.com/blog/the-impact-of-cyber-attacks-on-smes/

18. *Hasson, E. (2021, December 1). Account Takeover Attack (ATO) | Types, Detection & protection | Imperva. Learning Center. https://www.imperva.com/learn/application-security/account-takeover-ato/#:~:text=Account%20Takeover%20(ATO)%20is%20an,data%20breaches%20and%20phishing%20attacks.*

19. *How to protect your website from credit card testing fraud | Versapay*. (2023). Versapay. https://www.versapay.com/resources/how-to-protect-your-website-from-credit-card-testing#:~:text=Credit%20card%20testing%20fraud%20is,information%20to%20identify%20valid%20cards.

20. Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *The Journal of Risk Finance*, *22*(3/4), 240–260. https://doi.org/10.1108/jrf-02-2020-0024

21. *IT Service Management from a Perspective of Small and Medium Sized Companies | IEEE Conference Publication | IEEE Xplore*. (n.d.). Ieeexplore.ieee.org. Retrieved December 5, 2023, from https://ieeexplore.ieee.org/abstract/document/7814550

22. Islam, M. T., Islam, M. F., & Sawda, J. (2022). E-Commerce and Cyber Vulnerabilities in Bangladesh: A Policy Paper. *International Journal of Law and Society (IJLS)*, *1*(3), 184–202. https://doi.org/10.59683/ijls.v1i3.24

23. Magnusson, A. (2023, July 19). Man-in-the-Middle (MITM) Attack: Definition, Examples & More. *strongdm*. https://www.strongdm.com/blog/man-in-the-middle-attack#:~:text=(MITM)%20Attack%3F-,A%20man%2Din%2Dthe%2Dmiddle%20(MITM)%20attack,making%20unauthorized%20purchases%20or%20hacking.

24. Pawar, S., & Palivela, Dr. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

25. Rahaman, M. M. M. (2022). Recent Advancement of Cyber Security: Challenges and Future Trends in Bangladesh. *Saudi Journal of Engineering and Technology*, *7*(6), 278–289. https://doi.org/10.36348/sjet.2022.v07i06.002

26. *Ransomware Examples From Recent Attacks | CrowdStrike*. (n.d.). Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-examples/

27. Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the Unbearability of Uncertainty. *2016 Cybersecurity and Cyberforensics Conference (CCC)*. https://doi.org/10.1109/ccc.2016.29

28. Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal*, *1*(1), 24–46. https://doi.org/10.1108/ocj-03-2021-0004

29. Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*. https://doi.org/10.1111/risa.14092

30. SkillLogic. (n.d.). *Cyber Security Course Bangladesh - Fees 50% Off*. Cyber Security Course Bangladesh - Fees 50% Off. Retrieved November 28, 2023, from https://skillogic.com/cyber-security-certification-course-bangladesh/#:~:text=CYBER%20SECURITY%20CERTIFICATION%20COURSE%20IN%20BANGLADESH&text=The%20CYBER%20SECURITY%20certification%20course

31. Shojaifar, A., & Fricker, S. (2023). Design and evaluation of a self-paced cybersecurity tool. *Information & Computer Security*, *31*(2), 244–262. https://doi.org/10.1108/ics-09-2021-0145

32. Chandna, V., & Tiwari, P. (2021). Cybersecurity and the new firm: surviving online threats.
33. *Journal of Business Strategy*, *44*(1), 3–12. https://doi.org/10.1108/jbs-08-2021-0146

34. *SARDI Cybersecurity Awareness Campaign for MSMEs in Bangladesh*. (n.d.). Inspira Advisory and Consulting Ltd. Retrieved November 25, 2023, from https://inspira-bd.com/case-studies/sardi-cybersecurity-awareness-campaign-for-msmes-in-bangladesh/

35. Siddique, F. B. (n.d.). Cyber Security: Comprehensive Study And Remedies in Bangladesh Perspective. *Www.academia.edu*. Retrieved November 27, 2023, from

https://www.academia.edu/26339497/Cyber_Security_Comprehensive_Study_And_Remedies_in_Bangladesh_Perspective

36. Sharma, K., Singh, A., & Sharma, V. P. (2009). SMEs and Cybersecurity Threats in E-Commerce. *EDPACS*, *39*(5-6), 1–49. https://doi.org/10.1080/07366980903132740

37. Team, C. (n.d.). *Common Vulnerabilities in Cyber Space of Bangladesh*. BGD E-GOV CIRT | Bangladesh E-Government Computer Incident Response Team. https://www.cirt.gov.bd/common-vulnerabilities-in-cyber-space-of-bangladesh/

38. Van Tran, D., Nguyen, P., Nguyen, A. T. C., Vrontis, D., & Dinh, P. (2023). Exploring the influence of government social media on cybersecurity compliance: employee attitudes, motivation and behaviors. *Journal of Asia Business Studies*. https://doi.org/10.1108/jabs-09-2023-0343

39. Valimail, & Valimail. (2023, June 14). *Spear Phishing vs Phishing: The Differences and Examples - Valimail*. Valimail - DMARC SaaS Platform. https://www.valimail.com/blog/phishing-vs-spear-phishing/#:~:text=Spear%20phishing%20is%20a%20specific,specific%20individuals%20in%20an%20organization.

40. *What is friendly fraud? Chargeback fraud explained | Stripe*. (2023). https://stripe.com/resources/more/what-is-friendly-fraud#:~:text=Sometimes%2C%20friendly%20fraud%20occurs%20when,company%20about%20the%20stolen%20card.&text=Impulse%20buying%20can%20also%20lead%20to%20friendly%20fraud

41. What is the impact of cybercrime on SMEs? (2022, February 16). *CGTN*. https://news.cgtn.com/news/2022-02-16/What-is-the-impact-of-cybercrime-on-SMEs--17H6k6M2P04/index.html

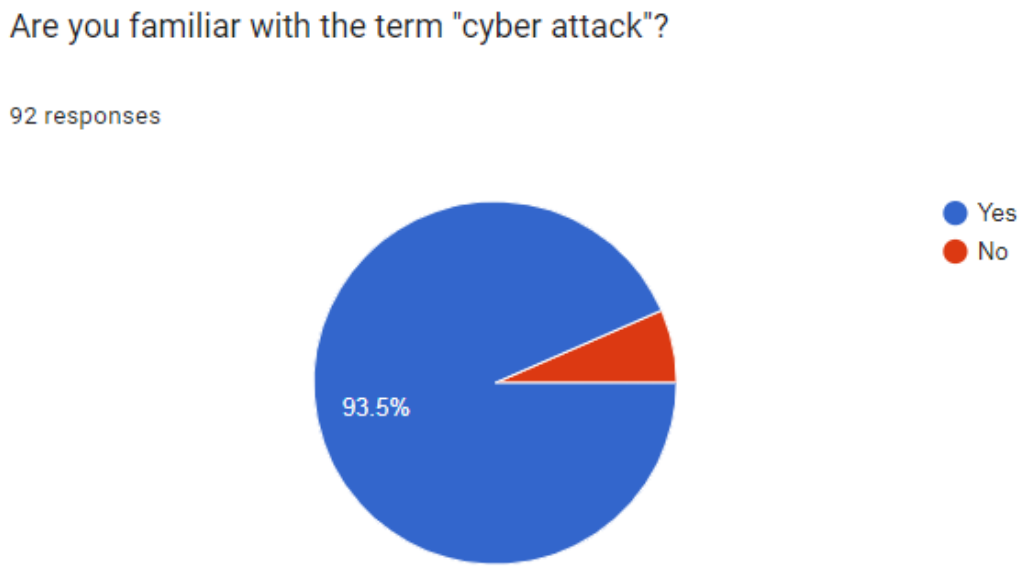
42. *What is a malware attack? Definition & best Practices | Rapid7*. (2023). Rapid7. https://www.rapid7.com/fundamentals/malware-attacks/#:~:text=A%20malware%20attack%20is%20a,command%20and%20control%2C%20and%20more.

43. *What is SQL Injection (SQLi) and How to Prevent Attacks*. (2022, July 21). Acunetix. https://www.acunetix.com/websitesecurity/sql-injection/

44. *What is Spoofing?* (2023, November 9). Forcepoint. https://www.forcepoint.com/cyber-edu/spoofing#:~:text=Spoofing%20is%20the%20act%20of,Name%20System%20(DNS)%20server.

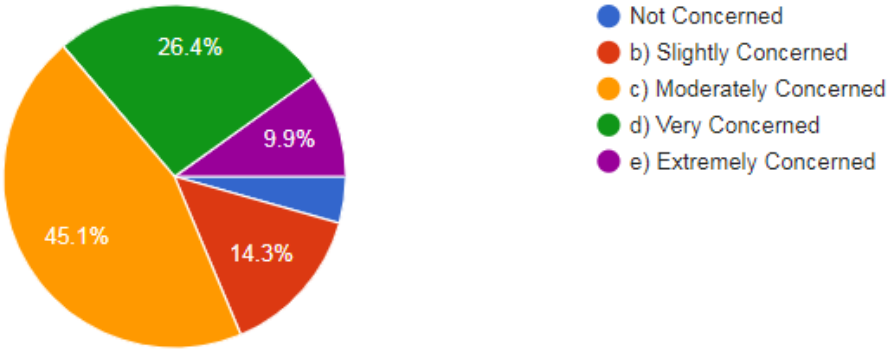
45. Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. Journal of Advanced Nursing, 52(5), 546–553. doi:10.1111/j.1365-2648.2005.03621.x

Appendix:


Are you familiar with the term "cyber attack"?
92 responses
93.5%
Yes
No

How concerned are you about the impact of cyber attacks on SMEs in Bangladesh?

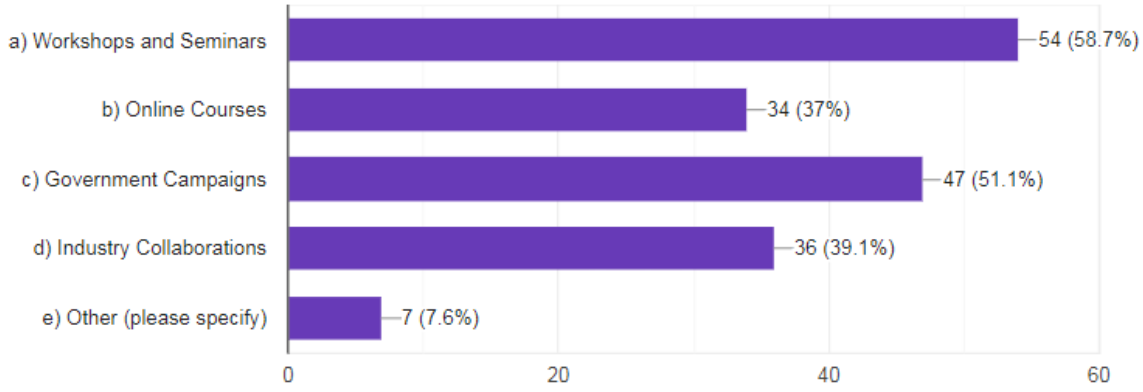
91 responses



What, in your opinion, are the most effective ways to raise awareness about cybersecurity among SMEs in Bangladesh?

Copy

92 responses



Have you ever attended any workshops or seminars related to cybersecurity?

92 responses