

Report on
Demands Of Cybersecurity In Bangladeshi Financial Sector

By

Fatema Tuz Zohra

17204058

Major in Marketing and Human Resource Management

BRAC Business School

BRAC University

An internship report submitted to the BRAC Business School (BBS) in partial fulfillment of the requirements for the degree of Bachelors of Business Administration (B.B.A)

BRAC Business School (BBS)

BRAC University

June, 2022

© 2022 BRAC University

All rights reserved.

Declaration

It is hereby declared that

1. The internship report submitted is my/our own original work while completing my 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 have acknowledged all main sources of help.

Student's Full Name & Signature: _____

Fatema Tuz Zohra

ID:17204058

Supervisor's Full Name & Signature: _____

Mr. Shamim Ehsanul Haque

Assistant Professor, BRAC Business School

BRAC University

Letter of Transmittal

Mr. Shamim Ehsanul Haque

Assistant Professor

BRAC Business School

BRAC University

Subject: Submission of the Internship Report

Dear Sir,

It is a great pleasure to submit the internship report that I have prepared for the last three months in Enterprise Infosec Consultants (EIC) under the marketing department. The report's title is **'Demands of Cybersecurity in the Bangladeshi Financial Sector.'** This report is prepared to fulfill all the requirements of my internship program. In my report, I have mentioned and described the work process followed by my assigned department, tried to identify a few drawbacks, and provided some recommendations from my undergrad learnings. I believe that the experience and knowledge I have gathered from my Internship period will be helpful for my upcoming professional career.

Lastly, I would like to thank you for your excellent guidance and support in preparing the report. I, therefore, pray and hope that you would kindly accept my report and oblige thereby.

Thank you.

Yours sincerely,

Fatema Tuz Zohra

Id: 17204058

BRAC Business School

BRAC University.

Non-Disclosure Agreement

This agreement is made and entered into by and between Enterprise Infosec Consultants. and the undersigned student, Fatema Tuz Zohra, of BRAC University.

**This page is for Non-Disclosure Agreement between the Company and The Student

Fatema Tuz Zohra

BBA Program, BRAC Business School

ID: 17204058

Major in Marketing and Human Resource Management

26, June, 2022

Preceding authorities Sign, Seal and

Date

Acknowledgment

It would have been impossible for me to complete this report if I had not received support from the people throughout the past 3 months. First of all, I would like to thank my internship supervisor, Mr. Shamim Ehsanul Haque, Assistant Professor, BRAC Business School, for granting me to write a report on this exciting topic. All his guidance and support helped me to complete my internship report promptly. Secondly, I would like to thank my workplace supervisor, Md. Faridul Islam played a vital role by assigning me various interesting projects and tasks, which allowed me to gain more knowledge about practical corporate life and helped me enhance my skills and abilities. During my internship, his constant support and guidance allowed me to complete my internship program successfully at Enterprise Infosec Consultants (EIC). Along with that, I would like to thank all the team members and HR for providing me with all the support throughout my internship journey.

Supervisor's Permit

This is to confirm that Fatema Tuz Zohra, ID No: 17204058, BBA Program, BRAC Business School, Major in Marketing and Human Resource Management, has completed the temporary position report on "Demands Of Cybersecurity In Bangladeshi Financial Sector" as the fractional satisfaction of a Bachelors of Business Administration (BBA) degree from BRAC University.

This internship report has been arranged beneath my recommendation, and it is of genuine exertion completed effectively.

Workplace Supervisor Sign, Seal and Date

Executive Summary

This report is the comprehensive highlight of my whole internship experience at Enterprise Infosec Consultants. It is aimed to portray to the whole company and my research project, which is based on **‘The demand of cybersecurity in the Bangladeshi financial sector.’** This report estimates the Enterprise Infosec Consultants overall business and the day to day operations among the three departments. It shows an analysis of the management and marketing practices and their operation, information system, and financial performance. In addition, Porter’s five forces model and SWOT analysis of the organization are also portrayed in this report. Furthermore, this report has in-depth information regarding the demand for cybersecurity in Bangladesh’s financial sector, the cyber risks of the banks in Bangladesh, ways to combat cyberattacks, the government's investment in cybersecurity measures, and how cybersecurity can ensure safety to country’s financial sector.

Table of contents

Letter of Transmittal.....	1
Acknowledgment.....	2
Executive Summary.....	3
List of tables.....	7
List of figures.....	8
Chapter 1: Overview of Internship.....	9
1.1 Student Information.....	10
1.2 Internship Information.....	10
1.2.1 Company Details.....	10
1.2.2 Internship Company Supervisor’s Information.....	10
1.2.3 Job Scope.....	10
1.3 Internship Outcomes.....	11
1.3.1 Student’s contribution to the company.....	11
1.3.2 Benefits to the Student.....	11
1.3.3 Problems/ Difficulties faced during Internship Period.....	11
1.3.4 Recommendations.....	12
Chapter 2: Organization Part.....	13
2.1 Introduction.....	14
2.1.1 Objective.....	14
2.1.2 Methodology.....	14
2.1.3 Limitation.....	14
2.1.4 Significance.....	14
2.2 Overview of the company.....	15
2.2.1 Background.....	15
2.2.2 Mission, Vision, Core Values.....	17
2.2.3 Organization Structure.....	18

2.3 Management Practices.....	18
2.3.1 Work Relationships.....	19
2.3.2 Attitude towards the customer and partners.....	19
2.3.3 Work attitude.....	19
2.3.4 Human Resource Planning Process.....	19
2.4 Marketing Practices.....	20
2.4.1 Market strategy.....	21
2.4.2 Target customers, targeting and positioning strategy.....	22
2.4.3 Marketing channels.....	22
2.5 Financial performance & Accounting practices.....	24
2.6 Operations Management and Information Systems Practices.....	26
2.6.1 Operations Management.....	26
2.6.2 Information System Practices.....	27
2.7 Industry and competitive analysis.....	28
2.7.1 Porter Five Forces Model.....	29
2.7.2 SWOT Analysis.....	30
2.8 Summary & Conclusions.....	31
2.9 Recommendations/ Implications.....	32
Chapter 3: Project Part.....	33
3.1 Introduction.....	34
3.1.1 Literature review.....	35
3.1.2 Objective.....	36
3.1.3 Significance.....	36
3.2 Methodology.....	37
3.3 Findings & Analysis.....	38
3.3.1 Cyberattack risk of the financial sector in Bangladesh.....	38

3.3.2 Investment in cybersecurity by the government.....	39
3.3.3 The legal structure to combat cybercrime in Bangladesh.....	40
3.3.4 Data Analysis.....	42
3.4 Summary & Conclusion.....	.48
3.5 Recommendations/ Implications.....	48
3.6 References.....	50

List of tables

Table 1: EIC brand, tagline, positioning strategy.....	22
Table 2: SWOT Analysis.....	30
Table 3: List of cyberattacks.....	39

List of figures

Figure 1: Company logo with tagline.....	15
Figure 2: PCI DSS Compliance, ISO27001 controls, VAPT.....	16
Figure 3: Bank and NBFIs Clients.....	16
Figure 4: Other clients.....	17
Figure 5: Logo of Mission, vision, values.....	17
Figure 6: Management strategies and Employee motivation.....	18
Figure 7: Social media engagement.....	23
Figure 8: Newspaper advertisement.....	23
Figure 9: Providing certificate to IPDC on project completion.....	24
Figure 10: Providing certificate to Lanka Bangla Finance Ltd.....	24
Figure 11: Annual Report 2018.....	25
Figure 12: Annual Report 2019 & 2020.....	26
Figure 13: Porter Five Forces Model.....	29
Figure 14: Cyber risk of Bangladeshi Banks.....	38
Figure 15: Cybersecurity budget.....	40
Figure 16: Number of respondents.....	42
Figure 17: Feeling while using the internet.....	43
Figure 18: Victimized of cybercrime.....	43
Figure 19: Trend analysis of cyberattack.....	44
Figure 20: Most cyber-attacked sector.....	45
Figure 21: Cyber risk of Bangladeshi banks.....	45
Figure 22: Cybersecurity strategy.....	46
Figure 23: Demand pf cybersecurity.....	47
Figure 24: Cybersecurity ensuring the safety of the financial sector.....	47

CHAPTER 1
OVERVIEW OF INTERNSHIP



Secure your business

1.1 Student Information :

Name : Fatema Tuz Zohra

Id: 17204058

Program: Bachelors of Business Administration (BBA)

Major/ Specialization : Marketing & Human Resource Management

1.2 Internship Information :

1.2.1 Internship Period: 4.5 months (August 16 – December 30, 2021)

Company Name: Enterprise Infosec Consultants (EIC)

Department/ Division : Marketing Department

Address: House-15, Road-7, Block C, Niketon, Gulshan, Dhaka-1212, Bangladesh.

1.2.2 Internship Company Supervisor's Information :

Name: Md. Faridul Islam

Position: Sales Manager, Marketing Department.

1.2.3 Job Scope :

Job description, duties, and responsibilities :

- As a marketing intern, I had to research the latest trend and perform market analysis
- Then, I had to prepare digital content for the social media platform
- I have prepared detailed promotional presentations for their different services
- Reaching out to customers and potential leads, attending initial meetings with the supervisor
- Researching and evaluating competitor marketing and comparing their SWOT analysis
- Lastly, assisting with day-to-day administrative duties such as preparing different excel sheets, updating them, making new content for social media, communicating through different platforms.

1.3 Internship Outcomes :

1.3.1 Student's contribution to the company :

I had tremendous contributions as a marketing intern during my internship at Enterprise Infosec Consultants (EIC). I was allowed to perform my job roles very professionally. I have contributed complete dedication from doing thorough market analysis and research, reaching out to potential customers and leads, and assisting in daily administrative tasks to visiting clients. Firstly, I was given the opportunity to prepare different marketing content for their social media platform. I had prepared various designs for their product brochure, such as four different brochures for four different products (ISO27001, PCI DSS, Vulnerability Assessment & Penetration Testing, SWIFT CSP Assessment), which was later presented to the company's Managing director. Then I had to do market research about our competitors our potential customers and update them in an excel file. Finally, I was actively involved in visiting our potential leads and initial meetings with my supervisor, who guided me throughout the internship journey.

1.3.2 Benefits to the Student:

Enterprise Infosec Consultants is one of the local companies in Bangladesh which has created a massive demand in the cyber security field. Therefore, they provided me with an opportunity to work here as a marketing intern. As a result, I gained so much knowledge and experience in the marketing field, which was immensely rewarding. In my four-month internship period, I learned about the daily administrative activities of the marketing team and where I was able to learn and groom myself by connecting the academic learnings with the corporate world. In addition, this internship opportunity has helped me improvise and evolve my traits and helped me develop in various ways. For instance, I used to have communication problems or gaps before. I was not particularly eager to communicate with others, but this internship opportunity revealed the importance of communication. Lastly, I have learned to value time and the importance of time management, which made me more punctual than before. Also, it has enhanced the organizational and professional skills in the work environment. To conclude, this internship period has benefited me in both ways, personally and professionally.

1.3.3 Problems/ Difficulties faced during Internship Period :

In Enterprise Infosec Consultants, my scope of learning was enormous. Therefore, despite having good bonding in the workplace, I would like to mention some difficulties and hardships. Firstly, I felt like there were some gaps in the communication process among the employees of my department and the other department. For example, there are other three departments, including the HR team, Governance Risk Compliance team, Vulnerability assessment, and Penetration testing team. However, if any dispute arises, They tend to

communicate less and keep the grudge themselves rather than share it. If I needed any help with any work-related problem, the other teams were quite busy. They tend to pay less attention to the marketing team, and being a single female employee in the marketing team, and I somehow felt some dominance. However, I could not learn more things and reveal my potential.

1.3.4 Recommendations :

Enterprise Infosec Consultants has provided me with an excellent opportunity to learn many new things, create my potential, and develop my skills which will help me in my future. In addition, they have allowed me to specialize in my area of interest through this internship period. However, if I had to recommend something to the company, then I would like to mention a few things which are given below :

- ✓ They can hire more female employees to increase the number of female employees, and the other female employees might feel more comfortable in the workplace.
- ✓ Secondly, they can take online classes or sessions regarding different activities to better the workplace environment, such as training and development.
- ✓ Lastly, they must do proper planning in dividing the activities in a team, which will help the employees work more efficiently. These recommendations might help the organization prosper more regarding employees' perspectives.

CHAPTER 2
ORGANIZATION PART



2.1 Introduction

2.1.1 Objective :

This report aims to understand how Enterprise Infosec Consultants is currently performing and operating, which has allowed me to analyze their strategies to manage their day-to-day activities. However, getting to know more about the company's details will help me know about their management practices and culture. Therefore, this report focuses on how the company works internally, including its management practices, marketing channels, operation and information system, financial performance, and competitive analysis. Also, it focuses on how they build coordination among the departments of the organization.

2.1.2 Methodology :

In order to prepare this report, to know more details about the company, I had to collect and analyze both quantitative and qualitative data while working at Enterprise Infosec Consultants. By using primary and secondary resources such as personal observations, interviews, and literature reviews, I collected these data with the help of my supervisor Md. Faridul Islam. He helped me to get access to various resources. However, I had to interview my other colleagues from different departments to know more about their department, how they operate, what type of tasks they do. In addition, I had to read online about the company's management practices. In addition, I had to go thoroughly about the company's annual reports to understand the financial performance properly.

2.1.3 Limitation :

During my internship, while preparing this report, the limitation I faced was data sharing. During the timeline of my internship learning, I had come across several data which were very confidential, and it was limited for me to share every part because of the confidentiality. However, with the help of my colleagues, I was able to come up with alternatives which helped me complete the report.

2.1.4 Significance :

While preparing this report, the most significant outcome was to get a clear vision or idea about how the different departments of Enterprise Infosec Consultants operate to achieve one goal. The strengths and weaknesses of this company came to my knowledge while preparing this report. I tried my level best to portray my educational and internship experience for the readers to get an in-depth idea about the operations and practices of Enterprise Infosec Consultants.

2.2 Overview of the company :

2.2.1 Background :

The importance of cyber security has been irreplaceable in recent times because we all know it protects the data, information, and devices safe from various cyber-attacks and threats. However, unfortunately, a less developed country like Bangladesh suffers from a cyber security crisis.



Figure 1: Company logo with tagline

Enterprise Infosec Consultants is a leading cybersecurity company that focuses on reducing cyber threats from your organization. With an aim to provide the best information security services to its valued clients, the company started its journey in 2016. Initially, EIC engaged its clients with IT Audit and Cyber Security Consultancy services. However, the knowledge gained over the years for protecting information assets from hacker attacks fueled our evolution into exploring more aspects of information security, compliance, testing, and information system governance engagements.

EIC has expanded its services and onboarded different cyber security solutions and training programs to fulfill the increasing demands of the clients. In addition, EIC provides professional consulting services in compliance auditing. For instance, PCI DSS, ISO27001, SWIFT CSP AUDIT, Vulnerability Assessment & Penetration Testing, IT Audit, and Security Operation Center.

EIC Services :

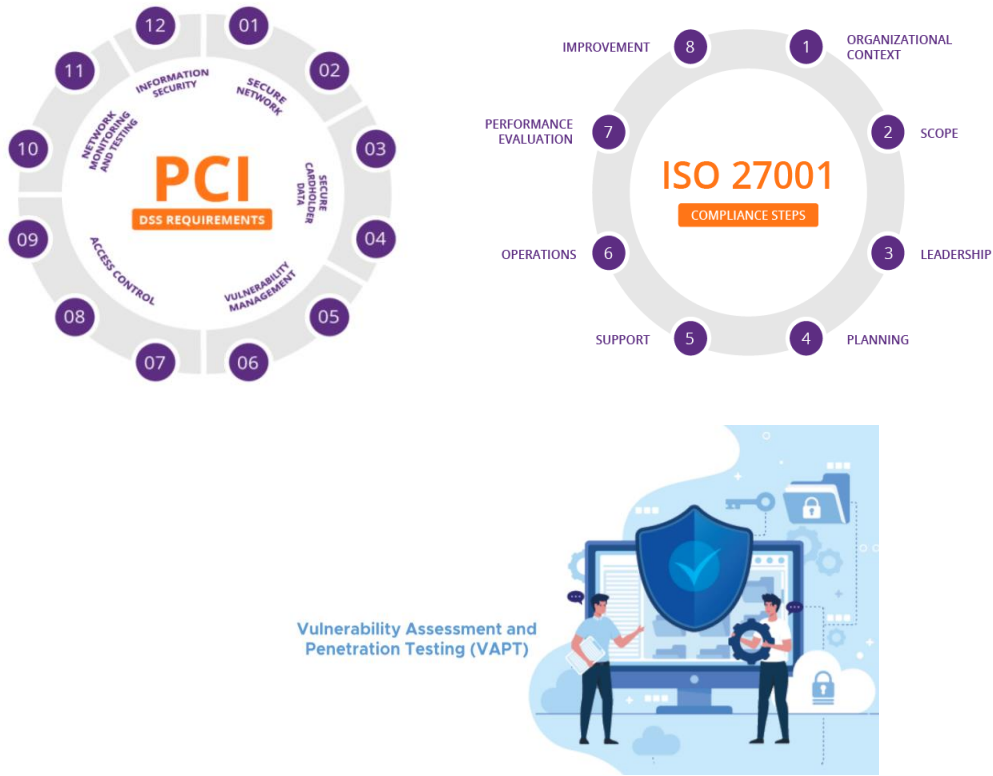


Figure 2: PCI DSS Compliance, ISO27001 Controls, VAPT

Clients of the company :



Figure 3: Bank and NBF clients



Figure 4: Other clients

2.2.2 Mission, Vision & Core Values :



Figure 5: Logo of Mission, Vision, and Values

Mission :

- The company's mission is to become a great cyber security company that sets the best controls to safeguard business and increase the confidentiality, integrity, and availability of business information with in-depth innovation.

Vision :

- To become the leading cyber security companies focused on having power over the risk universe.

Values :



2.2.3 Organizational Structure :

Enterprise Infosec Consultants works in four different departments with the same goal in mind. Such as the Marketing department, Human Resources department, Governance Risk Compliance department, and Vulnerability and Penetration testing department. Along with five stages between the lower-level employees, such as interns and the managing director, the company follows a flat organizational structure. In every department, the structure is followed in the same way, there is one leader in every department, and other employees follow his instructions and works accordingly. As the team is divided with qualified leaders, every department is mutually dependent.

2.3 Management Practices :

Since the beginning, Enterprise Infosec Consultants has maintained a very positive management system. The company follows a democratic leadership style which is also known as participative or shared leadership, in order to achieve its goal.

- The main asset of their company is their employees. Therefore, their main management task concerning employees is to identify, attract, develop, and retain the best.
- First of all, managers consider long-time prospects while making decisions. They aim to choose in favor of long-term prospects if there is a conflict between the long-term and short-term financial results.
- The management tries to ensure that each employee's performance is undeniably correlated with its success and contribution to this success. The company also objectively evaluates each employee's contribution to the company's overall success.
- The significant task of management is to identify the root causes of the problems rather than struggling with the consequences.



Figure 6: Management strategy and Employee motivation

2.3.1 Work Relationships :

Enterprise Infosec Consultants encourages employees to maintain respect, kindness, friendliness towards colleagues. The company wants to ensure that all the involved departments achieve the same goal. Therefore, they help the new employees adapt to their culture as soon as possible. They also try to enhance the ability among the employees to help each other in any situation.

2.3.2 Attitude towards the customer and partners :

Enterprise Infosec Consultants believes that the trust of their valuable customers and partners brings the most outstanding value to the company. Therefore, while interacting with the customers, the company tries to keep an eye on the mutual benefit, which is a 'win-win' situation for both parties. Furthermore, they aim to provide maximum convenience for the customers to work with them. Therefore, customer satisfaction is their primary criterion for employee performance evaluation.

2.3.3 Work attitude :

Enterprise infosec consultants strive for a positive image for their company and respect its history. In order to reach their goal, they believe teamwork is essential, and they try to improve their teamwork skills constantly. In addition, they believe their knowledge, experience, and character create the uniqueness of Enterprise Infosec Consultants.

2.3.4 Human Resource Planning Process :

The human resource planning process in Enterprise Infosec Consultants is very much appreciated, and they follow a simple yet effective planning process which is described below :

- First of all, their goal is to recruit well-educated, ambitious, and flexible people who thrive on change and challenges for the recruitment and selection process. In addition, candidates who are innovative self-confident. Finally, they seek excellent communication skills, leadership skills, strong academic performance, and relevant professional experience.
- They post a job circular on their social media platform, mentioning all the details for the selection process. Then if they find an appropriate candidate after going through all the resumes, their HR team calls the candidate to make sure that the candidate will be able to attend the interview based on their fixed interview date.
- They select a few candidates for the post and call them for the final interview based on their criteria. The interview occurs face to face where the CEO, the Head of HR, and the Head of other departments stay based on the departmental criterion. The interview board tries to make sure the candidate is comfortable and not pressured. First, they ask general and field-related questions to see the candidate's fluency. Then

If the interview goes well, the next step arises a task activity to see the candidate's capability. Finally, if the candidate is selected, The Head of HR sends a confirmation mail to the candidate and asks them to join on the particular date by bringing all the necessary documents.

- The compensation system is also straightforward. All the employees get their salary on the 25th of the month, and also they get a food allowance of 2000 BDT. If any employee is about to get a TDA, they need to make an invoice and submit it to the Head of HR, and HR clears out all the due payments.
- Currently, Enterprise Infosec Consultants does not provide any training and development initiatives, but they plan to make it happen soon. On the other hand, regarding the performance appraisal system, if any sales and marketing department employee helps bring any client, that employee will get a bonus. Also, if any employee is very dedicated and sincere, that employee will get recognition for the hard work.

2.4 Marketing Practices :

Since most of the work is business-to-business-related, marketing has less work. However, the company is still trying to increase the marketing team's efficiency by hiring more employees. Therefore, fulfilling their target marketing is very important at this stage for their brand recognition.

2.4.1 Marketing Strategy

As Enterprise Infosec Consultants is trying to create an advantageous position in the cyber security market with huge demand, their strategies are unique and adaptable. For instance:

- Firstly, they try to understand the power of the existing customers
- They know their targeted customers very well and try to emphasize their valuable position
- Then they try to analyze the market through market research
- They try to identify their core competitors and compare their SWOT analysis.

4p's strategy of Enterprise Infosec Consultants :

➤ **Product:**

Their products and services are all unique. Most importantly, they use local resources to provide onsite service full-time, whereas most competitors are outside the country and only provide online support. In addition, they provide different cyber security services such ISO27001, PCI DSS, SWIFT CSP Assessment, Vulnerability Assessment, Penetration Testing, Security Operation Center, IT Audit.

➤ **Price:**

When it comes to pricing, they try to ensure that the quality is served. They do not charge high, but they do not charge a low price to do business. Their only focus is ensuring the quality according to the price. The pricing of their services varies from organization to organization and depends on the scope of the work.

➤ **Place:**

The company is located in such a place, keeping in mind that most of the work can be done quickly. However, the employees of the other teams, such as the VAPT team and GRC team, need to stay onsite at the customer's organization. Most of them are located in Gulshan, Banani, Tejgaon, which is very close to Niketan, where our office is located, so it is pretty easy and convenient for both employees and the companies.

➤ **Promotion:**

They do not do anything for promotional purposes, but they try to decrease the price rate for their existing customers for relationship building.

2.4.2 Target customers, targeting and positioning strategy

The company's target customers, targeting, and positioning strategy are mentioned below:

Brand Name	Tag line	Product Name	Target customers	Positioning strategy
Enterprise Infosec Consultants (EIC)	Secure your business	ISO27001	IT Companies, Financial industry, Telecoms, Government agencies	Mass marketing, Currently in Dhaka
		PCI DSS	Banks, NBFI	Mass marketing, Currently in Dhaka
		SWIFT CSP Assessment	All banks (public, private)	Mass marketing, Currently in Dhaka
		Vulnerability Assessment & Penetration Testing	Private and public companies, Bank, NBFI, NGO, Educational institutes, super shops, IT companies	Mass marketing, Currently in Dhaka

Table 1: EIC brand, tagline, positioning strategy

2.4.3 Marketing channels

The scope for the marketing channels for the company is quite limited now, but it will expand soon.

Social Media Advertisement :

To cope with the modern era of technology, Enterprise Infosec Consultants is massively engaged in social media platforms to boost their marketing. As we know, social media plays a vital role in today's world, and it grabs the audience's attention, so the company is highly engaged in its social media platform. For instance, they have their Facebook and LinkedIn pages. In addition, they try to grab the customers' attention by posting significant events on their social media accounts.



Figure 7: Social media engagement

Mass Media Platform (Newspaper) :

Enterprise Infosec Consultants was emphasized in the newspaper for completing their PCI DSS Compliant, which is the highest security of payment cardholder with Uttara Bank. It has created massive fame for the company.



Figure 8: Newspaper advertisement

They post their job circular on their LinkedIn page, which grabs the candidates' attention on LinkedIn daily.

They have recently completed their project with IPDC Finance Ltd for ISO27001 and Lanka Bangla Finance for PCI DSS Compliance. They have also provided certification to each company for completing the work successfully.



Figure 9: Providing certificate to IPDC on project completion



Figure 10: Providing certificate to Lanka Bangla Finance Ltd

2.5 Financial performance and Accounting practices :

Over the last few years, Enterprise Infosec Consultants did an excellent job maintaining their financial stability. Even though they have witnessed the covid-19 pandemic, they managed to survive and ensured profit growth. As a result, the last three years financial highlights of Enterprise Infosec Consultants are given below :

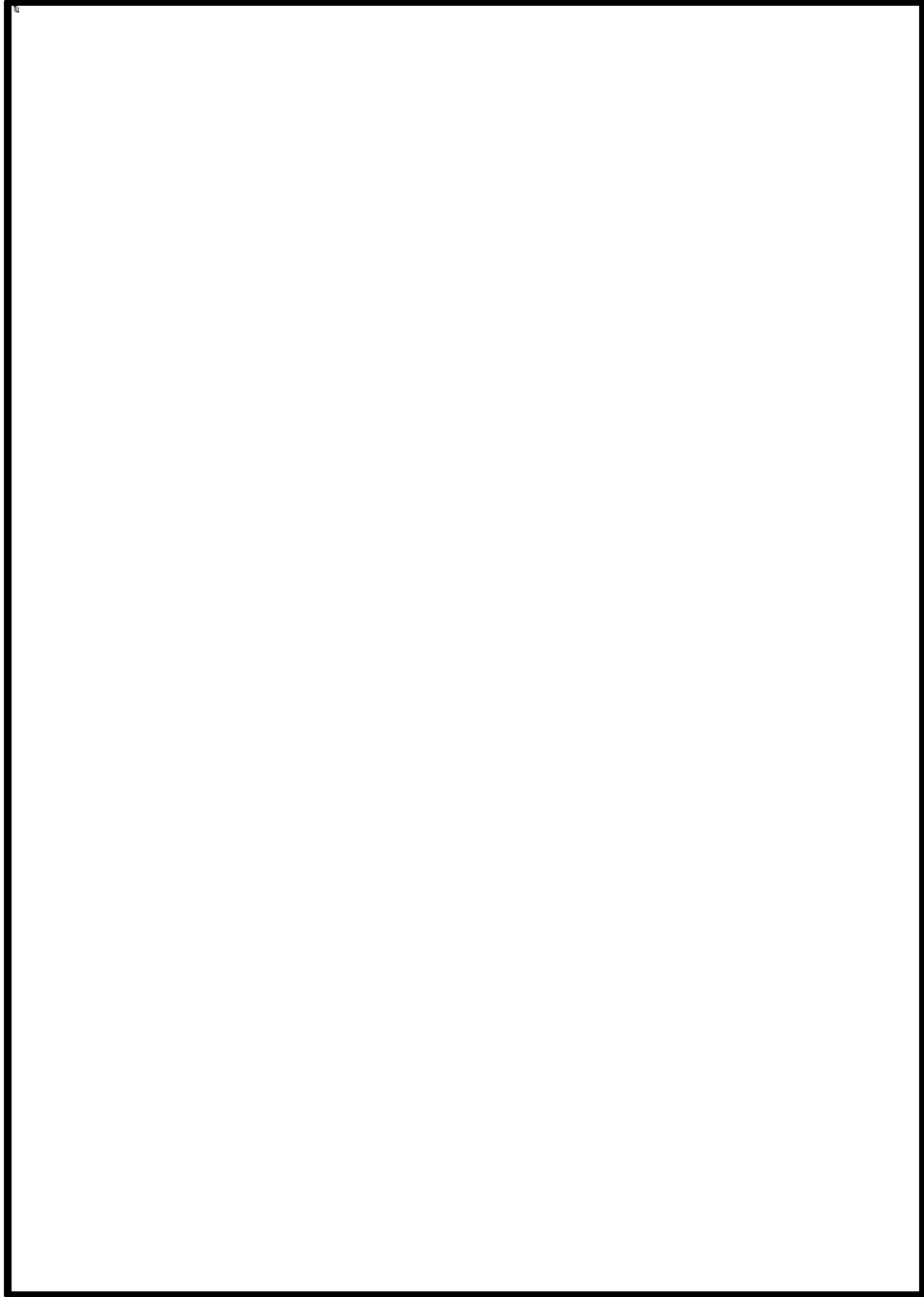


Figure 11: Annual Report 2018


ENTERPRISE INFOSEC CONSULTANTS			
Statement of Profit & Loss and other Comprehensive Income			
For The Year Ended 31 December, 2019			
PARTICULARS	Notes	Amount in Taka	
		31-12-2019	31-12-2018
Operating Income		2,510,200	1,705,214
Non Operating Income		-	-
		2,510,200	1,705,214
Salaries and Allowances	946,394		634,764
Postage, Stamp & Telephone	5,587		3,251
Conveyance & Transport	54,350		33,540
Entertainment Expenses	39,452		25,241
Annual Fee & Others	3,000		3,000
Audit Fees	3,000		2,500
Bank Charges	1,271		1,703
Office Expenses	205,418		102,540
Depreciation	61,185		47,952
Stationary Expenses	95,122		89,542
Office Rent	204,000		132,000
Total:		1,618,779	1,076,032
Net Profit before Tax		891,421	629,182
Income Tax provision		-	-
Net Profit Transferred to Statement of Changes in Equity		891,421	629,182

Saral Azah
Managing Partner

Subject to our separate report of even date

Dated : February 19, 2020
Place : Dhaka

Shafiq Basak & Co.
Chartered Accountants



3

ENTERPRISE INFOSEC CONSULTANTS			
STATEMENT OF COMPREHENSIVE INCOME			
FOR THE YEAR ENDED 31 DECEMBER 2020			
PARTICULARS	Notes	Amount in Taka	
		2020	2019
Operating Income		4,699,452	2,510,200
Non Operating Income		-	-
		4,699,452	2,510,200
Salaries and Allowances		1,104,600	946,394
Postage, Stamp & Telephone		3,851	5,587
Conveyance & Transport		65,240	54,350
Entertainment Expenses		45,600	39,452
Annual Fee & Others		359,450	3,000
Audit Fees		3,000	3,000
Bank Charges		4,035	1,271
Office Expenses		215,418	205,418
Depreciation		760,388	61,185
Stationary Expenses		115,008	95,122
Office Rent		725,400	204,000
Total:		3,401,990	1,618,779
Net Profit before Tax		1,297,462	891,421
Income Tax provision		-	-
Net Profit - Statement of Changes in Equity		1,297,462	891,421


The annexed notes form part of these financial statements.

Managing Partner

Subject to our separate report of even date

Dated : January 19, 2021
Dhaka

Shafiq Basak & Co.
Chartered Accountants



3

Figure 12: Annual Report 2019 & 2020

From the above reports, Enterprise Infosec Consultant's gross and net profit were relatively stable, and the turnover increased. Therefore, it has constantly been increasing its margin profit. At the end of the year 2017, the net profit after tax was 5,41,425, and later on in 2018, it increased to 6,29,182, which means the year's growth was 12.3%. Similarly, due to managements' keen interest in operating efficiency and cost minimization, the following year's net profit was 8,91,421, increased to 26.2% than the previous year. In the last year, we can see the net profit was 12,97,462. Over the years the company's profit kept increasing. To conclude, we can say that the gross and net profit increased along with the revenue.

2.6 Operations Management and Information Systems Practices :

2.6.1 Operations Management :

As a company, Enterprise Infosec Consultants is not a big organization. It falls under small and medium enterprises, so there are two units: the supply chain and operations departments in terms of operations management.

- **Supply chain department**

The supply chain department tries to ensure that the transaction between the raw materials to run the company's day-to-day operation is smooth enough. The supply chain department conducts supply and demand planning in a cybersecurity company the essential equipment used, such as servers, firewalls, desktops, mouse. In addition, the company is planning to include a procurement team by hiring new employees who will manage different assets of the company. The procurement team will ensure that all the equipment is in the inventory before the production plan dates.

- **Operations department**

The operation department tries to ensure the quality of the raw materials such as the equipment used here. In addition, they are doing machine maintenance constantly to ensure the level of productivity and minimum time loss.

2.6.2 Information System Practices :

Enterprise Infosec Consultants uses multiple different software for their daily operations. Although there are different departments, departments use different tools or software to complete their daily tasks. The different software or tools used by the company are given below :

VAPT team :

The vulnerability assessment and penetration testing team uses different types of tools and software to solve their daily activities and tasks, such as ;

- **Nessus:** this application is used to assess all sorts of vulnerabilities
- **Burp suite:** They use this platform to test web application weaknesses
- **Netsparker security scanner:** This application is used for vulnerability scanning and management solution. Also, it can find and exploit weaknesses such as XSS and SQL Injection
- **Intruder:** This is an online web vulnerability tool used to identify a wide range of threats.

Other tools are used, such as Nikto, Maltego, NmapautomaterAcuntix, Metasploit, recon-ng, netdiscover, sqlmap, and hashcat.

GRC team :

The Governance risk compliance team is divided into three sections, and they use software and tools according to their designated sections, such as ISO27001, PCI DSS Compliance, and SWIFT CSP Assessment.

- **(ISO27001:2013) Abriska 27001:**

This tool is specially developed to enable the information security risk assessment with the requirements of ISO27001. This tool is preloaded with ISO2700:2013 controls. It has supported over 200 successful ISO27001 certification projects.

- **PCI DSS Compliance tools :**

To achieve the PCI control objectives and their associated requirements, the team uses different tools and software such as SolarWinds Security Event Manager, SolarWinds Patch Manager, SolarWinds Access Right Manager, ManageEngine ADAudit Plus, Splunk Enterprise, Aruba RFProtect, Manage Engine Eventlock Analyzer, Paessler PRTG Network Monitor.

2.7 Industry and competitive analysis :

Enterprise Infosec Consultants operates in a very competitive field where different big competitors exist, such as PWC Bangladesh, KPMG, Beetles, SSL Wireless, One World, Dhaka Distributors.

In this part of the report, Porter's Five forces analysis model is used to analyze the company's structure and the competitiveness of the cyber security sector of Bangladesh. In addition, SWOT analysis of Enterprise Infosec Consultants will be carried out to assess the company's strengths, weaknesses, opportunities, and threats.

2.7.1 Porter Five Forces Model :

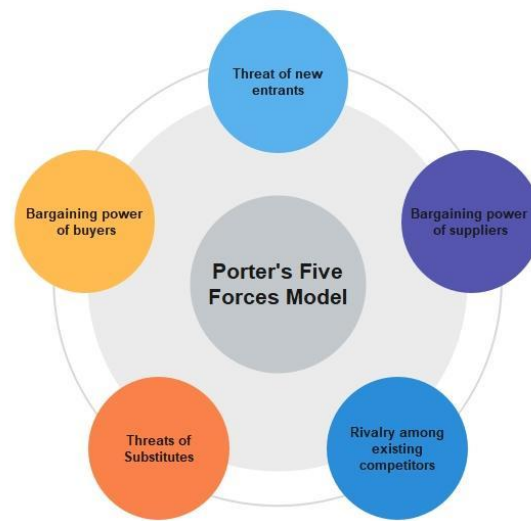


Figure 13: Porter Five Forces Model

- **Threat of new entrants :**

In Bangladesh, setting up a new company in the cyber security sector is challenging as many competitors exist. However, enterprise Infosec Consultants has created a valuable position in the marketplace. In this sector, the chances of the threat of new entrants are moderate as the market is proliferating.

- **Threats of substitutes :**

The threat of substitutes is low as they are trying to develop their services constantly according to the demands and changes of the customers.

- **Bargaining power of buyers :**

In the cyber security industry, the profit margin for each service is moderate to high, and the volume of sales for the company's profitability is dominating. In addition, the price of the services fluctuates depending on the customer's scope, and therefore there is no fixed price for any service. Hence, buyers' bargaining power is moderate to high.

- **Bargaining power of suppliers :**

The company's resources are locally based; the company is the supplier. As the employees will provide full-time onsite support in the customer's organization to complete the project, the supplier's bargaining power is elevated.

- **Rivalry among existing competitors :**

Enterprise Infosec Consultants is one of the leading local companies in the cyber security sector, so the rivalry among existing competitors is very intense. As I have mentioned earlier, there are some huge companies in this sector, and the rival companies constantly try to attack. However, as we know, customers want to get the service at a cheaper rate, and they look for companies who will provide the service at a lower price than the rival companies try to attack. Therefore, although Enterprise Infosec Consultants is trying to establish its brand, the rivalry among existing competitors is high.

2.7.2 SWOT Analysis :

In order to assess the strengths, weaknesses, opportunities, and threats of Enterprise Infosec Consultants, a SWOT Analysis was carried and the outcomes are elaborated in the given table :

S = Strengths	W = Weaknesses
----------------------	-----------------------

<ul style="list-style-type: none"> ● Enterprise Infosec Consultants is one of the local companies in Bangladesh in the cyber security sector. ● The resources are entirely local ● They can provide full-time onsite support, whereas most of the competitors are outside of the country and can provide online support ● The employees are experienced, innovative and sincere about the timeline for the project. ● Recently, they have worked with Standard Chartered Bank, an MNC, and it is an excellent opportunity for them to use it as a reference to grab the other clients' attention. ● Even though the company started its journey in 2016, they are actively working since 2019. The progress is appreciated as they have worked with many companies and are getting many work orders from other companies. 	<ul style="list-style-type: none"> ● In this competitive field, many big competitors exist, such as PWC, KPMG, Beetles, SSL Wireless. ● The company is hugely dependent on the sales department ● They need more employees in the company to cope with the work pressure as there are many upcoming projects. ● They must develop their pricing strategy to sustain the market for a more extended period. ● Training and development session is required in the organization.
O = Opportunities	T = Threats
<ul style="list-style-type: none"> ● The cyber security field in Bangladesh is a minimal area where the opportunities are higher and vast if they can get into a good market position. Then it might create massive demand among the customers. ● They have massive opportunities to work as the company's CEO is very well known in this field, he can use his connections to get more work. ● They can expand their business by introducing new services in their product line. 	<ul style="list-style-type: none"> ● There is a chance of threat of new entrants if Enterprise Infosec Consultants cannot get themselves into a good market position in the next 2-3 years, they might face enormous challenges. ● The competitors might provide the same service at a significantly lower price without ensuring the quality, so the company must be aware in that case. ● Price fluctuation

Table 2: SWOT Analysis

2.8 Summary and Conclusions :

To summarize, Enterprise Infosec Consultants started their journey in 2016 with the vision of becoming the leading local company in Bangladesh in the cyber security field. Currently, Enterprise Infosec Consultants provides professional consulting services in compliance auditings such as ISO27001, PCI DSS, SWIFT CSP, and VAPT. In addition, they have innumerable services, solutions, and training programs with the promise to provide the best leading-edge information security service to their valuable clients.

They are trying to provide an excellent work environment culture to their employees. They believe in equal work opportunities, a friendly work environment, good bonding among the employees through respect. In addition, their management practice is quite impressive, which may lead to longer employee satisfaction. Furthermore, with a unique marketing strategy, they are expanding their marketing channels and creating an advantageous position in the marketplace. Their financial performance also represents that they are maintaining good stability in the profit, which may lead to higher investment in the near future. As Enterprise Infosec Consultants witnessed the covid-19 pandemic, they managed to recover and ensure profit growth while making new potential customers.

2.9 Recommendations/ Implications :

As an intern in the marketing department, Enterprise Infosec Consultants has provided me with an excellent opportunity to learn many new things, create my potential, and develop my skills which will help me in my future. In addition, they have allowed me to specialize in my area of interest through this internship period. Finally, the vast range of responsibilities that I was assigned allowed me to learn many things about the organization.

However, while working as an intern over the past few months, I realize that there is still much scope to develop. If I had to recommend something to the company, I would like to mention that they can hire more female employees to increase their number. The other female employees might feel more comfortable in the workplace. Secondly, they can take online classes or sessions regarding different activities to better the workplace environment, such

as training and development. Lastly, they must do proper planning in dividing the activities in a team, which will help the employees work more efficiently. These recommendations might help the organization prosper more regarding employees' perspectives. Although, I have had a great experience working with Enterprise Infosec Consultants despite all this.

CHAPTER 3

PROJECT PART

Topic: Demands Of Cybersecurity In Bangladeshi Financial Sector



3.1 Introduction :

It is very known to us that Cyber security is a security system that protects the computer network and computing devices where all the critical data are stored, interchange against any attack. Therefore, the importance of cyber security has been irreplaceable in recent times because we all know it protects the data, information, and devices safe from various cyber-attacks and threats. Unfortunately, a less developed country like Bangladesh suffers from a cyber security crisis. Due to the covid-19 pandemic, online banking activities, mobile banking services such as Bkash, Nagad, Upay, and online transactions in e-commerce sites have increased drastically. However, due to the rapid adaption to the new technology, one question arises: 'how safe is the Bangladeshi financial system?' because our country lacks cyber threats' safety. According to Kaspersky Lab, Bangladesh ranked third in countries at risk of smartphone malware attacks. In addition, according to the report, ransomware attacks on computers have increased from 4-5% to 8-11% in Bangladesh. However, in the latest edition of the global cybersecurity index of the international telecommunication union, Bangladesh has provided continuous cybersecurity improvements and secured a position from the 78th to 53rd.

As we know, almost all organizations and enterprises worldwide use computers, devices, servers, and clouds to save their important data. As a result, all the data that belongs to that

company are saved in their database, and they are supposed to be seen and used only by the employees and related persons of the organization. However, sometimes they need to send the confidential data to another place through the internet and ensure it is not leaked. Therefore, there are developed mechanisms that are known as cyber security. Cyber security includes information security, application security, network security, operational security, and disaster recovery or planning. The demand for cyber security is increasing daily, especially after the scamming incident in Bangladesh Bank back in 2016. However, this report highly focuses on the demand for cyber security in the Bangladeshi financial sector, how we can combat the cyber threats, what benefits we can get by implying cybersecurity. Furthermore, I have tried to examine the cyber security scenario in the world with an in-depth emphasis on Bangladesh analytically.

Our country, especially the banks in the financial sector, is at risk of cyber threats. Even after the cyber heist from Bangladesh bank, most banks do not have adequate cyber security to protect their data. According to reports, only 4 out of 60 banks have set up cybersecurity operations with the Bangladesh Bank. The central bank has given written orders to set up cyber security systems from time to time. However, many banks cannot set up a cybersecurity system due to financial stability, and due to lacking a skilled workforce, they are facing this problem. As a result, according to experts, the banking system is now more vulnerable to cyber risks. Due to the speedy enlargement of digital banking, the risk will increase in the near future. Therefore, we can see an immediate demand and need for cybersecurity in all banks while preventing, detecting, and analyzing cybersecurity incidents. After working in a cybersecurity company, I have acknowledged that the banks in our country are facing a severe concern of cyber threats. The majority of the clients in Enterprise Infosec Consultants are banks, and the demand for cybersecurity is massively increasing.

3.1.1 Literature review :

In recent years, cybersecurity has advanced dramatically to keep up with the rapid changes. Naturally, therefore, the demand for it has also significantly increased. It refers to the methods that an organization or company can use to safeguard its data, information, and products. Nevertheless, even two decades ago, the term 'cybersecurity' was barely recognized in Bangladesh. Financial stability is essential for any country, and for that, we need a robust cybersecurity system to protect our data and confidential information. The relationship between cybersecurity strategy and the successful growth of the country is very significant because if the cybersecurity system is not safe in any country, it cannot grow financially (Teoh and Mahmood 2017). To keep the data safe, we need to combat or fight against the cybercrimes that are occurring on a daily basis. A report by Duic, Cvrtila, and Ivanjko (2017), has displayed that they have worked intending to find more long-lasting and effective ways to combat attacks and cybercrimes often happening around the world. They have also

highlighted how these cyberattacks will be a significant threat to international relations. (Bleyder 2012) reported that e-commerce is another significant challenge for Bangladesh's cyber security arena regarding financial transactions such as online banking. He also stated that cyber threats could lead Bangladesh into a severe economic downfall, especially in the banking sector. Due to proper maturity in the new field, an online financial transaction where Bangladesh is a new customer, Bangladesh cannot deny the inevitable consequences. As a result, it will be a significant security concern issue in the upcoming days. The wide usage of credit cards and the rise of electronic payment methods where customers put their personal information such as bank account name, bank account number, cell phone number, Email can cause severe cyber attacks. In addition, in recent times, Bangladesh law enforcement agencies have faced various cyber threats to Bangladesh's online banking sector and other online financial transactions. Apart from these threats, there are other threats in the banking sector known as phishing, which pulls out confidential information from the bank or account holders through deceptive emails. It is affecting a large number of victims in Bangladesh. In such a situation, the victim loses around 100-500 USD per case, and they feel hesitant to go to the police for a complaint which makes the case even more difficult for the law enforcers in Bangladesh (Alam, Md. Shah, personal communication, July 27, 2014). Therefore, The demand for cybersecurity in our country arises from the cases mentioned above. According to the report (Azad, Mazid, Sharmin July 2017), Bangladesh's cybercrime laws and problem areas have been highlighted.

3.1.2 Objective :

➤ **Broad Objective :**

This report aims to find out or analyze cyber security demands in the Bangladeshi financial sector and get the desired outcome or result. Therefore, the broad objective of this report is to find out the demand for cyber security in terms of the Bangladeshi financial sector, the benefits we can get from it, and what implications we might apply for the betterment of the country. Firstly, it is required for me to know about the current demanding situation of cyber security in our country. Then how are the financial institutions looking at this particular matter and the steps they might take for their organization for better protection. Therefore, this report will enlighten unaware people about the importance of cyber security.

➤ **Specific objectives :**

- To find out the cyber attack trend in Bangladesh
- To find out ways to combat cybercrimes
- To find out the percentage of cyber risks of the Bangladeshi banks
- Review and evaluate the investments in cybersecurity measures by the government
- Provide recommendations for further activities

3.1.3 Significance:

This report is about the demand for cybersecurity in the Bangladeshi financial sector, such as banks, nonbank financial institutes, mobile banking services. Due to the covid19 pandemic situation, we adopt the new technology and entirely depend on it. However, the question is, how safe is the financial sector of Bangladesh? As we all know, our country lacks the safety of cyber threats. Cyber-attacks are elementary and familiar in our country compared to other developing countries, creating demand for cyber security. The significance of cybersecurity is indescribable because it plays a massive role in protecting our essential data. Every organization or company consists of confidential data that cannot be shared with anyone except the organization's employees. Hence, cybersecurity plays a crucial role in protecting those data from cyber attacks or threats. Therefore, we can say the demand for cybersecurity is increasing as it is creating awareness among the financial industry, especially after the robbery case of the Bangladesh Bank. If we cannot measure its significance, we would not know about the benefits of implying cybersecurity. Thus, to combat the cyber attacks, it is required for me to know about the demanding situation of cybersecurity in our country and how the financial organizations are looking into this matter to protect their confidentiality. I will be utilizing my internship experience and textbook knowledge. Working in Enterprise Infosec Consultants, a cybersecurity consulting company, helped me know more about cybersecurity, cyber-attacks, and threats and how financial companies are taking the help of cybersecurity to protect their confidential data. Anyone searching to look for the demand of cybersecurity in the financial sector for opening up a new company or organization will find something of significance through this report.

3.2 Methodology

The research done in this report to find out the demand for cybersecurity in the Bangladeshi financial sector is based on preliminary information gathered from two various sources, such:

- **Primary sources**
- **Secondary sources**

The report requires analyzing quantitative and qualitative data obtained through primary and secondary resources.

In the case of primary data, those data have been obtained by examining Enterprise Infosec Consultants' annual reports of the last three years. Furthermore, to get access to crucial primary data, a questionnaire was distributed among the company's employees. In addition, many primary data were obtained through observation of activities at the workplace while directly working with the supervisor to make a technical proposal to send to the clients.

For the secondary resources, reviewing different research papers and reports published by various people helped me understand our country's current demanding cybersecurity situation and what might happen to the financial sector if they do not maintain cybersecurity properly. Furthermore, I have gone through different newspapers, articles, and websites regarding the demand for cybersecurity in our financial sector and how much safety they can ensure to combat cyber threats. In addition, I have explored different past activities of Enterprise Infosec Consultants regarding cybersecurity awareness, which helped me better understand its demand for the financial sector.

This report will be helpful for students who want their career in cybersecurity, researchers, and academicians who are willing to gain more in-depth knowledge about cybersecurity or about Enterprise Infosec Consultants and especially the culture and operations of the company.

3.3 Findings and Analysis

3.3.1 Cyberattack risk of the financial sector in Bangladesh :

Bangladesh is a less developed country, but they are trying to develop in every aspect. However, because of less knowledge about information access, Bangladesh has limitations. Therefore, cyberattacks are often occurring now and then, and it is one of the main reasons for the financial crisis or downfall in our country. Most of the banks in our country are at a high-security risk. According to (BIBM) Bangladesh Institute of Bank Management, in 2016, around Tk 1,793 crore was invested in the banking IT sector. However, even though after investing a considerable amount of money, this banking sector is not cybercrime-free at all. Recently, cyber security has been a burning question in the banking sector, especially after the Bangladesh Bank heist. In our country, a total of 52% of the banks are at high risk of cybersecurity issues, according to a study of (BIBM) Bangladesh Institute of Bank Management. A graph is provided below for a better understanding of the scenario.

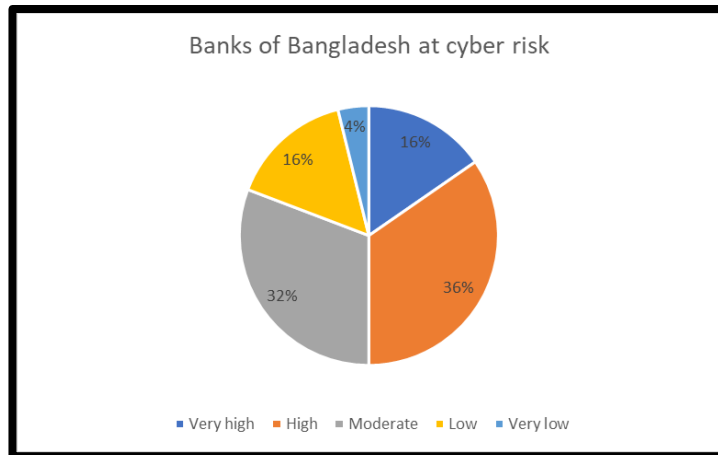


Figure 14: Cyber risk of Bangladeshi Banks

According to Dhaka tribune news, the above chart shows that 16% of banks are at very high risk out of 52% of banks, and 36% are at high risk. Furthermore, risks in 32% of banks are moderate, 12% are at low risk, and the remaining 4% are at very low risk. The Bangladesh Bank Heist incident held on February 4 created a horrible situation in the banking sector where the hackers are still unknown. They tried to steal \$1 billion but somehow managed to get \$81 million, which was sent to Rizal Commercial Banking Corporation in the Philippines and PABC Bank in Srilanka through four various transfer requests. In addition, an extra \$20 million was sent to Pan Asia Banking into a single request. According to the reports of Reuters, the malware's name was evtdiag.exe, and the attackers are called Reuters. A report by Lucian Constantin by PC World stated that the hacker hacked through malware that worked on the swift messaging system. In addition, this malware can delete any incoming message and the confirmation message before sending it to the office printer. On February 4, Thursday, the malware was activated after the working hour. The next day was Friday, which is a holiday in Bangladesh, so no one was there to monitor the transition message. The attacker did not succeed after giving many trying for the transition. However, they kept trying, and after that, they could transfer money through their fake bank accounts. After the weekend on Sunday, when the bank opened, the officials noticed that the malware stopped printing the transition information, so they assumed something wrong had happened. The malware handled the login and out process and controlled the modification and server. The moment they told the Philippines bank to stop the transition, it was impossible because it was the weekend over there. The malware was programmed for activation up to February 6. However, the transition was stopped after identifying the attack. Therefore, the hacker managed to transfer \$81 million. According to the journal of society and change, many bank criminals are destroying the banking sector by using cyberattacks utilizing different electronic mediums for fraudulent activities such as the web, email, and encoded messages (2016). Unfortunately, in the banking sector of Bangladesh, several security breaches have happened in the last few years, which are provided below.

Date of occurrence	Incidents
6 th January, 2013	Human Mind Cracker hacked the site of Islami Bank Bangladesh
2015	A private banks account were hacked, and money was withdrawn
2 nd December, 2015	The hacker broke the network security of Sonali Bank and took control over it for several hours.
February, 2016	Six ATM booths of three commercial banks were attacked
February, 2016	The hackers stole \$81 million money from Bangladesh Bank

Table 3: List of cyberattacks

3.3.2 Investment in cybersecurity by the government :

Compared to other fields, the cybersecurity market is the growing demand in recent times and remains the most expanding one. Nevertheless, unfortunately, we are losing our privacy and confidentiality day by day with the advancement of technology. However, companies and organizations need to invest more to protect their valuable data and information from stabilizing their financial condition to cope with the situation. Therefore, Bangladesh is frustrating compared to the other countries investing in cybersecurity. There are hardly any ICT organizations in the private sector that can allocate and spend considerable money to ensure their network security. Furthermore, the situation in the government sector is making an appearance day by day. In the government organizations, the IT sections are now allocating budget and increasing security for their network and website. According to ICT ministry news, to develop cybersecurity labs in different organizations and companies of the country, the ICT division has undertaken a massive project. According to the market capitalization data by Investopedia and cybersecurity market report by investing news, the graph below represents the investment in cybersecurity of various companies worldwide.

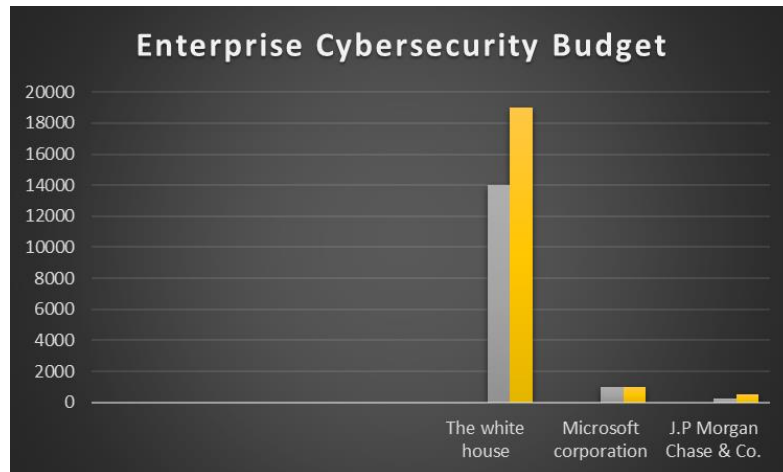
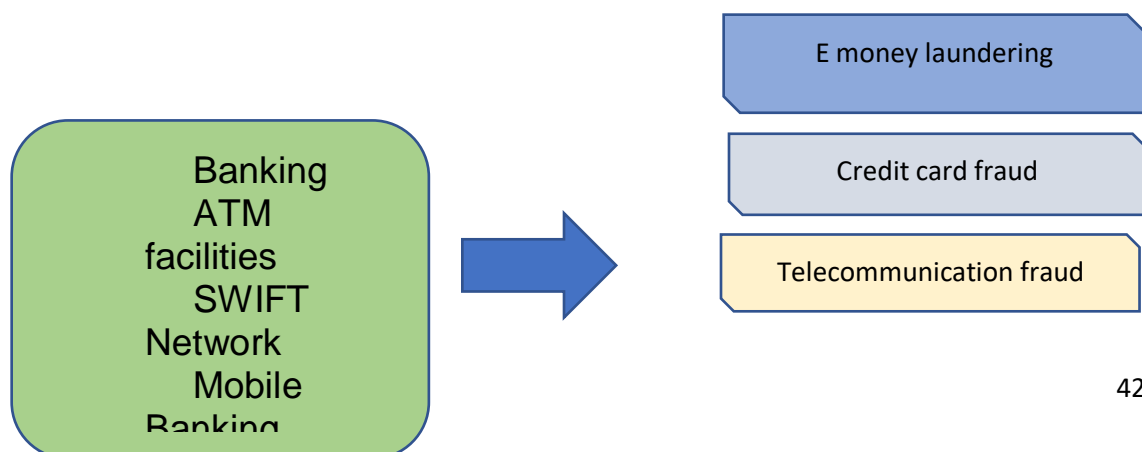


Figure 15: Cybersecurity budget

According to a cybersecurity market report, the Bangladesh government has invested around BDT 40 crore to build up a cyber security branch in the ICT division. After observing the cyber security condition and its demand in Bangladesh, it is inessential to mention that both private and public sectors need to invest a considerable amount of their budget to increase and enhance cybersecurity measures. On the other hand, the private sector, especially banks and organizations, needs to be encouraged to invest in cybersecurity to protect their business from cyberattacks.

3.3.3 The legal structure to combat cybercrime in Bangladesh :

As we know, the term ‘Cyber Law’ is used to describe the legal issues related to the use of ICT – information and communications technologies. An effective cyber law plays a vital role in ensuring that cybercriminals are judged fairly. Furthermore, cyber law is much needed to protect nations against cyberattacks and control the misuse and abuse of technologies.



Fraudelany use of accounts & credit cards

Frauds related to ecommerce

The government and private organizations need to combat cybercrime in Bangladesh. Our government has already taken some measures through the ICT division regarding this issue. Still, it is not enough because hackers are finding ways to hamper and destroy our privacy by messing with our valuable information through damages that take years to recover, especially for a country like us, which is less developed in this sector. The ways to fight against cybercrime is given below :

- **Legal Framework :**

Our government has successfully passed different legal acts to stop digital harassment and fight back the cyberattack. We have various legal acts in our ICT division, such as ICT acts 2006, 2009, 2013 (amendment), draft digital act 2016 [25], [26]. All these mentioned acts combine all the cybersecurity in our country. However, the draft digital act 2016 may be authorized or enacted at the earliest.

- **Computer Emergency Response Team formation :**

Computer Emergency Response Team is also known as CERT. When any instant devastating situation arises due to a cyberattack, this team deals with it. According to the cybersecurity market report, the Bangladesh government has given us 24x7 hours CERT support entitled BdCERT.

- **Training and seminar :**

To make people aware of the cybercrime issues, the government arranges various seminars and workshops in different colleges and universities. These workshops and seminars notify and enlighten people regarding cybercrime activities occurring in our country and worldwide and how to fight them back. In addition, according to the cybersecurity market report, many training programs are held under the supervision of the Bangladesh Computer Emergency Response Team.

- **Code of ethics :**

According to the ACM Code of ethics, each organization should have a culture complying with the code of ethics by their employees. In addition, the universities and other institutions

need to include ICT education and courses on the engineering code of ethics in their curriculum. However, the Bangladesh government has already made ICT education compulsory for both higher and secondary levels, and in this curriculum, the code of computer ethics may be included.

- **Cyber security strategies :**

To combat cybercrime and take immediate decisions when required, each organization must have a strategy. According to the cybersecurity market report, this strategy should be made as per the National Cyber Security Strategy.

3.3.4 Data Analysis :

For the data analysis part, I have performed a survey through a questionnaire and asked the respondents to fill it out. However, the analyzed data are interpreted below through various charts and graphs.

In my survey, the total respondents were 30; out of them, 16 were male, and 14 were female.

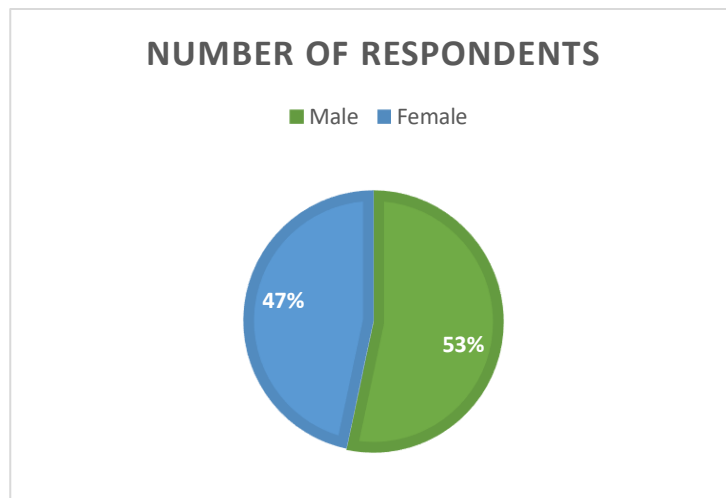


Figure 16: Number of respondents

My first question to the respondents was, ‘**While using the internet, do you feel safe enough?**’ There were three options to this question :

1. Yes
2. No
3. No comments

Out of 30 respondents, 26 were marked on ‘Yes,’ 3 others were marked on ‘No,’ and one was marked on ‘No comments.’

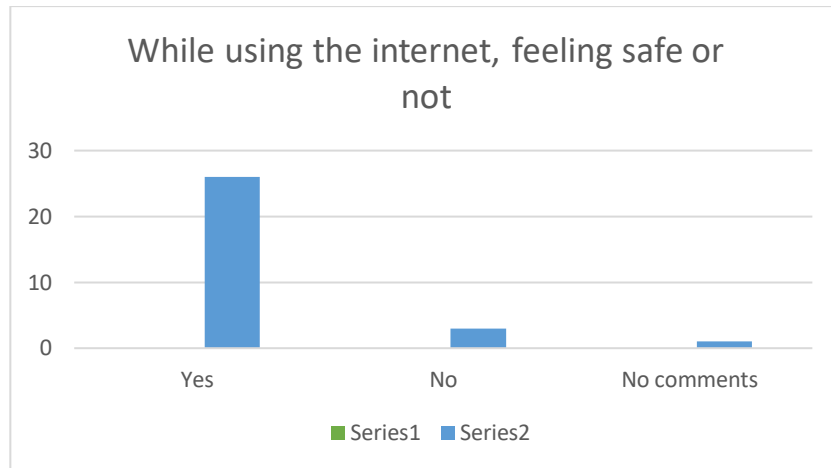


Figure 17: Feeling while using the internet

My second question was, ‘Have you ever been a victim of cybercrime?’

There were two options, ‘Yes’ and ‘No.’ 21 were marked on ‘Yes’ while the rest of the 9 people were marked on ‘No.’

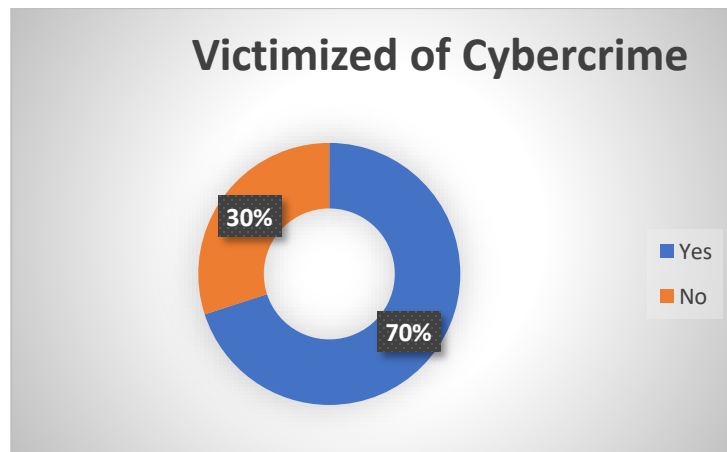


Figure 18: Victimized of cybercrime

My next question was, ‘What do you think about the trend analysis of cyberattacks in Bangladesh?’

There were three options.

1. High attacks
2. Moderate attacks
3. No idea

Out of 30 people, 18 people marked ‘**high attacks,**’ 10 marked ‘**moderate attacks,**’ and the rest of the 2 people marked ‘**No idea.**’

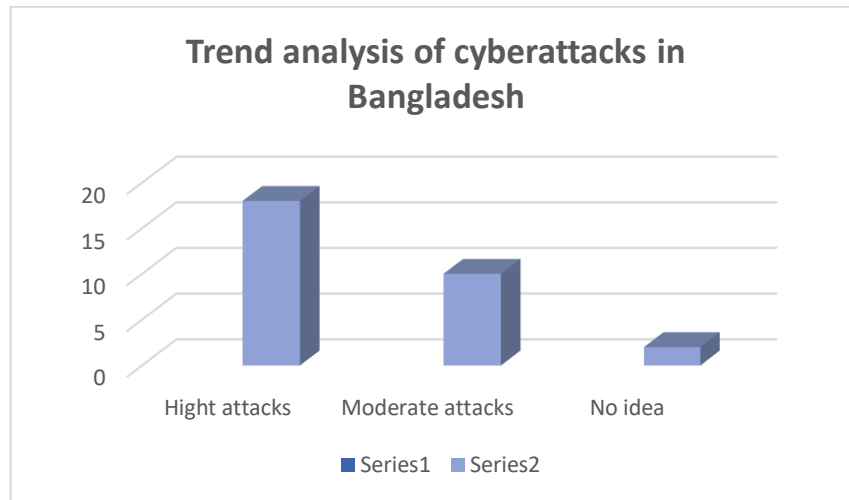


Figure 19: Trend analysis of cyberattack

The fourth question was, ‘**In Bangladesh, what do you think which sectors are mostly attacked?**’

There were three options.

1. Personal
2. State
3. Financial

In this response, 14 people marked ‘**Financial,**’ 9 marked ‘**Personal,**’ and the rest of the 7 marked ‘**State.**’

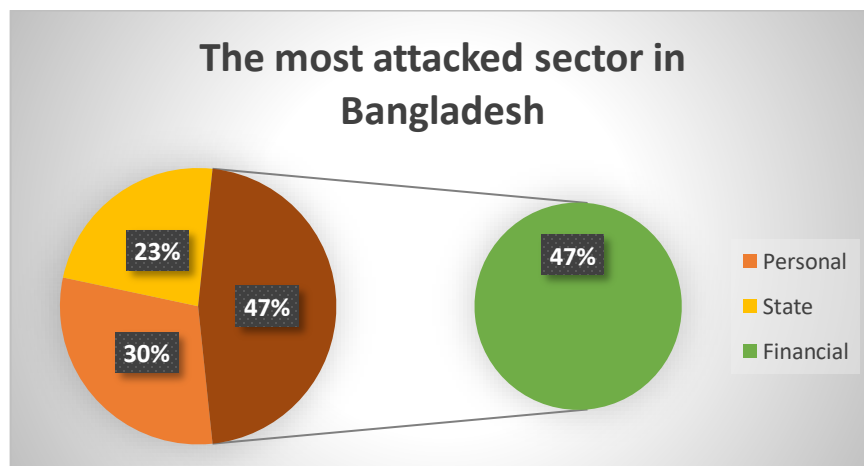


Figure 20: Most cyber-attacked sector

The fifth question was, ‘**Do you think the Bangladeshi banks are at high cyber risk after the Bangladesh Bank heist?**’

There were three options.

1. High risk
2. Average risk
3. Low risk
4. Not sure

20 people responded as ‘**High risk,**’ 5 others responded as ‘**Average risk,**’ 3 responded ‘**Low risk,**’ and 2 responded ‘**Not sure.**’

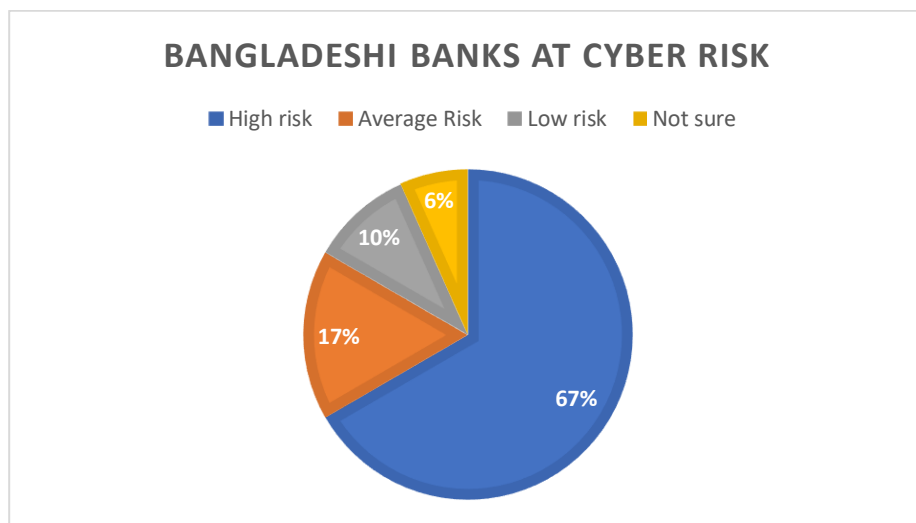


Figure 21: Cyber risk of Bangladeshi banks

The sixth question was, ‘**What do you think about the cybersecurity strategy of Bangladesh?**’

There were three options.

1. Productive
2. Inefficient
3. Needs improvement

Here, 2 people responded ‘**Productive,**’ 17 responded ‘**Inefficient,**’ 11 people responded ‘**Needs improvement.**’

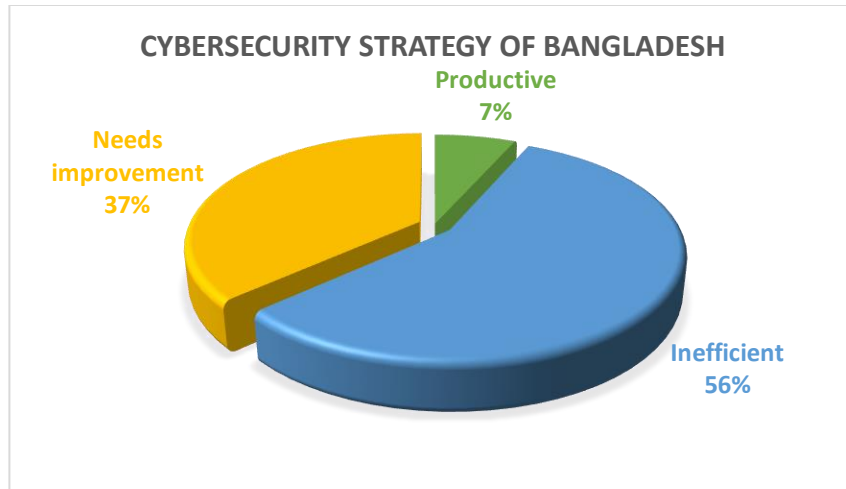


Figure 22: Cybersecurity strategy

The seventh question was, ‘Do you think there is any demand for cybersecurity in the Bangladeshi financial sector?’

There were three options.

1. High demand
2. Moderate demand
3. Low demand

They answered - 17 high demand, 9 moderate demand, and 4 low demand.

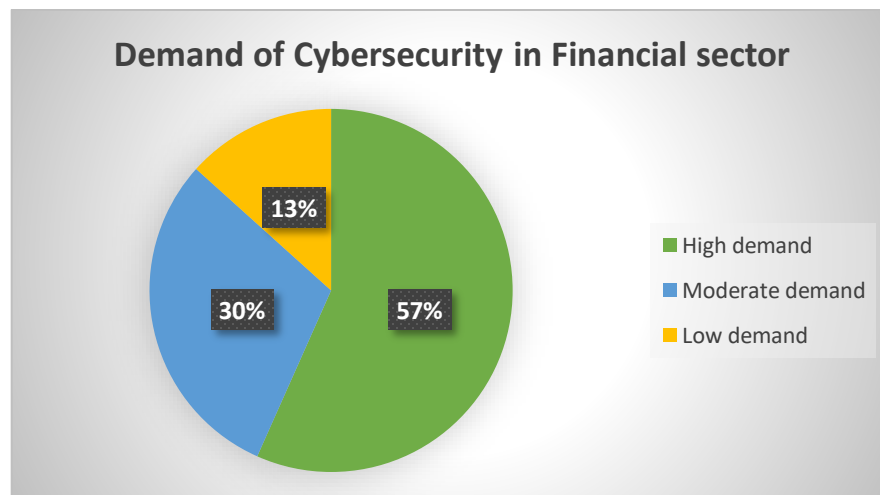


Figure 23: Demand pf cybersecurity

The last question was, ‘Do you think the proper implementation of cybersecurity can make Bangladesh's financial sector safe?’

There were three options,

1. Yes
2. No
3. Maybe

27 answered ‘Yes,’ and 3 answered ‘Maybe’, but one marked the option ‘No’.

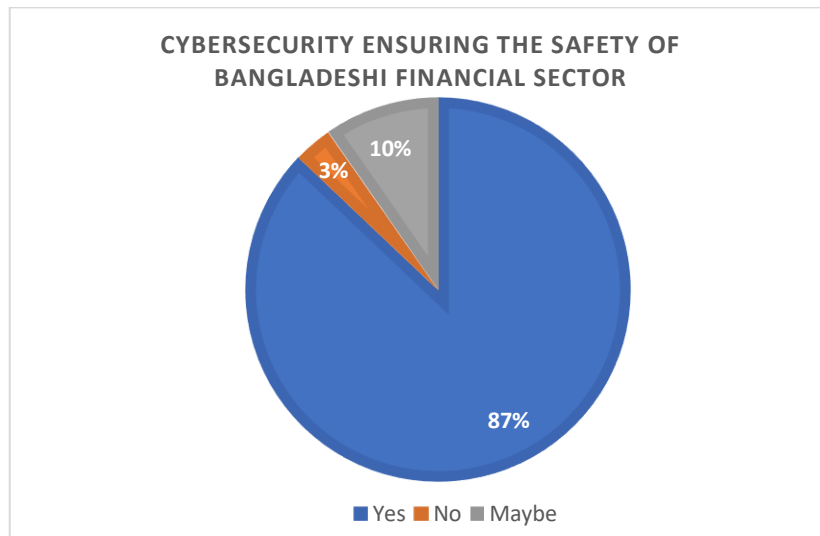


Figure 24: Cybersecurity ensuring the safety of the financial sector

3.4 Summary and Conclusions

To keep our cyberspace secure and safe against cyber-attacks, Bangladesh's current cyber attack tendency stipulates proper attention for maintaining and creating a powerful and workable cybersecurity strategy. This matter needs to consider the country's economic capacity and the availability of talented resources. However, the government of our country has prioritized this issue and invested a considerable amount of money in this sector. However, in our country, a robust cybersecurity strategy is yet to be prepared and put in action because of the vulnerable situation in the financial sector. In this report, I have tried to portray the demand for cybersecurity in the financial sector and how cyberattacks affect us. The increasing demand for cybersecurity, especially in the banking sector due to various cyber crimes, makes people aware day by day. From the findings and analysis, we can see that the banks are at high risk of cyberattacks. Therefore, the government should utilize their investment properly in this sector; otherwise, it will hamper the nation. The ways to combat cybercrimes and the measures to be taken are also

described here. Such as investing in the cybersecurity sector, legal framework, CERT formation, developing training and seminars, building a code of ethics, and creating cyber security strategies. In addition, the government and private organizations must create awareness by holding seminars and training programs. However, to deal with cybercrimes activities, the need for the culture of complying with the code of ethics is also mentioned here. Lastly, in this report, a few strategies are mentioned to enhance the strength of cybersecurity in Bangladesh.

3.5 Recommendations/ Implications

Unfortunately, Bangladesh's cybersecurity has proved to be widely ineffective till now. However, from the analysis of Bangladesh's cybersecurity strategy, a few recommendations are provided for the betterment of the system, which is given below :

- ✓ Private and other organizations must invest more in cybersecurity to protect their business from cyberattacks.
- ✓ Each sector dealing with sensitive and confidential data must be brought under the legal framework.
- ✓ There must be a 24x7 incident response capability from the BdCERT, and the budget of BdCERT should be made more substantial.
- ✓ Government must introduce information technology curricula such as digital security, information security, network security at the undergraduate and postgraduate levels to ensure that the nation is educated enough to fight against cyberattacks worldwide.
- ✓ The government must introduce innovative ideas such as idea contests and boot camps in the cybersecurity arena, which will help promote digital security providers and cybersecurity startups.
- ✓ The government must arrange different training programs, seminars, and workshops regarding cybersecurity to make awareness among the people of our country and how to fight against cyberattacks.
- ✓ Last but not least, the government must specify and develop a long-term vision for the cybersecurity strategy by making a to-do list for the next 5-10 years with detailed and correct funding and achievable objectives because, in the coming days, only an effective strategy can prevent another major disastrous tragedy like the Bangladesh Bank heist.

3.6 References :

- Enterprise infosec consultants. (n.d.). Retrieved, 2021, from <https://eic.com.bd/about-us/>
- Enterprise infosec consultants. (n.d.). Retrieved, 2021, from <https://eic.com.bd/services-and-solutions/>
- Enterprise infosec consultants. (n.d.). Retrieved 2021, from <https://eic.com.bd/our-approach/>
- Dhaka Tribune. (2021, July 10). Retrieved January 18, 2022, from <https://archive.dhakatribune.com/business/banks/2021/07/10/how-strong-is-financial-cybersecurity-in-bangladesh>
- TBS Report 22 October, & Report, T. B. S. (2020, October 22). The Business Standard. Retrieved January 18, 2022, from <https://www.tbsnews.net/bangladesh/cybersecurity-must-protect-financial-sector-148498>
- B. B. (n.d.). The Financial Express. Retrieved January 18, 2022, from <https://thefinancialexpress.com.bd/views/reviews/cyber-security-and-the-role-of-bangladesh-bank-1612015431>

- Banking sector vulnerable to Cyber Crimes. The Daily Star. (2020, December 9). Retrieved January 18, 2022, from <https://www.thedailystar.net/editorial/news/banking-sector-vulnerable-cyber-crimes-2008901>
- Kundu, S., Islam, K. A., Jui, T. T., Rail, S., Hossain, M. A., & Chowdhury, I. (1970, January 1). Cyber crime trend in Bangladesh, an analysis and ways out to combat the threat: Semantic scholar. undefined. Retrieved January 18, 2022, from <https://www.semanticscholar.org/paper/Cyber-crime-trend-in-Bangladesh%2C-an-analysis-and-to-Kundu-Islam/fac09a3288908fd5144eaa4473fd09548c2775c1>
- C. S. Teoh and A. K. Mahmood, "National cyber security strategies for digital economy," 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), 2017, pp. 1-6, doi: 10.1109/ICRIIS.2017.8002519.
- Azad, D. M. M., Mazid, K. N., & Sharmin, S. S. (2017, May 1). Cyber crime problem areas, legal areas and the Cyber Crime Law. International Journal of New Technology and Research. Retrieved January 18, 2022, from <https://www.neliti.com/publications/263300/cyber-crime-problem-areas-legal-areas-and-the-cyber-crime-law>
- Finkle, J. (2016, April 25). Bangladesh Bank hackers compromised Swift Software, warning issued. Reuters. Retrieved January 18, 2022, from <https://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-iduskcn0xm0dr>
- Constantin, L. (2016, April 25). Bangladesh Bank attackers used custom malware that hijacked Swift Software. PCWorld. Retrieved January 18, 2022, from <https://www.pcworld.com/article/414601/bangladesh-bank-attackers-used-custom-malware-that-hijacked-swift-software.html>
- Bleyder, K. (2012). Cyber Security: the emerging threat landscape (Issue 10). Dhaka: Bangladesh Institute of Peace and Security Studies.
- Alam, Md. Shah. (2007). Cyber Crime: a new challenge for law enforcers!. Retrieved 19.06.2014 from http://www.prp.org.bd/cybercrime_files/Cybercrime%20--%20Bangladesh%20Perspective.ppt.
- Baccarat, a card game that helped in the Bangladesh Bank cyberheist. Dhaka Tribune. (2017, August 5). Retrieved January 18, 2022, from <https://archive.dhakatribune.com/business/banks/2017/08/05/baccarat-bangladesh-bank-cyberheist>
- The National Cybersecurity strategy of Bangladesh. : (n.d.). Retrieved January 18, 2022, https://sherloc.unodc.org/cld/lessonslearned/bgd/the_national_cybersecurity_strategy_of_bangladesh.html