Report On

Analysis of Cybersecurity Threats to Financial and Accounting Data: Implications for Organizational Risk Management

By

Sadavi Sadiq
19104094

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

BRAC Business School
Brac University
May 2023

Declaration

It is hereby declared that

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

Student's Full Name & Signature:

Sadavi Sadiq
19104094

Supervisor's Full Name & Signature:

Mr. Md. Shamim Ahmed
Senior Lecturer, BRAC Business School
Brac University

Letter of Transmittal

Mr. Md. Shamim Ahmed
Senior Lecturer,
Brac Business School
BRAC University
66 Mohakhali, Dhaka-1212

Subject: Submission of Internship Report

Dear Sir,

It is my pleasure to inform you that I have completed my internship report on "Analysis of Cybersecurity Threats to Financial and Accounting Data: Implications for Organizational Risk Management" as a requirement for the internship program of Spring 2023.

The report was an insightful experience for me. It has helped me to express my learnings from my internship experience in the accounting and finance industry. Furthermore, it helped me to gain an idea about the sort of cyber threats that can impact my field and how to counter them.

I would like to express my heartfelt gratitude to you for your continuous guidance and support for the duration of this report. Your thoughts regarding the report considering its limitations are highly appreciated.

Sincerely yours,

_____

Sadavi Sadiq
19104094
BRAC Business School
BRAC University
Date: 22 May, 2023

Acknowledgement

Having the opportunity to work at ACNABIN for 3 months was a wonderful experience for me. As an accounting major, it gave me real life insights on the sector and helped me relate my learnings from university with practical work.

I would like to express my profound gratitude to my internship supervisor Mr. Md. Shamim Ahmed for his support and guidance throughout the internship period. His insights were crucial for the completion of this report.

I am also thankful to Muhammad Aminul Hoque FCA, Partner of ACNABIN Chartered Accountants, for granting me the opportunity to work with the Audit & Consultancy team of ACNABIN.

Furthermore, I am grateful to my workplace supervisor Mahmudul Hasan for enriching my knowledge not only in the accounting field, but also in a multitude of other areas as well.

Lastly, I would like to thank Brac University for all the academic support in the last 4 years of my university life, as well as Office of Career Service and Alumni Relations for helping me with the necessary paper works for my internship.

Executive Summary

This report consisting of three chapters focuses on overview of my internship experience at the organization, details of the organization and lastly, the topic which I selected for this report which is “Analysis of Cybersecurity Threats to Financial and Accounting Data: Implications for Organizational Risk Management”. In the first chapter, the main focus was the outcome of the internship. What I gained from the internship and what the company gained for keeping me as an intern has been highlighted here. Afterwards in the second chapter, I have discussed about some of the organization practices as well as the chartered accountancy sector in Bangladesh. Lastly in the third chapter, I have discussed about some of the major cyber security threats to accounting data, such as hacking, malware, ransomware etc. along with their impact. Moreover, I have also discussed potential countermeasures to be taken by the organization. Both qualitative and quantitative data collected through secondary method has been used for this part.

Keywords: Accounting: Chartered Accountancy: Cyber Security: Cyber Attacks: Risk Management

Table of Contents

List of Tables

List of Figures

List of Acronyms

ERP	Enterprise Resource Planning
NGO	Non-Government Organization
NPO	Non-Profit Organization
CA	Chartered Accountant
SME	Small and Medium Enterprise
AI	Artificial Intelligence
SWOT	Strength Weakness Opportunity Threat
IMF	International Monetary Fund
DDoS	Distributed Denial of Service
IT	Information Technology
PwC	Price Waterhouse Coopers
TTP	Tactics Technique and Procedure

Chapter 1

Overview of Internship

1.1 Student Information

My name is Sadavi Sadiq. Currently I am a student in the BBA program at BRAC University. My student ID number is 19104094. My major is accounting and my minor is human resource management.

1.2 Internship Information:

1.2.1 Period, Company Name, Department/Division, Address

I have completed my 3-month internship from ACNABIN Chartered Accountants. My internship period was from January 4th to April 3rd. During this period, I have worked in the Audit & Consultancy department of the company under the client "VolumeZero Limited". The home office is located at BDBL Bhaban, Level-13, 12 Kazi Nazrul Islam Ave, Dhaka 1215 and the address of the client office is House 121, Road 4, Block A, Banani, Dhaka 1213.

1.2.2 Internship Company Supervisor's Information: Name and Position

During my internship period, my organization supervisor was Mahmudul Hasan. He is currently a Senior Assistant Manager of Audit and Consultancy department in ACNABIN Chartered accountants.

1.2.3 Job Scope – Job Description/Duties/Responsibilities

During my internship period, I had the opportunity to work with articled students who are currently doing their articleship in ACNABIN Chartered Accountants. I was assigned to

conduct audits of vouchers & bills and accounting records of clients. The type of vouchers consists of cash receipt, cash payment, bank deposit, bank payment and journal voucher. I was also tasked with preparing occasional reports such as reports related to field visit and reports related to client integrity for management review. I have also participated in training sessions led by my seniors to increase my technical expertise which are mainly related to using excel and the ERP system of the client. Lastly, one of the main responsibilities of an auditor is to maintain the confidentiality of the client's information which I strictly followed over the course of my internship period.

1.3 Internship Outcomes:

1.3.1 Student's contribution to the company

I had the opportunity to contribute to the company in multiple ways. I was able to lighten the workload of my seniors by assisting them and free them up to work on other crucial projects. Furthermore, I also helped with receiving vouchers. It is a monthly task where vouchers are sent from the accounts team and the audit team has to receive it by matching all the vouchers with the top sheet and checking if all the information are correct. Moreover, there were vouchers from previous months that also needed receiving and reviewing, which I helped with as well. I also managed all the files of one of the concerns of the company. Overall, I believe I was able to leave a positive impact on the team which reflects the positive feedback I got from my workplace supervisor at the end of my internship period.

1.3.2 Benefits to the student

I gained a lot from finishing my internship at ACNABIN Chartered Accountants. First off, it gave me a real-life experience conducting audits, which can help me understand audit techniques and procedures much more clearly. This practical experience will help me stand out as a candidate for future positions in the industry. Second, I had the opportunity to learn about

a wide range of clients and industries, which has allowed me to diversify my knowledge and abilities. My professional network may expand as a result of this exposure, which could result in new job opportunities. I was able to gain a deeper understanding of accounting and auditing standards, regulations and laws by working in the Audit & Consultancy department. This knowledge will be useful for my future academic and professional endeavors. Furthermore, the valuable feedback and guidance which I received from my supervisor and seniors can also aid me in my personal and professional development. To summarize, hands-on experience, exposure to various industries and clients, professional growth, and a competitive edge in the job market are the benefits which I believe I have gained by working in ACNABIN Chartered Accountants.

1.3.3 Problems/Difficulties (faced during the internship period)

Even though it was my first time in a corporate environment, I did not face as much problem as I expected. All the necessary paper works were done very fast and smoothly. Furthermore, my seniors at workplace were also very helpful. When they gave me a task, they gave me proper guidance on how to solve that task as well. Moreover, if a task required a feature of excel which I was not familiar with, they taught me how to use that feature as well. Everyone was extremely friendly and after attending office for a few days, my initial nervousness about being in a corporate environment disappeared.

1.3.4 Recommendations (to the company on future internships)

As ACNABIN is one of the top Chartered Accountant firms in Bangladesh, there is not much to recommend in terms of how they operate. However, there is one small change which I would like to see. While they provide the allowance for every month on time, they provide the conveyance of the current month in the next month. For example, I started my internship on January. At the end of January, I was able to take my allowance but I had to wait till February

to get the conveyance of January. I think it would be convenient if the allowance and conveyance of each month were provided together on that particular month. Lastly, if an intern wants to collect their allowance/conveyance in cash, they are only allowed to do so on Mondays and Wednesdays from home office. As home office and client offices are in different places, an intern might have difficulties to only come on those particular days. Therefore, it would be nice to see more flexibility in terms of the days on which an intern can collect their allowance/conveyance.

Chapter 2

Organization Part: ACNABIN Chartered Accountants

2.1 Introduction

ACNABIN Chartered Accountants is one of the leading chartered accountancy firms in Bangladesh with more than 35 years of experience. The company provides clients from a broad range of industries with audit, tax, and consultancy services. ACNABIN works closely with its clients to comprehend their unique needs and provide specialized solutions that help them achieve their business goals as well as maintain a long-term relationship with the clients. At the core of its operations, ACNABIN is driven by a passion for seeing its clients thrive, and the company is dedicated to offering the highest quality service and support.

2.2 Overview of the Company

ACNABIN has an affiliation with the 9th largest accounting firm in the world, Baker Tilly International. ACNABIN acts as an independent network member of Baker Tilly. Prior to this, ACNABIN had an affiliation with Arthur Andersen, till it got shut down in 2002.

2.2.1 Vision

According to the organization's website, the vision of ACNABIN is – "We go beyond the traditional auditor and client relationship by becoming your Trusted Business Advisor."

2.2.2 Mission

According to the organization's website, the mission of ACNABIN is – "We adhere to the strictest principles of client confidentiality. The sensitive and competitive nature of proprietary information and the maintenance of trust-demands it. We have built our success on such principles. We do our utmost to earn and keep client trust."

2.2.3 Strategic Intent

According to the organization's website, the strategic intent of ACNABIN is –

"We want to become trusted leader in the market ensuring highest level of professional ethics and competencies. While securing safe & trusted position in the market for financial institutions, telecommunications, foreign branch & liaison offices and NGOs/NPOs, we still see wider space for us to get involved in other sectors in the country and in the region."

2.2.4 Core Values of the firm

ACNABIN Chartered Accountants follows the same core values Baker Tilly International. These values, as per their company's website are given below.

- To lead by example
- To deliver quality services with integrity
- To communicate openly, to act ethically
- And to foster a community built around civic responsibilities and teamwork.

2.3 Management Practices

Currently ACNABIN is run by 9 partners and all 9 partners take part in the decision-making process. In this case, we can say that ACNABIN follows a democratic leadership style. ACNABIN maintains the following hierarchy in their organization and the chain of command is maintained accordingly.

- Partner
- Director
- Associate Director

- Assistant Director
- Assistant Director
- Deputy Director
- General Manager
- Manager and Admin
- Deputy Manager
- Senior Assistant Manager
- Assistant Manager
- Executive
- Articled Student

According to this hierarchy, partners are responsible for all of the major decisions and then it comes down all the way to articled students, who make up the majority of the manpower of ACNABIN. Articled students are required to sit for a written exam in order to join the firm. After passing the exam, they have to sit for an interview and then the firm will select the best candidates among them. The written exam focuses greatly on English language proficiency as well as basic accounting knowledge. The compensation system varies between different articled students. Factors that affect this are, university of the student, CGPA and highest level of degree completed. Articled students are assigned to different clients after joining the firm and their trainee period of 6 months consists of doing practical work with their assigned clients to gain experience before the start of their articleship period. Articled students also get a raise in allowance based on how many subjects of CA they pass during their articleship period.

2.4 Marketing Practices

ACNABIN does not have a dedicated marketing department. Furthermore, their Facebook page is also fairly inactive. This might make people wonder how does the firm attract customers. The answer to this is networking and referrals. ACNABIN does a good job of retaining their current client base through their exceptional audit quality. For example, their client base consists of well-known organizations such as Biman Bangladesh, Grameenphone, Walton, Berger Paints etc. Auditing these big companies give other companies an assurance that ACNABIN is indeed reliable. As a result, those companies will approach ACNABIN themselves. Besides, firm partners also play a big role in this sector. They attend various seminars and workshops in educational institutions which also acts as one kind of advertisement for the firm. Students can become interested to join the firm by attending these seminars and workshops. Overall, ACNABIN does not follow a specific marketing strategy to attract clients and students.

2.5 Financial Performance and Accounting Practices

As a chartered accountancy firm, ACNABIN makes financial statements for its clients and verifies the authenticity of financial documents as well. However, when it comes to the financial statement of their own organization, access to that is not available to the public. Since ACNABIN is not a publicly listed company, their financial statement is confidential. For this reason, it is not possible to collect the last 3-5 years financial statements to analyze the financial performance and accounting practices of the organization.

2.6 Operations Management and Information System Practices

When it comes to the use of information system practices and what impact it has on the operations management of the organization, I had the opportunity to try out the ERP System (Enterprise Resource Planning) of ACNABIN. In this ERP system, everyone working in the

organization has their own employee ID or student ID. Within the ERP system, there were different sub-sections. Among these sub-sections, I was able to try out the job ticket entry, timesheet entry, conveyance entry and leave application. Below I will discuss their uses.

2.6.1 Job Ticket Entry

Job ticket entry is added monthly which contains information about the student/employee and which client they belong to. It also contains the location of the client as well as purpose of work in the client. After entering the client information and personal information, the remaining information such as manager name, supervisor name, partner name etc. will be automatically filled up. Job ticket entry is necessary every month in order to add timesheet later on. A picture of the job ticket interface is attached below.

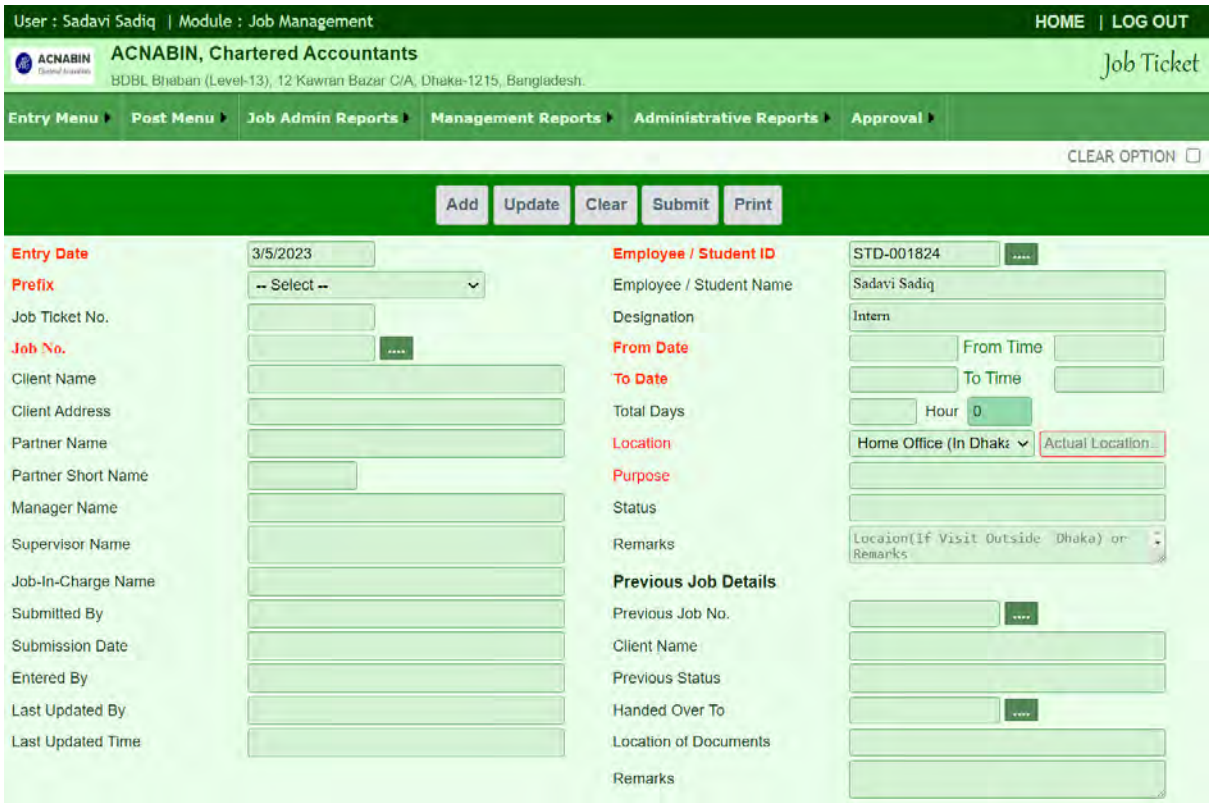

Figure 1 Job Ticket Interface

In the above picture, we can see that there are some fields marked as red. Those are the only ones that are required to be filled up. After filling up the red marked fields, the remaining fields are automatically filled up. After filling up the job ticket form, it has to be submitted. After submission, it will be recommended by the client manager. Afterwards, it will be approved by the partner responsible for the client. Once the job ticket is approved, timesheet entry can be done.

2.6.2 Timesheet Entry

Timesheet entry is done daily. However, it is divided into twice a month on a fortnight basis. The first 15 days of the month are counted as 1st fortnight while the remaining days are counted as 2nd fortnight. Timesheet is very straightforward. It contains the necessary information about the employee/student, which client they belong to and a detail explanation of their work activities on each day. It also contains how many hours an employee/student is working along with the work location, which can be either home office or client office. As a result, the organization can keep track of the daily activities of every employee through the timesheet entry. A picture of the timesheet entry interface is attached below.

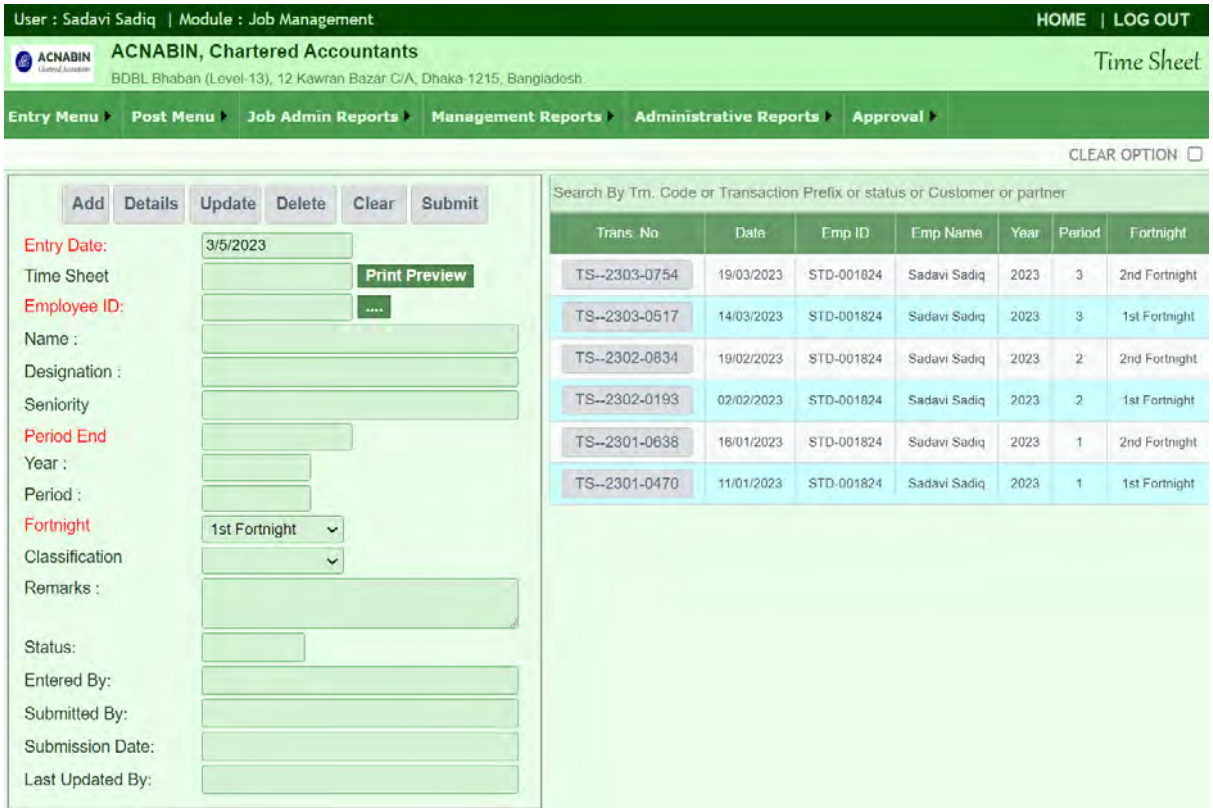

Figure 2 Time Sheet Interface

In the above picture, on the right part, there is a record of all the previously submitted timesheet. On the left side, there is the option to enter a new timesheet. The fields marked as red are the only ones to be filled up. The remaining ones will be filled up automatically. Similar to job ticket entry, after the timesheet is submitted, it will be recommended by the client manager first and then approved by the partner responsible for the client. After the approval of the timesheet, conveyance entry can be done.

2.6.3 Conveyance Entry

Conveyance entry is given based on the distance from home office to client office, method of transport used and whether it is one way or two ways. Conveyance entry is also given on a fortnight basis. Conveyance information has to be separately entered for each day. If an employee/student is on leave, then no conveyance will be provided for that day. A picture of the conveyance interface is attached below.

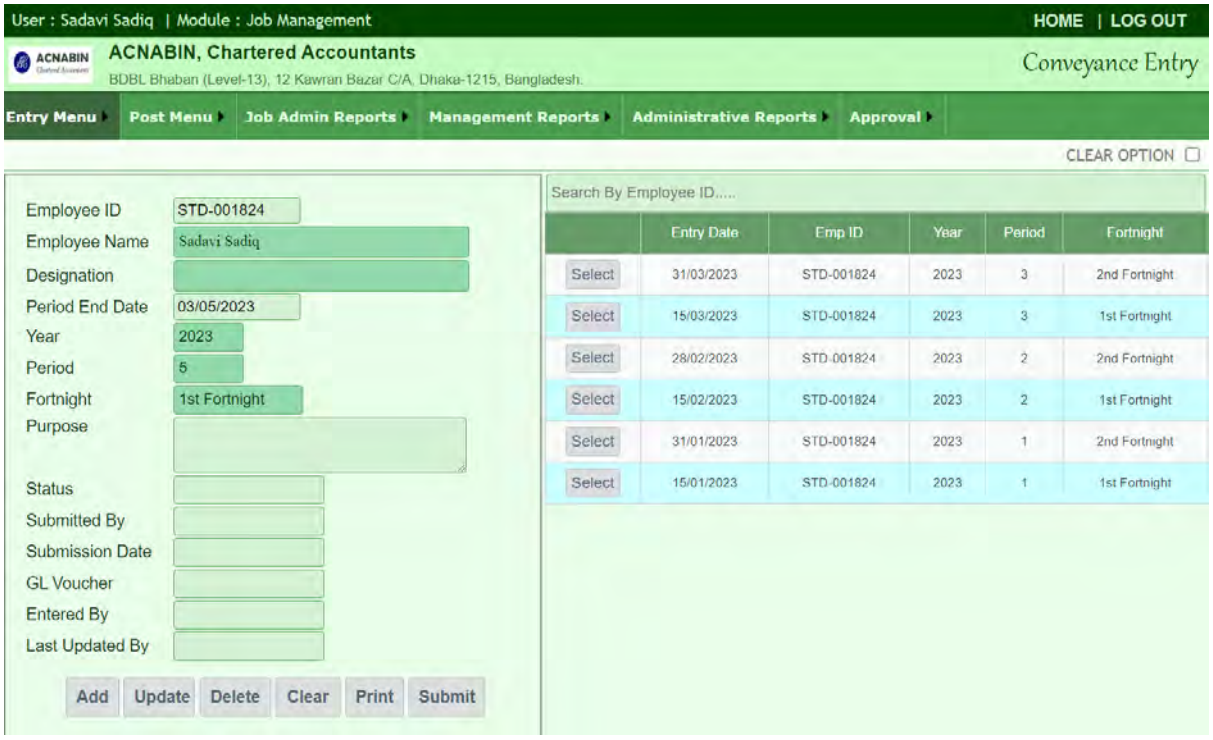

Figure 3 Conveyance Interface

In the above picture, on the right we can see the conveyance history. On the left, we can see the option for adding conveyance for a new fortnight. Conveyance can be collected in two methods. Through cash and through bank. If someone decides to collect it in cash, then the "Status" section in the above picture will say "Posted – Cash Payment". If someone wants the conveyance to go directly in their bank account, then it will say "Posted - Bank Payment".

2.6.4 Leave application

Application of leave is also done through the ERP system. It contains the duration of the leave period, type of leave, to whom the responsibility was handed over to during the absence of the leave applicant, address, phone number and of course the purpose of leave. A picture of the leave application interface is attached below.

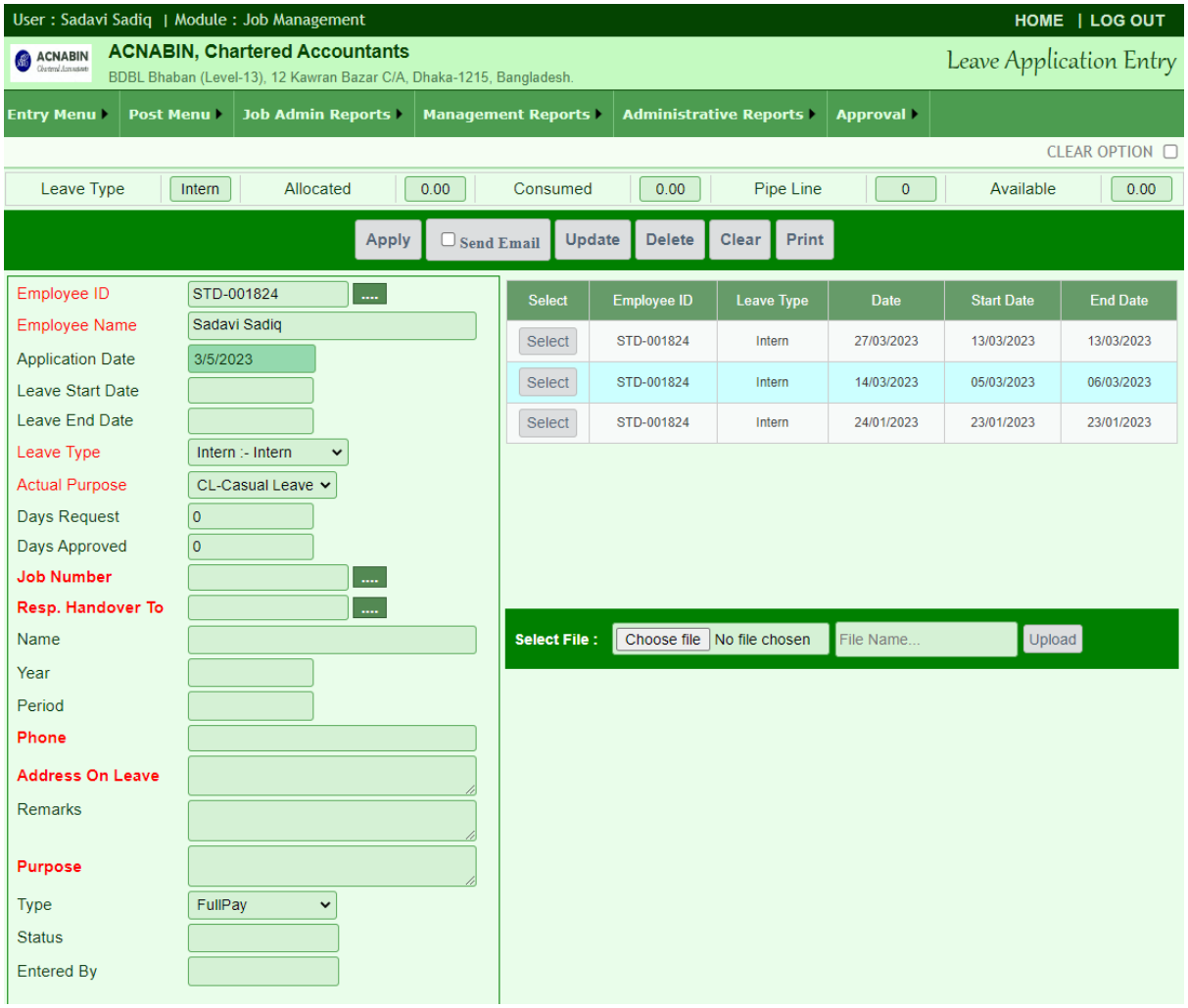

Figure 4 Leave Application Interface

In the above interface, on the right side, we can see the previously applied leaves and on the left we can see the necessary information we need to enter to apply for a new leave, with the red fields being mandatory to fill up. After applying for a leave, it will go through 3 phases. The first phase is “Open”, second phase is “Recommended” and the final phase is sanctioned. At the top of the interface, we can see how many leaves are allocated to the applicant, how many leaves have been consumed, how many leaves are currently in process and lastly how many leaves are left.

Overall, to conclude this segment, ACNABIN is heavily dependent on the use of information system as it is one of their main methods of data collection from every single employee/student.

2.7 Industry and Competitive Analysis

2.7.1 Porter's five forces analysis

1. **Threat of new entrants:** In my opinion, there is a low to moderate threat of new entrants in this sector. The reason for this is that, to become a chartered accountant in Bangladesh, one must go through extensive education, real life experiences, along with professional certification, which creates barriers to entry. However, experienced chartered accountants might be interested in establishing their own firms which may potentially create competition.

2. **Threat of substitutes:** The threat of substitutes is low. For an organization, chartered accountancy services are a specialized service as it requires the aid of experienced individuals. While similar services can be taken from a non-chartered accountancy firm, the quality level will not be the same.

3. **Bargaining power of suppliers:** The bargaining power of suppliers is low. One of the major supplies of a chartered accountancy firm in Bangladesh is the human resource, which they hire in the form of articled students. As there are many who aspire to become a chartered accountant, firms can choose to hire those who are more qualified than others.

4. **Bargaining power of buyers:** The bargaining power of buyers in this industry is moderate to high in my opinion. Clients have the option to select their desired firm from the numerous available firms in the market, which makes the bargaining power high. Clients can also negotiate about the fees as well as the work deadline, making it less flexible for firms and increasing their workload.

5. **Rivalry among competitors:** Rivalry among competitors is high in the chartered accountancy sector. In Bangladesh, there are a few firms with very strong brand names.

These firms not only have a high rivalry among them, but also other less popular firms in the industry along with recently established new firms are constantly providing quality services and keeping the market competitive.

2.7.2 SWOT analysis

Strengths:	**Weaknesses:**
• Highly reputed and has strong brand value. • Strong learning environment for students. • Renowned client base like Grameenphone and Walton. • Providing personalized services according to the needs of the client. • Provides additional consultancy, advisory and risk management services on top of the traditional auditing service.	• As big clients generate majority of the revenue, there is a strong dependence on these particular clients. • Due to having a huge number of articled students, it takes a lot of time for newer students to get their article-ship registration. This long wait time may discourage students to join the firm. • Not up to date with technology, especially workplace laptops which are crucial for daily use, compared to some of its competitors.
Opportunities:	**Threats:**
• Become more active in social medias and participate in digital marketing.	• Increased competition from newer firms along with existing bigger firms

• Implement the use of data analytics to enhance decision making. • At present, Bangladesh has a growing SME sector which presents ACNABIN with the opportunity to work in this industry and expand its client base.	at present can pressurize the firm in terms of pricing and client retention. • As ACNABIN only works with local clients, any negative impact on the country's economy can also affect their revenue. • Improvements in automation through artificial intelligence can pose a potential threat in the future. At present there are already multiple evidences of AI preparing a financial statement without any mistakes. In the future when AI becomes more stronger, it can pose a considerate level of threat.

Table 1 SWOT Analysis

2.8 Summary and conclusion

As one of the leading firms in the industry, ACNABIN has a strong presence in the local market along with global affiliation as well. All major decisions of the firm are made by the partners. Furthermore, networking and referrals are the main source of their marketing practices. As ACNABIN is not a publicly listed company, their financial statements and other documents are confidential and it is difficult to asses their financial performance over past years. In terms of the use of information systems, it is maintained through the ERP system of ACNABIN. As for the porter's five forces, the threat of new entrants is moderate to low, the threat of substitutes and bargaining power of suppliers is also low. However, bargaining power of buyers is

moderate to high. Lastly, the rivalry among competitors is high. The SWOT analysis highlighted the strengths, weaknesses, opportunities and threats in terms of client base, technology, firm condition and environment, entrance into a new sector, competitors, advancement of automation etc.

To conclude, since its establishment, ACNABIN has been one of the strongest contenders in the accounting and auditing sector of Bangladesh. Their ability to adapt with the competitive market is the reason why the firm has been around for 37 years. To maintain this strong position in the future, proper emphasis has to be given to eliminating weaknesses, reducing threats and focusing on available opportunities.

2.9 Recommendations/Implications

Based on my experience from working in ACNABIN and the SWOT analysis, I would recommend the following things.

- **Provide more up to date laptops in the workplace with better specifications:** While working in ACNABIN, I have noticed that a lot of the laptops have very old specifications and even struggle to run Excel properly. It is difficult to prepare financial statements or do other heavy work when the laptops provided are not strong enough.
- **Be more active in social media:** The last Facebook post made by ACNABIN was in January. As majority of the people in our country are active on Facebook, it will be easier to reach people. Furthermore, in this digital age, I think it is a must to remain active in at least one social media platform.
- **Improve the check in system at the client office:** In the client where I was assigned, the check in was done by calling one of the students/employees from home office and asking who are present. This method of checking attendance through a phone call is inefficient as there are a lot of student/employees and the person calling from home

office has a chance to miss someone's name. In that case, that person will not get the allowance/conveyance for that day. Therefore, a more modern and efficient check in system at the client office should be provided which can also assure employees/students that their attendance has been recorded properly.

Chapter 3

Analysis of Cybersecurity Threats to Financial and Accounting Data: Implications for Organizational Risk Management

3.1 Introduction

In the present age, the advancement of technology has brought drastic changes in every possible sector we can imagine. The Finance and accounting sectors are no exception. Although these advancements come with a lot of benefits, there are also a variety of threats involved here. One such threat is a breach of cybersecurity. A breach of cybersecurity of an organization can cause all of its stored data to be exposed which can cause negative consequences. These may include, financial losses and loss of the organization's reputation as well **(The Global Risks Report, 2022)**. Due to the rise in cyber-attacks, it is required to have sufficient knowledge of how to these attacks work as well as how to tackle them. In the year 2020, there was an increase in ransomware and malware attacks by 435% and 358% respectively **(The Global Risks Report, 2022)**. Spam emails and phishing websites are two of the most common attempts at cyberattacks. In 2020, the amount of spam email traffic was approximately 50.37%, where the attacker claimed to be from big companies such as Amazon or Microsoft and tried to make the victim call a particular number in the name of "support" or "confirmation of order" **(Kulikova et al., 2020)**. However, there are also risk management procedures to mitigate these threats. Some of the steps of risk management procedures are – identifying and prioritizing the risks, design of the control system of the organization and testing the control system, reporting to external parties such as shareholders **(Eaton et al., 2019)**. Through this paper, the different types of cybersecurity attacks that are directed towards financial and accounting data will be

analyzed. Furthermore, preventive measures that are to be taken in order to minimize organizational risk will also be discussed.

3.1.1 Background

As mentioned earlier, the finance and accounting sector has been significantly transformed due to digitalization, making data management smoother and more efficient. Technologies such as AI, big data and cloud-based accounting can help with resource management as well as decision making. However, technologies that can pose threats and vulnerabilities are also rapidly developing as well, increasing the risk of financial and accounting data being exposed.

Due to the evolution of cyber threats, it is now getting more and more difficult to detect such threats. According to an article published by **Bloomberg (Sponsored by Siemens)**, people did not have any sort of malicious intent using viruses. However, when people came to realize how powerful viruses can be and what they can potentially do, that is when cyber threats started to increase. As a result, in the 21st century, people are now abusing those threats for their gain. In terms of the finance and accounting sector, people can sell exploited information to other parties for financial gains or even use the information for themselves to blackmail the victim.

Regardless of the awareness and actions taken by organizations to mitigate cybersecurity threats, the breaches are still happening even today. Financial institutions in particular are at a bigger risk. The finance and accounting firms are 300 times more likely to be the victim of a cyber-attack compared to other companies **(Eide, 2019)**. Furthermore, due to being a likely target of cyber-attacks, finance and accounting firms have to constantly spend money to resolve the damage done by the attack. According to a report published by **Accenture (2019)**, approximately $243,000 is required to resolve per insider attack. Besides, money is not the only factor here. It also requires a significant amount of time as well. In the same report by **Accenture (2019)**, it is mentioned that on an average, insider attacks can take approximately

55.1 days to resolve, ransomware being 33.8 days and web-based attacks being 25.9 days. According to a blog post made by IMF, a survey was conducted to see which risk is the most vulnerable for financial institutions and cyber risk was on top of the list **(Lagarde, 2018)**.

According to **Adrian & Ferreira, 2023**, a survey was conducted by IMF consisting of 51 countries and the following numerical data were found.

Type of vulnerability	**Numerical expression (%) of vulnerability**
No national cyber strategy	56%
No risk management system dedicated to cyber security	42%
No specialized risk unit	68%
No testing or implementation of cyber security measures	64%
No assigned authority for reporting cyber threats	54%
No cybercrime regulations	48%

Table 2 Cyber Security Vulnerabilities

The above data is applicable for financial supervisors of the 51 countries that were part of the survey.

3.1.2 Objectives

Broad objective: Determining the nature of cybersecurity threats and what impact it may have on financial and accounting data as well as providing relevant risk management methods to protect organizational data.

Short objective:

1. Identifying the different types of cybersecurity threats that financial and accounting firms have to deal with and what impact they have on organizational activities, such as– phishing attacks, ransomware, insider threats etc.
2. Consumer perspective towards their financial data and cyber threats management ability of companies.
3. The impact of organizational culture and providing training to staff on risk mitigation.

3.1.3 Significance

This project on "Analysis of Cybersecurity Threats to Financial and Accounting Data: Implications for Organizational Risk Management" is extremely significant in the present technology and business reliant world. No business can function without the proper use of financial and accounting knowledge. Assets, liabilities, revenue and expenses are all crucial parts of every business. It is necessary to ensure that data related to these things are maintained with proper confidentiality in order to ensure the accuracy of financial statements. Maintaining this accuracy also ensures a healthy relationship with stakeholders. Furthermore, customers will also feel safe when they have an assurance that their data such as bank details or assets such as cash in bank are maintained with proper security. As cyberattacks continue to grow, the risk faced by organizations towards financial and accounting data is also growing.

Therefore, this project aims to provide a valuable understanding of the rapidly growing scenario of cyber threats and their impact through a detailed analysis. With the help of this analysis, organizations can determine the most critical risks they can possibly face and then plan out their prioritization of threats accordingly.

Moreover, this project will also act as a stepping stone for future research regarding this topic. As we know, technology is evolving day by day and the countermeasures provided in this project will not be relevant forever. Therefore, this paper can provide future researchers with an initial idea about the cybersecurity scenario of the present timeline. Lastly, the insights of this project can help organizations determine what sort of training they should give to the staff and in which areas, in order to mitigate cyber threats.

3.2 Methodology

By using both qualitative and quantitative data, this project will follow a mixed approach to analyze the cyber security threats to financial and accounting data along with the risk management procedures that should be followed by an organization. Moreover, a secondary method of data collection has been used to collect the qualitative and quantitative data. Sources of secondary data includes research articles, publicly available databases, reports published on the related industry, journals etc.

3.3 Findings and Analysis

The qualitative and quantitative data collected through secondary data collection method will be presented in this segment.

3.3.1 Types of Cybersecurity threats

In the finance and accounting sector, the most notable threats are hacking and malware. However, there is also a rise in insider threats and accidental disclosures. Moreover, with the

rise of technology like cloud adoption, it is predicted that these threats will increase in the upcoming years **(Bowcut, 2023)**. A statistical representation of the mentioned threats in the finance and accounting sector is also available as well which is shown below.

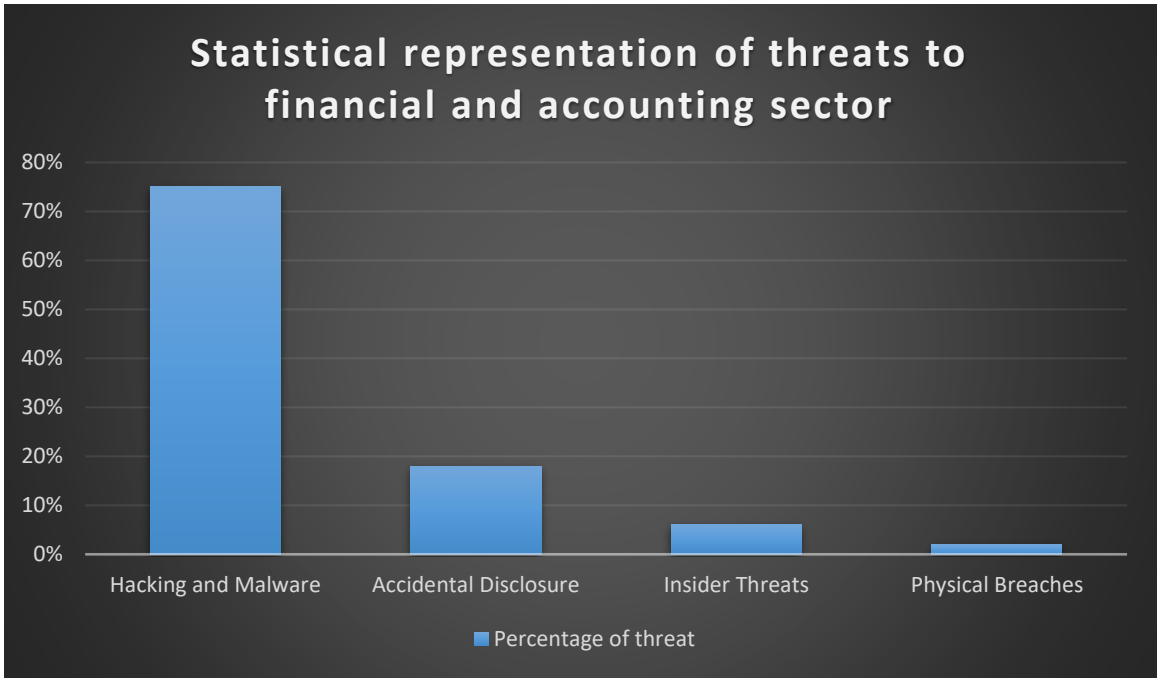

Figure 5 Statistical representation of threats

Another recent study claims that phishing attacks are the most popular type of cyber attack due to phishing emails being hard to recognize and the financial sectors are targeted 90% of the time with a phishing email to start a cyber attack for the first time **(Kost, 2023)**. Moreover, **Kost (2023)** also claims that in the year 2021, phishing attacks saw a rise of 22% only in the first half. Moreover, financial apps saw an increase of 38% in the same period. Another common threat in the finance and accounting industry as claimed by **Kost (2023)** is DDoS attacks. Out of all the industries in the world, the financial industry is on the list of the top 3 most target industries of DDoS attacks between the years 2020 and 2021. Furthermore, between the years 2019 and 2020, there was an increase of 30% DDoS attacks in the financial service sector. Password login attacks also saw an increase during this period. Another notable threat faced by the financial and accounting industry is the ransomware threat. In fact, this threat is

extremely effective against the financial industry from the attacker's point of view. The reason for this is that, the attacker owns valuable data of the customer and if these customer data get leaked online, then the organization will completely lose all their reputation. As a result, when financial industries are unable to deal with a ransomware attack, they are forced to pay a ransom to the attacker to protect their organization. Besides, in the year 2020, a huge spike of 520% increase in ransomware attacks were seen in the baking sector between the period of March to June. The most popular types of ransomwares that target the financial industry are as follows.

- Sodinokibi Ransomware
- Conti V2 Ransomware
- Lockbit Ransomware
- Clop Ransomware
- Egregor Ransomware
- Avaddon Ransomware
- Ryuk Ransomware
- Darkside Ransomware
- SunCrypt Ransomware
- Netwalker Ransomware
- Phobos Ransomware

Lastly, in a report published by **Akami (2019)**, it is claimed that 94% of the attacks in the finance and accounting sector were due to:

- SQL Injections
- Cross-Site Scripting

- Local File Inclusion
- OGNL Java Injection

Apart from the threats mentioned in this segment, there are numerous other threats targeting the financial and accounting sector. However, the threats mentioned here are some of the major and common ones faced by companies.

3.3.2 Impact of Cybersecurity Threats

Due to the threats mentioned in the previous section, financial and accounting institutions can face severe consequences. According to **Filipkowski (2021)**, some of these consequences are financial loss, loss of productivity in the organization, losing clients, loss of reputation.

Financial loss: Previously we have stated that financial organizations often have to pay a ransom to the attackers in case of a ransomware attack. Now let's take a look a look at the range of this ransom payment. Fillipkowski (2021) states that $150,00 is the average cost of a ransom payment, with reports of some organizations who had to pay over $1.2 million. This alone is a huge financial loss for the organization. If we take other related factors into consideration, such as investigation fees, regulatory fees, client compensation fees, IT fees, downtime losses etc. then the average cost can rise up to $4.24 million.

Loss of productivity: When a financial organization faces a cyberattack, their organizational activities are interrupted. Furthermore, it also raises a feeling of distress in case of a future attack. Besides, it may also make employees feel like the attack was successful due to their irresponsibility. As a result, employee morale will fade away and productivity will decrease.

Losing clients: A business cannot run without clients. When a data breach happens, clients no longer feel safe to trust that organization. Especially when it is a financial or accounting firm where there is more emphasis on money. According to an ERP based financial company

Multiview (2022), due to losing clients because of a cyber-attack, 60% small businesses have to shut down within 6 months.

Loss of reputation: Failure to protect sensitive financial data raises questions about the security of the business. Furthermore, other businesses will be unwilling to collab with the attacked business as well. Even if the business manages to pull itself together in the future, old customers might still fear past incidents of data breaches and choose to avoid the business completely. To back this up, according to **PwC US Protect me Survey (2017),** if a company has a bad reputation of security breach, 85% of consumers are unwilling to do any business with that company.

3.3.3 Consumer's perspective of financial and accounting data in relation to cyber attacks

According to an online survey conducted by one of the leading accounting firms in the world, PwC, with a sample size of 2000 Americans who are above the age of 18, the following findings were discovered.

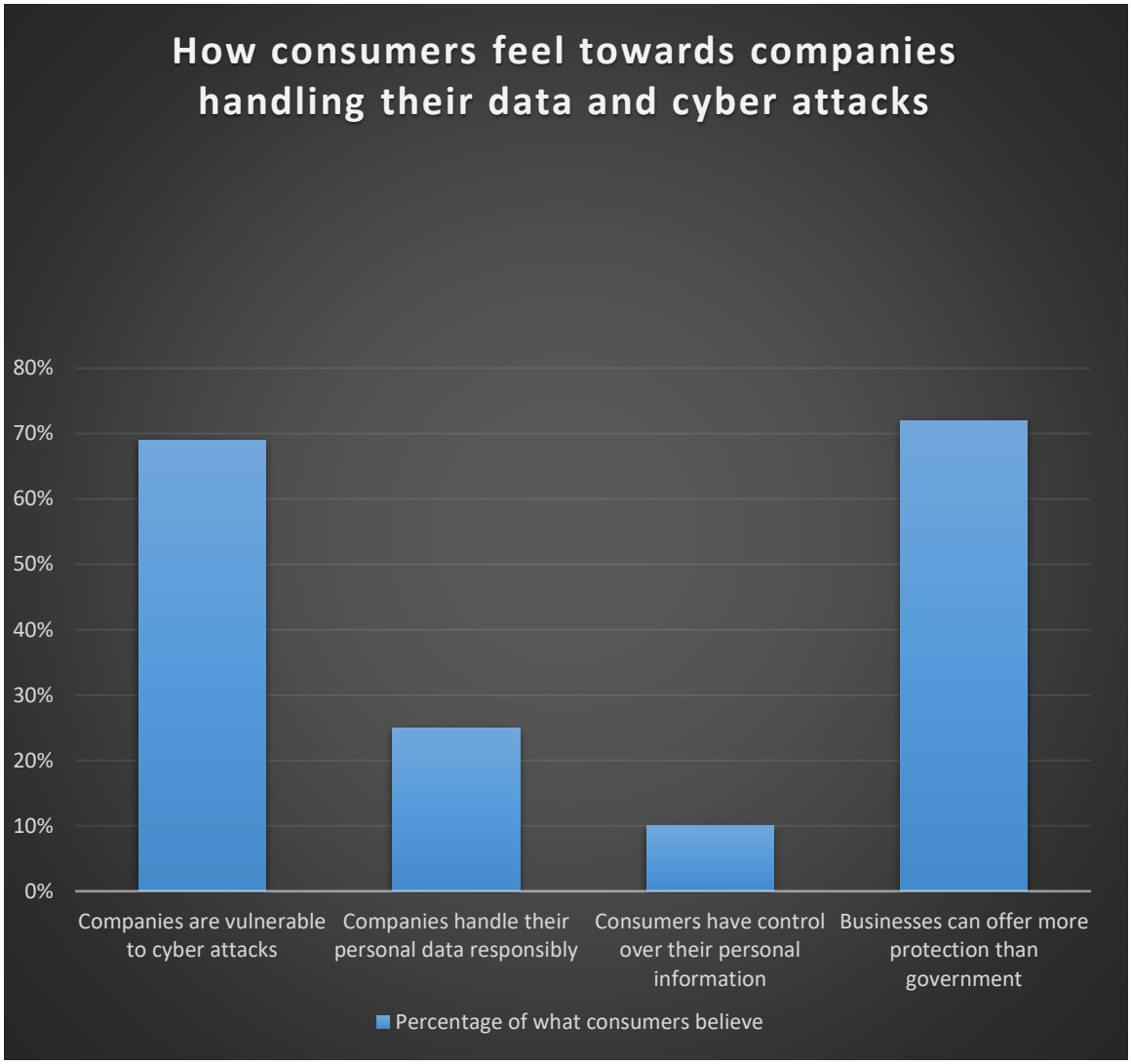

Figure 6 Consumers perspective towards company's data management

From the above statistics, we can notice that a large portion of customers believe that companies are vulnerable to cyber attacks. However, a larger portion of consumers also believe that the companies themselves despite being vulnerable to cyber attacks can offer more protection compared to the government. Furthermore, only 10% of the consumers believe that they have proper control over their own information. Lastly, only 25% of consumers believe that companies are being responsible with their data. From this, we can conclude that even though the first three statements claim that consumers are not confident enough about the companies, the companies are still doing a better job at data protection compared to the government.

3.4 Summary and Conclusion

To summarize, since financial, accounting and other monetary data are extremely sensitive content for an organization, attackers are more likely to target them. Through qualitative and quantitative data collection using a secondary method, it has been found that the most used methods targeting financial and accounting data are hacking and malware. Besides, accidental disclosure, insider threats and physical breachers are also responsible as well. Furthermore, due to the such attacks on financial and accounting data, organizations may suffer from financial losses, employees may lose their productivity and the organization can lose clients & reputation as well. Moreover, majority of the consumers also believe that organizations are vulnerable towards cyber attacks on financial and accounting data. As a result, organizations need to take proper precautions to prevent cyber attacks. Some of these precautions include, authentication system, TTP hunting, attack surface management, keeping backup data and keeping all software up to date.

Lastly, to conclude, even though new technologies are emerging to mitigate threats against financial and accounting data, new forms of threats are also emerging as well. As a result, aside from the recommendations/implications proposed in this report, organizations need to constantly look out for new procedures as well. The reason for this is that, the recommendations/implications mentioned in this report may be viable at present, but they might become obsolete few years from now. This is why organizations must not settle for a particular preventive method, but rather keep developing their security over the years constantly and make it harder for the attackers to launch a cyber attack.

3.5 Recommendations/Implications to be followed by organizations for risk management

So far, we have discussed the various types of cyber threats, their impact on the organization, how they affect consumers and employees etc. Now let's take a look at the risk management procedures of the threats mentioned earlier.

Authentication system: Two-factor authentication is common among us. However, on an organizational scale, it won't provide enough security. In such cases, the implementation of a multifactor authentication system can greatly reduce risk,

TTP Hunting: TTP or in other words tactics, techniques and procedures hunting can hunt down the latest tactics, techniques and procedures used by cyber attackers. By knowing this information about the attacker, it is possible to completely shut down the attacker. Since this is intelligence based, TTP Hunting can constantly keep learning new and new things about the attackers and keep the organization's defenses up to date.

Attack surface management: Attack surface management can not only detect data leakage, but also it can act from the perspective of the attacker. By doing this, it can know what to expect when an attacker actually attacks. It is also an excellent management system for controlling internal data breachs.

Backing up data: If an organization loses all its data due to a cyber attack, in that case having a back up data would help them get on track fast. A separate external hard drive or a cloud backup service that is not in the same network as the organization can be used for storing backup data.

Software updates: Often we see that there are updates available for software that we use but choose to ignore the update. This can increase vulnerabilities to cyber attacks. According to

Truta (2019), 60% of cyber attacks were possible due to a software update available, but not updated. Therefore, it is crucial to use up to date software in the organization.

In a research article published by **Eaton, Grenier & Layman (2019)**, they have explained how accounting risk management can be achieved in a step-by-step manner. They also claim that in the case of an accounting firm, a person who has expertise in both accounting and IT is to be utilized. Their risk management steps are discussed below.

Steps	Actions
Identify the risk and prioritize the threat level of the risk	Use IT expertise combined with knowledge of currently known threats
Designing proper control system	The design is to be done based on the type of risk identified in the first step
Testing the control system	Run testing on regular basis based on available data to control system up to date
External reporting of cybersecurity	Submit a report to external parties such as shareholders about the risk management system of the company, to restore investors faith
Assurance of external reporting	Conduct assurance engagement of the report mentioned in the previous step

Table 3 Accounting risk management

References

[1] World Economic Forum. (2022, January 11). *Global risks report 2022*. World Economic Forum. https://www.weforum.org/reports/global-risks-report-2022

[2] Kulikova, T., Shcherbakova, T., & Sidorina, T. (2021, May 13). *Spam and phishing in 2020*. Securelist English Global securelistcom. https://securelist.com/spam-and-phishing-in-2020/100512/

[3] Eaton, T. V., Grenier, J. H., & Layman, D. (2019, March 1). *Accounting and Cybersecurity Risk Management. American Accounting Association*. https://publications.aaahq.org/cia/article/13/2/C1/7123/Accounting-and-Cybersecurity-Risk-Management

[4] Bloomberg. (n.d.). *A brief history of cybercrime and security*. Bloomberg.com. https://sponsored.bloomberg.com/immersive/siemens/a-brief-history-of-cybercrime-and-security

[5] Accenture. (2019, July 16). *Cost of cybercrime continues to rise for financial services firms, according to report from Accenture and Ponemon Institute*. Newsroom. https://newsroom.accenture.com/news/cost-of-cybercrime-continues-to-rise-for-financial-services-firms-according-to-report-from-accenture-and-ponemon-institute.htm

[6] Adrian, T., & Ferreira, C. (2023, March 2). *Mounting cyber threats mean financial firms urgently need better safeguards*. IMF. https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards

[7] Lagarde, C. (2018, June 22). *Estimating cyber risk for the financial sector*. IMF. https://www.imf.org/en/Blogs/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector

[8] Eide, N. (2019, June 21). *Cyberattacks hit financial services 300 times more than other sectors*. CIO Dive. https://www.ciodive.com/news/cyberattacks-hit-financial-services-300-times-more-than-other-sectors/557372/

[9] Bowcut, S. (2023, March 23). *Cybersecurity in the Financial Services Industry*. Cybersecurity Guide. https://cybersecurityguide.org/industries/financial/

[10] Akamai Threat Research: *Phishing and Credential Stuffing Attacks Remain Top Threat to Financial Services Organizations and Customers*. (2019a, July 30). https://www.akamai.com/newsroom/press-release/state-of-the-internet-security-financial-services-attack-economy

[11] Kost, E. (2023, April 6). *The 6 biggest cyber threats for financial services in 2023: Upguard.* RSS. https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services#toc-2

[12] Filipkowski, B. (2021, September 8). *4 big risks cyber attacks pose for financial institutions*. Field Effect. https://fieldeffect.com/blog/financial-institutions-cyber-risks/

[13] PwC. (2017). *Consumer intelligence series: Protect.me* - FIS. fisglobal. https://www.fisglobal.com/-/media/fisglobal/worldpay/docs/insights/consumer-intelligence-series-protectme.pdf

[14] Multiview. (2022, August 2). *Accounting cybersecurity: Keeping your financial data secure*. Multiview ERP. https://multiviewcorp.com/blog/accounting-cybersecurity-keeping-your-financial-data-

secure#:~:text=Breaches%20in%20security%20put%20your,action%20by%20the%20affected%20clients

[15] Truta, F. (2019, October 31). 60% of breaches in 2019 involved unpatched vulnerabilities. Security Boulevard. https://securityboulevard.com/2019/10/60-of-breaches-in-2019-involved-unpatched-vulnerabilities/