ROLE OF CYBER SECURITY IN PROTECTING CONFIDENTIAL DATA: BLUE FORTRESS

Prepared for

Madiha Rehman

Lecturer, National University of Computer and Emerging Sciences
Karachi

Prepared by

Abu Bakr Wamiq, Sarim Khan, Lachman Das, Shah Muhammad,
Ali Mehdi badami and Zain Raza

Student, National University of Computer and Emerging Sciences
Karachi

April 28, 2023

Table of Contents

1.Cover Letter

Date: 28 April, 2023

Madiha Rehman Lecturer

FAST NUCES
Shah Latif town, National Highway
Sindh, Karachi

Dear Ms Rehman .

As approved, we are submitting the attached report entitled *ROLE OF CYBER SECURITY IN PROTECTING CONFIDENTIAL DATA: BLUE FORTRESS*.

The report offers solutions to the current problems related to data confidentiality and security by proposing a business plan that provides security solutions. It also discusses each of their respective tasks. The report will also highlight the time period that will be needed to establish and launch the business. The report also includes the budget that is required by the business.

I hope you find this report satisfactory.

Sincerely yours,
Mehdi Badami, Student
FAST NUCES
Shah Latif town, National Highway
Sindh, Karachi

2.Executive Summary

2.1. Introduction:

This proposal is for an online business that targets the privacy and protection of the data of our clients. Through this business we will be providing digital forensics, security operations centre(SOC), and incident response (IR) to any kind threats the client may receive.

2.2. Problem/opportunity addressed:

Through this idea the issue of data theft and weak security infrastructure of any organisation will be addressed. This is important because without these elements of security it is useless for an organisation to operate today in these times of vulnerability.

2.3.Benefits/solution:

To counter these issues our business will provide the client with a digital forensics team, a Security Operations Center (SOC), an Incident Response (IR) team, and a legal team to fight for the clients against the intruders in the court.

2.4.Highlighting team:

Our technical team is divided into digital forensics, SOC , and IR teams. All of these teams are ready 24/7 to monitor and counter any threat and look into any previous incident that may have occurred.

Our legal team comprises lawyers and legal consultants that are highly educated in their respective fields as well as the field of cyber security.

2.5.Outline:

This project will take 10 months to operate at its full capacity, while the basic infrastructure will be made available within 6 months. The required seed funding is estimated at around $ 250,000. There will be two major milestones , the basic infrastructure and the fully functional business, and several other sub milestones that are divided in these two major goals.

2.6.Conclusion:

As discussed above this project can prove to be ground breaking if everything goes accordingly. Therefore it is requested to arrange a meeting to discuss the idea in more detail and get the fundings as soon as possible.

3.Introduction to Report

The first message to be transmitted over the network was done in 1969, by the research team at Department of Defense's Advanced Research Projects Agency (ARPA), led by computer scientist J.C.R. Licklider. Nowadays, we transmit nearly 88 terabytes of information including pictures, conversations, voice calls and important documents. Although this revolutionised communication, it created a new way for criminals to steal data for malicious reasons, they are referred as cyber criminals. Inoder to protect business, companies and individuals from cyber attacks and threat Cyber security companies have started to offer services to the public.

The purpose of this proposal is to outline the objectives and services that our company _name_ will be offering. Moreover, this report will also discuss the various interconnected procedures, the proposed budget, the setup schedule of the company as well as the responsibilities of the major departments and the team who will be responsible for supervising these crucial operations.

The four parts of this report will discuss:

A. Departments and their functions
B. The constant and crucial interconnected internal and external processes
C. various services provided
D. proposed technical methodology for setting up the company

The budget section will describe the financial strategy as well as the projected revenue. Finally the schedule section will describe the expected plan to set up the company

4.Technical Approach

4.1 Introduction:

The purpose of this section is to highlight the technical working of our organisation and to explain the working of the different departments and how they are interconnected.

4.2 Threat assessment:

There are many cyber threats a company might face. These can be classified as either internal or external. Our organisation implements solutions that prevent against both of these type of risk

4.3 Internal Threats:

A company might faces many internal issues such as:

A. Data breaches : which can be a result of social engineering, human error or even privilege abuse.
B. Social engineering: where attackers use publicly available knowledge to trick and manipulate employees to give up information or company secrets.
C. Privilege abuse: company staff members who use their privilege to engage in malicious activities such as modifying data and installing unauthorised software.
D. Malicious insiders: many companies nowaday have a serious problem with company moles, who leak confidential information under the guise of a normal employee.
E. Credential theft: attackers who steal or compromise employees' credentials, such as usernames and passwords, to gain access to the company's systems and data.

4.4 External threats:

A. Malware attacks: these are malicious codes that have a variety of ways to harm a company’s system.
B. Hacking: Hackers may exploit vulnerabilities to access a system to install malware, steal data or to perform any other type of malicious activity.
C. Social engineering: these attacks consist of attackers misleading employees to unsecured websites or malicious links to collect confidential information or sensitive data. They may even manipulate workers into giving sensitive data.
D. Denial of service: this is an attack where an attacker floods a network or website with fake requests to overwhelm it to cause disruption in operations, financial losses and damage the company reputation.

E. Ransomware attacks: attackers encrypt sensitive data of the company and force the company to pay them money.

4.5 Risk:

All these threats have a significant effect on the company. They may cause the company to suffer huge financial losses or even force them to close down. Some cybercriminals aim to collect information or company secrets and act as double agents, this can devalue the company and allow competitors to steal profitable ideas.

Another big reason hackers might attack a system is to ruin the company's reputation, and cause it significant business harm. This causes the company to bear a heavy financial toll. They occasionally target employees and hardware assets. This can raze the company, and can even significantly impact those businesses and individuals who are connected to the company.

The company might also face data loss and operational disruption which can exponentially increase losses.

In the end the company might face legal liability in terms of legal fees, employee recompense, lawsuits and even regulatory fines.

4.6 Technical Solution:

Our company offers solutions to mitigate these risks. Our technical department consists of SOC, incident responder and Digital forensics investigators. We also have a legal team to assist firms in recovering financial assets as well as facilitating them in matters of courts and legislative matters.

4.7 Security Operations Center (SOC):

The first line of defence that our company offers is the Security operations centre (SOC). It consists of a team of skilled individuals who monitor the system 24/7 to identify any type of malicious activity. Additionally, there are 3 divisions in the SOC hierarchy:

A. Tier 1: their sole responsibility is to monitor the system and report any type of suspicious activity. They monitor the complete system of the company from servers, firewalls, web servers to storage systems and databases. If any type of criminal illegitimate is observed it is escalated to a Tier 2 SOC.

B. Tier 2: their responsibility is to analyse the threats and issues escalated by tier 1 SOCs. They perform an in-depth analysis and determine the severity of the incident. They will also provide recommendations for containment, eradications and recovery to mitigate threats. If threat can not be dealt it will be escalated to the highest SOC authority tier 3

C. Tier 3: these represent the highest level of security. They work with other departments to contain and mitigate risks. They handle any cases which cannot be resolved by a T1 or a T2. Tier 3 SOCs are also responsible for managing T1 and T2 and are responsible for managing security policies, procedures and controls.

The company also provides 3 main services for companies that are already affected by a cyber attack, these include:

4.8 Incident Response(IR):

These skilled personnel are trained to locate and mitigate the effects of an unwanted cyber attack. They mainly target external threats.Their main task include, but not limited to:

A. Detection: Monitoring systems for breaches
B. Containment: Isolating affected systems to prevent further contamination.
C. Investigating: Collecting and analysing evidence to identify the scope and nature of the incident.
D. Mitigation: they work to create solutions to prevent attacks from occurring in the future.
E. Recovering: this includes recovering data and repairing systems to their original operational state.
F. Reporting: this includes documenting the incident as well and reporting it to the relevant personnel.

4.9 Digital Forensics Investigators:

Similarly to a normal investigator, forensic investigators target internal threats and their main purpose is to identify the culprit party or individual and collect legal evidence which can be used by a lawyer to catch the perpetrator and prosecute them to the fullest extent of the law.

A. Acquiring digital evidence: this includes using specialised tools to collect, analyse, and document digital evidence in a way which maintains its integrity and admissibility in court.
B. Recovering deleted or hidden data: this involves using techniques to recover intentionally or unintentionally lost and hidden data.
C. Analysing digital evidence: this involves reading metadata, file signatures, network logs, and other data to draw conclusions as well as determine how it is related to the case and the perpetrator.
D. Report findings: another crucial task of an investigator is to present findings in a concise manner, written and in a court testimony. They also must have the ability to explain complex technical concepts to non-technical stakeholders and executives.
E. Preserving the evidence trail: this is the most important task of a digital forensic investigator. All evidence must be handled and stored properly to maintain its integrity and its admissibility in court.

4.10 Legal team:

Our company also provides a very experienced legal team, who are highly experienced in the persecution of cybercriminals as well as the law that are related to such cases.

They can also assist the firm to recover any financial assets that have been lost. Additionally they are to recommend the best course of action in indicting criminals as well as drawing terms and conditions which have the company's interests in mind. Here is a sample list of our legal teams core functionality:

A. Proving legal advice and guidance to clients
B. Drafting and reviewing contracts related to cyber security.
C. Conducting risk analysis and developing cyber security compliance programs for clients
D. Representing clients in negotiations in cyber security matters.
E. Investigating and responding to cyber security incidents and breaches and recommending the correct course of action
F. Conducting due diligence for clients in mergers and acquisitions to assess cybersecurity risks and liabilities.

4.11 Limitations:

There are many limitations we face as a new company. From financial constraints to company experience these can not be bought but need to be developed over time. Currently we are proposing a medium business, meaning that if our clients face an extremely risky or a large-scale attack, we will have to sacrifice a significant amount of resources to mitigate the risks.

There is also the nature of the cyber security field, which is adversarial in nature. Cyber security firms are forced out of business by firms with more experienced personnel and more resources.

4.12 Conclusion:

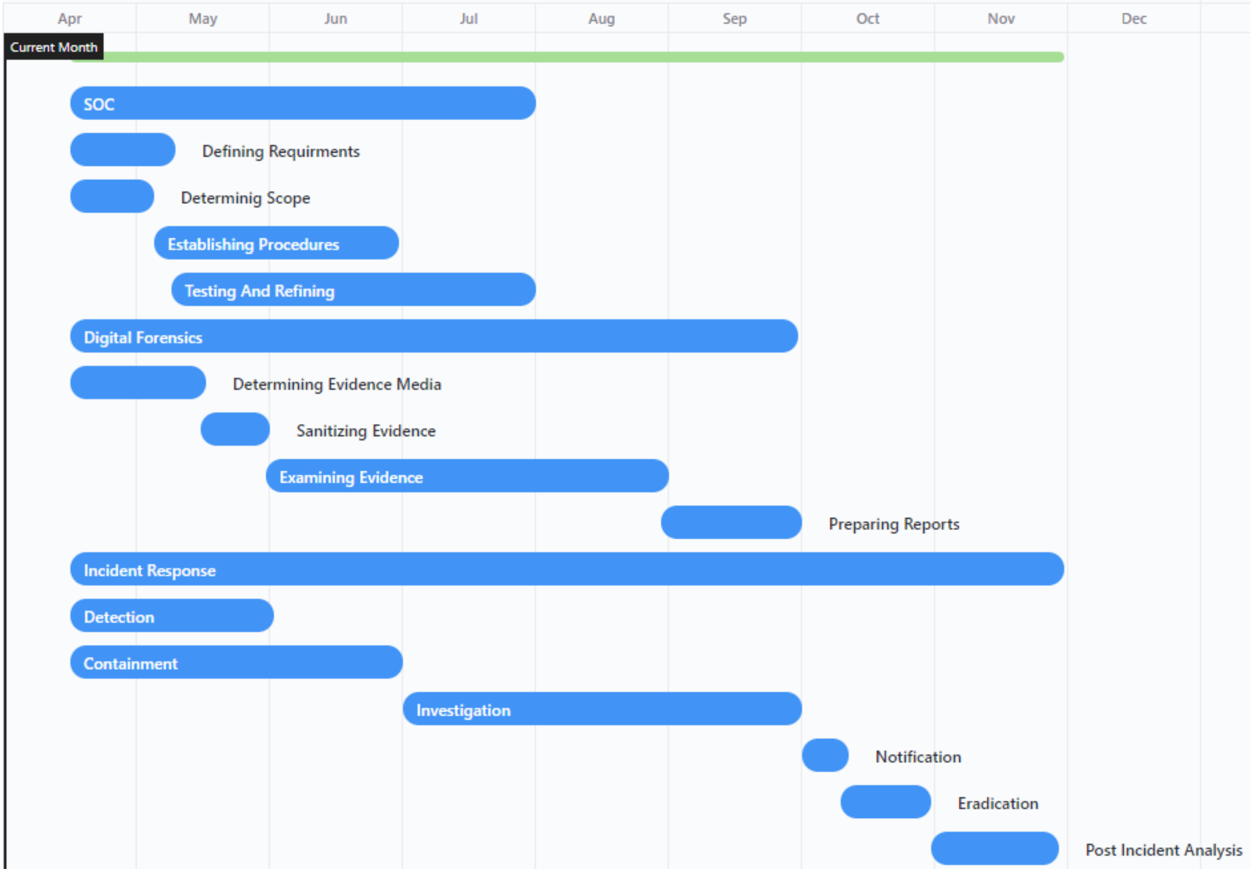
We propose a medium sized cyber security company that offers 4 main services to clients. Our objective is to increase cyber security awareness as well as secure unprotected systems. Our company provides budget friendly security services at economical prices. Additionally, we also offer a legal team to assist your company's legal qualms.

5. Schedule

As the project is approved it will approximately take 10 months to complete. The three main milestones are:

A. Setting up the SOC
B. Performing Forensics to sanitise the organisation
C. Performing IR incase of any threats

These milestones are further divided into subtasks which are dynamic depending on the scale of organisation and its activity. A gantt chart below shows the general timeline for the events.These milestones can be started as soon as the physical office is set up with equipment and the staff is hired. This process of physical setup and staff hiring can take up to four months. Therefore, the total duration of the project can add up to 14 to 15 months approximately.



6. Budget

BLUE FORTRESS	
Salaries	**Cost**
SOC tier 3	$30,000
SOC tier 2	$20,000
SOC tier 1	$10,000
Forensics investigator	$20,000
IR	$10,000
Legal team	$10,000
Material	
Computer workstations	$20,000
Servers	$10,000
Cables	$5,000
Stationary	$5,000
Office equipment	$10,000
Rental Cost	
Office building	$80,000
Miscellaneous	
Other	$10,000
Bonus	$10,000
Total Cost	**$250,000**

7. Conclusion

To conclude the proposal here are the main points that are discussed above. The main goal of this business proposal is to overcome the gap in the digital industry regarding integrity, confidentiality, availability, and recovery of data. To overcome these problems our business presents four solutions namely SOC,IR, Digital Forensics, and Legal team that will assist with counselling and court activities. There is an objection that the business may not be able to handle larger amounts of data due to it being in its initial stage. To address the objection it should be noted that the business stakeholders would not accept an assignment before analysing its size, so they would not accept an assignment that is beyond their resources. If the concerned person agrees that the business will prove to be beneficial for everyone involved, I would like to propose launching this business on the first of next month with a one-year trial commitment, to be reviewed after the first six months of operation.

Proposal Prepared By:

Abubakr Wamiq	**21k-3574**
Sarim Khan	**21k-4754**
Lachman Das	**21k-3632**
Mehdi Badami	**21k- 4771**
Shah Muhammad	**21k-3557**
Zain Raza	**21k-4755**