CyberLock Solutions

Professional Practices in IT - Assignment 3

Group Members:

Komal Waseem	20L-1114	(l201114@lhr.nu.edu.pk)
Nabeeha Mudassir	20L-1080	(l201080@lhr.nu.edu.pk)
Nisa Nadeem	20L-1141	(l201141@lhr.nu.edu.pk)

National University Of Computer and Emerging Sciences
Department of Computer Science
Lahore, Pakistan

Business Plan:

1. **Vision Statement and Profile**

   CyberLock solutions is primarily a cybersecurity company, providing digital security solutions to our customers. The vision behind the company is to be the leading provider of cutting-edge cybersecurity solutions, safeguarding the digital landscape and empowering organizations to thrive in a secure and trusted environment.

   Our mission is to deliver comprehensive digital security solutions, leveraging advanced technologies and industry expertise to protect businesses and individuals from evolving cyber threats. We are committed to providing unparalleled customer service, fostering long-term partnerships, and continuously innovating to stay ahead of emerging security challenges. Our ultimate goal is to contribute to a safer digital world, where organizations can operate with confidence, knowing their valuable assets and sensitive information are secure.

2. **Market Size and Target Customers**

   Due to the increasing reliance on IT solutions in every industry, cybersecurity is becoming a priority for organizations of every kind. The cybersecurity market comprises revenue generated from two types of products: Cyber Solutions and Security Services. According to *statista*, the revenue in the cybersecurity market of Pakistan is estimated to be $162.90 Million in 2023 and a market volume of $89.37 Million is from Cyber Solutions. The expected annual growth rate for the revenue is 12.13% for the next five years. The **total addressable market** for cyber solutions can thus be estimated to be around $100 Million to $150 Million per year.

   Moreover, the **market opportunity** for cybersecurity related software in Pakistan is approximately 35% according to the *PWC report*. Currently, cybersecurity based software houses have a limited presence in Pakistan since according to *Clutch Co*, there are only 39 firms in total in Pakistan that provide cybersecurity solutions. These facts make it a promising opportunity for growth and development.

   Businesses of every size can require cybersecurity solutions. The **target customers** can be divided into the following categories:
   - Government, military, security agencies and law enforcement agencies
   - Businesses using Automated Software Solutions
   - Software development companies looking for external cybersecurity solutions
   - IT Security Consultants

3. **Revenue Stream**

CyberLock Solutions is a company which focuses on keeping things safe in the digital world and makes money in different ways. One main way is by offering subscription plans for businesses to stay protected from online dangers. These plans act like shields for computers and networks, come with regular check-ups to make sure everything is secure. Another way CyberLock Solutions makes money is by creating special computer programs that keep out malicious content like viruses and hackers. Businesses pay to use these programs, making their online spaces safer.

Moreover, CyberLock Solutions teaches people how to be smart online through workshops. They teach employees in companies how to avoid falling into the traps that hackers set. If something goes wrong, like a cyber-attack happens, CyberLock Solutions is there to help businesses get back on track. They offer services to fix the problem and make sure it doesn't happen again.

4. **Value Proposition**

At CyberLock Solutions, our commitment will be to safeguard your digital world by offering unique solutions. We offer robust cybersecurity solutions designed to protect your online presence and protect against evolving threats and malicious activities. With our innovative security plans, companies will be able to trust that their business is shielded from cyber risks, ensuring a worry-free digital environment. What sets CyberLock Solutions apart is not just the strength of our defenses but the simplicity in which we keep you secure. We believe in making cybersecurity accessible to all, providing peace of mind through user-friendly solutions.

5. **Economic and cash flow assessment**

	2023
CASH OUTFLOW	
Salaries	($300,000)
Office rent	($36,000)
Utilities	($12,000)
Software Licenses	($50,000)
Taxation	($20,000)
Marketing Expenses	($80,000)

Interest and Loan Repayments	($15,000)
Net Cash Outflow	($513,000)
CASH INFLOW	
Return on Investment	$50,000
Revenue	$500,000
Funding	$350,000
Net Cash Inflow	$900,000
NET CASH FLOW	**$413,000**

6. Marketing and Expansion Plan

For the marketing of CyberLock Solutions, four main strategies will be used:

- **Social Media Marketing:**

  CyberLock Solutions uses the power of social media marketing to connect with its audience showing its presence in cybersecurity. By strategically analyzing platforms where its target audience is most active, such as LinkedIn and Twitter, the company ensures it stays at the top of the discussions. Engaging content, ranging from informative articles to insightful cybersecurity tips in the form of short videos, animations and posts is shared to showcase expertise. Moreover, CyberLock Solutions runs targeted ads to reach potential clients. Through social listening, the company gains valuable insights into the evolving needs and perceptions of its audience.

- **Email marketing:**

  At CyberLock Solutions, we make sure to stay connected with our friends, clients, and everyone interested in cybersecurity. We keep things simple by creating a big list of email addresses. This way, we approach people directly, whether they're clients, future partners, or people in the cybersecurity world. We intend to send them regular emails like easy tips for staying safe online, news about our cybersecurity tools, and even some special deals. This not only helps us keep everyone up to date but also makes our clients feel special, building strong and lasting connections with CyberLock Solutions.

- **Paid Advertising:**

  Our plan is to invest in advertising our company through various ways including targeted online advertising as well as native advertising. Google Ads and Social Media Ads on Instagram, LinkedIn and Twitter will be used to attract our target customers. We aim to leverage the precision targeting capabilities of Google Ads, optimizing campaigns to align with the cybersecurity-related needs and preferences of our target customers. Moreover, we also aim to invest in traditional advertising methods including television ads and billboards to gain a broader reach.

- **Event Marketing:**

  We aim to employ event marketing by having our company representatives actively attend various events such as cybersecurity-focused events, conferences, webinars and workshops. By participating in such events and networking with other participants, we aim to develop connections with potential clients and exhibit the capabilities of our company. For this purpose, we will continuously monitor the occurrence of cybersecurity-related events taking place in Pakistan or in online sessions to ensure our company representatives are able to attend as many events as possible in order to gain a broader reach for CyberLock Solutions.

As for the expansion plan, the following 2 strategies will be adopted.

- **Product development**

  The first expansion strategy is to increase sales and market share by offering customers innovative and new products that meet their changing needs and preferences. For this a thorough market research and customer needs analysis will be conducted to identify emerging cybersecurity threats, industry trends, and changing customer needs. Then after analyzing feedback from existing clients and engaging with potential customers to understand their specific pain points and requirements, we plan to identify innovation opportunities. As the market trend evolves, we plan to explore areas of innovation within the cybersecurity landscape. This could include advancements in threat intelligence, machine learning, behavioral analytics, or emerging technologies like blockchain for enhanced security. Particularly, AI in Cybersecurity is a recently emerging field, one common example of which is Predictive Threat Intelligence. This includes utilizing AI algorithms to analyze vast amounts of data from various sources, including the dark web and historical attack data, to predict and identify emerging

cybersecurity threats. This provides predictive insights, helping organizations anticipate and prepare for potential cyber threats. Another application is AI-Powered Endpoint Protection, in which we integrate machine learning models into endpoint security solutions to identify and prevent new and evolving malware threats.

- **Market penetration**

  The second expansion strategy is market penetration by maximizing the use of existing resources and gaining a larger share of the existing market. This approach involves selling more of our current products or services to our existing customer base or attracting new customers to your current market. We plan to enhance Product Features by identifying opportunities to improve and add features to existing cybersecurity solutions. This could include advanced threat detection capabilities, more comprehensive reporting, or integration with other security tools. As an example, we could enhance an existing endpoint protection solution with machine learning algorithms for better malware detection and behavioral analysis. We could also revise pricing strategies by introducing tiered pricing plans to cater to different-sized businesses, making the solutions more accessible to smaller enterprises. We could also offer limited-time discounts or promotional bundles for existing customers or new clients to encourage them to invest in additional cybersecurity services.

7. Damage Control Plan

We have identified the following risks and defined the damage control plan on how to deal with each of these risks:

- **Market Competition**

  To tackle the challenge of facing many other companies in the market, CyberLock Solutions has a plan to take proactive measures. We keep coming up with new and better ideas, work closely with partners, focus on what our customers need, use flexible marketing methods, make our brand more known, spend money on training our team, and keep an eye on what's happening in the market. These approaches will help keep our clients happy, and quickly adapt to what's happening in our industry. This way, we make sure we stay ahead and keep being a top choice for reliable and smart cybersecurity solutions.

- **Technological Complexity**

Since cybersecurity is an advanced field which is growing rapidly along with the growth in technology, building cyber solutions is a complex task. Developing software that is highly challenging to implement or integrate within existing systems can potentially lead to compatibility issues or operational complexities for clients. Additionally, adapting to rapidly evolving technologies in cybersecurity, such as Artificial Intelligence/Machine Learning, Blockchain, IoT security, etc requires ongoing learning and development. Moreover, dealing with advanced cyber threats that surpass conventional security measures is a challenge. Furthermore, while developing cyber solutions, legal compliance is necessary to ensure data privacy regulations and compliance standards are met.

To deal with such complexities, it is necessary to employ highly skilled and experienced cybersecurity professionals or to collaborate with industry experts for guidance throughout the development of cyber solutions. Moreover, it is necessary for employees to continue their professional development by continuous learning about new technologies and threats. Additionally, the focus should be on developing easy to use and integrate cyber solutions. Rigorous testing and quality assurance must be done to ensure cyber solutions work properly. Moreover, a compliance management department should be set up to ensure relevant industrial standards and legal requirements are met. Furthermore, partnerships can be done with more experienced software companies to create better cyber solutions by utilizing the skills and knowledge of employees of multiple companies.

- **Reputation Risks**

  The most significant reputation risk for our cybersecurity company is experiencing a data breach or security incident. If security solutions are compromised, it can lead to a loss of trust among clients and the broader industry. If our products or services do not perform as promised or fail to protect against emerging threats, our company's reputation for providing reliable solutions may suffer. Inadequate or slow customer support can lead to dissatisfaction among clients, damaging the company's reputation for responsiveness and assistance in times of need.

  To mitigate these, we plan to implement rigorous security measures internally to prevent data breaches. In addition, we plan to regularly conduct penetration testing and vulnerability assessments to identify and address potential weaknesses and develop a comprehensive incident response plan that outlines the steps to be taken in the event of a security incident. This plan should include communication protocols, responsibilities, and a clear chain of command. In the event of a security incident, we intend to communicate promptly and transparently with

affected clients, provide clear and honest information about the nature of the incident, steps taken to mitigate it, and future prevention measures, invest in thorough testing and quality assurance processes for all cybersecurity products, regularly update and patch software to address vulnerabilities and stay ahead of emerging threats and build a robust customer support infrastructure with well-trained staff capable of providing timely and effective assistance.

Plan for Initial Capital

Funding for our project will be potentially sourced through these 3:

1. **Business Angels.** Business angels commonly finance start-ups and established small and medium-sized enterprises (SMEs), providing a quick and straightforward way to secure the funding needed. It is important to develop a personal relationship with the business angel, as they can bring more to a business than just money. For this purpose Angel Investment Network PK was considered which is a network connecting business angels with growing companies. Business angels often provide between £25,000 and £750,000 (roughly 9,000,000 PKR). This type of investment is common when an early investment capital is required and when a business needs more than money. For our company, expertise of a seasoned investor would be handy and this is why business angels would be the top priority for us.
2. **Venture Capitalists.** A venture capitalist (VC) is an investor that provides young companies such as ours with capital in exchange for equity. Sarmayacar is a Pakistani VC Firm which backs daring entrepreneurs building market-transforming technology startups in Pakistan. Its portfolio is diverse and includes Bykea (ride-hailing app), Dot & Line (tech-education startup), Jiye(B2B marketplace), Oladoc (Digital healthcare platform). Recently they provided $13 million for Bykea as a startup investment capital. Similar to this, i2i Ventures is another VC Firm with an impressive portfolio with fintech companies, women-led tech startups etc. We feel they are closely aligned with our company's core values.
3. **Overdraft Loans**. Overdraft loans are a form of debt financing where a business is allowed to withdraw more money from a bank account than it actually has, up to a certain limit. Interest is typically charged only on the amount overdrawn.

Financial projections include:

Revenue Projections	**Expense Projections (Year 1 to Year 3):**	**Gross Margin and ROI**
Year 1: Projected Revenue: $500,000 Sources: Initial contracts with small businesses and local clients. Assumptions: Conservative estimate based on the first few projects.	Year 1: Projected Operating Expenses: $350,000 Categories: Salaries, office rent, utilities, software licenses. Assumptions: Initial hiring, setting up infrastructure.	Year 1: Gross Margin: 40% ROI: 10%

Year 2: Projected Revenue: $1.2 million Sources: Expanding client base, more projects from existing clients, and partnerships. Assumptions: Increased brand recognition and successful project deliveries.	Year 2: Projected Operating Expenses: $800,000 Categories: Increased salaries, marketing expenses, additional staff. Assumptions: Expanding team and marketing efforts.	Year 2: Gross Margin: 45% ROI: 15%
Year 3: Projected Revenue: $2.5 million Sources: Diversification of services, entry into a larger market. Assumptions: Expansion into new geographical markets and industries.	Year 3: Projected Operating Expenses: $1.5 million Categories: New office space, advanced software tools, employee training. Assumptions: Expansion into new markets requires additional investment.	Year 3: Gross Margin: 50% ROI: 45%

Some of the **risks** associated with these sources of funding include.

- Reliance on Individual's Decision: The investment is often dependent on the individual business angel's decision, which can be subjective and may change based on personal circumstances.
- Limited Funding Capacity: Business angels may have limited funds compared to institutional investors, potentially leading to insufficient capital for scaling operations.
- Equity Dilution: Accepting VC funding entails giving up a portion of ownership, leading to equity dilution for founders and early investors.
- High Expectations: VCs may have high expectations for rapid growth, and failure to meet these expectations could strain the founder-investor relationship.
- Debt Repayment: Overdraft loans require periodic repayment, and failure to do so can result in high-interest payments and strain on cash flow.
- Interest Costs: The cost of borrowing, including interest rates and fees, can be relatively high compared to equity financing.

These risks may be **mitigated** by.

- Diversify Investor Base: Seek funding from multiple business angels to reduce dependence on a single source.

- Negotiate Terms: Carefully negotiate investment terms to strike a balance between funding needs and equity dilution.
- Budget Planning: Develop a comprehensive budget to ensure the ability to meet loan repayments without impacting day-to-day operations.
- Negotiate Terms: Negotiate favorable terms with the bank, including interest rates and repayment schedules, to minimize financial strain.

There are various potential **exit strategies** for business angels and for VCs.

- Acquisition: A common exit strategy for business angels is through the acquisition of the startup by a larger company. This allows angels to sell their equity to the acquiring company.
- Buyback Agreement: Entrepreneurs may negotiate a buyback agreement with business angels, allowing them to repurchase the equity at a later stage or upon reaching specific milestones.
- Initial Public Offering (IPO): VCs often aim for exits through an IPO, where the company goes public, and VCs can sell their shares on the stock market.

Sample Project Plan - SecureVault: Advanced Database Security

Project Overview

SecureVault is a database security application which aims to provide confidentiality, integrity and authentication for sensitive data stored in databases. This application will be developed for ABC Bank since their database contains personal information about their customers such as their names, contact details, addresses, and identification documents as well as details about credit and debit cards associated with the bank, transaction data, and other sensitive business information. Therefore, a need arose to protect this data against database vulnerabilities. To solve this problem, CyberLock Solutions proposes SecureVault.

Key Features

The key features of SecureVault are listed below:

- **Data Encryption and Access Controls**: Strong database encryption mechanisms will be implemented to protect data at rest and in transit within the database in order to keep data confidential and provide data integrity. Granular access controls will be developed to restrict and monitor user access based on roles and permissions to ensure only authorized personnel are able to access relevant data.
- **Anomaly Detection and Intrusion Prevention:** Advanced anomaly detection algorithms will be deployed to identify unusual activities or access patterns within the database. Immediate alerts will be triggered and further activity may be blocked in case of suspicious activity depending on the severity of the actions.
- **Dynamic Masking and Tokenization**: Dynamic data masking and tokenization techniques will ensure that sensitive information is never exposed in its entirety. Even if authorized users are accessing data, the data will be masked. This minimizes the risk of data breaches.
- **Compliance and Audit Tools:** Comprehensive compliance tools for regulatory standards will be provided, enabling automated audits, logging, and reporting to ensure adherence to data security regulations. By automating these procedures, the problems regarding human errors will be eliminated and the compliance with legal and regulatory requirements will be ensured.
- **Automated Patch Management**: Automated patch management systems will be integrated to promptly address and update database vulnerabilities. This shall reduce the exposure to potential threats, making the database more secure.

Team Structure

The structure of the team required to develop SecureVault shall contain the following roles:

- **Project Manager:** manages the entire project and ensures project is delivered on time and on budget
- **Requirements Engineers:** elicit and negotiate requirements from the client, analyze requirements and document requirements
- **UI Designers**: design the UI for SecureVault
- **Data Scientists:** analyze data, detect anomalies in data, identify potential vulnerabilities and threats in database and design algorithms to prevent such threats
- **Cybersecurity Experts:** design the security architecture, encryption methodologies, and access control mechanisms
- **Database Engineers and Developers:** develop the system by implementing the security protocols, encryption methodologies, and access control mechanisms
- **Quality Assurance Team:** ensure the security system conforms to the requirements and meets quality standards
- **Compliance Specialists:** ensure the security system conforms to legal and regulatory requirements
- **Maintenance Team:** maintain the security system after deployment

Deliverables and Milestones

The phases of this project plan are listed below along with the deliverables to be completed at each milestone:

1. **Requirements Analysis and Security Mechanisms Research**

   Requirements must be gathered from ABC Bank through interviews, inspection and document analysis. Any infeasible or conflicting requirements must be negotiated. Once the requirements have been negotiated, they must be analyzed and prioritized.

   Extensive research must be conducted regarding the database vulnerabilities and threats as well as the security protocols that can be used to prevent and mitigate any possible attacks on the database. Moreover, data anomaly detection measures and data access control mechanisms must also be studied. Furthermore, different encryption methodologies must be analyzed and compared. The deliverable that will be created upon the completion of this phase will be a research report containing the complete findings and conclusions obtained from the research.

2. **System Design and Architecture**

   The system shall be designed before the development starts. The security mechanisms to be used and their architectures must be well-defined in order to proceed with their development. In this phase, the deliverables will be the System Architecture Document which shall contain the system and subsystem architecture diagrams, sequence diagrams, design and architectural strategies, and any other relevant information.

3. **UI Design**

   An easy to use and simple user interface must be developed for SecureVault. The developed interface must be approved by the client and end-users before proceeding with the next phase. The deliverable created in this phase will be the GUI screens for SecureVault.

4. **System Development**

   The complete system will be developed in this phase. Prototyping will be used to develop each feature, gain client and user feedback, implement the feedback, and develop the next prototype in an iterative manner. There will be a minimum of five prototypes created to develop each of the five features listed above separately. The final deliverable from this phase will be the complete application of SecureVault approved by the client.

5. **Testing**

   After the system has been developed, system testing will be done. Once system testing is complete, if any changes are required then further development will be done. Once all the test cases have been passed, user acceptance testing shall be conducted. The deliverables produced in this phase will be test execution reports.

6. **Deployment and Maintenance**

   After the user acceptance tests have been completed and passed, the system will be ready for deployment. If required then machines that support SecureVault shall be installed at ABC Bank and SecureVault will be launched. ABC Bank will be provided with a maintenance support team for the application.

References:

1. https://moitt.gov.pk/SiteImage/Misc/files/Roadmap%20for%20IT%20ITeS%20Growth.pdf
2. https://www.statista.com/outlook/tmo/cybersecurity/pakistan
3. https://clutch.co/pk/it-services/cybersecurity
4. https://solutions.technologyadvice.com/blog/b2b-cybersecurity-targeting/
5. https://www.data1qbit.com/markets-competition.php
6. https://www.upwork.com/resources/business-expansion-plan#:~:text=A%20business%20expansion%20plan%20outlines,or%20 invest%20in%20new%20 technologies