

online shopping system

Individual Essay Report



university of essex

Launching into cyber security 2024

In today's fast-paced digital world, businesses are always looking for innovative ways to improve their efficiency and adapt to the ever-changing needs of their customers. As the director of an IT consultancy firm that specializes in cyber security, we were approached by an online shop business seeking a tailored solution for their website. We have created a proposal that addresses their operational needs and includes robust cyber security measures to protect against potential threats.

Our primary goal is to expand our client base by providing customized solutions to businesses. We were approached by a local grocery shop looking for an IT solution to manage the challenges that arise from their expansion and growing customer base. Our proposal suggests implementing an Online Shopping System (OSS), considering the potential threats to cyber security and customer data protection.

The benefits of implementing an OSS are numerous. Firstly, it improves operational efficiency by streamlining processes. Online Shopping Systems make it easier to find what's needed because of the ability to search, and automation allows staff to handle increasing demands efficiently, reducing manual workload and errors. Secondly, an OSS enhances the customer experience by offering convenience. As it is available 24/7, customers are not limited by timing constraints, saving them time and energy. Thirdly, an OSS facilitates market expansion by allowing businesses to reach beyond their local catchment area. Lastly, an OSS is cost-effective as it optimizes resources and improves cost-effectiveness. Also, the employees will work efficiently with the lowest number of them we will save on salaries and accommodation extra. At the same time, working in an online shop will be optional for a vesical store. Better prices for the customers and cheaper deals are available online and accessible for price comparisons.

Cyber Threats and Mitigation Strategies: -

Potential Cyber Threats and Mitigation Strategies: The grocery shop owner should be concerned about the cyber threats and their type. The recent surge in cybercrime poses a heavy risk to businesses, especially online businesses. The owner should train their employees with special courses to avoid any risk that can reflect positively on their work. Online shops contain a lot of sensitive data that can affect their customers, like credit card details, addresses, and names.

1. Phishing Attacks:

This is the one potential threat that attacks target customer’s data. Phishing attacks steal sensitive information like usernames, passwords, credit card numbers, and information or other essential data to utilize or sell the stolen information.

1. Man-in-the-middle attack:

This attack is a type of cyber attack that stays between the parties. During the MiTM attack, the parties are communicating directly with each other without knowing there is someone who is spoofing and stealing the information. This attack is one of the most intense attacks; it allows the attacker to capture and manipulate sensitive personal information.

1. Ransomware:

It is a type of personal hacking that targets a person or company. Hacking aims to encrypt the files inside the device or block the operating system and then blackmail the owner for many.

1. Insider Threats:

This threat can compromise the integrity of the system. Addressing this risk involves regular security audits and vulnerability assessments. By periodically assessing system vulnerabilities and conducting penetration testing, potential weaknesses can be identified and rectified, and rectified proactively.

1. Data Encryption and Secure Transmission:

Implementing data encryption during the transmission is essential. This ensures that customer information remains secure during the online transaction. This process can create secure channels with suppliers and partners and is crucial for maintaining the integrity of the entire supply chain.

Customer Data Protection Compliance: -

Is protection compliance referring to the adherence of businesses and organizations to regulations and standards that are designed to protect the privacy and security of customer data. This compliance is essential to ensure that personal information collected from customers is handled, stored, and processed in a manner that respects individual privacy rights and meets legal requirements. The primary focus is safeguarding sensitive customer information from unauthorized access, use, or disclosure.

1. Government Regulations:

Compliance with local data protection laws is imperative in an online shopping system. At the Grocery shop, it is essential to stay updated and informed about all relevant regulations to avoid legal complications. Regular updates on regulation changes will be incorporated into the business strategy to ensure continuous compliance and secure all the customers’ data.

1. Privacy policies and transparency:

Presenting clear policies for the customers is essential for building trust. Delivering the data handling practices transparently is equally crucial. An online grocery shop will provide customers with a clear understanding of how their data is collected, processed, and protected.

Implementation Plan:

This plan for strengthening IT infrastructure through system development, employee training, and cyber insurance is a detailed strategy outlining the steps, processes, and actions an organization will undertake to enhance its overall cybersecurity posture and resilience. This plan focuses on three key pillars:

1. System Development

The developer’s experience is vital for successfully implementing the online shopping system (OSS). An implementation plan featuring a phased rollout will be established to avoid disruptions to the grocery shop’s requirements.

1. Employee training:

It is essential to conduct comprehensive cybersecurity training for all employees. The training will cover threats, secure online practices, and responses. Regular testing will be available for the employees to keep them updated on cyber threats and to send awareness.

1. Cyber insurance

Exploring cyber insurance options is a proactive measure to mitigate financial risks associated with potential cyber incidents. A comprehensive insurance plan covering potential losses resulting from data breaches and other cybersecurity-related events will be pursued.

UML diagrams in my proposal: a use case diagram and a class diagram:

1. Use case diagram.

Is a diagram that visually represents the interactions between users and a system under consideration.

A diagram of a person

Description automatically generated

In the use case diagram summary, the customer and the admin can log in/out of the system. Customers can search for the product, add to the cart, or update the cart by adding or deleting some items and adding the details for the credit card and shipment details. The seller can control the system, confirm transaction details, and prepare and shape the order. The admin follows up with orders and updates the website.

Class diagram:

It is a Unified Modeling Language diagram representing the structure and static relationships among a set of classes and their instances in a system. It visually represents the classes and their associations, attributes, and operations within the system.

A diagram of a customer

Description automatically generated

Summary of class diagram:

Customers log in with their ID and make some updates to their profile. The admin has the right to log in and out, as well as the customers' details if needed. The customer does some shopping and adds to the cart items so it is easy to check the total price; as well it can also be manage by the customer to add or delat from the cart or empty the cart. the payment has lots of Sanstev data like name, address, credit card number and date, and the payment method.

Summary:

In the rapidly advancing digital era, businesses constantly seek innovation to enhance efficiency and cater to evolving customer needs. As the director of an IT consultancy firm specializing in cyber security, we recently engaged with an online shop seeking a tailored solution for their website. Our proposal addressed operational requirements and incorporated robust cyber security measures to combat potential threats. The overarching goal is to expand our client base by offering customized solutions, as evidenced by another project with a local grocery shop that prompted the recommendation of an Online Shopping System (OSS). While emphasizing the potential cyber threats, this proposal outlines the significant advantages of implementing an OSS, including operational efficiency, enhanced customer experience, market expansion, and cost-effectiveness. The cyber threats outlined in the proposal underscore the need for businesses to be vigilant in the face of increasing cybercrime risks, especially for online enterprises. Mitigation strategies encompass employee training, security audits, vulnerability assessments, and data encryption during transmission. Phishing attacks, man-in-the-middle attacks, ransomware, insider threats, and data encryption are critical focus areas in safeguarding sensitive information such as credit card details and customer names.

Furthermore, the proposal emphasizes the importance of Customer Data Protection Compliance, necessitating adherence to regulations and standards designed to protect the privacy and security of customer data. Government regulations and transparency in privacy policies are crucial components of this compliance. The commitment to staying updated on local data protection laws and incorporating changes into the business strategy is essential to ensure continuous compliance and the security of customer data. The implementation plan outlines a detailed strategy focusing on System Development, Employee Training, and Cyber Insurance. System Development is crucial for the successful implementation of the OSS, with an emphasis on phased rollout to avoid disruptions to the grocery shop's operations. Employee training is identified as an essential component, covering threats, secure online practices, and responses, with regular testing to keep staff informed and aware of emerging cyber threats. Finally, exploring cyber insurance options is highlighted as a proactive measure to mitigate financial risks associated with cyber incidents, covering potential losses from data breaches and other cybersecurity-related events. In conclusion, the proposed solutions and strategies address businesses' operational and security needs and underscore the importance of compliance, transparency, and continuous improvement through comprehensive employee training and proactive cyber insurance measures. Collectively, these measures aim to strengthen IT infrastructure, enhance cybersecurity posture, and ensure the long-term resilience of businesses in the face of evolving cyber threats.

References:

# Daniel bossard, 2023. Cyber Resilience: Building a Strong Defense Against Cyber Threats. Linkedin.

# Daniyal M alghazzawi and Sahar badri, 2022. Using the B/S Model to Design and Implement Online Shopping System for Gulf Brands.MDPI.

# Julian de groot,2023. What Is Data Encryption? (Definition, Best Practices & More).digital guardian.

# 2023. How Security Automation Works. Centraleyes.

2023. Security, Compliance, and Governance, by Actian.