Sri Lanka Institute of Information Technology

Introduction to Cyber Security - IE2022

Lab Submission 01

IT22151056

De Silva K.R.K.D

Group – WD.CS 01.02

Exercise 01

i. Highest availability – Public information should be available.
Low confidentiality – Anyone can access public information.
Low integrity – public information integrity may not have a significant impact.

ii. Highest confidentiality – They have sensitive data, so unauthorized users should not have access to them.
High integrity – There should be no unauthorized modification of their sensitive data.
Low availability – Sometimes some sensitive data may not be in their organization.

iii. Highest availability - Administrative information should be available in their system.
Low integrity – Their administrative information is not important financially.
Low confidentiality – They are not sensitive like financial information.

Exercise 02

The physical setup

Vulnerabilities	Threats	How to prevent
The office is in the owner's house.	• Family members can access the office room. • Chances of losing important information.	Important information should be hidden.
Deadbolt lock.	• Anyone can unlock the deadbolt lock.	Use a biometric lock or a high-security lock.

Two open-able windows	Thieves easily can access the office.	Close all windows at the house when the users are not at home.
Has smoke alarms and external motion–sensor lights.	Unauthorized access.	• Use CCTV cameras. • Implement a backup power source.
A computer is use to store sensitive data without protection	Will hackers hack that computer so they can access all sensitive data and can moderate them.	• Keeping backup to sensitive data. • Applying passwords to all sensitive data.
An old desktop running Linux so it may not be able to support the latest security versions.	• Cyberattacks • Data loss	• Update frequently. • Keep backup and recovery.
• iBook laptop stores inventory database and credit card authorization software. • This database has past credit card transactions.	• Easy to theft. • Unauthorized access. • Data loss. • Malware attacks can happen. • Hackers can access bank details	• Owner can encrypt data. • Keep backup. • Apply network security. • Operating system and software update regularly.
Use a network printer.	• Unauthorized access and printing. • Data leaked.	• Apply high network security. • Use securing printer.
Use a wireless/wired router.	• Unauthorized access. • Hackers can attack.	• Change the password immediately. • Use encryption. • Update firmware.
iBook is connected via normal category five network cabling.	• Unauthorized access. • Attackers can create network traffic.	• Use a secured network and device. • Encrypt data.

Unsecured network	• Unauthorized access • Data loss	• Secure the router. • Update devices and the router.
Storing stocks in filling cabinets and plastic bins or using the garage.	• Theft • May have damaged stocks. • Unauthorized access.	• Use a cupboard or secure one to store stocks. • Protect them using key or biometrics. • Track and record about stock.

The Ordering Process: Web Orders

Vulnerabilities	Threats	How to prevent
This site is running an open-source shopping cart system	Unauthorize modification	Regularly update
Unencrypted email send	• Unauthorized access • Phishing attacks	Emails should be encrypted
Use insecure file transfer type	• Unauthorized access. • Data modification • Data loss	Use secure FTP like SFTP.
Store customer's details on the hard drive of big mac.	• Data loss • Details modifications	• Install antivirus software. • Data backup • Use firewall
Use printed orders	• Unauthorized access • Data loss	Secure 'Orders' clipboard printed only when necessary.

The Ordering Process: Phone Orders

Vulnerabilities	**Threats**	**How to prevent**
Writes down the order and all the customer's information on a scrap of paper.	Anyone can get customers' information with credit card details.	Use a secure method for note customer's information.
Orders are taped to the computer monitor.	Unauthorized access.	Remove orders from the computer monitor, when they are no longer needed.

The Ordering Process: Mail orders

Vulnerabilities	**Threats**	**How to prevent**
Customers write down orders in the system through emails.	• Data loss • Data entry errors	• Use the verification process. • Backup data
The owner places the money order in a bank bag for deposit.	• Theft of the bag.	• Use a secure bag for depositing.

Order Fulfillment

Vulnerabilities	**Threats**	**How to prevent**
The owner takes the 'Orders' clipboard to the garage	Unauthorized access.	Secure the 'Orders' clipboard.
Create customer record on iBook.	Unauthorized access.	Backup data.

Use POS software	• Financial losses. • Unauthorized access.	Software updates regularly.
runs the customer's credit card in the credit card authorization module.	• Unauthorized access.	Use a secure credit card module.

Data Storage/Retention

Vulnerabilities	**Threats**	**How to prevent**
The receipt from each order places in a pile.	• Unauthorized access. • Data loss.	Place the pile in a safe place.
Moves the order files on the Big Mac	• Unauthorized access. • Data loss.	Use secure file organization
The file boxes are kept on open wooden shelves in the garage for seven years	• Data loss • Unauthorized access	Store file boxes in a secure place

Policies

Vulnerabilities	**Threats**	**How to prevent**
The business has very few policies.	Lack of a definite policy	Expand policies
Employees not have require key or logins.	Unauthorized access	Apply access control.