

# Introduction

Basically, data protection involves protecting anonymity and dignity, while also ensuring the system's functionality. This indicates that 46 percent of corporations reported data breaches or cyber assaults in the 2017 Cyber Breach Study. The CIA triad is a paradigm developed for the management of information security protocols. In this context, we can find whether privacy is a collection of rules that forbid unwanted access to confidential data, integrity is the assumption that the information is trustworthy, secure, and finally, usability is the guarantee that access to the information is secured by permitted individuals. In IT, the four primary threats we have are intrusion, monitoring, modification, interception (Anon., n.d.)

## Fabrication

It typically sidesteps or avoids authenticity checks and mimics a fabrication attack. Therefore, preventing data redundancy and user verification is necessary in order to preserve secrecy in the system. It efficiently integrates information into counterfeiting or manufacturing or modifies the method. Consumers must also be aware of these kinds of risks and should still be ready to confront them in order to reduce demand and retain reputation. Since the key purpose of production is to obtain access to a device or facility, it is important to teach users and managers how to execute and withstand these forms of attacks.

## Interference

In order to protect secrecy in the system, we must block and delete all third-party intrusions from the system by hackers and other cyber criminals, who would otherwise damage the system and will hijack our connection. In order to maintain security in the system, we need to take steps such as user access restrictions and file permissions to ensure that our data and documents are not modified or hindered by any intruders. In order to continue functionality, malicious threats such as network intrusions and derailed service attacks must be stopped by taking additional security precautions, such as deploying proxy servers and firewalls.

## Modification

The details and information in the system can be branched or classified according to the harm that an attacker might do in order to continue confidentiality. It is a must to preserve honesty, precision and conformity in the system. Precautions should be taken to prevent or mitigate any wrongdoing from illegitimate actors that can be carried out. Additional protection appliances and applications such as firewalls and virus guards may be installed to continue availability. In the framework, additional safeguards must also be enforced against any intruders.

Interception  
The key approaches are data protection to preserve secrecy in the device and it is possible to use factor authentication. It may also be useful to educate workers to become more acquainted with How to Protect the device against potential confounders. To preserve credibility, a procedure such as an extreme accident or electromagnetic pulse must be used to detect interception (EMP). It is important to ensure the availability of system hardware and software on a timeline and to properly operate the system. It is also important to prevent the incidence of bottle neck by having sufficient bandwidth.

# Basic measures to strengthen a system's security

It is important to assess security threats and then define the strategies to handle them in order to manage and reduce cyber-attacks. An attacker may be a group or person whose abilities are focused on the expertise and resources they use to perform and strike. The initial step in mitigating and avoiding the risk is to identify the attackers' possible risks. The insecurity of our device must be measured by the possible danger or risks found. Vulnerabilities in the physical system may be vulnerability, or they may be in a non-physical way that may cause the attacker to weaken the system. We should define the possible ways to mitigate these vulnerabilities and to reduce the risks during this vulnerability review. In addition to how to develop effective compliance procedures, these risk tests will aid and the security staff in the system can be updated on current risks and must conduct daily reviews of any flaw in the system. In addition, in this vulnerability process, if an attacker is successful and the device is broken, we should understand what the consequences would be. Where and when an assault happens,

1)Obtaining data from illegal organisations or persons

2)Data control or modification that results in the lack of legitimacy

3)Customers would not be able to use it, and functionality may be destroyed.

In order for an attacker to succeed, since there should be flaws in the system, we should take several simple steps such as removing all unwanted user accounts Deleting all default or unnecessary file shares Deleting or aborting unsafe ports and services Enforce registry and file systems access protection Creating encryption mechanisms. While these security measures can help detect delaying or refusing attack, it is impossible to avoid all attacks until and attack is detected, without any rain forcing auctions, incident management operation can be launched. In order to detect any device attempts or intrusions, intrusion detection mechanisms for firewalls must be tracked on a daily or hourly basis. We need to define the base line for the usual working system and for the user activity until the tracking system has begun. Any anomalous behaviour could be detected, investigated after studying the predicted normal activity, and if it is a risk, we could take steps to eliminate the risk. By using automated software to assist with tracking and reporting, control of the device may be more efficient.

# Online Threats

Since we are building an online shopping store in the scheme, we need to consider the potential risks that might exist, such as,

* Data breaches
* Unsecured connection link

## Eavesdropping

This is a stealthy attack, Often known as spying, where someone seeks to take data from PCs, laptops, or other gadgets sent over a device. An unbound eavesdropping of attack vulnerabilities arranges communications to get to and receive the information being sent. It is difficult to detect eavesdropping attacks because they do not allow transmissions to be synchronized to give the impression that they are working strangely. It is difficult to detect stealthy eavesdropping attacks on the grounds that they do not enable scheme transmissions from all accounts to look anomalous. (Anon., n.d.)

## Identity Theft

In an online shopping environment, the principal security threat is identity fraud. Cyber criminals aim to loot personal information such as name, email address, phone number, home address, etc. in order to sell or use them in other malicious activities or to imitate the victim. A data breach is named anytime a hacker primarily obtains unauthorized access to a particular website through phishing. This privacy leaks have caused financial damage and have stolen their personal and financial details from customers. Because of the transactions carried out in this online shopping framework, the relationship must always be secured. T The customer's credit card numbers, identification information and other confidential data should be encrypted and stored in a secure server and database.

# Safety Infrastructure Plan

## Possible System Risks/Threats

Web-based applications such as this are wide-open during the service to different risks and challenges related to hardware and software or resulting from physical security vulnerabilities. Whenever such a flawed field occurs in a web-based information system, it really affects the organization's business function and willingness to deliver the service that the service collectors need. In this case, which is connected to the organization that aims to introduce an electronic business registration service in Sri Lanka, with the introduction of a web-based mobile supported solution that will include business registration services With the approach, and will strengthen the operation. It is worth evaluating the value of a variety of potential hazards, challenges, weaknesses and defects that the organization would have to move through in the event of instigating and enforcing the method before taking the measures of introducing the concept. The following can be defined primarily as the types of hazards and challenges found in the scenario for the system.

## Denial Of Service

There are types of quick but powerful outbreaks that can threaten the availability of web-based solution providers. What would happen here is that the computing capacity, bandwidth and other numerical variables will be absorbed by the DoS attack, rendering the real customers or users feel little beyond the service. This is a very lethargic online service and for a time, users will not be able to access the website. It often acts in a manner that would result in unwanted access to the infrastructure of the information system at these times of assault and stealing of information.

(Geek, 2019)

## Password Theft

Such kinds of risks can occur for a web-based infrastructure like this that provides big web services. What will happen is that criminals will attempt to steal users' credentials with password cracking tools to try to enter certain accounts inappropriately and access company information that is private and sensitive.

## Cross Site Scripting

This works in a manner where a hacker or intruder will insert JavaScript lines into the website's web pages and if this is not adequately protected, the hackers can deliver malicious code as a side script from the server and can publish it as a user message.

## Session Highjacking

Cookie hijacking or session spoofing is often referred to when it aims to bypass a valid session and the attacker may use this valid session and the identity of the user to access the data on the websites, connect with internal servers, and control the relevant information system.

## Sql Injection

This would be like cross-site scripting which includes the injection of malicious SQL statements into the website and subsequent access to the database by an attacker through deletion and access to important and confidential data.

## Insider Attacks

Workers operating inside the organization may serve as allies of the attackers and may leak the sensitive details needed by the attackers to initiate any attack.

# Main application/users/infrastructure protection specifications.

The organization listed here that plans to launch the latest web-based information system to provide business services should concentrate on defining the real security needs to be tackled to minimize the above-mentioned categories of risks, weaknesses and threats.

Enabling encryption

In order to secure website interactions such as client server contact and the identity of the server, database and network against threats such as phishing attacks, eavesdropping, SQL injection, cross-site scripting and Dos attacks, etc., the website should be encrypted.

It is possible to use Hypertext Transfer Protocol (HTTPS), IPsec and Secure Sockets Layer (SSL) to allow it, which applies security to all website communication.

## Enabling Multifactor Authentification

The organization will use various authentication methods in the authentication process, such as smartphone verification, e-mail verification, one-time passwords and temporary passwords, etc. This will be effective in combating risks such as login theft and intruders stealing accounts.

## Implementing RAID

This is a virtualization computing technology that can be used for many physical disk drives where database device crashes and disappointments associated with database disk drive malfunctions are prevented in server environments. The overall efficiency of the database can be improved with RAID, and data redundancy can be improved.

## Server continuous backup and archiving

The company will have to operate constantly on database and server backup to meet dangers such as data failure due to human errors, device climate and infrastructure failures, water and fire damage, virus infections and other facets of any possible danger associated with servers and databases.

## Doing security audits and network monitoring

Conducting compliance audits and intrusion detection with risk assessment techniques relevant to data security is essential. Network monitoring can be especially useful with this type of web-based network systems, as it can help system administrators identify some anomalous behaviour in the network traffic, identifying unfamiliar network requests. This would help to improve leverage over the live network's quality, which would be useful for improved network handling.

## Usage of VPN for remote networking purposes

This infrastructure can be related via a digitally generated tunnel or private network to contact on the public site which is internet. This will be very effective in removing such threats and obstacles in the internal communication processes and in engaging with consumers.

# Main features /security elements

## Application Level Gateway

It uses a software proxy whereby, when a user demands a service from the proxy, it validates the requests for their authenticity, then forwards the request and returns the response to the user. Here, in this type of setup, it is important to have separate proxies for each service, such that if the HTTP (web) proxy is being used, the user must first be authenticated to obtain external access from the proxy server. As they operate on different ports, it is not possible to access mail using a web proxy server.

## IDS

The IDS is a device or software program that may do tasks redirection engine, to identify any intruder operation. Network traffic is inspected by the traffic monitor module and data trends are checked by the recognition engine.

Accessible in data packets, and detecting whether there is an irregular existence by examining the pattern of data in data packets available within its database. The redirection engine will play the task of forwarding those packets to the IPS via this operation if it is sensed that there is some sort of intrusion.

## Implementing Honeypot

This is some kind of fake server that serves as a legitimate network server or information system that offers a phony target for attacking intruders and will not harm the real server. Honeypots provide a folder that holds fake knowledge that will pull the attacker into it.

## Firewall

This is indeed a network protection system which can be used to enforce network security where it could be programmed to accept or reject network traffic in a configured DMZ internal network or server environment. A firewall's simple duty avoid congestion between networks of different levels of trust and, in turn, to have a controlled gateway of different levels of trust between these areas. This emerges with the adoption of a security architecture and communication model that focuses on the notion of least privilege and separation of tasks.

## Using Vpn

It includes the use of a protected private network as the basis of communications for internal communications by organisations that operate the public network or the internet. In VPN communication, encryption is used by A VPN routing strategy that tightens the mechanism of contact.

# A comprehensive plan and actions taken to improve public user confidence, outlining both technological and non-technical measures.

* The organization can ensure that no software-based server errors occur at any time and that the web service is accessible at a rate of 99.9 percent. This security infrastructure should ensure that the action of any unauthorized action to downgrade performance or any Dos attack does not impact this website.
* Protection infrastructure should ensure that the user identity of the people who have enrolled on the website to get a particular service completed is not vulnerable to password stealing and account hijacking.
* Protection infrastructure should ensure that the user identity of the people who have enrolled on the website to get a particular service completed is not vulnerable to password stealing and account hijacking.
* As clients pay for the services they offer, the organization should ensure that they receive a safe checkout or purchase. For this reason, it is important to tighten internal compliance processes using improved security infrastructure and, at the same time, ensure that the business hires a reliable and stable third-party payment provider. It can help to block unwanted entry by intruders by using SSL encryption and HTTPS.
* Companies should follow a blog deployment plan and periodically update the blog with their national service standard, performance, protection and service effectiveness, security measures they have used, and guidance about how to do a service without being targeted by an attacker, etc.
* Via the good execution of the above-mentioned activities and procedures, it would be possible for the organization to raise the degree of public interest in both its security and service infrastructure.

# References

Anon., n.d. *commonplaces.* [Online]   
Available at: https://www.commonplaces.com/blog/6-threats-to-web-application-securityhow-to-avoid-it  
[Accessed 1 1 2021].

Anon., n.d. *skillsforcare.* [Online]   
Available at: https://www.skillsforcare.org.uk/Documents/Topics/Digital-working/AnIntroduction-to-Cyber-Security.pdf  
[Accessed 11 1 2021].

Geek, C., 2019. *ashandarshana97.blogspot.* [Online]   
Available at: https://ashandarshana97.blogspot.com/2020/01/are-sri-lankan-laws-sufficient-to.html  
[Accessed 1 1 2020].

# Workload

10707202 …… INTRODUCTION

10707193 …… Basic measures to strengthen a system's security

10707375…… Online Threats

10707363……… Possible System Risks/Threats

10707428…… Main application/users/infrastructure protection specifications.

10707297….. A comprehensive plan and actions taken to improve public user confidence, outlining both technological and non-technical measures.