**Priyanka Chaurasia**

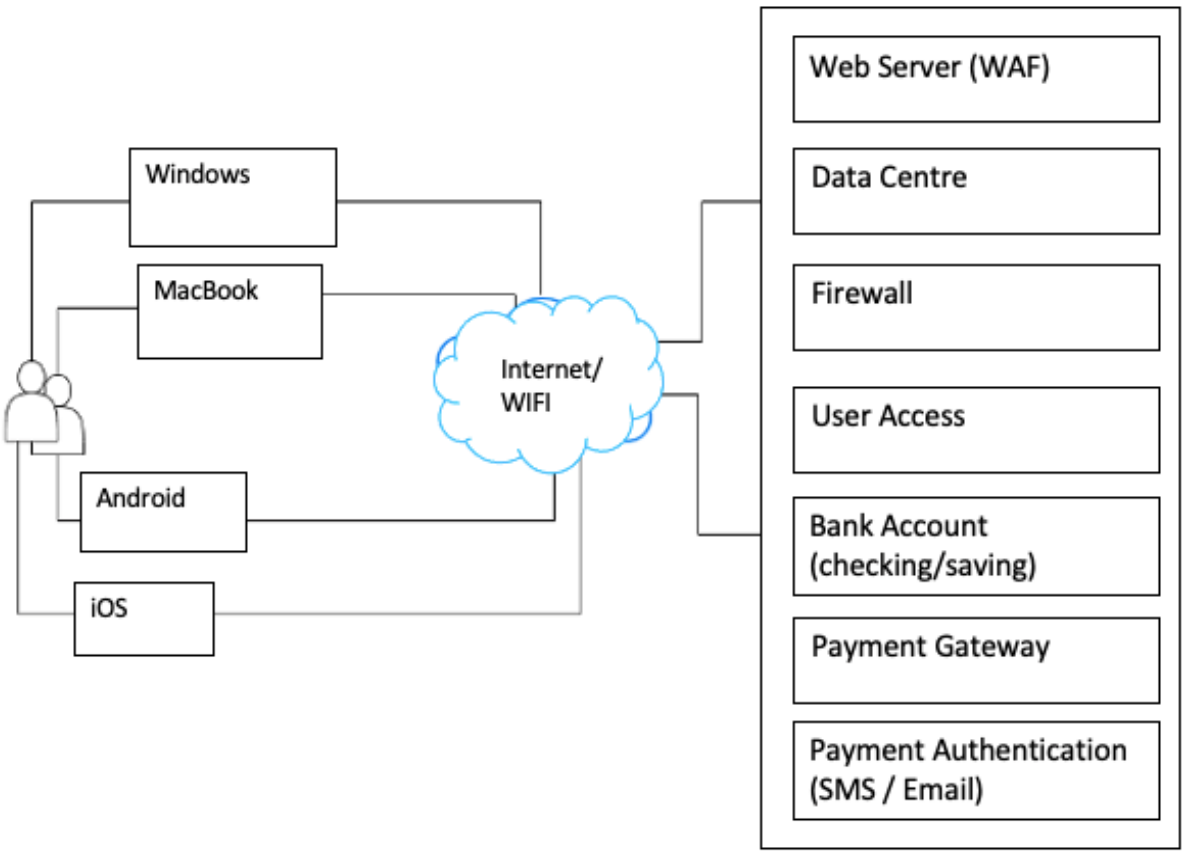
**CWID: 10478921**

# CS573- Cybersecurity Assignment 1

Banking application is an application which helps users to access their banking related activities, online. Banking application has a complex networking infrastructure, comprised of multiple data centres and edge computing to ensure smooth service. Users of Banking application use Windows, MacBook, iOS and Android devices for accessing the application; these devices are connected to Banking applications internal network via internet/WIFI. Banking application allows authorized users to handle checking/saving bank account as well as allows payment transaction using Payment gateway, and Payment authentication via SMS or email.

The diagram represents the valuable assets of Banking Application.

**Valuable assets for Banking Application**



# Threat Asset Matrix for Banking Application

**P=Probability, C=Consequences, R=Risk**

**Range: High=3, Medium=2, Low=1**

| Assets | Confidentiality | Integrity | Availability | Theft/Fraud |
|---|---|---|---|---|
| **Windows Devices** | P = 2, C = 3, R = 6 | P = 2, C = 3, R = 6 | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 |
| **MacBook Devices** | P = 2, C = 3, R = 6 | P = 2, C = 3, R = 6 | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 |
| **Android Devices** | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 |
| **iOS Devices** | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 |
| **Web Server** | P = 3, C = 2, R = 6 | P = 2, C = 2, R = 4 | P = 1, C = 1, R = 1 | P = 1, C = 1, R = 1 |
| **Data Centre** | P = 3, C = 3, R = 9 | P = 3, C = 3, R = 9 | P = 3, C = 3, R = 9 | P = 3, C = 3, R = 9 |
| **Firewall** | P = 3, C = 3, R = 9 | P = 3, C = 3, R = 9 | P = 1, C = 3, R = 3 | P = 1, C = 1, R = 1 |
| **User Access** | P = 2 C = 2, R = 9 | P = 3, C = 3, R = 9 | P = 3, C = 3, R = 9 | P = 3, C = 3, R = 9 |
| **Bank Account (Checking/Savings)** | P = 1, C = 2, R = 2 | P = 1, C = 2, R = 2 | P = 1, C = 1, R = 1 | P = 2, C = 2, R = 4 |
| **Payment Gateway** | P = 2, C = 3, R = 6 | P = 1, C = 2, R = 2 | P = 1, C = 1, R = 1 | P = 1, C = 1, R = 1 |
| **Payment Authentication (SMS or Email)** | P = 3, C = 3, R = 9 | P = 2, C = 3, R = 6 | P = 1, C = 3, R = 3 | P = 3, C = 3, R = 9 |

1. **Windows Devices:**

- **Confidentiality**- Source code is valuable to competitor but enterprise window operating system is well protected using Microsoft Defender, and other Anti-malware software.
- **Integrity-** Integrity of code is important; any changes in code can break the system. Enterprise windows operating system is well protected using Microsoft Defender, and other Anti-malware software.
- **Availability-** Disruption to the code is unlikely. Enterprise windows operating system is well protected using Microsoft Defender, and other Anti-malware software.
- **Theft/Fraud-** Theft or fraud is unlikely; systems are monitored through windows activity monitor and can easily be tracked using Microsoft's "Find My Device" feature.

2. **MacBook Devices:**

- **Confidentiality**- Source code is valuable to competitor but mac operating system is well protected using Apple's strong privacy policy and Anti-malware software.
- **Integrity-** Integrity of code is important; any changes in code can break the system. Mac operating system is well protected using Apple's strong privacy policy and Anti-malware software.
- **Availability-** Disruption to the code is unlikely. Mac operating system is well protected using Apple's strong privacy policy and Anti-malware software.
- **Theft/Fraud-** Theft or fraud is unlikely; systems are monitored through mac operating system activity monitor and can easily be tracked using Apple's "Find My Device" feature. Device data can also be erased remotely, if required.

3. **Android Devices:**

- **Confidentiality**- Android devices are well protected against any unauthorized access using Password, Passcode, Biometric, and other MFA features.
- **Integrity-** Integrity of mail and messages is essential, but android devices are well protected with Password, Passcode, Biometric, and other MFA features.
- **Availability-** Disruption to the android devices are unlikely as they are regularly updated with latest firmware and security updates.
- **Theft/Fraud-** Theft of Android devices is unlikely. However, if required, Android has many features like device tracking, remote phone lock, and remote data erasure.

4. **iOS Devices**:

- **Confidentiality**- iPhones devices are well protected against any unauthorized access using Password, Passcode, Biometric, and other MFA features.
- **Integrity-** Integrity of mail and messages is essential, but android devices are well protected with Password, Passcode, Biometric, and other MFA features.
- **Availability-** Disruption to the iPhones are unlikely as they are regularly updated with latest firmware and security updates.
- **Theft/Fraud-** Theft of Android devices is unlikely. However, if required, Android has many features like device tracking, remote phone lock, and remote data erasure.

5. **Web Server:**

- **Confidentiality**- Web servers act as a medium between the users and the actual application (data). They as a gateway to interface with the backend APIs. Users use internet to access Web Servers. Therefore, it is important that this access is secured using SSL/TLS i.e., the customer can access the Web servers using only HTTPS connections. This would help in maintaining the confidentiality of the data.
- **Integrity-** Web servers are an interface where the users query their data. Therefore, to ensure that the data integrity is maintained, it is important to implement features like input validation. Web Application Firewalls (WAF) can also be used to monitor, and filter the incoming traffic.
- **Availability-** It is important to make sure that the Web Servers are available 24/7 to ensure smooth user experience. For this, we can use multiple Web Servers and distribute the load between these servers using a load Balancer. This would also us make sure that the Web Servers are Highly Available.
- **Theft/Fraud-** Implementing above features along with a valid SSL certificate (signed by a Certificate Authority), can help us prevent fraud related to fraudulent websites, that are posing as the bank's website.

6. **Data Centre:**

- **Confidentiality**- Data centres are very important as all the data is stored here. Methods like Access Control List, Role based Access Control, Principle of least privilege, can be helpful here.
- **Integrity-** Even a minor change in the data can be very severe. It is important to ensure that the data centre is always protected. Encrypting the data using strong encryption keys, Digital Signatures, etc. can help us maintain the integrity of the Data Centre.
- **Availability-** Making sure that the Data Centre is Highly Available is very important. We can also use features like redundancy, Fault tolerance, DR, to ensure that Data from the Data Centre is available 24/7.

- **Theft/Fraud-** Data theft can affect the customers as well as the bank in a negative way. It is important to ensure that the Data is protected using the measures mentioned above.

7. **Firewall**:

- **Confidentiality**- Firewall is the first line of defence. It segregates the intranet from the internet and helps in monitoring the incoming and outgoing traffic using features like stateful and stateless ALs.
- **Integrity-** Firewalls can be very helpful in ensuring the integrity of the data transferred.
- **Availability-** We can use two firewalls using a Virtual IP. This can help us ensure High Availability, in case one of the firewall fails.
- **Theft/Fraud-** Firewalls can help us prevent Theft/Fraud of the data. To do so, it is important that we implement al the security features provided by firewall.

8. **User Access:**

- **Confidentiality**- Protecting customer data is very important. This can be implemented using Authentication mechanism.
- **Integrity-** Data on the fly, can be intercepted and hacked. Therefore, it is important that the customer always initiate a connection using https.
- **Availability-** making sure that the Authenticated user is always able to access the data that they are Authorized to do so, is very important.
- **Theft/Fraud-** It is important that measures are in place, to make sure that the customer data is always protected.

9. **Bank account (Checking/Savings):**

- **Confidentiality**- Banking services are built keeping in mind the security best practices and PCI DSS standards. It is also important to ensure that the customer's PII is protected all the time.
- **Integrity-** The integrity of Bank Account is well maintained using latest security protocols.
- **Availability-** Banking services should be available 24/7. This can be ensured by following the earlier-mentioned practices.
- **Theft/Fraud-** Bank Account theft/fraud is always possible. Hackers might be highly interested in these details. However, this can be protected using PCI DSS, PII, and other security best practices.

## 10. Payment Gateway:

- **Confidentiality**- Payment Gateways are protected using Authentication, Authorization, and Auditing (AAA) framework.
- **Integrity-** Payment Gateways helps us in maintaining the integrity of the user data.
- **Availability-** Payment Gateways are Highly Available and Fault tolerant.
- **Theft/Fraud-** Payment Gateways ca helps us reducing the chances of data theft.

## 11. Payment Authentication (SMS or Email):

- **Confidentiality**- It is important to make sure that only Authorized users have access to data (like OTP), sent using SMS or Email.
- **Integrity-** SMS and Email are a service on their own that follow the security best practices, to ensure that the data set via these services are not modified.
- **Availability-** Since SMS and Email are separate services, we do not have a direct control over its Availability. However, the service providers ensure that they provide the service 24/7.
- **Theft/Fraud-** SMS or Email data theft/fraud can be very dangerous (for example, consider One time Password for a transaction). It is important to make sure that the data sent through SMS and Email services are accessible only to the Authorized users.

| Asset | Estimated Risk |
|---|---|
| **User Access** | Total risk = 36 – 1st Highest Risk Asset |
| **Data centre** | Total risk = 36 – 1st Highest Risk Asset |
| **Payment Authentication** | Total risk = 27 – 2nd Highest Risk Asset |
| **Firewall** | Total risk = 22 – 3th Highest Risk Asset |
| **MacBook Devices** | Total risk = 16 – 4rd Highest Risk Asset |
| **Windows Devices** | Total risk = 16 – 4rd Highest Risk Asset |
| **Web Server** | Total risk = 12 – 5th Highest Risk Asset |
| **Payment Gateway** | Total risk = 10 – 6th Highest Risk Asset |
| **Bank Account** | Total risk = 9 – 7th Highest Risk Asset |
| **Android Device** | Total risk = 8 – 8th Highest Risk Asset |
| **iOS Device** | Total risk = 8 – 8th Highest Risk Asset |