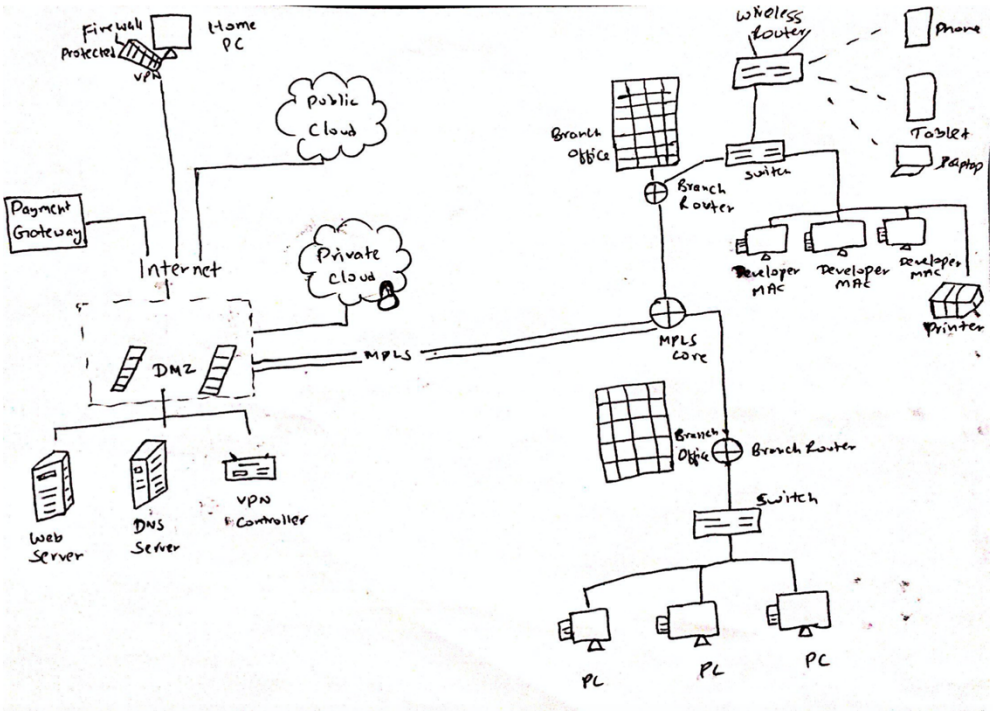
Stevens Institute of Technology

CS 573-A
Fundamentals of Cyber Security

Assignment 1

Name: Rachi Rana
CWID: 10455300

My company is a music company named Soothing your mind it handles musicians it includes various famous artists where they record music and also the production of music is handled. The company's main objective is to make music and look after the artists; like contracts and royalty fee. The cloud stores information about the artists, their contracts and most importantly information about the money and upcoming releases. Even though payment is handled by different outer agency since various artist are famous the company is very prone to cyberattacks; to get the information about the artists, unreleased music's, copyright infringement, etc.



Attack is not a vulnerability.

- Threats are outcomes, but outcomes as a result of some malicious actions.
- CIA- Confidentiality another way of saying Disclosure
- Integrity embedded to the system, surveillance, assets altered.
- Availability is another way of saying denial of services
- Theft- money or goods, take advantage of without actually having to pay for it.

P = Probability of threat

C = Consequence of threat

Risk (R) = (P *C)

Assets / Threats	Confidentiality	Integrity	Availability	Theft/Fraud
DMZ	P = 1 C = 1 R= P*C = 1	P = 1 C =1 R= P*C =1	P = 1 C =1 R= P*C =1	P = 1 C =1 R= P*C =1
Web Server	P = 3 C = 2 R = P*C = 6	P = 2 C= 2 R= P*C= 4	P = 1 C= 1 R= P*C= 1	P = 1 C= 1 R= P*C= 1
DNS Server	P = 2 C =2 R = P*C =4	P = 2 C = 2 R = P*C = 4	P = 2 C = 1 R = P*C = 2	P = 1 C = 1 R = P*C = 1
Virtual Private Networks (VPN)	P = 1 C = 1 R = P*C = 1	P = 1 C = 2 R = P*C = 2	P = 2 C = 1 R = P*C = 2	P = 1 C = 1 R = P*C = 1
Private Cloud	P = 3 C = 3 R = P*C = 9	P = 3 C = 3 R = P*C = 9	P = 1 C = 2 R = P*C = 2	P = 2 C = 3 R = P*C = 6
Public Cloud	P = 3 C = 2 R = P*C = 6	P = 2 C = 3 R = P*C = 6	P = 2 C = 2 R = P*C = 4	P = 3 C = 3 R = P*C = 9
Branch Router	P = 2 C = 3 R = P*C = 6	P = 1 C = 1 R = P*C = 1	P = 1 C = 1 R = P*C = 1	P = 1 C = 1 R = P*C = 1
Wireless Access Router	P = 1 C = 2 R = P*C = 2	P = 1 C = 1 R = P*C = 1	P = 1 C = 1 R = P*C = 1	P = 1 C = 1 R = P*C = 1
Switch	P = 1 C = 1 R = P*C = 1	P = 1 C = 1 R = P*C = 1	P = 1 C = 1 R = P*C = 1	P = 1 C = 1 R = P*C = 1
MPLS Core	P = 1 C = 2 R = P*C = 2	P = 1 C = 2 R = P*C =2	P = 2 C = 3 R = P*C = 6	P = 1 C = 1 R = P*C = 1
Payment Gateway	P = 2 C = 1 R = P*C = 2	P = 2 C = 1 R = P*C = 2	P = 1 C = 1 R = P*C = 1	P = 2 C = 1 R = P*C = 2
Printer	P = 1 C = 2 R = P*C = 2	P = 1 C = 1 R = P*C = 1	P = 1 C = 2 R = P*C = 2	P = 2 C = 1 R = P*C = 2
Developer MAC	P = 2 C = 3 R = P*C = 6	P = 3 C = 2 R = P*C = 6	P = 1 C = 2 R = P*C = 2	P = 1 C = 2 R = P*C = 2
Phone/Tablet	P = 1 C = 2 R = P*C = 2	P = 2 C = 1 R = P*C = 2	P = 1 C = 1 R = P*C = 1	P = 2 C = 2 R = P*C = 4

Firewall	P = 3 C = 3 R = P*C = 9	P = 3 C = 3 R = P*C = 9	P = 1 C = 2 R = P*C =2	P = 1 C = 1 R = P*C =1
PC	P = 2 C = 2 R = P*C = 4	P = 3 C = 2 R = P*C = 6	P = 3 C = 2 R = P*C = 6	P = 1 C = 2 R = P*C =2

DMZ: DMZ Network gives organizations extra layer of protection in detecting and mitigating security breaches before they reach the internal network, where the valuable assets are stored. It routes different servers to different zones and networks which makes the risk estimate not that high hence making the effect on the overall Confidentiality, Integrity and Availability (CIA) low and also the occurrence of use of product illegally is also low.

Web Server: The web server links the internal database server through firewall while still falling under the DMZ protections it also stores sensitive information to ensure the safety of the internal database.

Confidentiality: It does contain sensitive information but not that it would hamper the company's workflow, but they are very prone to cyberattacks for obtaining access.

Integrity: An inconsistency it affects the contents the user will see on the website, as it is in charge of getting and sending data accurately to the interface to display the information to the user.

Availability: Though susceptible to attack it is abundantly available and are changed between load balance and maintenance.

Theft/Fraud: Actually, monetizing from the information is short as the information it contains is not quite that sensitive/valuable.

DNS Server: DNS is the phonebook of the Internet responsible for finding the correct IP address for the needed sites. The attackers want to trick users into entering their private data into unsafe websites. **Theft/Fraud** is not that high.

Confidentiality: It has a probability of being targeted to steal the corporate information by performing some kind of phishing attack.

Availability: Only a large DNS outage would make notable portion of the DNS unavailable so even if the probability of an attack is high, the consequences is quite low.

Integrity: Inject malware into the victim's system. If the company's DNS is down the individuals can use the public DNS server it would mean more threats but, it would be until the company's DNS is back and running making the risk estimate on the higher side.

VPN: The VPN uses two factor authentication which makes it difficult to affect the overall CIA profoundly. The chances of **surveillances** are low but the consequence or after effect is a little high. **Availability** is secured. **Theft/Fraud** is less as mentioned due to the use of two factor authentication(when the user wants to login to the company's site using their username and password they will also need to confirm it by using another encrypted code sent to their phones/tablet) which makes it difficult to actually use the datas without actually having to pay for it.

Private Cloud: It contains highly sensitive and classified data of Soothing your mind company; finished product to be released, artists contracts and other information that are valuable to the company.

Confidentiality: Well as it does contain a lot of information about the upcoming releases like albums, lyrics, new unreleased music, artists contracts, etc. So, the probability of an attack and when the attack does get through the consequences both are high, as the cloud contains important datas of the company.

Integrity: In cloud data is stored in multiple locations making it exceptionally difficult to lose. If you ever experience difficulty retrieving your **data** from the **cloud** it **can** always be retrieved from another **data** center. Since **data** center storage is decentralized in nature it's actually much safer than on-site storage yet if an attack does get through it would hit hard.

Availability: The cloud has the capacity and hardware to store large values of data for longer times so there is a small risk for data unavailability. As it is a private cloud and not many people can access the cloud in the system the consequences are low because the flow of traffic to access those data is already not that high in the first place. Hence, the data unavailability is low.

Theft/Fraud: As it holds information that could be sold off involving money; cryptocurrency, or copyright infringement. For Soothing your mind company, the probability of theft is high but not as high as when or if the attacks get through which puts consequences even higher.

Public Cloud: It contains data that are being currently worked on like music that will be released into the world from famous musicians.

Same as the private cloud but the **confidentiality** consequence is not on red high alert as it can create a wide range of scenarios such as like free promotion since it will be released eventually.

Integrity: Most cloud systems use multi-layer cryptography to ensure its integrity. Although a little more chance than in private cloud, when the attack does occur it can cause a lot of damage to the core of the system.

Availability: Data unavailability is more considered to private cloud as there is more traffic flow however since cloud has the capability and hardware to store large values of data for longer times the chances of data unavailability is low.

But **theft/fraud** is high cause can monetize from the stolen datas/music's and that has happened before in the music industry.

Branch Router: **Confidentiality/Integrity;** Attacks can occur in the form of **distributed denial of service and brute force attacks** which makes it susceptible and affect the accuracy of the data that passes through it.

But generally, it **does not have much impact to the work of the network**.

Wireless Access Router: Although wireless routers are an easy opening, for Soothing your mind company an attack would not be alarming cause these attackers could only gain access to the personal devices of the employees and even if the information maybe **sensitive**, from the company's perspective it would **not be of high value**. The Soothing your mind company also orders routers from a **different router company** thus making it more difficult for hackers to get through even with the use attacks like **brute force attack**. The **CIA** affect as a whole is **low**.

Switch: Switch are used to route different servers to different zones and networks and **do not necessarily affect the CIA of the of the systems**.

MPLS Core: It is a traffic routing mechanism that makes the feeling of private by directing the packets based on predetermined labeled paths within the network while allowing shared network

elements. But since there is no encryption involved it does create a security risk. **Confidentiality/ Integrity:** Although a breach of this does not lead to a security problem, an intrusion would be to gain unauthorized access to resources, but it would not be high risk to the system as a whole.
Availability: DoS (Denial of Service) attacks can cause unavailability to authorized users making the consequences of those attacks high.
Given that it would be easier to gain access to the system if the attacker knows the address but if the address is not known an attack becomes much more strenuous. From this kind of attack **Fraud** is very low.

Payment Gateway: Since the payment gateway is connected to the Internet it is prone to attack but since it does not fall under my company's network even if the chance of it getting attacked is high, access to information would be little hard to pinpoint and the chance of just for the surveillance is also low. The theft/fraud occurrence is high but again as it is connected to the public internet and it falls under the jurisdiction of another company, handling it. There might be the case that the musicians might get delayed payment but that would be it. I would say for Soothing your mind company the consequence of an threat is not that high but does have a high probability of getting attacked.

Printer: Confidentiality and Integrity, it does produce a security risk when or if the attacker gets hold of the printer's OS and someone could view all of those information, but overall CIA threat is low compared to other assets.
Availability: Printer is not the most core aspect of the company but in case of an attack it might cause traffic influx which can cause unavailability.
Theft/Fraud: Since this is a record label even if the theft probability is low the consequence is a little high as there is a chance of use of the product without actually having to pay for it. Especially in case of Soothing your mind company which in public spotlight there is a chance of theft and illegal use of data.

Developer MAC: The Developer MAC is already quite secure and for the Confidentiality and Integrity as the employees are working on it the probability is not that high but in case it occurs

that could cause damage once embedded into the company's system. But other than that, since MAC computers are pretty secure the risk is not that alarming.

Phone/Tablet: For phone and tablet since these are used by the workers for their personal use even if the probability is high the overall risk of CIA is not that high, but incase these attackers get hold of the devices of musicians or more important person they could sell the contents, so theft/fraud could take place.

Firewall: Firewall is a network security system that monitors, and controls incoming and outgoing network traffic based on predetermined security rules.

Confidentiality: Affected most in attacks as the first in line of defense making it more exposed to cyberattacks.

Integrity: Due to the imitation of actual packets there is a high chance to go through the firewall making the system at risk as a whole.

Availability: If the firewall is not responding most networks have reinforcements.

PC: For the company Soothing your mind the PC is mostly used to handle the information regarding royalty fee and this is used in a more secured zone making the area more prone to attacks. As attacks can be in the form of trojan horse, DDos, to traffic hijacking, spyware so the CIA would be affected mildly even if the probability of an attack is quite high.