Assignment 1

Threat Asset Matrix

CS 573 - Introduction to Cyber Security

Fall 2021

Rahul Godugupally

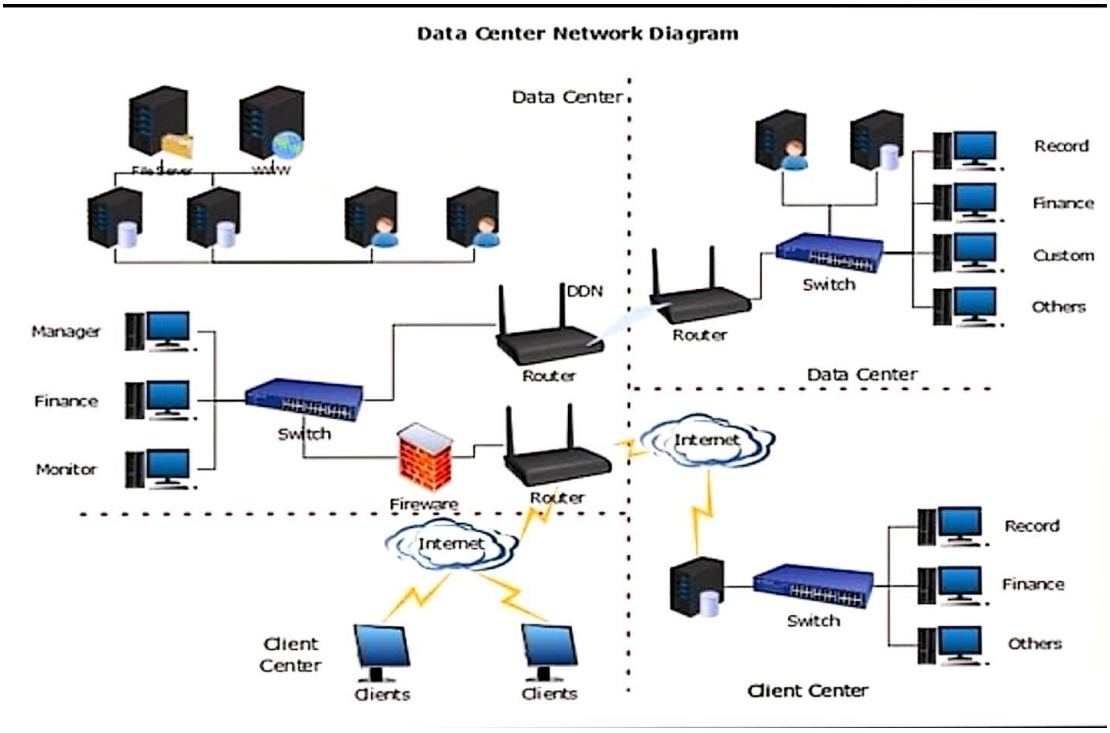
CWID: **10470581**

Stevens Institute of Technology

This is a detailed threat assessment (Threat asset matrix) of a Cloud service provider's Data Center. The main aim of the data center is to have a 99.98 percent uptime(availability) and a good fault tolerance. The Data Center here can be classified as a tier 3 data center. The data center provides PAAS (platform as a service) and IAAS (infrastructure as a service) facilities to its clients. The client data is also a crucial part of looking at the risk assessment.

Since the data center must maintain an uptime of 99.98 percent, Availability becomes a critical aspect in the assessment of assets in the data center. In case a downtime occurs, the data center will switch to a temporary backup power supply, as the clients of the data center expect their consumers to have its services available to them 24/7. Similarly, with internet connectivity from various ISPs as the bandwidth it requires is very huge.

The data center also houses the company's data such as its own software database, access information etc. Also, sensitive information such as PII, Employee payroll etc.



A Fictitious Data Center Network Diagram

THREAT ASSET MATRIX

ASSETS	**CONFIDENTIALITY**	**INTEGRITY**	**AVAILABILITY**	**THEFT/FRUAD**
Servers (Application, web, File, Proxy servers etc.)	P-4 C-4 | **R-16**	P-4 C-5 | **R-20**	P-5 C-5 | **R-25**	P-2 C-4| **R-8**
Data center management software- DCIM (Orion)	P-4 C-5 | **R-20**	P-4 C-5 | **R-20**	P-3 C-5 | **R-15**	P-4 C-5 | **R-20**
Client Data (Database, Storage)	P-5 C-5 | **R-25**	P-5 C-5 | **R-25**	P-5 C-5 | **R-25**	P-5 C-5 | **R-25**
Company database (Proprietary data, privilege access info,)	P- 5 C-5 | **R-25**	P-5 C-5 | **R-25**	P-5 C-5 | **R-25**	P-5 C-5 | **R-25**
Cloud Software Code	P-5 C-5 | **R- 25**	P-5 C-5 | **R- 25**	P-5 C-5 | **R-25**	P-5 C-5 | **R-25**
HVAC	P-2 C-3 | **R- 6**	P-2 C-4 | **R- 8**	P-2 C- 4 | **R- 8**	P-1 C-1 | **R-1**
Network Security Devices (Firewall, IDS, IPS)	P-4 C-3 | **R- 12**	P-3 C-5 | **R- 15**	P-3 C-4 | **R- 12**	P-2 C-3 | **R-6**
LAN (devices, Routers, Switches etc.)	P-2 C-2| **R- 4**	P-2 C-2 | **R-4**	P-2 C-4 | **R-8**	P-1 C-2 | **R-2**
Employee Workstation (PC's, Tablets)	P-3 C-3 | **R- 9**	P-3 C-4 | **R- 12**	P-2 C-3 | **R-6**	P-1 C-4 | **R- 4**
Employee - Email, Calendar, Office	P-4 C-4 | **R- 16**	P-4 C-4 | **R- 16**	P-3 C-3| **R-9**	P-3 C-4 | **R-12**
Employee Payroll (PII, Account info etc.)	P-3 C-4 | **R- 12**	P-3 C-4 | **R- 12**	P-2 C-3 | **R- 6**	P-2 C-4 | **R- 8**
Network connectivity (internet)	P-1 C-2 | **R-2**	P-2 C-4 | **R-8**	P-4 C-5 | **R-20**	P-2 C-2 | **R-4**
Power supply (Electricity)	P- 2 C-3 | **R- 6**	P-3 C-3 | **R-9**	P-4 C-5 | **R-20**	P-2 C-3 | **R-6**
Logs, (account info, access logs etc.)	P-2 C-3 | **R- 6**	P-3 C-4 | **R-12**	P-2 C-2 | **R- 4**	P-2 C-3 | **R- 6**
Retired Disk Drives.	P-1 C-3 | **R-3**	P-1 C-1 | **R- 1**	P-1 C-1 | **R- 1**	P-1 C-3 | **R-3**

R- RISK, C- CONSEQUENCE, R- RISK = P*C.

Scale (Risk level estimate)

1. Very low
2. Low
3. Medium
4. High
5. Very high

PRIORITY	ASSET	ESTIMATED RISK
1	CLOUD SOFTWARE CODE	100
2	COMPANY DATABASE	100
3	CLIENT DATA	100
4	DATA CENTER MANAGEMENT SOFTWARE	75
5	SERVERS	69
6	EMPLOYEE -EMAIL, CALENDAR, OFFICE	53
7	NETWORK SECURITY DEVICES	45
8	EMPLOYEE WORKSTATION (PC'S, TABLETS)	41
9	POWER SUPPLY	41
10	EMPLOYEE PAYROLL	38
11	NETWORK CONNECTIVITY	34
12	LOGS, (ACCOUNT INFO, ACCESS LOGS ETC.)	28
13	HVAC	23
14	LAN EQUIPMENT	18
15	RETIRED DISK DRIVES.	8

EXPLANATION : -

A) SERVERS (Application, web, File, Proxy servers etc.): They are the main components of the data center. They include powerful processors with huge computing power and should be well secured. They respond to requests made by the clients and fetch the right information for them. They could be vulnerable to a botnet attack.

1. CONFIDENTIALITY - Since it's a physical box located on the rack, disclosure of its information such as the OS it is running would not have a huge impact on the data center unless there is a vulnerability for that type of system. Still better to avoid disclosure.
2. INTEGRITY – Servers are responsible for providing data to the client if the data is somehow fiddled with the client will not receive what he seeks. Data processed is at risk and it is important to safeguard.
3. AVAILABILITY- Data in the servers should be always available as the goal of the data center is to have 99.9% fault tolerance. A DDos attack will lead to huge impact in this sense. No one likes error 404.
4. THEFT/FRAUD - As it is a physical box in a secured data center room the chances of it being stolen are low unless someone manages to break into the data center server room and manages to open the rack.

B) DATA CENTER MANAGEMENT SOFTWARE (DCIM): This software monitors, measures and manages the data center resources. It is essential for properly running the data centre in an efficient manner.

1. CONFIDENTIALITY - As it keeps logs and monitors the different assets in the data center, they might be valuable to a competitor or an attacker. It is important that this information is not obtained by anyone else.
2. INTEGRITY - The DCIM database should not be tampered with as it has baselines for alerting employees in case anything out of the ordinary occurs. Hence a high risk is estimated.
3. AVAILABILITY-It must be available for the engineers to monitor the data center. Hence availability is important for them to monitor the systems well and in time.
4. THEFT/FRAUD - As DCIM controls and monitors the rest of the assets in the data center. It should have a good level of confidentiality. Unauthorized access could lead to a lot of trouble

C) CLIENT DATA: This includes everything that the client decided to store in the data center. It might include Sensitive and critical data which is very valuable to the client.

1. CONFIDENTIALITY - It is imperative that this data remain confidential and only the client has access to the data. As it might include sensitive information, High risk is estimated as if the data falls into the wrong hands it will lead to a lot of trouble.
2. INTEGRITY - The data should remain unaltered and any changes in this data could lead to the client's service not functioning as expected. Destruction of this data will be very expensive. Hence high risk is expected.
3. AVAILABILITY- A DDos attack might lead to serious impact for the client and since the data center promises 99.98% uptime it is imperative to maintain availability. If the clients can't access the data in time that could lead to a loss in revenue and impact the business.
4. THEFT/FRAUD - As the data might include sensitive information, PII etc. the estimated risk is very high.

D) COMPANY DATA – This includes anything from Companies own data storage. From its records to employee Privilege access records, PII etc. Has confidential information so risk is high. (It should be closed off from the internet and come under the local network, if all the data contained is used for internal purposes.)

1. CONFIDENTIALITY - High risk of unauthorized party getting access to the data. Should be well protected against unauthorized access. (For reasons same as above)
2. INTEGRITY - Data should not be tampered with as an attacker may access privilege and make his way into the system. High risk expected.
3. AVAILABILITY-Data should always be always assessable, and denial of service could result in huge impact. High risk expected.
4. THEFT/FRAUD - As it contains Confidential Information, expected a high risk of theft.

E) CLOUD SERVICE CODE (CLOUD SOFTWARE): This includes the code on which the cloud service company runs on. Proprietary code and documentation

1. CONFIDENTIALITY - No one should be able to access the source code of the service provider as the code is not open source. Hence a high risk is estimated if it is falls into someone else's hands.
2. INTEGRITY - Changes and destruction of code will lead to massive impact on the company. No part of the code should be tampered with. Hence a high risk is estimated.
3. AVAILABILITY- Need to be able to access it for functioning of the operations. Disruptions could lead to a lot of impact on business. So high risk is estimated.
4. THEFT/FRAUD - As this is an intellectual property theft and fraud of any kind will have a huge impact on the company. High risk is estimated.

E) HVAC (HEATING, VENTILATION AND AIR CONDITIONING): Essential for proper functioning of the servers as they generate a lot of heat. The servers need to be cooled down in a proper manner (usually in hot and cold aisles), taking security into account as HVAC systems can be used to break into the data center or could be shut down to reduce the efficiency of the servers

1. CONFIDENTIALITY - it is important to keep the layouts of the hvac system confidential as it can be used to break into the data center server room. But breaking into a data center is very difficult.
2. INTEGRITY - Hvac system should not be tampered with as it is essential for maintaining the temperature of the server room, which in turn helps in efficient working of the systems.
3. AVAILABILITY- Hvac should always be preset, for proper functioning of the servers. If the system is down it will lead to the servers heating up and not functioning efficiently.
4. THEFT/FRAUD - Very low risk (negligible) of someone stealing or using data centers HVAC system.

F) NETWORK SECURITY DEVICE

i)FIREWALL: Primary line of defense. Used to only allow communication (filter traffic) to certain ports which are allowed.

ii) IDS, IPS: IDS (INTRUSION DETECTION SYSTEM), IPS (INTRUSION PREVENTION SYSTEM) Used within the network infrastructure to identify and prevent network attacks such as DDos.

1. CONFIDENTIALITY - Attacker can see what ports are used to communicate or allowed through the firewall, through enumeration using tools such as NMAP, fair amount of risk expected as it might lead to an **attack vector.**
2. INTEGRITY -Firewall rules being tampered with will lead to huge amounts of impact and servers not communicating to the client. Fair amount of risk expected.
3. AVAILABILITY- Firewall should always be available to keep an eye out on the inbound traffic. High risk expected. With IDS and IPS if they are not functioning then the data center could face network attacks such as ddos.
4. THEFT/FRAUD - low risk expected for theft of firewall rules, and for IDS and IPS systems.

G) LAN EQIPMENT (SWITCHES, ROUTERS ETC): These include all the devices which are connected to the local area network in the data center. They are fairly low risk but are important in the network infrastructure.

1. CONFIDENTIALITY - Fairly low risk is estimated for the confidentiality of the devices as they can be easily replaced in case of vulnerability. However, it is important to avoid disclosure.
2. INTEGRITY - Equipment being tampered with would not lead to a huge issue as it is in LAN and can be easily replaced
3. AVAILABILITY- Unavailability of the devices can lead to some problems but not a huge issue.
4. THEFT/FRAUD - Very low risk estimated of theft of devices in the data center.

H) EMPLOYEE (ENGINEERS) DEVICES (WORK PC'S, TABLETS): These devices are used by the employees working on the floor of data center and Network operations center (NOC) and Security operations center (SOC). Eqipped with antivirus software etc. and hardened with own software for monitoring the data center.

1. CONFIDENTIALITY - Fair risk estimated, the workstation is well protected against malware and requires multifactor authentication to log in, but it does contain critical information on the data center services and monitoring.
2. INTEGRITY - Changing or tampering with the device could be of significant impact on the workings of the data center but risk is moderate as they are well secured so the probability of them facing a threat is low.
3. AVAILABILITY-unavailability could lead to minor issues but should not be a huge hindrance.
4. THEFT/FRAUD - Since they are physical devices located inside a data center the probability of them being stolen is very low. Hence low risk is estimated.

H) EMOPLOYEE EMAIL CALENDAR, OFFICE: used for communication within the company, might include confidential and mission critical information.

1. CONFIDENTIALITY - Fair risk is estimated as emails and other means of conversation might contain valuable critical information which could have an impact in the hands of a competitor.
2. INTEGRITY - Considerable risk is estimated as any changes in the email message could impact the workings of the data center. Destruction of critical emails would be a very serious concern.
3. AVAILABILITY-May include mission critical information, but availability of emails is not a huge issue. Medium risk is estimated
4. THEFT/FRAUD - Could have considerable impact if emails are lost. Or accessed as they might include some confidential information which could be very valuable to a competitor.

I) EMPLOYEE PAYROLL (PII, ACCOUNT INFO ETC.) - Includes confidential information about employee's salary, health insurance, taxes, bonuses etc. which includes PII (Personal Identifiable Information)

1. CONFIDENTIALITY - High risk is estimated as the information contains PII and Sensitive information.
2. INTEGRITY - Could be quite impactful if the information is changed, hence high risk is estimated
3. AVAILABILITY- Lower risk is estimated if the service is not available.
4. THEFT/FRAUD - Very important that this data is not stolen as this contains confidential information.

I) NETWORK CONNECTIVITY (INTERNET): Included as an asset as it is an essential component for a data center to function. Any disruptions in connectivity will lead to serious problems.

1. CONFIDENTIALITY - Low risk estimated. Knowing the ISP for the data center will not have a considerable impact on the working of data center.
2. INTEGRITY - Internet data should not be faltered with if it happens then clients will not receive the right information. Considerable impact is estimated hence medium risk estimated.
3. AVAILABILITY- Imperative that the Internet connectivity is always present. If the data center is not accessible, then it will lead to a huge impact on clients. High risk is estimated even if backup is present.
4. THEFT/FRAUD - Low risk is estimated. Theft of connectivity will not lead to a huge impact.

J) POWER SUPPLY (ELECTRICITY): Included as an asset because it is also an essential mission critical component to the working of a data center. Without electricity the data center cannot function and will make achieving 99.9% availability a huge issue. Data center switches to a backup power supply but only for a limited period.

1. CONFIDENTIALITY - Power supply information could have an impact on the data center if an attacker could learn about the power supply lines or grid and turn it off. Hence medium risk is estimated.
2. INTEGRITY - Power supply could be tampered with and can lead to significant impact. High risk estimated
3. AVAILABILITY-Power availability is a crucial issue for a data center. High risk is estimated. The data center being a tier 3 data center has a power backup available which will turn on immediately after the power supply is gone. But only for a certain amount of time. Data centers consume huge amounts of electricity.
4. THEFT/FRAUD - Minimal risk is estimated.

K) LOGS (ACCOUNT INFO, ACCESS LOGS ETC.): Includes all the log data for the data center such as access logs, server room logs and equipment logs. Important for security and for identifying information during an audit

1. CONFIDENTIALITY - Low risk estimated as not it will not have a huge impact on the functioning of data center. They are not as valuable to attackers.
2. INTEGRITY - Log data should remain untampered with as they can help with a breach or recognizing if an attack has occurred.
3. AVAILABILITY- Low risk is estimated for the availability of logs as they are not mission critical
4. THEFT/FRAUD - It is of low impact on the data center in case of any unauthorized access or if stolen. Hence low risk is estimated.

L) RETIRED DISK DRIVES.: These include disk drives that are discarded after their life cycle is complete. It might still be possible to get data out of the hard drive hence they are disposed of by Shredding etc.

1. CONFIDENTIALITY - Since they are disposed of within the data center, they are not that likely to fall into unauthorized users.
2. INTEGRITY - Integrity of the hard drives do not matter as they will be disposed of.
3. AVAILABILITY- very low risk is estimated as the drives inside the data center will be well looked after.
4. THEFT/FRAUD - An attacker can still be able to get some information off the hard drive but the likelihood of that happening is low as it would involve obtaining the hard drive.