Assignment 1

Tejas Vijay Adhav

CS 573 Fundamentals of Cyber-Security

CWID – 20012193

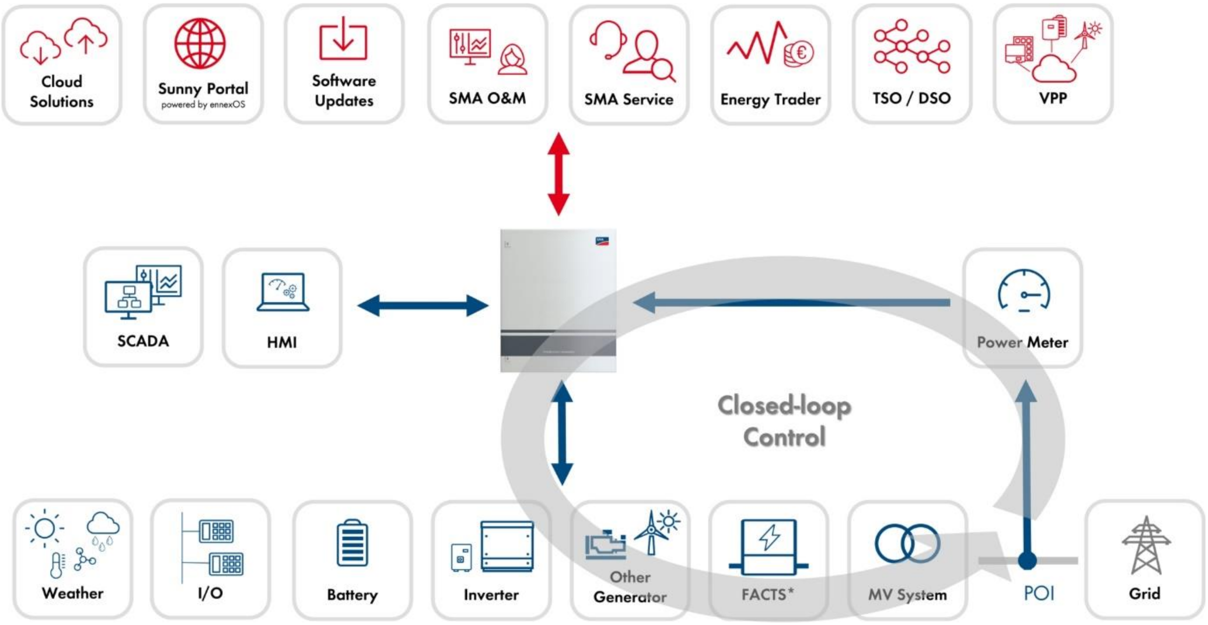
Dept. Computer Science

Threat Asset Matrix of Power Company

Introduction

As a power company, ensuring the security and reliability of our assets is critical to our operations and the communities we serve. To effectively manage potential threats and vulnerabilities, we have developed a Threat Asset Matrix to assess and prioritize risks to our assets. This matrix allows us to identify potential threats to our infrastructure, determine their likelihood and potential impact, and develop appropriate measures to mitigate these risks. By proactively addressing potential threats, we can ensure the safe and reliable delivery of electricity to our customers and maintain the trust of the communities we serve.

Asset Distribution: -



The potential system architecture of a Power plant distribution using the assets

Assets/Threats	*Confidentiality*	*Integrity*	*Availability*	*Theft/Fraud*
File Server	*P = 3 C=3* *R=9*	*P = 2 C=3* *R=6*	*P = 1 C=3* *R=3*	*P = 2 C=2* *R=4*
Application Server	*P = 2 C=3* *R=6*	*P = 3 C=2* *R=6*	*P = 2 C=1* *R=2*	*P = 1 C=3* *R=3*
Payment Gateway	*P = 2 C=2* *R=4*	*P = 1 C=2* *R=2*	*P = 2 C=2* *R=2*	*P = 3 C=3* *R=9*
ADP Payroll	*P = 1 C=1* *R=1*	*P = 1 C=2* *R=2*	*P = 2 C=2* *R=4*	*P = 1 C=2* *R=2*
Wells Fargo bank	*P = 2 C=2* *R=4*	*P = 1 C=2* *R=2*	*P = 1 C=2* *R=2*	*P = 1 C=2* *R=2*
AWS Cloud	*P = 1 C=2* *R=2*	*P = 1 C=3* *R=3*	*P = 2 C=3* *R=6*	*P = 3 C=3* *R=9*
Web Server	*P = 1 C=2* *R=2*	*P = 1 C=3* *R=3*	*P = 1 C=3* *R=3*	*P = 1 C=3* *R=3*
Power Meter	*P = 3 C=1* *R=3*	*P = 1 C=3* *R=3*	*P = 2 C=3* *R=6*	*P = 3 C=3* *R=9*
Distribution Equipment	*P = 3 C=1* *R=3*	*P = 1 C=2* *R=2*	*P = 1 C=3* *R=3*	*P = 1 C=3* *R=3*
Power Generation Facilities	*P = 2 C=1* *R=2*	*P = 1 C=2* *R=2*	*P = 1 C=1* *R=1*	*P = 1 C=3* *R=3*
Employee Database System	*P = 1 C=2* *R=2*	*P = 1 C=3* *R=3*	*P = 1 C=3* *R=3*	*P = 1 C=3* *R=3*

Colour Description: -

Green: - Low Risk < 3

Blue: - Moderate Risk Above 3 below 6

Marron: - Risky Above 6 below 9

Red: - Extremely Risky 9

Confidentiality*: refers to the protection of sensitive or confidential information from unauthorized access, use, disclosure, or modification. An attacker may attempt to access confidential information through various means such as phishing, hacking, social engineering, or physical theft.*

Integrity*: refers to maintaining the accuracy, completeness, and trustworthiness of data and ensuring that it has not been tampered with or altered in any way. This can be achieved using techniques such as encryption, digital signatures, and access controls.*

Availability*: refers to ensuring that services and data are available and functioning properly when needed by authorized users. This can be achieved through measures such as redundancy, fault-tolerant systems, and disaster recovery plans.*

Theft/Fraud*: refers to the acquisition of data or services illegally, which can lead to financial loss or damage to reputation. This can be prevented using security measures such as access controls, monitoring systems, and employee training.*

File Server of a Power Station:

(A file server of a power station basically consists of all the records regarding the daily power generation of data, amount of fuel used to generate power, waste generated to produce power, etc)

- *Confidentiality:* The file server containing all confidential company information is highly vulnerable to attacks from hackers or government agencies seeking to obtain internal information, making it an extremely risky asset.

- *Integrity:* The file server holds critical information for the company, and an attack on the server would pose a significant risk. Any attempt to manipulate or alter the data could result in substantial losses for the company.

- *Availability:* The file server is a repository for all of the company's important files, making it highly unlikely that all data on the server could be erased. However, if such an event were to occur, it would have catastrophic consequences for the organization.

- *Theft/Fraud:* In today's world, it is increasingly common for hackers and cybercriminals to steal information from file servers.

Application Server of a Power Station:

(Despite having multiple layers of protection, application servers remain highly vulnerable to attacks due to their critical role in the functioning of an organization's software applications. Any breach in the security of an application server can result in unauthorized access, data theft, and other malicious activities, leading to significant financial and reputational damage.)

- *Confidentiality:* The application server stores data like that found on the file server, but it is subject to more stringent security measures to ensure its protection. Due to its critical role in running an organization's software applications, the application server is a prime target for cyber-attacks, making its security an essential consideration for any company seeking to protect its assets and reputation.

- *Integrity:* Although application servers in power plants are designed to be highly secure, hackers are still able to identify and exploit vulnerabilities, making them vulnerable to attacks. The consequences of such attacks can be severe, potentially resulting in power outages, damage to critical infrastructure, and even loss of life. As such, it is crucial for power plants to regularly assess and update their security measures to stay ahead of emerging threats and protect against potential breaches.

- *Availability:* Erasing all data on an application server is typically a challenging task for intruders, which makes the consequences of an attack on the serverless severe. However, this does not mean that the threat should be taken lightly, as a successful attack on the application server can still result in unauthorized access, data theft, and other malicious activities that can cause significant financial and reputational harm to an organization. It is essential to implement comprehensive security measures and regularly update them to ensure the protection of the application server and its data.

- *Theft/Fraud:* Stealing data from an application server can be difficult for individuals or government entities due to the heightened security measures in place, including access controls, encryption, and other safeguards. However, if someone manages to bypass these security measures and steal data, the consequences for the company can be significant, including financial losses, reputational damage, and loss of customer trust.

Payment Gateway for the PowerStation:

(The payment gateway for a power station is a critical component of its financial operations, as it is the primary means by which external organizations can make payments to the station. Any disruption or compromise of the payment gateway can have severe consequences for the power station, potentially resulting in financial losses and damage to its reputation. As such, it is essential to implement robust security measures and continuously monitor the payment gateway to ensure its integrity and protection against potential breaches.)

- *Confidentiality:* While the payment gateway is a crucial component of any organization's financial operations, reading the data of the payments processed through the gateway can potentially lead to significant security breaches and financial losses. Unauthorized access to payment data can result in the theft of sensitive financial information, which can be used for fraudulent activities such as identity theft and unauthorized financial transactions.

- *Integrity*: The payment gateway is a critical component of any modern organization, and it is typically handled with utmost precaution and monitored closely to ensure its integrity and protection against potential security breaches. Unauthorized access to the payment gateway can result in significant financial losses, reputational damage, and legal liabilities, making it a prime target for cybercriminals and hackers.

- *Availability:* Changing, modifying, or deleting payment gateway details without proper authorization or authentication can be a difficult task for unauthorized individuals, as these systems are typically well-secured and closely monitored. However, any unauthorized changes to the payment gateway can cause significant disturbances in terms of its availability, potentially resulting in the disruption or termination of financial transactions processed through the gateway.

- *Theft/Fraud:* Theft or fraud in a payment gateway is a common occurrence and can have significant consequences for both the organization and its customers. Payment gateways deal directly with financial services, and any fraudulent activity can result in financial losses, reputational damage, and legal liabilities.

ADP as Payroll company:

(A leading provider of payroll and human resource management services for businesses of all sizes. As a payroll company, ADP offers a range of services and solutions to help organizations manage their payroll processes, including payroll processing and compliance, time and attendance tracking, benefits administration, and more.)

- *Confidentiality:* ADP has developed a reputation for providing secure and reliable payroll services to businesses of all sizes. ADP leverages advanced technologies and robust security measures to protect the confidentiality of payroll data and ensure the integrity and availability of payroll services.

- *Integrity:* As a payroll company, ADP is committed to maintaining the integrity of payroll data and ensuring the accuracy and consistency of payroll processing. ADP employs multiple checks and balances to ensure that payroll data is accurate and that any errors or discrepancies are identified and corrected in a timely manner.

- *Availability*: While errors and data inconsistencies can occur in any payroll process, ADP is committed to ensuring the availability of payroll services and minimizing any disruptions to payroll processing. ADP uses a variety of strategies to ensure that payroll services are always available and accessible to businesses.

- *Theft/Fraud:* ADP takes security very seriously and has implemented a range of measures to prevent theft or fraud related to payroll processing. For example, ADP uses advanced security technologies to protect against cyber threats, including multi-factor authentication and encryption of sensitive data.

Wells Fargo as a bank for all the transactions for power company:

- *Confidentiality:* Wells Fargo places a high priority on maintaining the confidentiality of customer information. The bank has implemented a range of measures to protect against unauthorized access to customer data, including multi-factor authentication, encryption, and access controls. However, the bank has faced some high-profile data breaches in recent years, which has led to concerns about the effectiveness of its security measures.

- *Integrity:* Integrity is also important for financial institutions like Wells Fargo, as it ensures that the data is accurate and trustworthy. While Wells Fargo has implemented measures to ensure data integrity, such as data backups and internal controls, it has faced some controversy related to the accuracy of its reporting and the integrity of its internal controls.

- *Availability:* Ensuring the availability of financial services is critical for a bank like Wells Fargo, as customers rely on the bank to access their accounts and perform transactions. While the bank has measures in place to ensure availability, such as redundant systems and disaster recovery plans, it has faced some technical issues in the past that have led to disruptions in service.

- *Theft/Fraud:* Preventing theft and fraud is a key priority for Wells Fargo, as it protects both the bank and its customers from financial losses. The bank has implemented a range of measures to prevent fraud, such as fraud detection systems and employee training programs. However, the bank has faced some high-profile cases of fraudulent activity by employees, which has led to reputational damage and regulatory scrutiny.

AWS of a Power Company:

- *Confidentiality:* The overall risk rating of 2 indicates that while there is some level of risk to confidentiality, it is relatively low. This could be due to the use of encryption and other security measures to protect data in transit and at rest.

- *Integrity:* The risk rating of 3 suggests that the risk to integrity is moderate. While there are measures in place to prevent unauthorized modification of data, there is still a chance that data could be altered or corrupted.

- *Availability*: The risk rating of 6 indicates that availability is a significant concern. AWS is known for its reliability and uptime, but there is always a risk of outages, especially if the power company is relying heavily on AWS for its infrastructure.

- *Theft/Fraud*: The risk rating of 9 indicates that theft and fraud are high risks when it comes to the AWS cloud for a power company. This could be due to a variety of factors, such as inadequate access controls, vulnerabilities in third-party software, or insider threats. It is crucial to have strong security measures in place to mitigate these risks.

Web Server of a Power Company:

- *Confidentiality*: This refers to the protection of sensitive information from unauthorized access or disclosure. In the case of a web server for a power company, this could include customer data, financial information, or proprietary technology.

- *Integrity*: This category relates to the accuracy, consistency, and trustworthiness of data. For a web server, this could mean ensuring that data is not modified or corrupted in transit and that it remains consistent across different parts of the system.

- *Availability*: This category focuses on ensuring that services and data are available and working correctly when needed. For a web server, this could include minimizing downtime, responding quickly to issues, and handling large volumes of traffic.

- *Theft/Fraud*: This category encompasses any unauthorized acquisition of data or services, which could include hacking, identity theft, or other forms of fraud. For a web server, this could mean preventing unauthorized access to the system or protecting against phishing attacks.

Power Meter Indicator of a Power Plant:

(Meters are basically used for readings which can be anything such as gas input /output, temperature, Electricity production, etc)

- *Confidentiality: -* As such, there is no point in meter reading confidentiality usually meters are placed where each and everyonen can take the readings.
- *Integrity: -* Usually readings in the meter cannot be changed as it covered with glass
- *Availability: -* Meters are important for a power company and there is a possible scenario that they can be damaged which causes the lack of data availability and which will cause all the ongoing operations to pause.
- *Theft/Fraud*: - This has been seen that theft of meters is common irrespective of whatever the company is but talking about power companies it is very important and if theft occurs everything can be compromised.

Distribution Equipment (hardware) of a power company

(Distribution equipment of a power company poses significant risks to confidentiality, integrity, availability, and theft/fraud. It is important to implement robust security controls and monitoring measures to mitigate these risks and prevent potential breaches.)

- *Confidentiality*: The information stored in the distribution equipment is highly confidential as it contains sensitive data related to the power company's operations. The probability of unauthorized access to this information is high due to the low confidentiality controls in place. The impact of a breach would be significant, as it could result in the compromise of critical infrastructure and could potentially cause widespread power outages. Therefore, the risk level for confidentiality is high .

- *Integrity*: The integrity of the distribution equipment is moderately important, as any tampering or manipulation of the hardware could result in significant disruptions to the power grid. The probability of a breach is low, as the hardware is typically physically secured and monitored. However, the impact of a breach could be severe, resulting in significant damage to the power infrastructure. Therefore, the risk level for integrity is moderate.

- *Availability*: The availability of the distribution equipment is critical to the functioning of the power grid. The probability of disruptions is low, as the equipment is designed to be highly reliable and is monitored for malfunctions. However, the impact of a breach could be significant, resulting in widespread power outages and disruption to critical infrastructure. Therefore, the risk level for availability is moderate.

- *Theft/Fraud*: The probability of theft or fraud related to distribution equipment is low, as the hardware is typically secured in place and monitored. The impact of a breach would be significant, as it could result in the compromise of critical infrastructure and could potentially cause widespread power outages. Therefore, the risk level for theft/fraud is moderate.

Power Generation Facilities of a power company:

(All the types of equipment and technology required to generate power e.g.: Turbine, digital meters, computers to control the process)

- *Confidentiality*: The power generation facilities have a moderate level of protection against unauthorized disclosure, with a low likelihood of a breach and moderate potential impact if one were to occur.

- *Integrity:* The facilities have a low level of protection against unauthorized modification or destruction of data, but there is a low likelihood of a breach and moderate potential impact if one were to occur.

- *Availability:* The facilities have a low level of protection against disruptions or denials of access to information or services, with a low likelihood of an event occurring and a low potential impact if one were to occur.

- *Theft/Fraud:* The facilities have a low level of protection against theft, fraud, or other malicious activities, but there is a low likelihood of an event occurring and a moderate potential impact if one were to occur.

Employee Database System of a power plant

- *Confidentiality*: The system is not highly confidential, as the probability of a breach is low, but the impact of a breach could be moderate, affecting the privacy of the employees. Therefore, the system requires some level of protection to ensure the confidentiality of the data.

- *Integrity*: The system requires a high level of integrity, as any breach could have a significant impact on the accuracy and reliability of employee data. Therefore, measures should be taken to ensure that the data is protected from unauthorized modification, deletion, or corruption.

- *Availability*: The system requires a high level of availability, as any downtime or interruption could affect the ability of the power plant to perform its functions. Therefore, measures should be taken to ensure that the system is always up and running and that there are appropriate backup and recovery mechanisms in place.

- *Theft/Fraud*: The system requires a high level of protection against theft or fraud, as any unauthorized access or misuse could have a significant impact on the power plant's operations and the privacy of the employees. Therefore, measures should be taken to ensure that the system is protected from unauthorized access and that there are appropriate monitoring and detection mechanisms in place.

ASSETS	TOTAL RISK
File Server	22
POWER METER	21
AWS Cloud	20
Payment Gateway	19
Application Server	17
AWS Cloud	20
WEB SERVER	11
Distribution Equipment	14
Employee Database System	11
ADP Payroll	9
Power Generation Facilities	8