**CYBER SECURITY**

HAN22080031

HAN22080120

HAN22080221

HAN22080144

# Introduction

DigiTech Corporation has moved to the Hualon Tower, specifically occupying floors 6 through 8, due to its rapid growth and operational expansion. This move was necessary to meet the company's increasing number of employees and expanding technological infrastructure. Nevertheless, new security assessments have brought attention to weaknesses in current processes, which might potentially endanger valuable assets and activities. As cyber security experts, our responsibility is to perform a thorough evaluation and suggest strong security improvements. This report details our strategy, employing well-established frameworks like NIST, to strengthen DigiTech's security position in its new buildings. The purpose of this project is to enhance our comprehension of realistic security procedures and help protect DigiTech's assets and reputation.

# Physical Security Assessment

## Assets Table

### Physical Asset

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LOCATION | Device | Quantity | Classification | Price |
| FLOOR 8 | PC | 50 | Sensitive | $1,500 |
| Printer | 5 | Internal | $100 |
| Scanner | 5 | Internal | $100 |
| Camera | 4 | Sensitive | $100 |
| Switch | 3 | Sensitive | $100 |
| Access point | 3 | Sensitive | $30 |
| Keycard reader | 3 | Internal | $30 |
| UPS 10 kVA | 2 | Sensitive | $4300 |
| FLOOR 7 | PC | 100 | Sensitive | $1,500 |
| Printer | 10 | Internal | $100 |
| Scanner | 10 | Internal | $100 |
| Camera | 4 | Sensitive | $100 |
| Switch | 3 | Sensitive | $100 |
| Access point | 5 | Sensitive | $30 |
| Keycard reader | 3 | Internal | $30 |
| FLOOR 6 | PC | 2 | Highly Sensitive | $1,500 |
| Keycard reader | 3 | Internal | $30 |
| Firewall | 2 | Highly Sensitive | $2,100 |
| Access point | 1 | Sensitive | $30 |
| Camera | 6 | Sensitive | $100 |
| Switch | 4 | Sensitive | $100 |
| Router | 2 | Highly Sensitive | $300 |
| Multilayer switch | 4 | Highly Sensitive | $200 |
| DNS server | 1 | Highly Sensitive | $2300 |
| DHCP server | 1 | Highly Sensitive | $2400 |
| Web server | 1 | Highly Sensitive | $3000 |
| Mail server | 1 | Highly Sensitive | $2200 |
| Log server | 1 | Highly Sensitive | $2500 |
| Database server | 10 | Highly Sensitive | $3000 |
| UPS 30 kVA | 2 | Sensitive | $7500 |
| Company | Security personnels | 10 | Sensitive | N/A |

### Logical Asset

|  |  |
| --- | --- |
| Assets | Classification |
| Website | Public |
| DNS | Public/Internal |
| Mail | Public |
| DHCP | Internal |
| Log server | Highly Sensitive |
| Database | Internal/ Sensitive / Highly Sensitive |
| Camera footage | Sensitive / Highly Sensitive |
| RFID reader data | Sensitive |
| IT security personnels | Highly Sensitive |

## 1. Physical Layout

### 1. Floor 6

### 1.1 Floor layout

The floor layout includes 4 rooms: data center for internal and public servers, security office for guard and camera control, networking devices room, and storage. Refer to the following figure for physical assets arrangement.

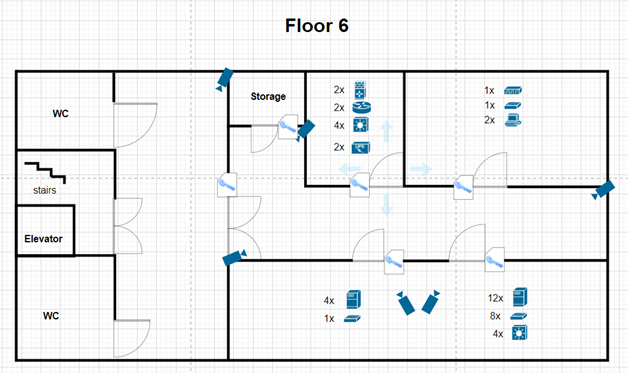


Figure 2.1.1.1 Floor 6 layout

Access to this floor is restricted and only accessible by guard and some IT personnels, each room also has a second layer of authentication to ensure only authorized personnel can access. Cameras are deployed to monitor and manage access to the area. The floor has 2 uninterruptible power supplies (UPS) installed, preventing any power disruption. The area is highly secure and strictly monitored.

### 1.2 Areas classification

The floor contains sensitive assets which are extremely important to DigiTech operations and security, assets within the floor are considered highly sensitive.

* **Highly Sensitive**:
  + **Networking devices room**: handles communication between floors and the company to the internet, failures can disrupt operations and cause great damage.
  + Servers room: the room contains both internal and public servers, failures can disrupt operations and cause great damage.
* **Sensitive**:
  + **Workstations**: workstations contain camera footage.
  + Company areas: can only access by authorized personnels
* **Public**:
  + **Outside of company areas**: elevator, restrooms, stairs, outside hall

### 1.3 CIA triad evaluation

With the classified asset in mind, physical and logical security requirements will be evaluated based on the CIA triad.

* **Confidentiality:**
  + **Physical:**

Use RFID readers to ensure access control, deploy surveillance cameras and guards to monitor and secure the area.

* + **Logical:**

Enforce strict access control, encrypt all data at rest and in-transit, and implement authentication to access critical areas.

* **Integrity:**
  + **Physical:**

Use tamper-evident mechanism on all hardware, conduct routine physical audits, and limit access to only those authorized.

* + **Logical:**

Implement strong access controls, conduct regular integrity checks, maintain detailed logs for all activities.

* **Availability:**
  + **Physical:**

Install UPS, backup generators, backup servers, and ensure an efficient heating venting air conditioning system is in place.

* + **Logical:**

Verify system redundancy for all critical assets, frequently backup important assets, and have a comprehensive disaster recovery plan.

## 2. Floor 7

### 2.1 Floor layout

The Applications Development lab layout consists of 8 rooms, including 5 department rooms, a networking devices room, a meeting room and a lounge. Refer to the following figure for physical assets arrangement.

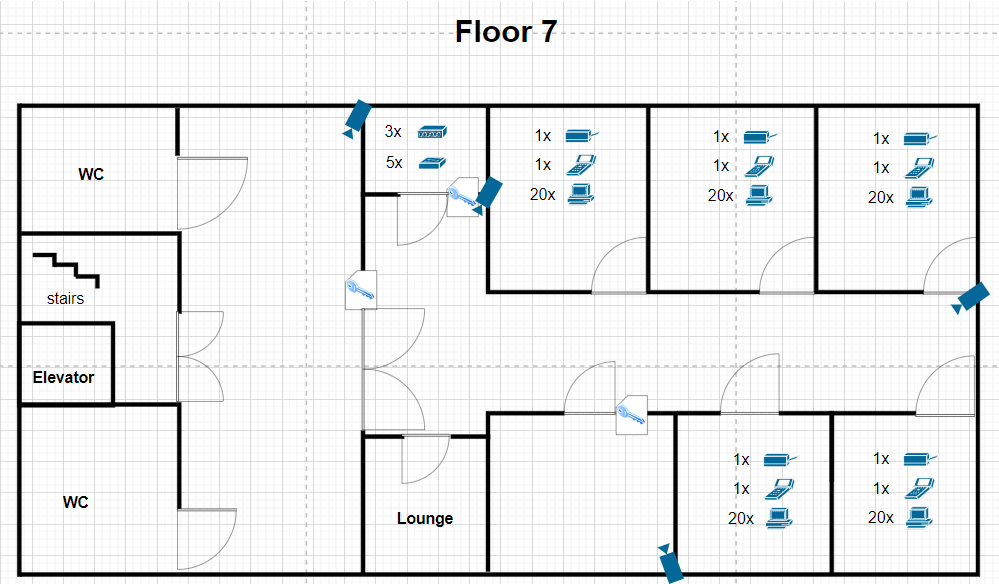


Figure 2.1.2.1 Floor 7 layout

As shown in the figure, employees are required to use their keycard to access the company development area. Other rooms such as the meeting room and networking devices room require a keycard with equivalent privilege to access. Cameras are placed around the facility for surveillance and managing access within the floor. With this layout, the area should be physically secured.

### 2.2 Areas classification

The floor primarily handles normal business operations but still contains sensitive assets, addressing and classifying sensitive areas is crucial:

* **Sensitive**:
  + Workstations: data in workstations can contain important business information and development progress.
  + **Networking devices room**: the room connects the floor to company network; unauthorized access can disrupt the floor ongoing operations.
  + **Meeting room**: conversations and topics discussed in the meeting room might be sensitive and highly sensitive.
* Internal:
  + Company areas: can only access by someone with company keycard or invited guests
* **Public**:
  + Lounge: despite inside the company area, the lounge can be used by both employees and guests
  + **Outside of company areas**: elevator, restrooms, stairs, outside hall

### 2.3 CIA triad evaluation

With the classified asset in mind, physical and logical security requirements will be evaluated based on the CIA triad.

* **Confidentiality:**
  + **Physical:**

Use RFID readers to ensure access control, surveillance cameras and guards to monitor entry and sensitive areas and manage visitor access strictly.

* + **Logical:**

Enforce strict access control, encrypt all development and sensitive data, and implement authentication to access development environments.

* **Integrity:**
  + **Physical:**

Use tamper-evident mechanism on hardware to detect unauthorized access, conduct regular audits, and limit access to only those authorized.

* + **Logical:**

Implement version control system, maintain development logs for all development activities, and have periodic code reviews.

* **Availability:**
  + **Physical:**

Ensure having reliable power supply and backup storage.

* + **Logical:**

Regularly backup code repositories and have a disaster recovery plan in place

## 3. Floor 8

### 3.1 Floor layout

The Cyber Security intelligence lab layout is like the Applications Development lab; refer to the following figure.

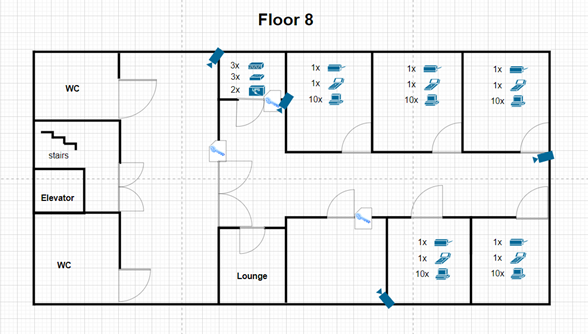


Figure 2.1.3.1 Floor 8 layout

Similarly, employees can only access the area with their keycard, sensitive areas such as the meeting and networking devices room requires equivalent privileges to access. Surveillance cameras are placed in positions allowing them to monitor and manage access within the area. In addition, with 2 UPS equipped, the floor is physically secured and redundant.

### 3.2 Areas classification

The floor has an important role and crucial in DigiTech’s security and operations, including research and development, incident response, policies and upheld sensitive data. The lab is required to be always active.

* **Highly Sensitive**:
  + **Workstations**: data in workstations contains research data and security threatening documents (floor plan, protocols, etc.). If exposed, they would cause great damage to DigiTech
  + **Networking devices room**: Operations within the floor are very crucial, disruptions will make the company vulnerable to attacks.
  + **Meeting room**: conversations and topics discussed in the meeting room should be confidential.
* **Sensitive**:
  + **Cyber Security intelligence lab**: can only be accessed by someone with suitable role or related to its operation.
* **Public**:
  + **Outside of company areas**: elevator, restrooms, stairs, outside hall

### 3.3 CIA triad evaluation

With the classified asset in mind, physical and logical security requirements will be evaluated based on the CIA triad.

* **Confidentiality:**
  + **Physical:**

Use RFID readers to ensure access control, use surveillance cameras and guards to secure the area and manage access.

* + **Logical:**

Enforce strict access control, encrypt all sensitive data, and maintain a least privilege access policy.

* **Integrity:**
  + **Physical:**

Use tamper-evident mechanism on hardware to detect unauthorized access, conduct regular audits and integrity check, and limit access to only maintenance.

* + **Logical:**

Use hashing and digital signature to ensure integrity, implement logging and monitoring, and IDS, IPS to detect and prevent unauthorized changes.

* **Availability:**
  + **Physical:**

Install UPS, backup generators, and ensure climate control practices are in place

* + **Logical:**

Make sure critical assets are redundant with high performance, and have a disaster recovery plan in place

## 2. Network Layout

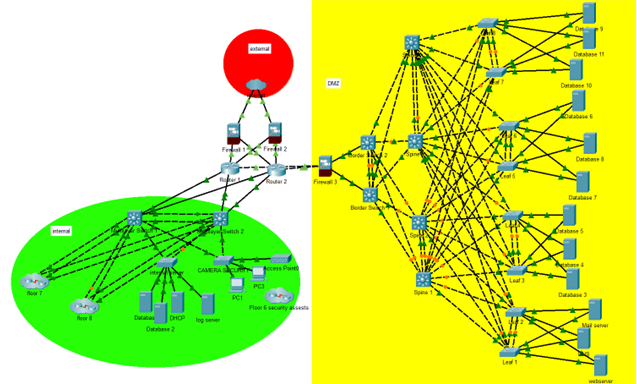


Figure 2.2.0.1 Network Topology (Floor 7,8 can be viewed in appendix)

DigiTech network is divided into three areas: Internal, DMZ and External. The internal network is only accessible by the company strict policy; DMZ, the data center, contains servers and services available to the public. The 2 networks are connected using routers. Firewalls are placed between the company network (Internal and DMZ) and the External network (Internet), providing a layer of protection. Since DMZ allows public access, a fire wall is used as a second layer of protection.

The internal network is built based on the 3-tier network architecture with access, distribution and core layer:

* **Core layer**: Routers connect the entire network together and the internet with high speed
* **Distribution layer**: Layer 3 switches govern local traffic between the access layer with the core layer
* **Access layer:** Layer 2 switches are used to connect with end devices

Data centers should be high performance and scalable, the DMZ network is designed with that in mind, using Spine-Leaf architecture. Spine-Leaf architecture is optimized for server-to-server communications with high scalability, low latency, load-balancing and cost efficiency. The DMZ is be divided into 3 layers:

* + **Core layer**: Routers connect the entire network together and the internet with high speed
  + **Spine layer**: Interconnect the leaves within the network topology.
  + **Leaf layer:**
    - Layer 2 switches are used to connect with end devices
    - Border leaf consist of a pair of layer 3 switches providing high performance external connectivity.

Server latency can be controlled by the number of hops to reach its destination, in this case, 2 hops from one leaf to another. Since the network is connected in full-mesh and travels in fixed hops, Equal Cost Multi-Path can be used to reduce cost and provide load-balancing. The network is highly scalable due to the simplicity of just adding more leaf switch or spine for the need of access or bandwidth, respectively.

Using this architecture also increases availability and redundancy of services running in the data center. Virtualization methods can be used virtual extensible local area network (VxLAN) to smoothly migrate servers with minimal down time. In this scenario, switches are made into pairs using multi-chassis link aggregation group links, providing redundancy without the risk of looping. Furthermore, software defined networking (SDN) solutions can be implemented to the architecture, allowing dynamic and programmatically efficient network configuration.

## 3. Overall CIA evaluation and area classification

### 1. Overall CIA evaluation

1. **Confidentiality:**
   * Logical Measures: Encryption, strong access control, least privilege access policies.
   * Physical Measures: RFID readers, cameras, security personnel.
2. **Integrity:**
   * Logical Measures: Hashing, digital signatures, comprehensive logging and monitoring, IDS/IPS.
   * **Physical Measures:** Tamper-evident seals, regular integrity checks, restricted access.
3. **Availability:**
   * Logical Measures: Redundant systems, high-availability configurations, regular backups, disaster recovery planning.
   * Physical Measures: UPS, backup generators, HVAC systems.

## 2. Area classification

* Highly sensitive: Data center, Cyber security intelligence lab
* Sensitive: Application development lab
* Public: Non-company areas

# IT Security and Risk Assessment

## Introduction:

* After identifying the assets in the company, we need to consider which factor could have a negative effect on the company. To avoid these factors, we need to conduct risk management on each asset we identify.

## Risk Management:

* *To be able to conduct the risk management, we divide the process into two parts, which are operational and technical. Risk assessment on the operational side will be the risk that happens in the physical world that impacts the operation of the company, while the technical will be for the digital world. Each of these risk assessments will 12 categories to measure the overall level of the risk, these categories include:*
* *Name: the name of the risk*
* *Description: information about the risk includes the vulnerability and threat*
* *Asset affected: which asset were affected by the risk*
* *Asset classification: show how important the asset is*
* *Impact: the impact the risk might cause to the company*
* *Impact level: how bad the impact on the company*
* *Likelihood: the chance of the risk happens*
* *Total price: the total price of all the asset*
* *Exposure Factor: percentage of loss compared to the total price*
* *Loss: how much loss the company will suffer from the risk*
* *Risk scores: The score of the risk*
* *Overall Level: the overall level of the risk based on risk score*

* *Overall level formula:*

*impact level: low = 1, medium = 2, critical = 3*

*likelihood: low = 1, medium = 2, critical = 3*

*Asset classification point: internal = 1, sensitive = 2, highly sensitive = 3*

*Loss = Total price \* Exposure Factor*

*Loss < $1000 = 1, $1000 < Loss < $15000 = 2, Loss > $15000 = 3*

*Risk scores = (Asset classification + impact level X 2 + Likelihood + Loss X 2)/6*

*Overall level: 0~1.9 = Low, 2~2.5 = Medium, 2.6~3 = Critical*

* *Each category will be divided into 3 parts: Risk identify, quantitative analysis, Risk analysis. Each of these tables help make the risk clearer and help us rank these risks.*

### Risk identification:

*This table’s main functionality is to give overall information about the risk. This information includes the risk name, the risk description, the assets affected by the risk and its impact on the company. The risks identified in the operational and technical are different, with both parts aiming at different types of assets. When we identify the risk in operation, we mostly consider what risk could affect the company physically, such as employee exploitation, equipment vulnerability and theft, outsider break in the company or natural disaster. As operational risk often focuses on what the risk can physically affect, the assets that were affected in this phase often were: internal assets such as computer or camera, employee which could unintentionally give away important data. Unlike operational risk, technical risk often impacts the data that the company owns such as customer data, employee data and project data, which are all data that need to be heavily protected. Other than data getting stolen, the attacker needed to get into the system to be able to do so, which results in different types of attack to the company server such as web server, mail server, DNS server, DHCP server. Some of the key attacks are SQL injection, Malware infection, Phishing and Brute force attack, which pose a more serious threat than operational because of how often these attacks happen.*

## Quantitative analysis:

*Other than identifying the risk, conducting a quantitative analysis is also an essential part of risk management. This table helps us understand the loss the risk could bring to the company financially. To be able to calculate the loss of the risk, we need to bring the total price of the asset that the risk affects and the exposure factor into the equation. By multiplying these two factors, we can see the loss that the company suffers from the risk, and by learning this loss, we can plan to migrate that help lower the loss or completely remove them. For example, if we want to calculate the loss of the risk “equipment theft”, we took it total cost ($85,580) multiply with it exposure factor (30%) and we will get it Loss ($25,647), which is higher than $15,000 so we classify this loss as critical. Between the loss of operational risk and technical risk, operational tend to have higher loss than technical due to most cost coming from the physical equipment rather than the server that the company owns.*

## Risk Analysis:

*Finally, to be able to rank these risks, we need to calculate the risk score and base it on classifying the risk. To get the score, we need to calculate using asset classification, impact level, likelihood and the level of loss. This formula focuses on impact level and loss more due to how much these impact the company, so these two factors will affect the formula more. After getting the score and the overall level of the risk, we will rank them from the highest score to the lowest so we know what risk to prioritize first and what we should leave to later. Due to technical having more valuable assets, high impact level and higher likelihoods, its scores are often higher than operational, which tells us to focus more on the technical side of the company rather than operational. For example, if we calculate “Malware infection” and “ear dropping” and then rank them, first we need to know their risk score. For “Malware infection”, all its level and classification are high and critical, we get 3 in the risk score. As for “ear dropping”, all its level and classification are high and critical except likelihood which is medium, from this we get 2.8. So, when ranking these two risks, “Malware infection” has a higher risk score so it should be higher than “ear dropping”, which should be focused more when doing migration.*

## 

## Operational risks:

### Risk identification: ￼

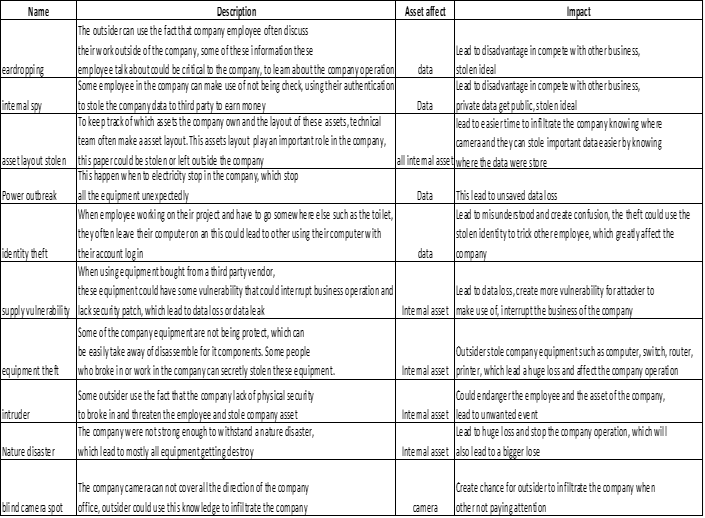


figure 3.2.0.1

### 

### Quantitative analysis:

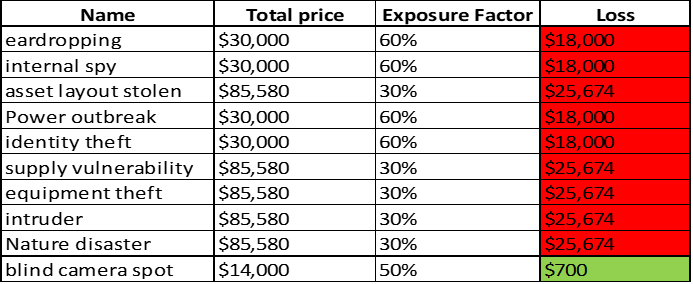


figure 3.2.0.2

### Risk analysis:

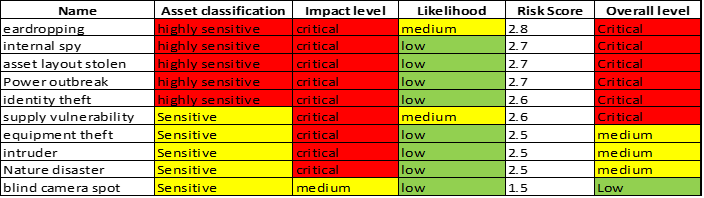


figure 3.2.0.3

## Technical:

### Risk identification:

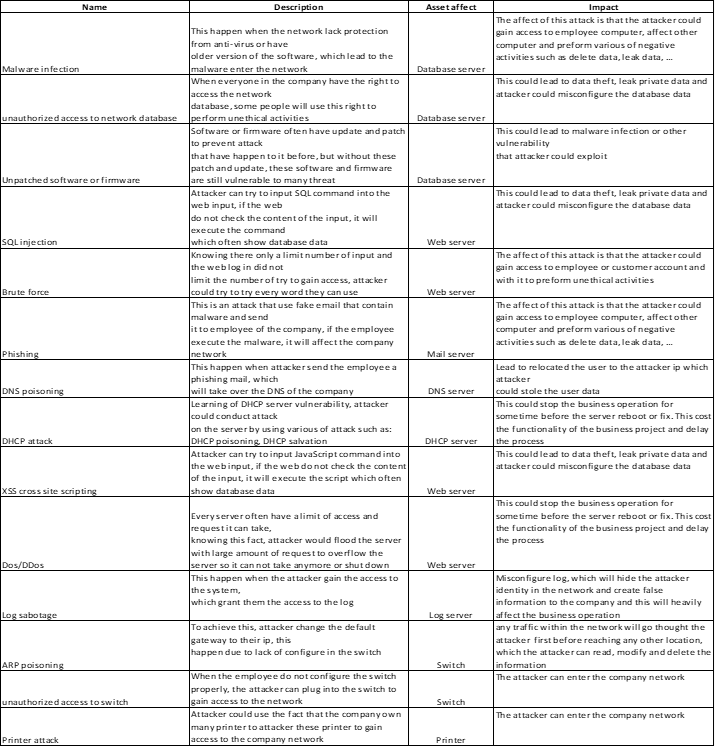


figure 3.2.0.4

### Quantitative analysis:

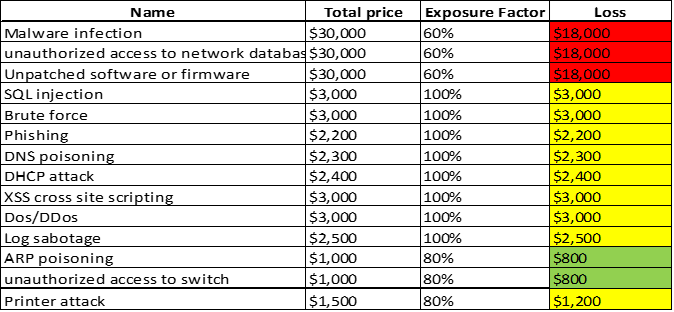


figure 3.2.0.5

### Risk analysis:

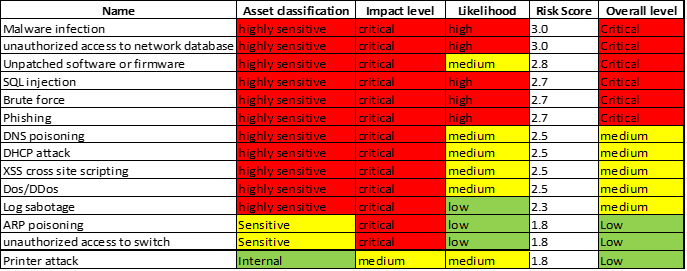


figure 3.2.0.6

# Assets and Security Controls Assurance Review

## 

## Identify objectives

This section will discuss the security and control assurance for DigiTech Corporation when moving to the new location. Firstly, we will briefly go to network architecture again and draw a trust boundary in the network. Secondly, threat models are developed based on the identified technical threats in section 2, and some threats and vulnerabilities are added and concentrated deeply in this section. After that, security controls are given to detect or prevent potential risks, threats and vulnerabilities that are discussed in the threat model and in task 2.

## Create Architecture Profile

As we discussed in section 1, we divided the 3-tier architecture into 3 separated zones which are external, DMZ and internal. However, for developing the threat model in this section, I am going to divide into 2 types of threats which are external threats and internal threats.

External threats are threats coming from outside of the company. Typically, external threats can happen to the assets in the DMZ zone because it is the zone that interacts with the public network, and the DMZ zone’s assets include webserver, user database and mail server.

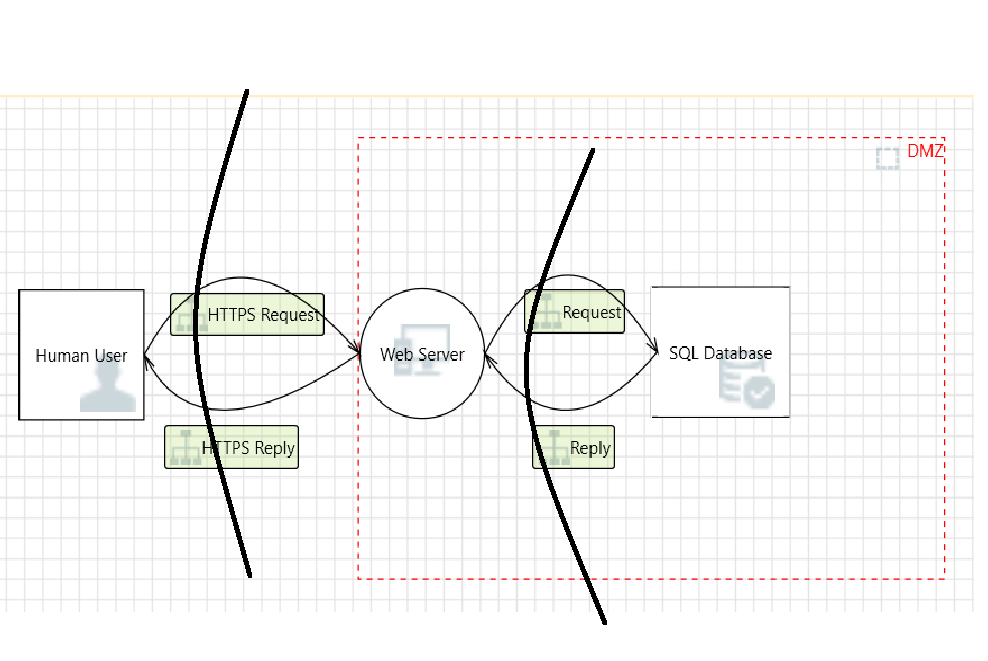


figure 4.2.0.0

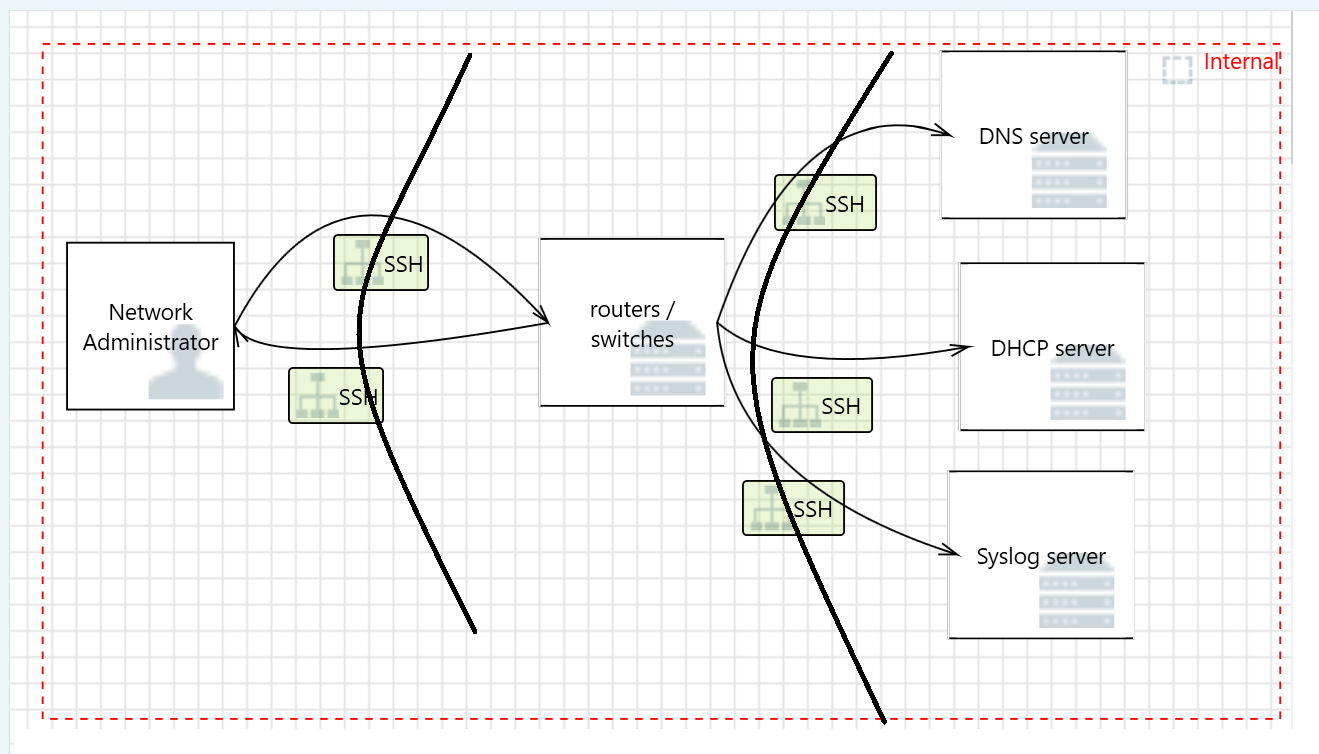
As we can see in figure 4.2.0.0, there are 2 external communication which are HTTPS request and reply between user and web server and request and reply from SQL database back to the web server. To structure a specific threat model, I will draw trust boundaries which are the lines separating zones based on its security level, so it will be easier to structure the threat model and implement security control for the whole process.

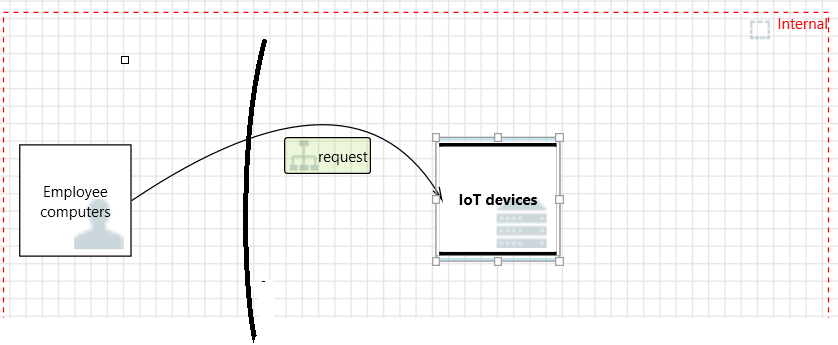
A diagram of a mail server

Description automatically generated figure 4.2.0.1

For mail communication, users are in the internal zone and the mail servers are in the DMZ zone.

Internal threats are threats coming from inside of the company and it is the threats that can damage the most to the company. As mentioned in section 2, there are many operational inside threats, but we are going to draw trust boundaries between 3 communications which are network administrators / engineer to network devices, network admin / network devices to internal servers and employees to printers.

 figure 4.2.0.2

 figure 4.2.0.3

## Threat modelling

As we discussed before, threats are categorized into 2 types which are internal and external threats. In this part, we will specify possible attacks and threats which can happen in trust boundaries in 2 types of threats by modelling them.

### 3.1) External threat modelling

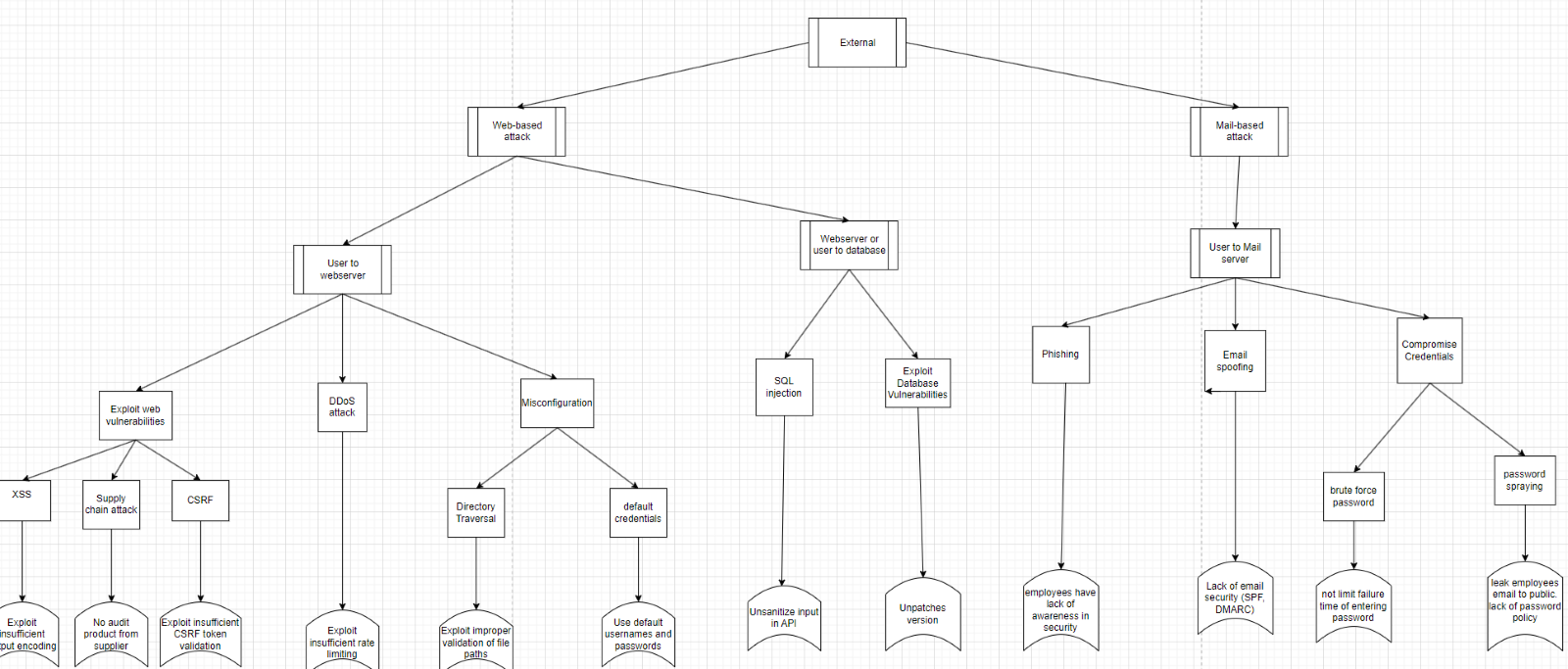
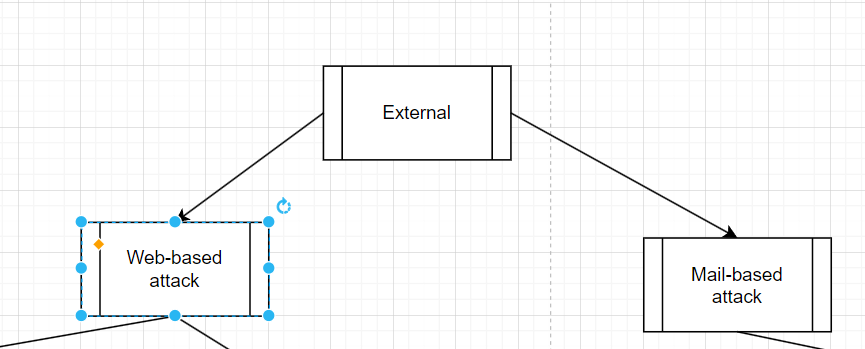
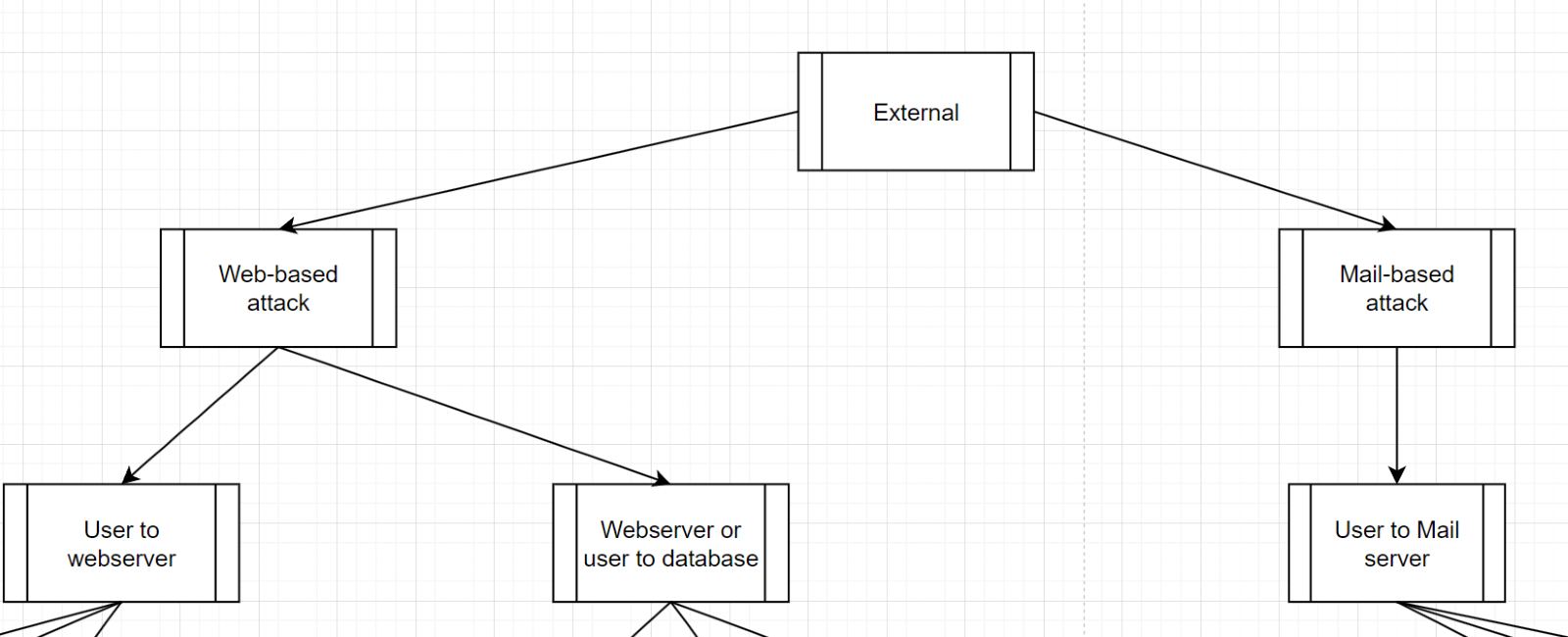
figure 4.3.1.0

Figure 4.3.1.0 illustrates the whole attack tree for the external threats. The first and second layer of the attacks tree contains the types of attacks which are Web-based attack and Mail-based attack.



figures 4.3.1.1

The third layer contains trust boundaries in web server and mail server communication.

 figure 4.3.1.2

The fourth and fifth layer are some attacks and threats that could happen in those trust boundaries.

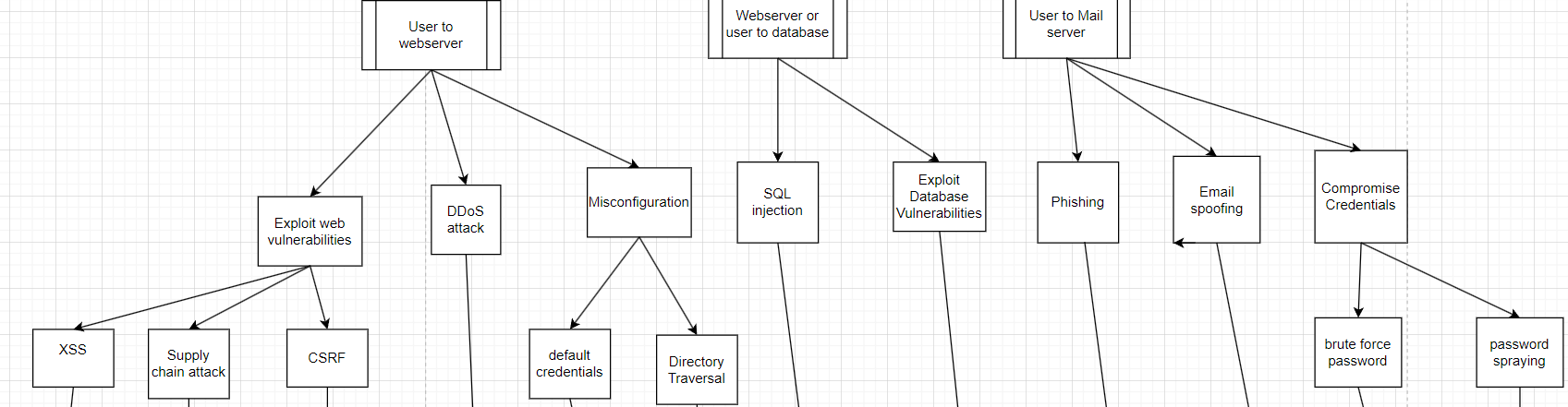


figure 4.3.1.3

For the user to webserver trust boundary, there are 3 threats could happen which are exploit web vulnerabilities, DDoS attack and Misconfiguration. Then in each threat, we listed some possible attacks that could happen to the webserver which are: XSS, supply chain attack, CSRF, directory traversal, etc. The case also be applied with the webserver or user to database and mail server communication trust boundary listed in the figure 4.3.1.4 and 4.3.1.5 below:

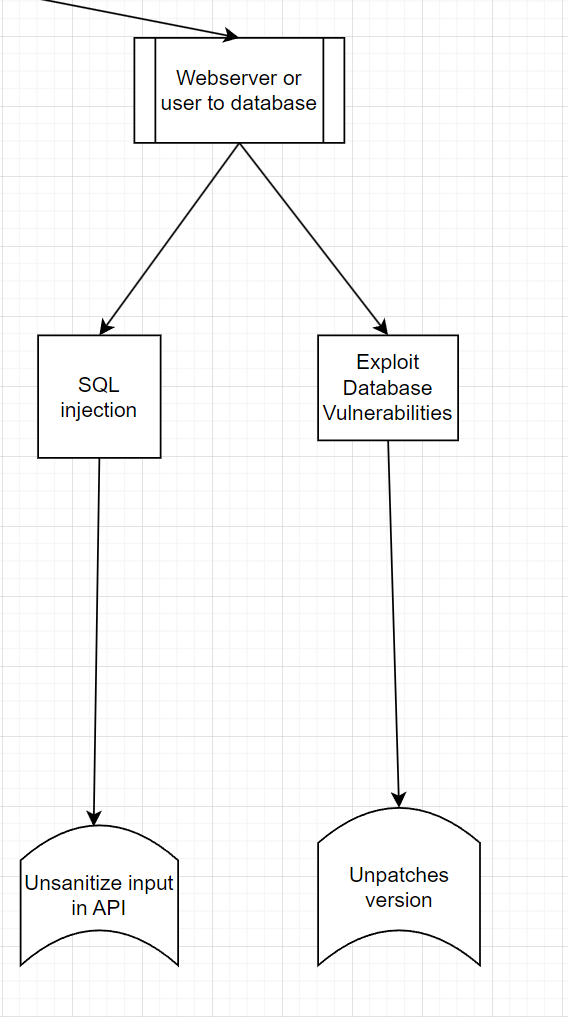
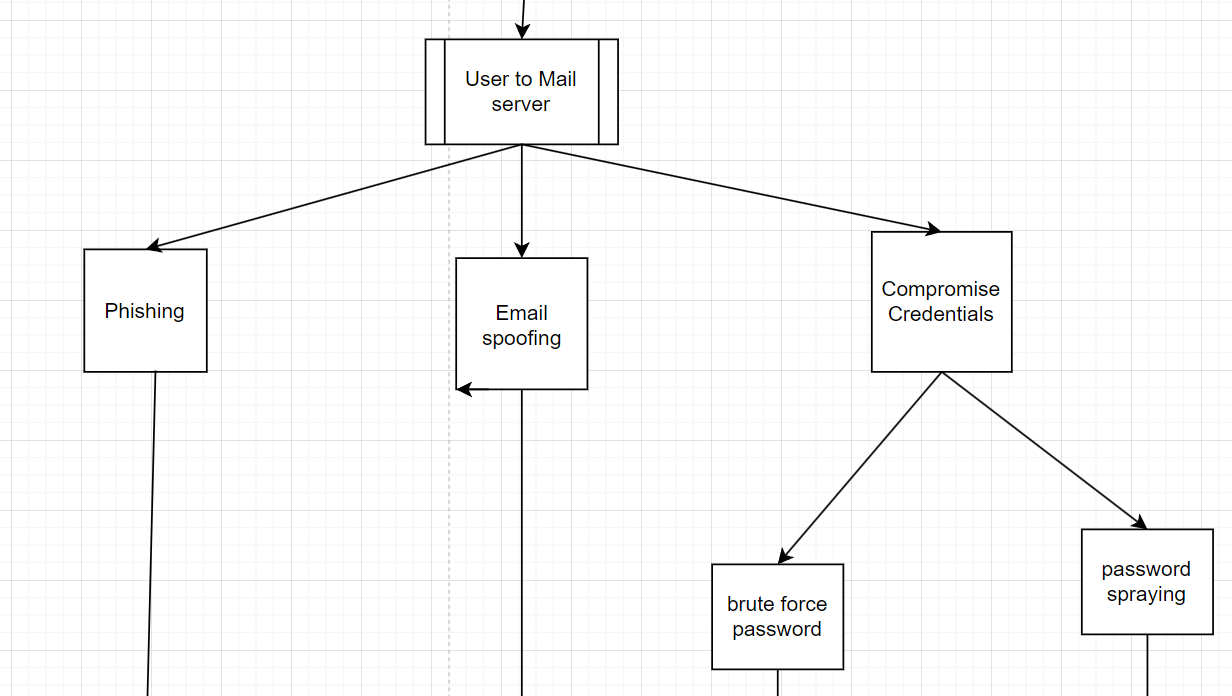


figure 4.3.1.4

 figure 4.3.1.5

In the final layer of the attack tree, it contains vulnerabilities that result to the specified threats.

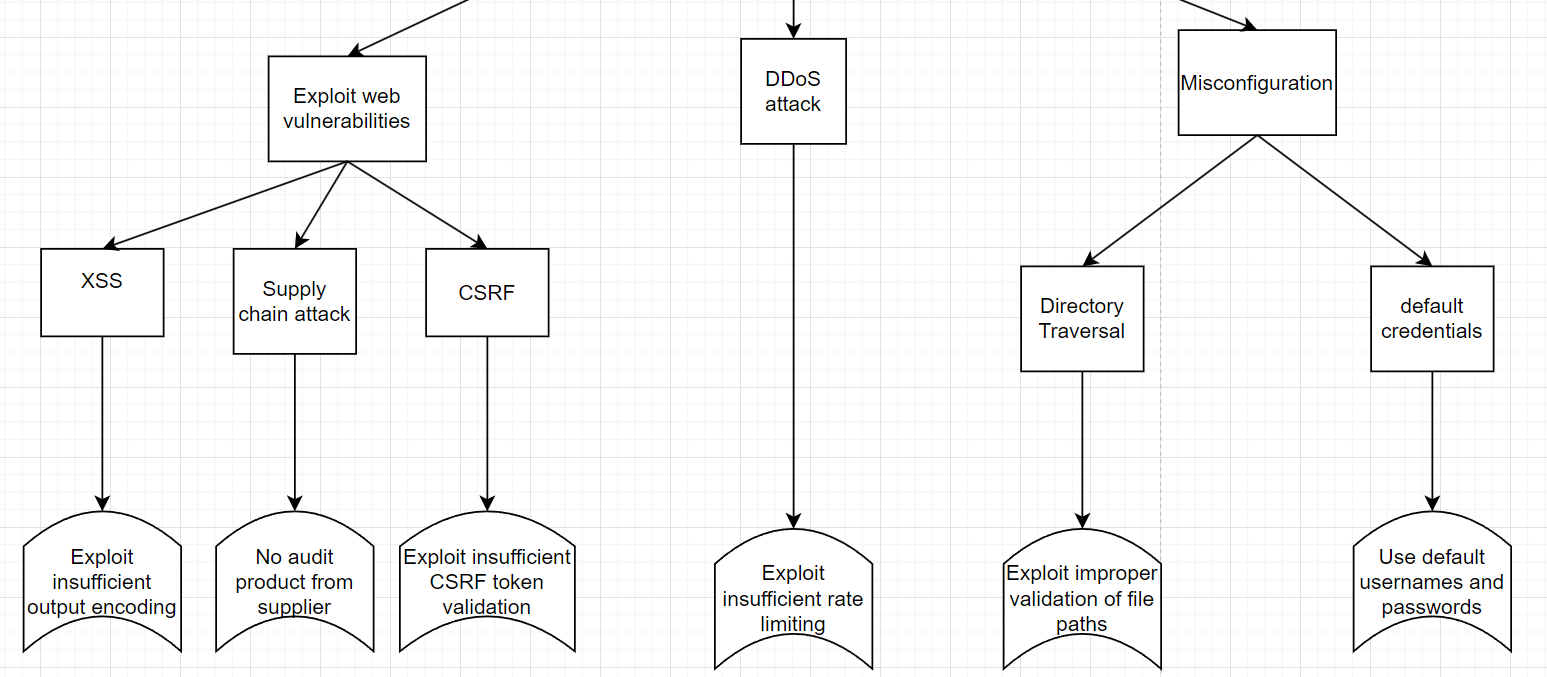
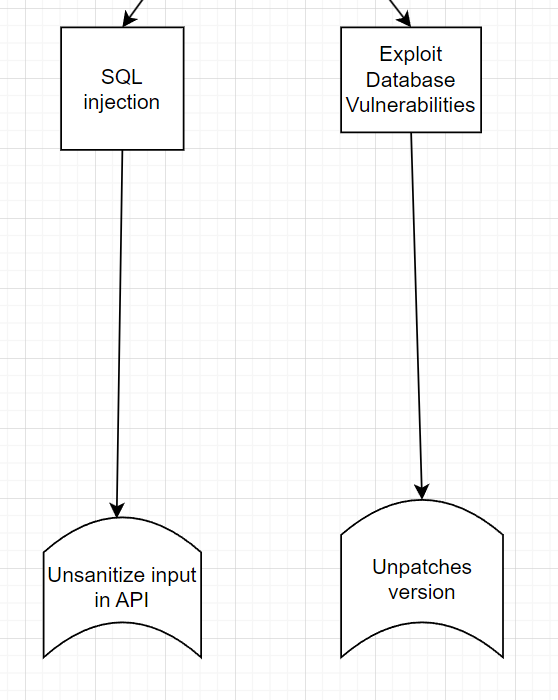


figure 4.3.1.6

For example, the cause of XSS is insufficient output encoding in the URL, cause of DDoS attack is uncontrol of request rates or cause of default credentials attack results from misconfiguration and lack of policy in using usernames and passwords. The case also be applied with the mail server or database vulnerabilities in figure 4.3.1.7 and 4.3.1.8 below:

 figure 4.3.1.7

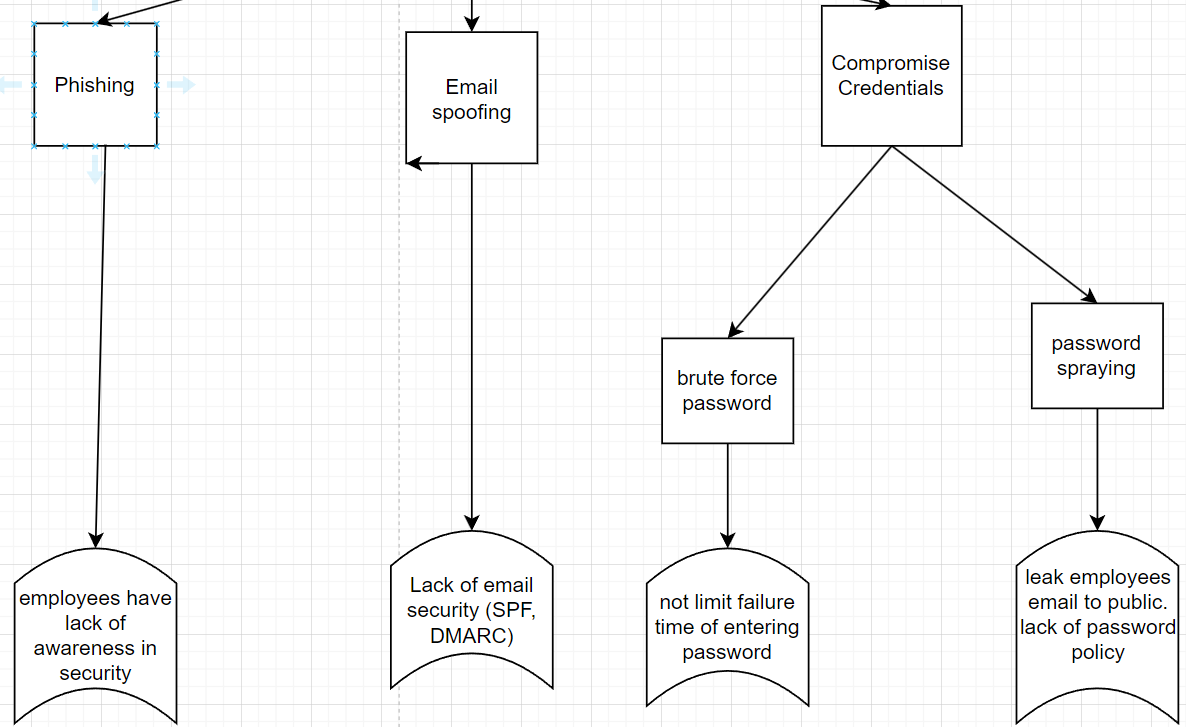
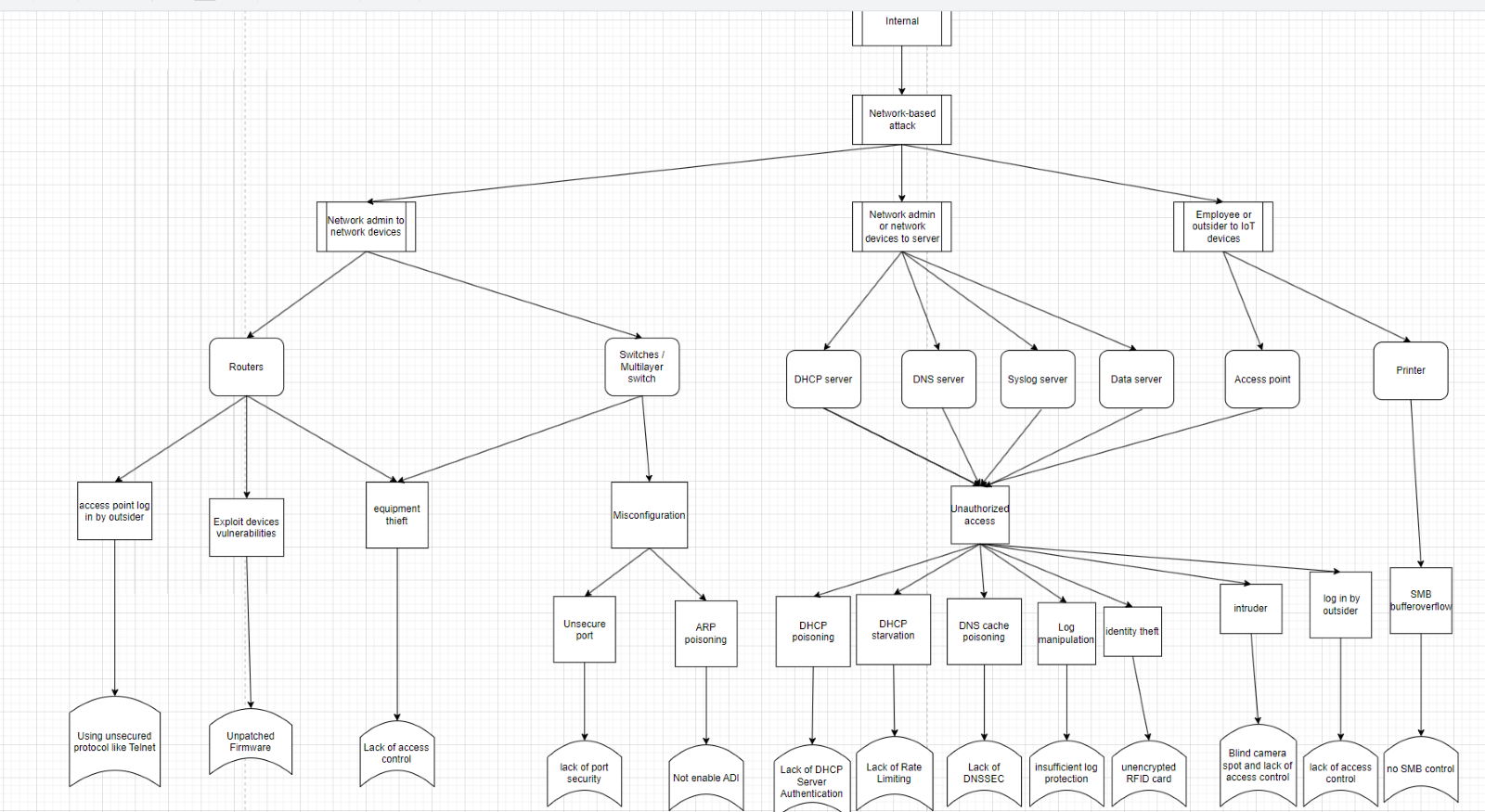


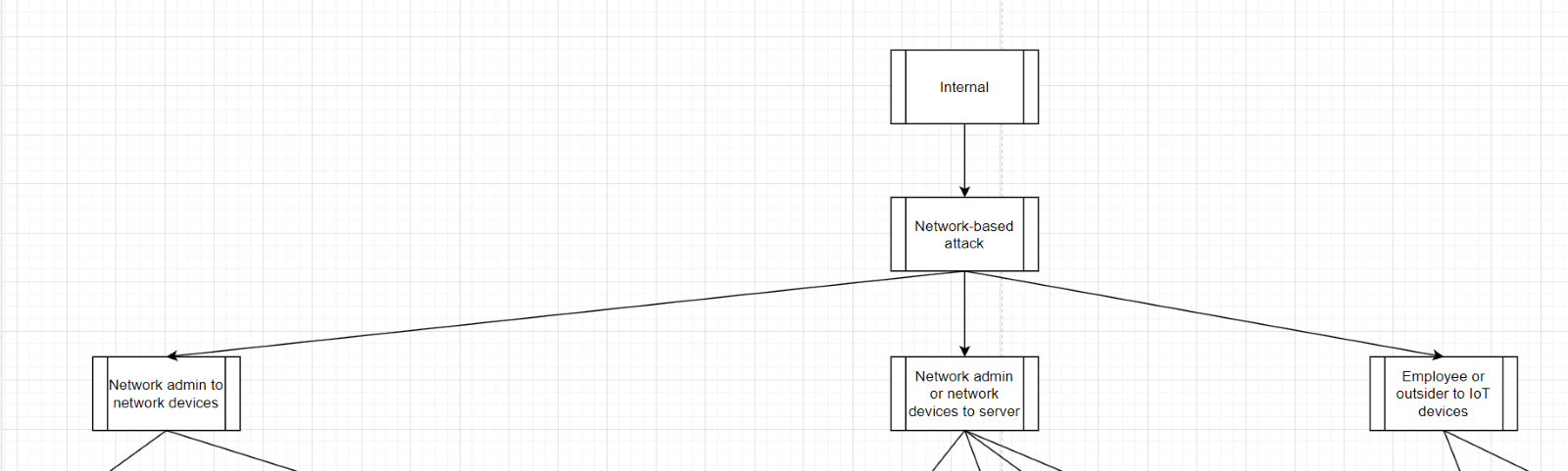
Figure 4.3.1.8

### 3.2) Internal threat modelling

To improve the quality of the model, we made a separate attack tree for the internal threats, and it is showed in the figure 4.3.2.0 below:

 figure 4.3.2.0

Same as the external attack tree, the first and second layer are about the threat which is only network-based attack because this threat normally happens in the LAN network. Then we have layer 3 of the attack tree for trust boundaries that we identified in the previous part which are configuration between network administrator to network devices, network admin or network devices to servers, and employee to the printer.

 figure 4.3.2.1

After that in the next layer, we specified all the network infrastructures that are vulnerable to insider threats and can cause large impact if being exploited

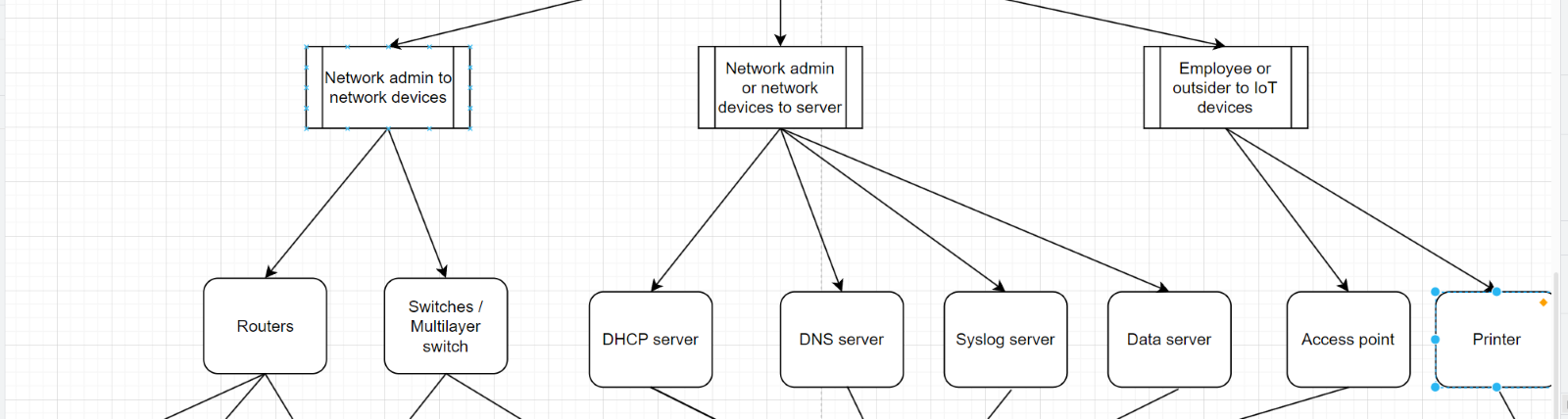
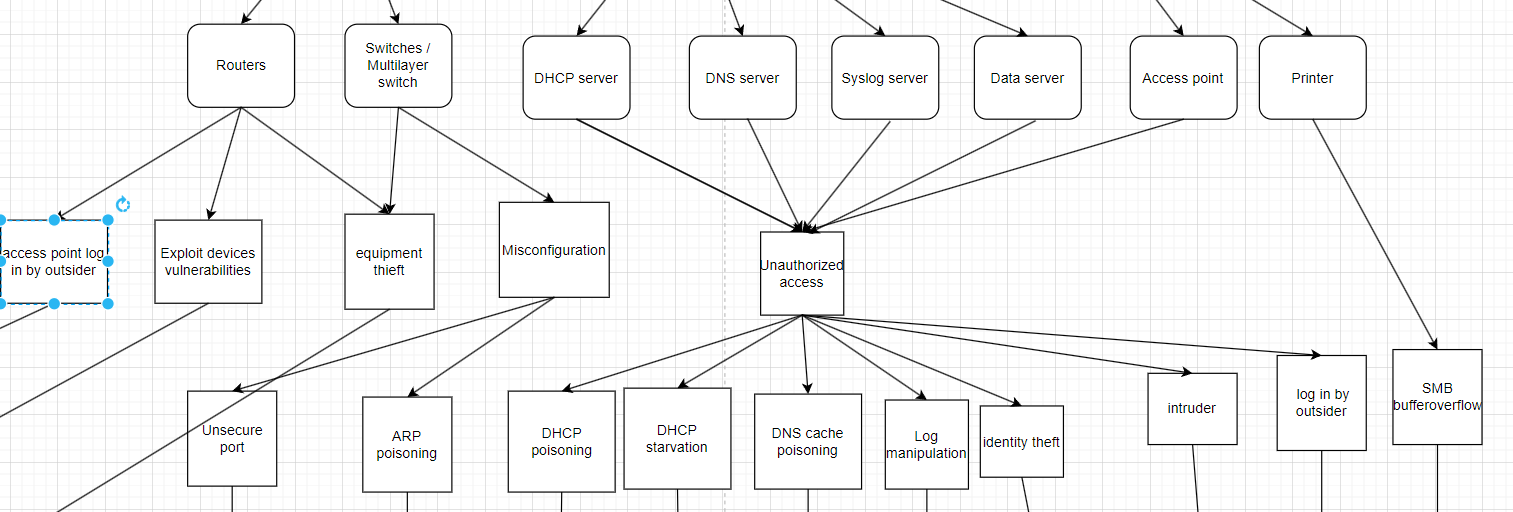
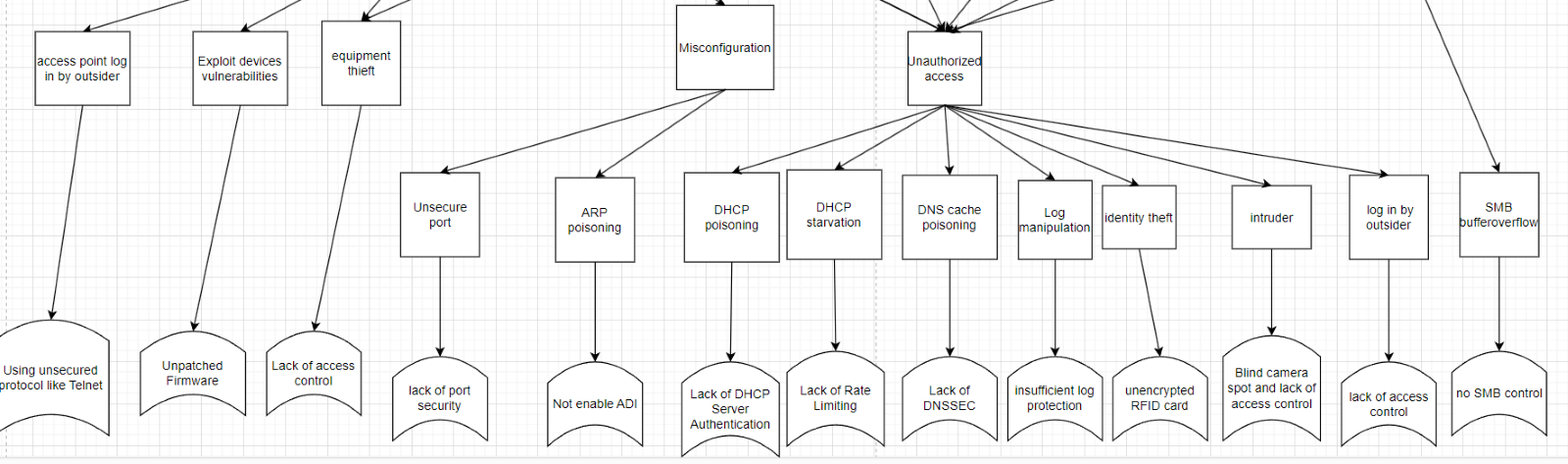


figure 4.3.2.2

By specifying critical assets like this, we can list some attacks could happen to the corresponding asset:

 figure 4.3.2.3

We can see in figure 4.3.2.3, attacks usually happen in layer 2 in network devices like switches due to misconfiguration, and there are also attacks to the network servers based on the protocols that it is using. Finally, possible vulnerabilities that result to the attack are listed in the last layer for implementing security control to prevent potential threats from happening.

 figure 4.3.2.4

## Security controls evaluation

### 4.1) Introduction

After modelling all the threats, we are going to implement security controls based on the trust boundaries to mitigate all the identified threats. We are going to divide the controls into 3 types which are administrative controls, technical controls and physical controls.

### 4.2) Administrative controls

Administrative controls focus on creating policies and procedures to secure the company and ensure efficient operations. Each employee has an account to access the workspace, necessitating robust password policies. Passwords should be at least eight characters long, including special characters, capital letters, and numbers, expiring after one year without reuse. Moreover, login attempts and logging failed attempts should be implemented to prevent brute-force and dictionary attacks on employee accounts.

Specific procedures for web development teams are crucial to prevent exploitation by hackers. Security compliance should be integrated into each phase of the Software Development Lifecycle (SDLC). This includes conducting threat modeling during the design phase to identify threats and vulnerabilities, implementing secure coding guidelines like input sanitization to prevent SQL injection, and using multi-factor authentication (MFA) during development phase. (AI)

Authorization and access control policies are also essential. There are three types: MAC, RBAC, and DAC. MAC is too strict and not adaptable to environmental changes. DAC is flexible but hard to manage for each employee. RBAC is the most suitable as it is scalable and consistent, assigning permissions based on roles. Additionally, the principle of least privilege should be implemented within RBAC, as employees in different positions within a department have varying privileges. (AI)

Finally, software and firmware should be regularly updated after careful research, and hardware should be thoroughly audited before use to avoid supply chain attacks.

### 4.3) Technical Controls

Despite having two firewalls for redundancy, we must manage network traffic access control. Implementing a stateful firewall is essential for inspecting packets destined for the server. Integrating technology like Fastemon into the firewall can prevent server downtime caused by DDoS attacks on both web and mail servers. Strong cryptographic measures, such as SHA256 for password security and AES for encrypting stored data, should be adopted with proper key management.

To prevent identity theft from unauthorized RFID signal copying with devices like Flipper Zero, strong encryption algorithms must be applied to each RFID. For mail-based attack prevention, regular security training for employees and integrated anti-virus programs are crucial to prevent phishing attempts. Configuring mail servers with SPF, DKIM, or DMARC protocols helps verify email sender authenticity and prevents fraudulent emails from reaching users.

Additionally, robust network security configurations are vital. Implement layer 2 security on switches, such as dynamic ARP inspection, to protect against ARP poisoning, and port security to prevent MAC table attacks. Enable DHCP snooping to monitor and control DHCP messages, creating a database of valid IP address allocations with trusted and untrusted ports. DNSSEC adds security to the DNS system by using digital signatures. When a computer looks up a domain name, it uses a public key to verify the digital signatures of the records, ensuring their authenticity and integrity.

### 4.4) Physical Controls

Although we have cameras in the building, redundancy is necessary in case the primary camera fails. Cameras should be positioned accurately to minimize blind spots. Additionally, network devices and servers should be locked in cabinets. Authorized personnel must use physical keys, biometric authentication, and RFID cards to access network infrastructure. While working with servers or network devices, their actions should be recorded by cameras and logged on to the Syslog server. In case of fire, the alarm should trigger sprinklers in specific areas to prevent the fire from spreading.

|  |  |  |  |
| --- | --- | --- | --- |
| **Administrative controls** | | | |
| **Control Name** | **Description** | **Needs to be implemented (X)** | **Priority** |
| Password policy | Passwords should be at least eight characters long, including special characters, capital letters, and numbers, expiring after one year without reuse | X | High |
| Secure coding procedures | Secure every stage of the SDLC | X | medium |
| Access control policies | RBAC (permissions based on roles) | X | High |
| Least privilege principle | Employees and people just have enough privilege to access material or perform their tasks | X | High |
| Update and patching policies | Prevent exploiting old version of the system | X | medium |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Controls** | | | |
| **Control Name** | **Description** | **Needs to be implemented (X)** | **Priority** |
| Firewall | filter malicious traffic from entering internal network | X | High |
| Encryption | makes confidential information/data more secure | X | High |
| Anti-virus | detect and quarantine known threats from phishing email | X | High |
| Port security | Protect the physical port from unauthorized access | X | Medium |
| DDoS prevention | Implement Fastnet Mon which is a solution for DDoS | X | Medium |
| DHCP snooping | monitor and control DHCP messages, creating a database of valid IP address allocations to prevent DHCP attacks | X | Medium |
| Dynamic ARP inspection | protects against Address Resolution Protocol (ARP) spoofing and ARP cache poisoning attacks by using binding table of IP address and MAC address | X | Medium |
| DNSSEC | When a computer looks up a domain name, it uses a public key to verify the digital signatures of the records, ensuring their authenticity and integrity. | X | Medium |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Controls** | | | |
| **Control Name** | **Description** | **Needs to be implemented (X)** | **Priority** |
| Closed-circuit television surveillance | can reduce risk of certain events; can be used after event for investigation | X | High |
| Locking cabinets | prevent unauthorized user access network infrastructure | X | High |
| Fire alarm and fire sprinkler | detect fire to prevent damage to inventory, servers, etc. | X | Medium |
| RFID card reader | Prevent unauthorized access in some location | X | High |
| Biometric authentication system | Increase the authentication for RFID card reader in some critical location like server room | X | Medium |

# MITIGATION AND SECURITY RECOMMENDATIONS

Given DigiTech Corporation's recent move to the Hualon Tower, it is crucial to prioritize the implementation of strong and flexible security measures. Due to the identification of significant vulnerabilities and risks in the infrastructure of the new facility in prior evaluations, it is crucial to create and execute a comprehensive strategy to tackle these difficulties. This plan would not only mitigate the identified threats but also adhere to internationally recognized security standards. In this assignment we will follow the NIST Cybersecurity Framework.

## I. Identify

DigiTech Corporation places significant emphasis on the crucial role of comprehending and controlling cybersecurity risks to its essential physical and logical assets during the Identify phase of the NIST. This first phase required risk assessment and asset management. DigiTech carefully catalogued its physical assets, as discussed in Part 1. This included the infrastructure of its Cyber Intelligence Lab, Application Development Lab, and Data Center. These facilities house a variety of computers, printers, surveillance systems, and network equipment. Logical assets, including critical operational systems, proprietary software, and sensitive data, were given equal priority. DigiTech conducted a comprehensive risk assessment to identify all risks, vulnerabilities, and the consequences they could pose to protect these critical assets. DigiTech identified these elements through a methodical process. This allowed them to implement a savvy approach and strategy to protect their operations (discussed in Part 2). This increased their defenses against cyber threats.

## II. Protect

In the NIST Protect phase, DigiTech emphasizes the protection of critical assets and enhanced system protection. According to part 3, DigiTech uses absolute protection strategies including strong access control, data encryption and network segmentation, user containment to ensure absolute security for the company. The application development and cybersecurity intelligence lab is equipped with secure access points, RFID card readers and monitoring systems to prevent unwanted intrusion. In addition, we arrange and teach employees about basic cybersecurity measures. Through the above measures, DigiTech ensures a certain safety capability to prevent and counter cyber threats or attacks to ensure a highly reliable infrastructure.

## III. Detect

Detect (DE) is the third domain of NIST. It aims to improve the ability to detect and understand cybersecurity incidents immediately, minimizing the potential consequences.

To monitor user and entity behavior across the entire network, you should use Splunk User Behavior Analytics (UBA). To provide real-time analysis, behavioral baselines must be established, anomaly detection algorithms customized, and interfaced with existing SIEM systems. Use Splunk UBA to monitor and analyze user and entity behavior across the entire network to detect insider threats and anomalous activities.

When a UBA alert is triggered (for example, when an employee logs in at an unexpected time in the Cyber Security Intelligence Lab), the SOC Tier 1 team examines the alert to comprehend its context and initial level of seriousness. If the warning signals a possible insider threat or a substantial divergence from typical conduct, elevate the incident to SOC Tier 2 for a more thorough examination.

Moreover, installing IDS on dedicated monitoring stations or using distributed sensors in important network segments to detect and alert attacks. For example, Snort can identify outgoing network traffic from a computer in the Apps Development Labs on the 7th floor. Install IDS sensors at the entry points of the Data Center on the 6th floor, between the internal network and the development environments on the 7th and 8th floors, and at the perimeter gateway where external traffic enters. All network-based IDS sensors should be placed after the firewall. This is the architecture we suggest for using IDS:

In addition to being sent to the firewall, internet traffic will also pass through the Network tab, where it is duplicated and sent to the IDPS load balancer. Here, the traffic will be divided into two sources for the IDPS sensor to identify warnings. If traffic bypasses the firewall and flows directly through it, the spanning port functions as a network tap to forward the traffic to the next IDPS sensor. Consequently, the Management server will notify all the traffic. When an IDS alarm is activated (for example, when abnormal traffic is discovered from the Application Development Labs), the SOC Tier 1 team evaluates the warning to ascertain its characteristics and origin. If the incident involves intricate or high-risk traffic patterns, such as a possible attempt to extract data from the Data Center, it should be escalated to SOC Tier 2.A diagram of a computer network

Description automatically generated

## IV. Respond

The next area of focus at NIST is Respond (RS), which involves the development and implementation of suitable measures to be taken in response to an identified cybersecurity incident. For this region, we recommend using IPS (intrusion prevention system) technology.

IPS can promptly obstruct or segregate harmful network traffic to confine and restrict the propagation of a cyber-attack. For example, in the case that malware is identified, IPS has the capability to obstruct its ability to establish communication with its command-and-control server or propagate to other segments of the network. For Network Segmentation, configure IPS at critical points in the network, such as between the main network and the development lab, to monitor network traffic and protect critical development data. In addition, IPS supports real-time blocking. For example, IPS has the ability to automatically block specific IP addresses, kill ongoing sessions, or change access control lists (ACLs).

DigiTech’s SOC team must continuously update IPS using the latest threat signatures collected from threat intelligence sources. This is critical to protecting against emerging cyber threats, such as zero-day vulnerabilities. Additionally, integrating IPS with Security Information and Event Management (SIEM) platforms, such as Cortex XSOAR, ensures that response activities are synchronized and automated across multiple security systems and tools. Changes to firewall rules can help prevent attackers from accessing their IP addresses and notify the security team.

DigiTech’s SOC team must continuously update IPS using the latest threat signatures collected from threat intelligence sources. This is critical to protecting against emerging cyber threats, such as zero-day vulnerabilities. Additionally, integrating IPS with Security Information and Event Management (SIEM) platforms, such as Cortex XSOAR, ensures that response activities are synchronized and automated across multiple security systems and tools. Changes to firewall rules can help prevent attackers from accessing their IP addresses and notify the security team.

SOC Tier 2 is responsible for thorough analysis of escalated incidents passed on by the first tier. The goal is to gain a comprehensive understanding of the scope and impact of these events. Remediation may need to be performed after the incident is contained. This includes removing malware, disabling compromised user accounts, and remediating any exploited vulnerabilities. During remediation, it is important to accurately identify all the company’s servers that were affected. Using SIEM integration with IPS allows for events to be connected and response actions to be automated, such as adjusting firewall rules or prohibiting access to suspicious IP addresses. Tier 2 analysts work together with Tier 3 professionals, such as forensic teams or threat hunters, to do sophisticated technical analysis and forensic investigations.

## V. Recover

The final element of NIST is the Recover (RC) component, which is implemented to guarantee the organization's ability to promptly and effectively recover from cybersecurity incidents, thereby resuming normal operations and reducing the impact on business activities. For this component, we recommend using Continuous Data Protection.

Develop and maintain recovery strategies and mechanisms to guarantee prompt reinstatement of operations. We recommended using Veeam Backup & Replication to offer uninterrupted data protection by collecting real-time data changes and duplicating them to secondary storage locations. This will ensure the latest data will be accessed for retrieval in order to decrease all the possible risks of losing data. We suggest using Veeam as a technology for back-up or replication data. The data can be taken in a primary system like database server, application server or file storage system. Then it will be sent and copied to another location by using Real-Time Data Replication. This could be an on-premises disaster recovery (DR) facility or off-site cloud storage. For example, DigiTech uses Veeam to backup data from HaNoi to Ho Chi Minh city. After back-up, the data can still be retained and accessible after the disaster. DigiTech might also utilize Veeam to recover the damaged database immediately before the incident happened. This procedure minimizes data loss and downtime.

Improve recovery processes by leveraging past experience and making necessary changes to meet organizational needs. Zerto delivers logs and chronological records of data updates for incident analysis. This enhances knowledge of the effects of occurrences and accelerates forensic investigations. For example, DigiTech’s security team used Zerto’s logs after a ransomware attack to pinpoint the moment the infection encrypted important files. This allowed them to restore the system to its original state, minimizing data loss. Besides that, DigiTech needs to constantly revise Zerto's rules to optimize data replication and recovery settings for new business applications and client data requirements as it expands its services to new markets.

## Tier

The NIST CSF implementation tiers delineate an organization's perception of cybersecurity risk and the measures in place to alleviate it. Tiers indicate a progressive level of proficiency in the implementation of cyber risk management strategies. They assist in comprehending the impact of business requirements on a company's comprehensive risk management protocols and cybersecurity risk management. There are 4 NIST implementation tiers: Partial, Risk-informed, Repeatable and Adaptive.

**1. Tier 1**

This tier comprises firms that have either on-demand or no security protocols in place. Businesses in Tier 1 are classified as having a minimal understanding of cybersecurity risk. They often neglect to adequately prioritize cybersecurity measures.

**2. Tier 2**

At Tier 2, organizations have initiated the implementation of structured risk management procedures. They possess a rudimentary comprehension of their cybersecurity vulnerabilities and are commencing to implement proactive actions to mitigate them.

**3. Tier 3**

Tier 3 organizations have established official policies and procedures to effectively handle cybersecurity concerns. Enterprises in this sector are typically more prepared to address vulnerabilities, cybersecurity risks, and attacks.

**4. Tier 4**

Tier 4, the top level, shows organizations have a proactive, alert cybersecurity approach that adapts to changing threats. They monitor and improve their cybersecurity protocols as information and risks change. Flexible incident reactions and cybersecurity are part of the firm's risk management.

Based on what we suggested for DigiTech company's cybersecurity practices and processes aligned with the NIST Cybersecurity Framework (CSF), here is my evaluation of which tier Digitech belongs.

In the initial stage, known as the Identify phase, we determined that the company operates at Tier 3 (Repeatable). This assessment was based on the observation that the methods used to manage assets and evaluate risks are characterized by a systematic and methodical approach, suggesting a standardized approach throughout the business. The next phase is Protect, where there are systematic methods for overseeing and improving security measures. With various protection methods provided, this phase is evaluated as Tier 4 (Adaptive). About the Detect phase, we evaluated Digitech as Tier 3 (Repeatable). Digitech's employment of Splunk UBA and IDS to detect cybersecurity incidents and Tier 1–Tier 2 escalation mechanisms demonstrate a mature detection capacity. In the Respond phase, DigiTech integrates IPS, SIEM, and structured incident response processes meets Repeatable tier (Tier 3). In the final stage is the Recovery phase, effective data protection and recovery methods necessitate the implementation of a structured cybersecurity recovery approach. Consequently, this phase is likewise assessed as Tier 3.

Based on our analysis, Digitech seems to closely correlate with Tier 3 (Repeatable). To advance Digitech to Tier 4 in the NIST Cybersecurity Framework, prioritize strategic alignment and leadership commitment. Enhance risk management with advanced threat intelligence and predictive analytics. Invest in AI-driven analytics and continuous monitoring for early threat detection. Automate incident response and refine recovery strategies with automated processes to minimize downtime. Foster a culture of continuous improvement, conduct regular assessments, and adapt strategies based on best practices. Collaborate for threat intelligence, enhance employee training, and maintain regulatory compliance. Pursue cybersecurity certifications to demonstrate resilience and readiness.

# Conclusion

As the security consultants, we have provided recommendations for DigiTech Corporation to enhance their security posture. First, we suggested a physical and logical architecture along with a CIA (Confidentiality, Integrity, Availability) evaluation and identified all physical assets for DigiTech to follow. In the risk assessment phase, we identified potential risks by dividing the process into three parts: risk identification, quantitative analysis, and risk analysis. Based on these identified risks, we created threat models and proposed security controls. Finally, we recommended implementing the NIST Cybersecurity Framework to mitigate potential threats, risks, and vulnerabilities, and to continuously improve the security posture in the future.

**Word count: 6209**

References:  
PRODUCT BRIEF Splunk User Behavior Analytics Detect advanced and insider threats using machine learning Product Benefits. (n.d.). Available at: <https://www.splunk.com/en_us/pdfs/product-briefs/splunk-uba-product-brief.pdf>. IBM (2023).

What is an intrusion prevention system (IPS)? | IBM. [online] [www.ibm.com](http://www.ibm.com/). Available at: <https://www.ibm.com/topics/intrusion-prevention-system>.

Data Backup. (n.d.). What is Veeam Backup & Replication? | Definition from TechTarget. [online] Available at: <https://www.techtarget.com/searchdatabackup/definition/Veeam-Backup-Replication#:~:text=Veeam%20replicates%20VM%20backups%20to>.

# Appendix:

## I) AI supporting language

- There are 2 types of attacks in the external attack tree which are web-based attacks and mail-based attacks. For web-based attack, we can see there are some attacks happen due to unsecure coding like XSS, CSRF, path traversal and SQL injection. Therefore, teaching secure coding to developers is very crucial to the company. Firstly, user input should be carefully sanitized to prevent XSS and SQL injection, and do not use unsecure libraries while coding. Moreover, strong cryptography should be implemented like SHA256 to secure the password, all stored data should be encrypted by using AES and the key should be properly managed. MFA should be enabled to protect user accounts on the web. Next, Fastnetmon, which is a DDoS detection and prevention, should be implemented in the firewall to prevent server downtime due to DDoS attack for both web server and mail server. For mail-based attack solution, security training should be conducted regularly for employees and anti-virus programs should be integrated. Moreover, to prevent email spoofing, mail servers should be configured with SPF, DKIM or DMARC protocols. Secondly, for credential compromised attack, we should limit login time to prevent brute force and set strong password policy to prevent password spray attack.

* Administrative controls concentrate on creating policies and procedures to secure and ensure the company operates effectively. Firstly, each employee has an account to access to the workspace, so it is very important to set robust password policies. The password of each employee should be at least 8 characters long and must contain special characters, capital letters, and numbers. All passwords should expire after 1 year and cannot be reused. By implementing these controls, we prevent brute-force attacks and dictionary attacks that happen on employee accounts. Secondly, there must be also specific procedures for web developers' teams to prevent web exploitation from hackers. Security compliance should be applied in each phase of the Software Development Lifecycle (SDLC) for example: conducting threat modelling during the design phase to identify all threats and vulnerabilities, then implement secure coding guidelines like how to sanitize inputs to prevent SQL injection, how to use MFA for authentication and many more coding techniques for the developers team. Moreover, one of the most important policies should be applied, which are authorization and access control. There are 3 types of access controls which are MAC, RBAC, DAC. MAC is too stricted, so it is not adaptable to changes in environment. DAC is flexible control, but it is hard to manage privileges of each employee in the company. Therefore, RBAC is the most suitable access control because it is scalable if the company’s employees grow, and it is a consistent policy because each employee has permission based on their role. In addition, the least privilege principle should be also implemented along with the RBAC for each employee because in one department, there are employees that have different positions in ranking, so their privileges are also different. Finally, for the patching and updating, software and firmware should be checked for updating to the new version after carefully researching the new version, and hardware should be carefully audited before using to avoid supply chain attack.
* SOC tier 2 does research for the information Tier 1 provided. This goal is to have a deep understanding of threats. Repairing methods need to be applied after the attack. This includes deleting malware, disabled compromised account, remediating any exploited vulnerabilities. In this method, we must specify all the company’s servers affected.
* DigiTech needs to update IPS regularly due to latest threats which collected from any sources. The benefits of this are to protect against the newest cyber-attacks such as zero-day. Work and use SIEM platforms to ensure response activities are synchronized and automatic. We suggest Cortex XSOAR. We need to make changes or fix the firewall rules to protect from attackers due to their behavior of accessing IP addresses. ￼
* As the security consultants, we have given recommendations for DigiTech Corporation to improve their security postures. Firstly, physical and logical architecture are constructed as a suggestion along with the CIA evaluation and all physical assets are identified for DigiTech to follow. After that, in the risk assessment part, we have identified all the potential risks by dividing them into 3 parts which are risk identification, quantitative analysis and risk analysis. Based on the identified risks, threat modelling is constructed with security controls. Finally, NIST Cyber Security Framework is proposed to mitigate all possible threats, risks and vulnerabilities with future improvement on security posture.

## II. Network topology

A diagram of a computer network

Description automatically generated