# Bole Sub-city Risk Assessment

# Introduction

- The Cyber Attack continues to have a massive economic impact on the government as well as indirectly on everyone.
- As the government offices store all of our personal information and data in the remote databases this might result in direct consequences, if someone gain unauthorized access to the database server, and corrupt or delete the information.

# Purpose

- The purpose of the risk assessment is to identify the threats and vulnerabilities related to Bole sub city Administration and their data protection mechanism.
- To identify risk mitigation techniques used in Bole-sub city Administration.

## Scope

- This risk assessment is limited to Bole sub city administration. It carry out municipal functions within the bounds of the physical space located for it in accordance with the principle of decentralization and in conjunction with the center of the city.

# Findings of the Security Assessment

- The Bole sub city administration is dedicated to maintain and control access to public information, personal information and data related to their employee, and everyone who take service in that sub- city.
- The sub city has its own assets also it monitors and control public assets. So the sub city is in charge of protecting assets like employee information, customer information.

**The Assets of the Sub- city**

- CCTV camera data, Personal computers,Employee information and Customer information

To secure the assets it has data center which have CCTV camera controller room and server room. The data center has local data base system and backup system.

- The room has AC system, temperature controller sensor, fire sensor, emergency light, alarm sound system, and public address sound.
- They have manual fire extinguisher to control any accident related to fire.
- They also have automatic fire extinguisher in place. However, they are not using it because it need high expense to install it.

- The first room inside the data center contain all information related to CCTV camera.
- The CCTV camera control the surrounding. It also controls any activities that occur around Megenagna.
- The CCTV camera has 40 hard disk each with 3 TB storage capacity.
- However, there is no technician who control the camera records frequently. They just assess the data if they need information or if accident happen.

- Next to the CCTV camera controller room there is server room.
- They use the server for local data control.
- In order to open this room, they use token card and finger print authentication mechanism.
- They have file server, network server, web server, Redundant file servers, email servers.
- However, they are not using the Email and web server currently.
- The network server has firewall that can be used by each joined users.

# Mechanisms used to secure the system

- **Physical security**

  They use a CCTV camera to control the surrounding environment of their building

- **Network security**

  They use a VPN service provided by Ethio Telecom using Ethernet technology to reduce the risk of Cyber Attack from the internet.

- They use three tier architecture of network divided into core, distribution, and access layers.

## Authorization

- They use an RF ID card and fingerprint authentication mechanism to authenticate each individual who enters to their data center
- Access control rights is also set individually on each system resource for each individual user and group.

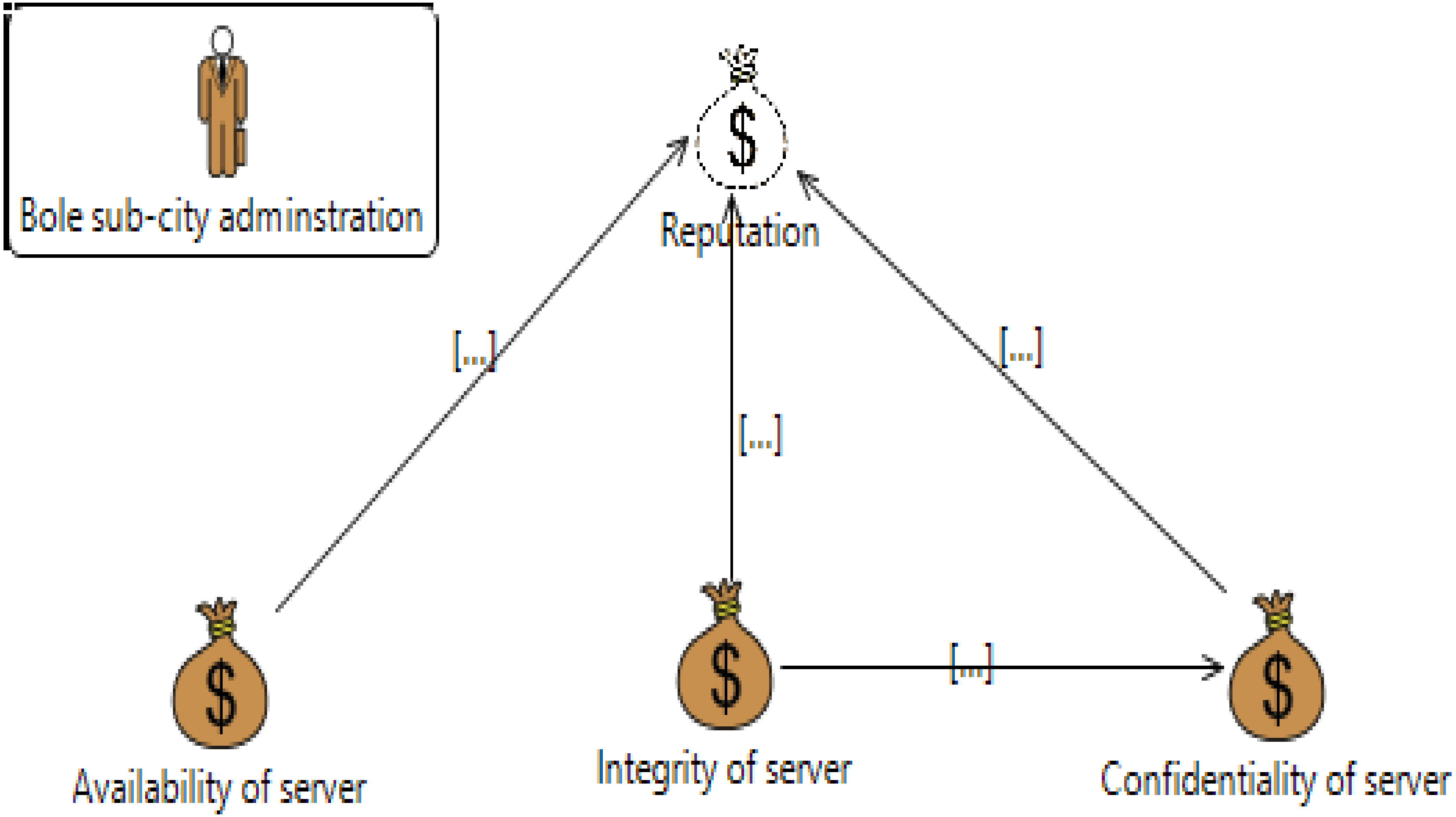
# METHODOLOGY

## ASSET IDENTIFICATION

From our assessment the asset contained in the sub city data center server are:

- CCTV cameras data that the sub city used for checking the sub city also the surrounding
- Server which is found in the sub city. They use decentralized server.
- Employee information
- Personal computers

# Coras Asset Diagram



# RISK Analysis

- Once the Assets were identified the next thing to do was find out the vulnerabilities, threats, and Risks associated with the assets.

**RISK IDENTIFICATION**

**Identification of vulnerabilities**

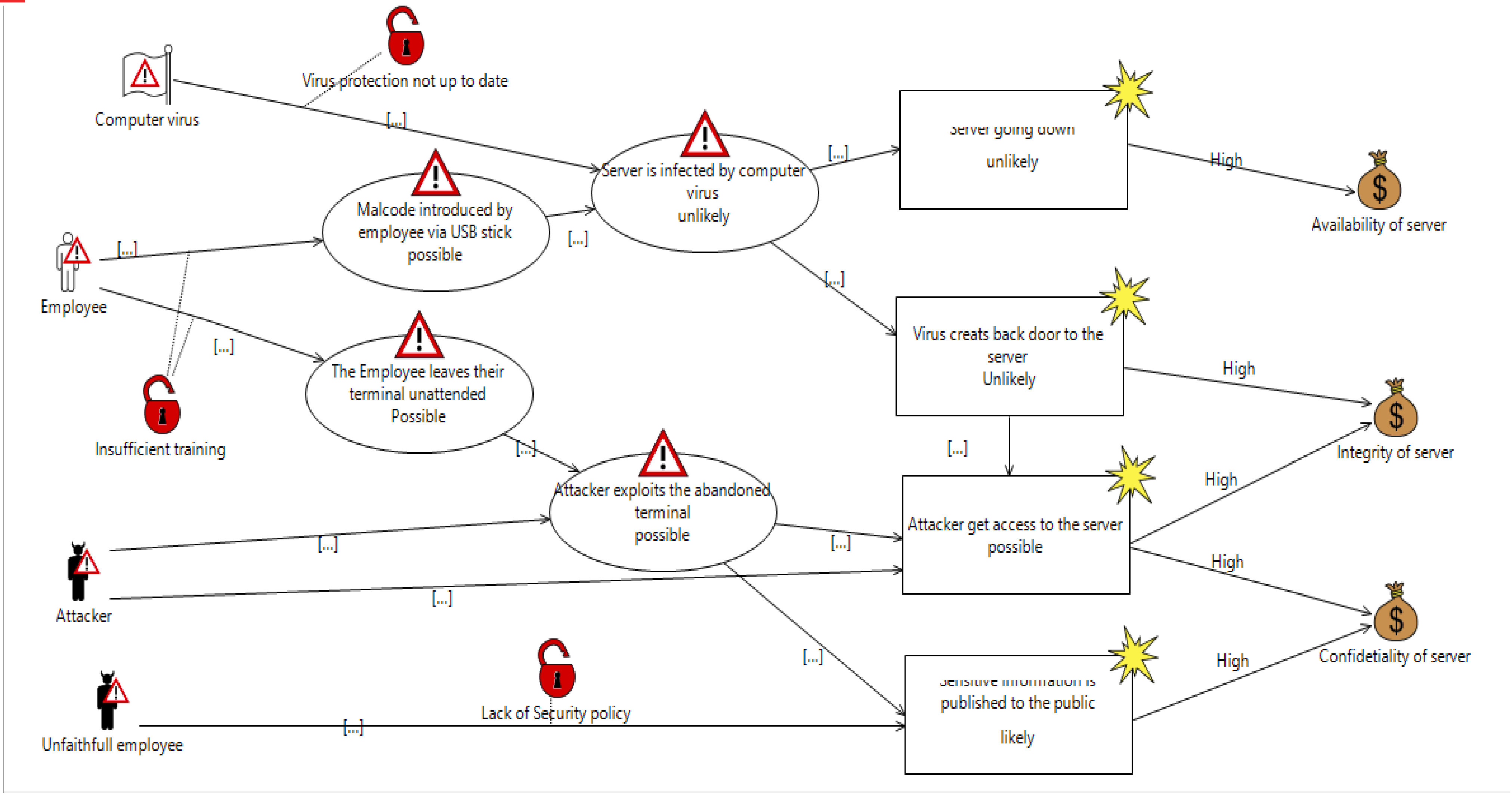
- Lack of security policy
- There virus protection is not up to date
- Lack of proper security training for the employees.
- Identification of threats

## Identification of threats

We identified the following threats

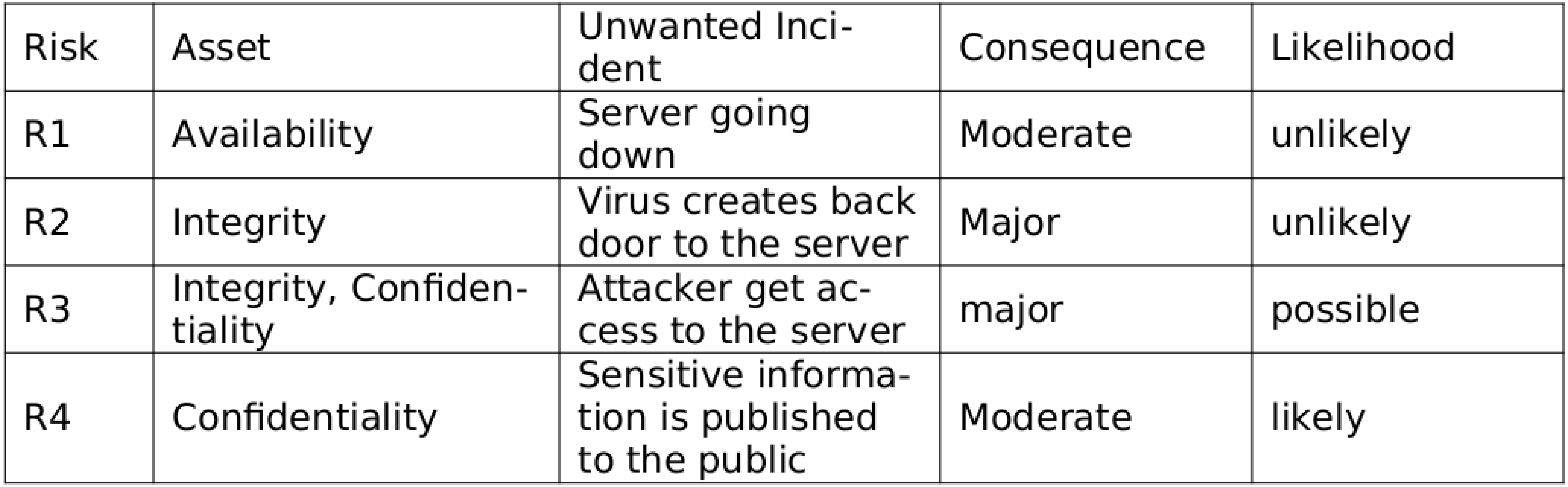
- Pawns (insider threats)
- Turnclocks (insider threats)
- Terminal hijackers (Attackers)
- Computer viruses

# Coras threat diagram



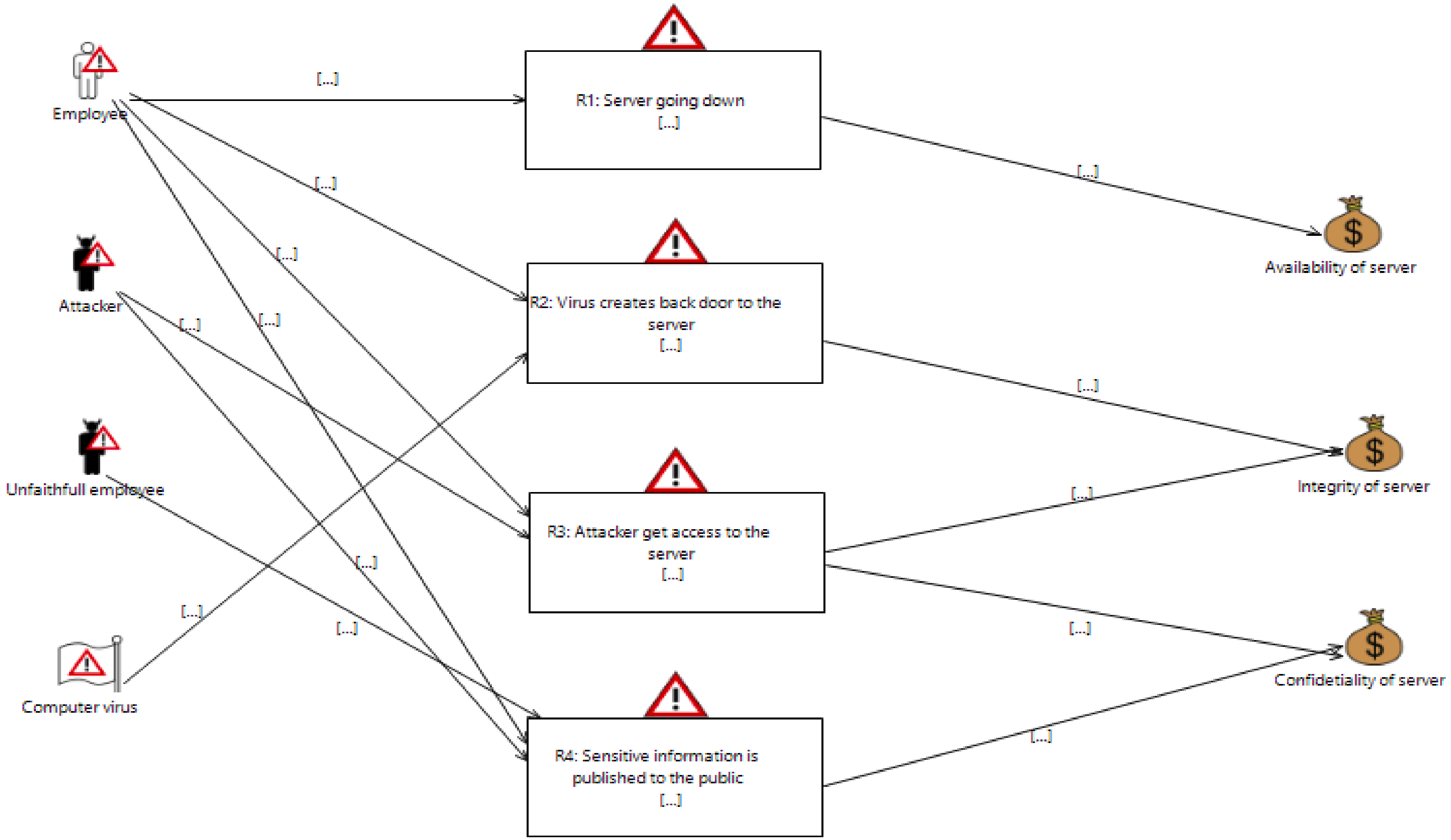
# RISK ESTIMATION

- After identifying the risks, we estimated the consequence and likelihood of each risk as follow

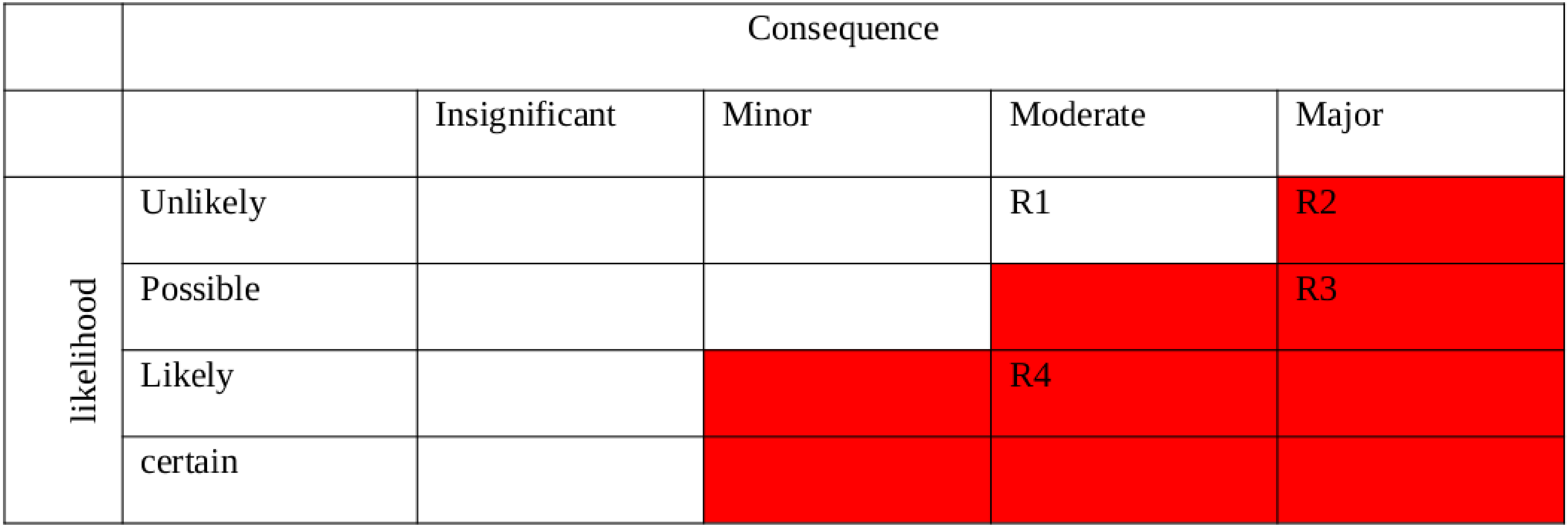


| Risk | Asset | Unwanted Incident | Consequence | Likelihood |
|---|---|---|---|---|
| R1 | Availability | Server going down | Moderate | unlikely |
| R2 | Integrity | Virus creates back door to the server | Major | unlikely |
| R3 | Integrity, Confidentiality | Attacker get access to the server | major | possible |
| R4 | Confidentiality | Sensitive information is published to the public | Moderate | likely |

# RISK EVALUATION



# The evaluation is summarized below.



|  | Consequence |  |  |  |  |
|---|---|---|---|---|---|
|  |  | Insignificant | Minor | Moderate | Major |
| likelihood | Unlikely |  |  | R1 | 🟥 R2 |
|  | Possible |  |  | 🟥 | 🟥 R3 |
|  | Likely |  | 🟥 | 🟥 R4 | 🟥 |
|  | certain |  | 🟥 | 🟥 | 🟥 |

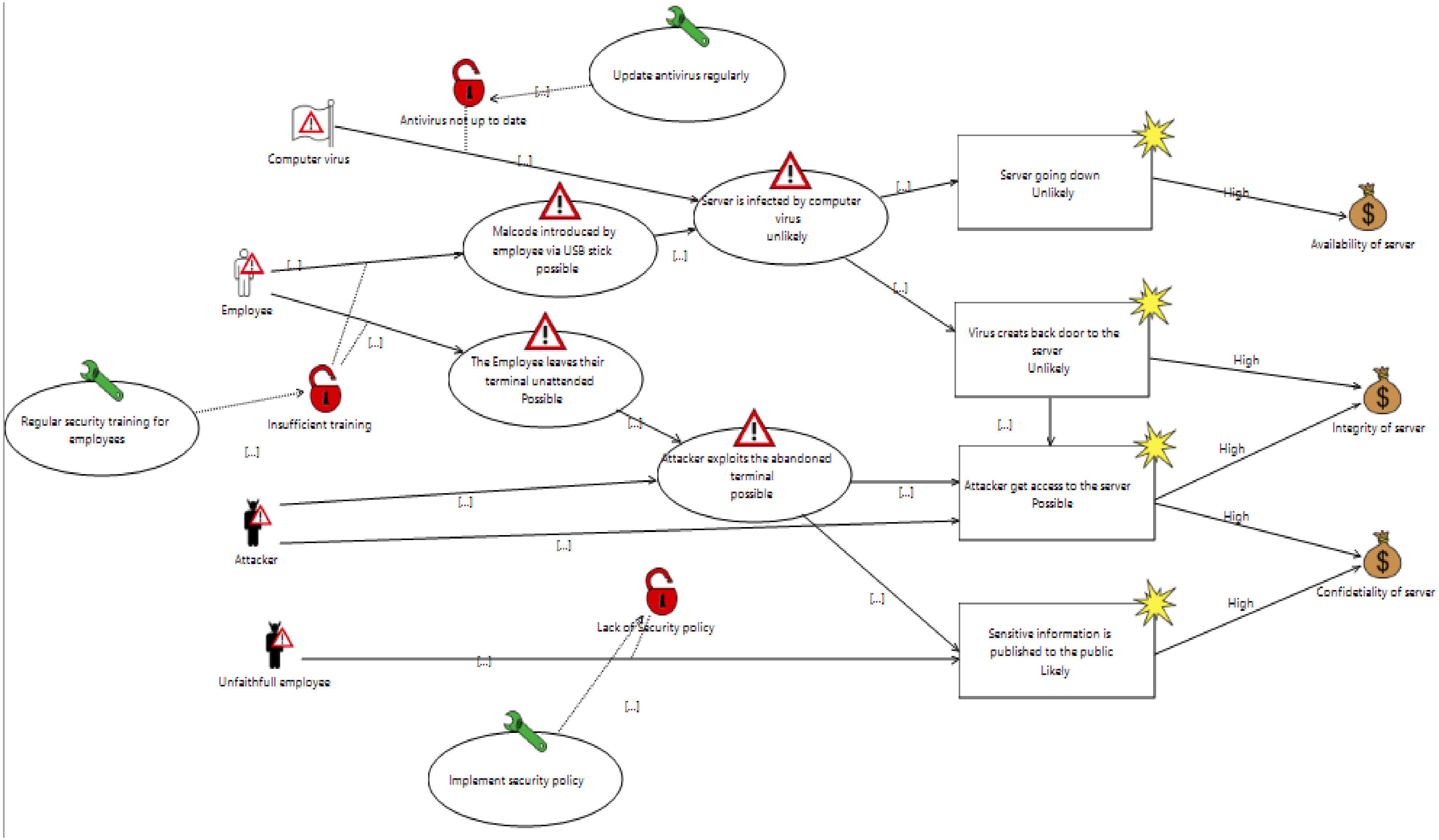
Note: regions marked red are threats that must be treated further

# TREATMENT

Some of the treatment need to take are mentioned below:

- Properly documented proper security polices
- Updating their anti-virus protection,
- Properly organized security team
- Employee training

# Coras treatment diagram


Update antivirus regularly
[...]
Antivirus not up to date
Computer virus
[...]
Server is infected by computer virus
unlikely
[...]
Server going down
Unlikely
High
Availability of server
Malcode introduced by employee via USB stick
possible
[...]
Employee
[...]
[...]
Virus creats back door to the server
Unlikely
High
Integrity of server
[...]
The Employee leaves their terminal unattended
Possible
Regular security training for employees
Insufficient training
[...]
[...]
Attacker exploits the abandoned terminal
possible
[...]
Attacker get access to the server
Possible
High
High
Attacker
[...]
[...]
Confidetiality of server
[...]
High
Lack of Security policy
Sensitive information is published to the public
Likely
Unfaithfull employee
[...]
[...]
Implement security policy

# CONCLUSION & RECOMMENDATION

Overall, the implementation of the system security was found to be poor. The fact that no written policy is maintained in the organization shows the lack of knowledge and ignorance in their part.

- Also, the lack of disaster recovery and fault tolerance system. Most of the data in their server is not backed up remotely which poses the danger of losing the data if something catastrophic like a natural disaster occurs.

So as a government organization, they need to work on their security mechanism in order to protect their assets form intruders

- So, we recommend that they should have properly written security policy.
- They need to have disaster recovery and fault tolerance system.
- They need to have properly organized security team