**Author:** *Alessandro Ferro*

**ICTSAS505**

**Task 3**

**PART 1**

The following report lists the threats that have been identified for the **Online Systems Solutions – Web Hosing Services.**

In the attached file (Part 2 – Disaster Recovery Plan) The risks and vulnerabilities will be further investigated. The document will also contain suggestions and strategies to prevent and minimize the effects of the threats and to ensure business continuity.

**Potential Threats**

* **Fire**
  + No other security measure other than a fire escape is mentioned.

*The entirety of the business hardware and software assets are located on the same premises. Inc ase of a fire, without the appropriate counter-measures the destruction of these assets can be highly probable and would have a catastrophic effect on the business capacity to operate.*

* **Power outage**
  + Room 1 doesn’t have any measure to provide alternative power supply in case of blackout, brownout or power surge.

*The disruption of some of the services hosted in the servers in room 1 could lead to major issues to business and also to people. The monetary loss and the severity of the impact on people well being can range from minor to substantial.*

* **Humidity**
  + Room two has no air conditioning system
  + Room one has two air conditioning system but no alternative power supply

*Humidity can damage the hardware. The two air conditioners in room one runs on two separate circuits, but the lack of an alternative power supply in case of power outage makes the servers still potentially subject to this issue. Server room two has no measure to prevent this problem.*

* **Water damage**
  + There is no metion of any water leackage detection system

*As per humidity, water can damage the hardware, causing the loss of hardware, software and data.*

* **Natural disaster**
  + There is no mention of measures adopted to minimize the effects of flood, lightning, earthquakes and any other possible natural calamity.
  + The operations servers and the backup are stored in the same building

*The document doesn’t specify to what natural events the system can be subject to and doesn’t specify its location, the features of the building, etc. The effects of a natural disaster can be catastrophic.*

* **Unauthorized access to premises**
  + Room one is not locked and has minimal surveillnace by staff members during business hours
  + Room two is locked, but is positioned next to an external access
  + Both room one and room two are given access to more people than necessary
  + Critical data secret backup storage is easily accessible by staff even just by accident

*Critical assets and data could be compromised, corrupted and stolen.*

* **Malicious software**
  + There is no mention of measures to protect the system from **virus, trojans, worms, spyware, sey loggers, adware, denial of service attacks** and other security threats

*Corruption of data, disruption of services, data theft can cause major monetary loss to the business.*

* **Unauthorized access to the system**
  + Full access to the system granted to laptops provided to remote staff for work and personal use.
  + There is no mention of security measures for the staff accessing the system remotely
  + There is no mention of security measures to access the system

*Corruption of data, disruption of services, data theft can cause major monetary loss to the business.*

* **Malicious attack**
  + There is no mention of measures to prevent intrusion in the system

*Corruption of data, disruption of services, data theft can cause major monetary loss to the business.*

* **Data loss/corruption**
  + Backup secret storage can be easily accessed (even by accident) by staff members.
  + Backup storage is in the same building
  + Servers nearly reached maximnum capacity

*Corruption of data, disruption of services, data theft can cause major monetary loss to the business.*

* **Other issues**
  + No formal documented procedure for disaster recovery
  + The business continuity and disaster recovery plan adopted, relies an a vague agreement between companies.
  + The above mentioned plan doesn’t keep into account hardware and software environment compatibility
  + The plan has not been tested.