MULTIMEDIA UNIVERSITY OF KENYA

Course: BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

Unit Code: BIT 2318

Unit Name: INFORMATION SYSTEMS AUDIT

Registration No.: CIT-221-039/2013

Name: MAKENA YVONNE

Date Submitted: 24/05/2017

Your Tasks

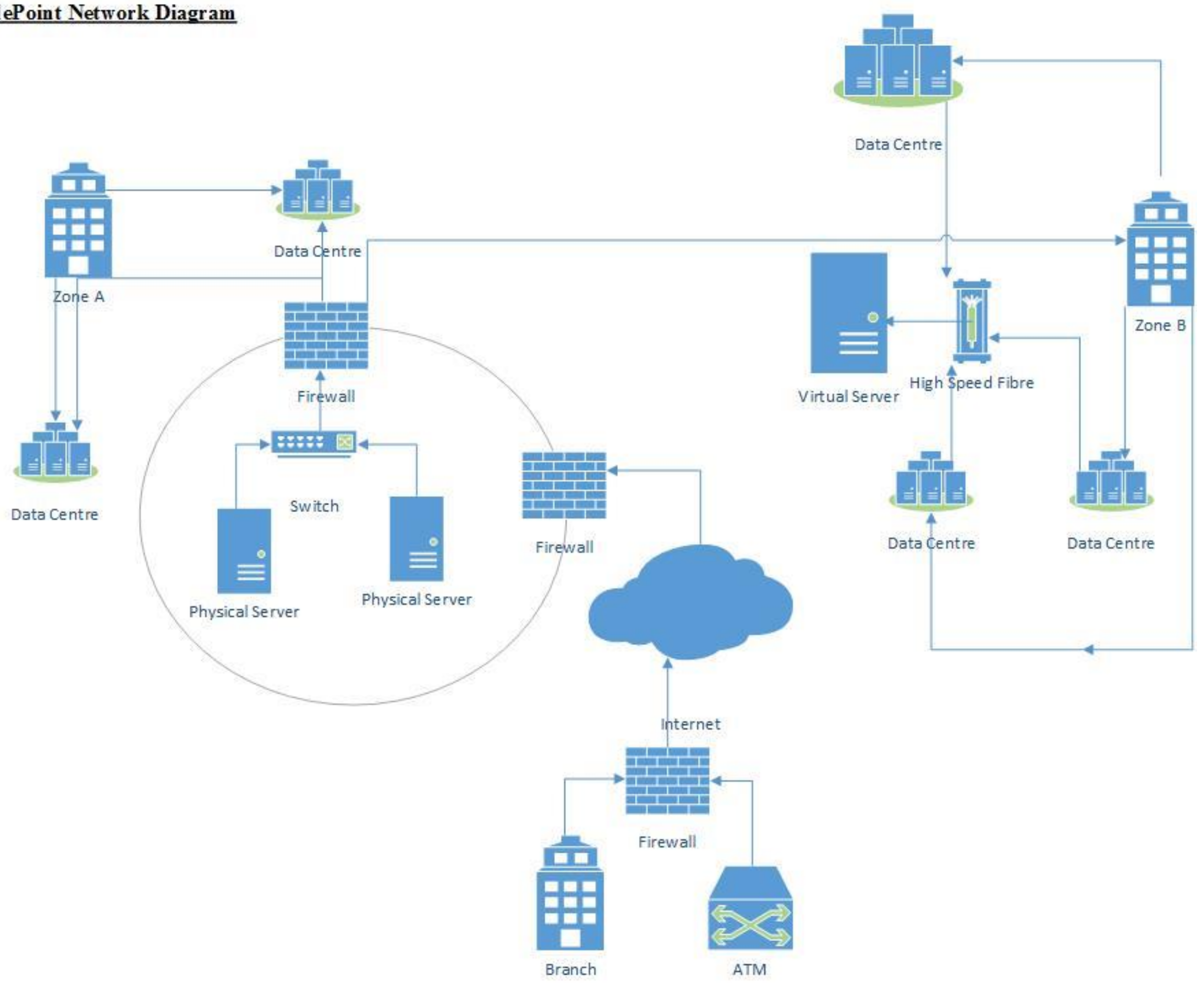
1. Prepare a network diagram based on your interviews, reflecting your understanding of the PridePoint network in its current state. Include:

a. Zone boundaries

b. Connection points and links

c. Known security capabilities

PridePoint Network Diagram



2. Review the list of risk identified by the Director of Technology Operations. For each risk, based on your interviews:

a. Estimate the difficulty in detecting the threat event given current capabilities.

- Regional event affecting connectivity and/or power – It would be so difficult to detect this threat because it is not given a priority according to the interviews given.
- Consolidation into a single-zone network – This threat would be easily detected because according to data recovery interview, each network has a disaster recovery plan.

- Loss of cooling capacity within a data centre – There would be less difficulty due to the disaster recovery plan already set.
- Customer data accessed without permission – It is easy to detect that because it is customer facing and customer facing situations are given priority.
- Key knowledge lost due to employee departures – Very difficult to detect because priority is given to anything customer facing and not anything non-customer facing.
- External parties direct cyber-attacks against the network – Somehow difficult to detect due to the cut security awareness training as stated by the information security officer. 67% failed a phishing test meaning the company is very vulnerable. Also easy to detect because perimeter is probably stronger than most of the competitors' networks.
- IT projects cost more or take longer than planned – It is difficult to detect because the CIO rejected the projects that were proposed even though the ideas were great.
- Data transaction processed on wrong system - It is easy to detect that because it is customer facing. According to CIO, customer-facing situations are given priority.

b. Identify a vulnerability that aligns with the threat event.

- Regional event affecting connectivity and/or power – Lack of backup sources of power.
- Consolidation into a single-zone network – There is no vulnerability since it is well handled by having a disaster management plan.
- Loss of cooling capacity within a data centre - There is no vulnerability since it is well handled by having a disaster management plan.
- Customer data accessed without permission - There is no vulnerability since it is well handled by the fact that customer-facing situations are given first priority.
- Key knowledge lost due to employee departures – Fading away of innovative skill in the business.
- External parties direct cyber attacks against the network – Unknowingly disclosing of company's information by employees.
- IT projects cost more or take longer than planned – Lack of innovation and creation of new ideas.
- Data transaction processed on wrong system - There is no vulnerability since it is well handled by the fact that customer-facing situations are given first priority.

c. Summarise a possible consequence associated with the risk.

- Regional event affecting connectivity and/or power – Discontinuation of the business activities and loss of unsaved data.
- Consolidation into a single-zone network - Reduced consequences but there would be a slow down in performance of work.
- Loss of cooling capacity within a data centre – Reduced consequences due to the backup plan.
- Customer data accessed without permission - Reduced consequences since it is a priority.
- Key knowledge lost due to employee departures – Risk of being beaten by competing businesses.

- External parties direct cyber attacks against the network – Misuse or mishandling of company secret information.
- IT projects cost more or take longer than planned – Being behind the competition in the market.
- Data transaction processed on wrong system - Reduced consequences since it is a priority.

3. Select the most serious risk based on your assessment and your understanding of the enterprise risk appetite (Prioritize Risks).

According to my assessment, regional event affecting connectivity and/or power is the most serious risk. This is because this risk will lead to discontinuation of all the business activities (operations/service) and loss of unsaved data.

All the other risks can be solved in one way or the other since they can be predicted. The fact that they are predictable brings the need for future planning on how to handle and minimize those risks.