ICT 380: Scenario for the Research Paper on Governance and Security Policy

Assignment 2

Introduction

Below is the scenario for the group project for ICT 380 - Information Security Policy and Governance. Based on the scenario, you need to create a security master plan for your organisation. The plan will be based on the work that you will be doing in the weekly workshops and in your group meetings that will follow the workshops.

Owing to the fluid nature of the scenario and the slightly different direction each team/group may take in their discussion, the scenario may change, be modified or additional information may be provided to ensure it stays relevant.

Amendments or additions to the scenario will be provided either as a download in LMS, and/or distributed in class.

Scenario

1.0 Details of organisation

Name : Insert the name of your company here

Address :<name of company> Tower

: <insert address>

: Perth 6000. Western Australia.

Staffing : 500+ staff in various departments

Building : Basement - Carpark / Security Office / Loading & Unloading bay

: Ground Level - Reception

: Level 1 - Building maintenance / Training room / R&D

: Level 2 - General Administration / Human Resource / Finance

: Level 3 - Sales / Software and technical support

: Level 4 - Information Technology / Server room

: Level 5 - Data Centre / Seismic Exploration

: Roof - Air-conditioner cooling towers, water tanks

Floor Plan : See attached

Key Personnel : CEO

: Chief Security Officer

: Chief Information Technology Officer

: Director Sales & Product

: Division Head - Research and Development

: Division Head - Software

: Division Head - Data Processing

: Division Head - Service and Technical Support

: Director - Back Office

: Manager Building and Maintenance

: Manager Officer Administration

: Manager Finance

: Manager Human Resource

: Manager Legal Department

: Legal Officer

2.0 Company Background

The company is a mid-size software company specialising in developing software and hardware for the oil and gas industry as well as providing services to oil and gas companies in processing seismic data to assist in locating new oil and gas fields.

2.1 Monitoring Software *

SensorDrill - Software and hardware used to monitor the drilling of oil and gas wells

MeasureMe - Software and hardware package used to monitor the pumping of oil and gas

2.2 Services *

Provide services in processing and interpreting collected seismic data using internally developed software (Shake and Quake).

**** NOTE***

1. SensorDrill and MeasureMe software are licensed to the client for their own use

2. Shake and Quake software not licensed for client use, client provides seismic data and the organisation will process the data, format it into human readable form (e.g., graphs, charts, reports) and then provide the client with a completed report

3.0 Market Information

The company currently holds about 40% of the market share in the oil and gas monitoring software market. Their nearest and biggest competitor is Another Company Pty Ltd who also holds about 40% of the market share. The competitor provides the same Seismic processing services to the oil and gas industry and their version of the monitoring software has roughly the same functionality as the company's versions.

The other 20% of the market is held by several smaller independent software firms providing either monitoring software or Seismic processing services but not both. Generally speaking, these companies do not pose a serious threat to your company or to the competitor as the service they provide are not as comprehensive nor do their software have the same wide range of functionality.

4.0 Research and Development

4.1 Project 1

The company is currently working on several R&D projects that may allow them to overtake their primary competitor in terms of market share. A major upgrade to both the monitoring software is expected to be released in around 6 months time. This upgrade provides real time remote monitoring of the drilling and pumping process via satellite or landlines. Remote monitoring is a function frequently requested by clients but nobody has been able to provide that function reliably in their software yet.

This project is currently in close beta testing stage but the company believes it will be able to start limited field tests in a month's time. Some of their larger clients will be given the

opportunity to test the prototype in a parallel run scenario and feedback will be obtained to perform fine-tuning of the software.

The company believes that they have the problem licked with their custom design chip/software. They forecasted that they can gain an additional 10% (around $100 million) of the market at the expense of their competitor. This project is considered top secret as the company believes that their competitors are nowhere near having a similar product and estimates that they will have a technology lead against their competitor for at least 2 years, provided their competitors are caught unaware at release date.

4.2 Project 2

The company is also working on software that will allow their data processing software to speed up data processing by distributing the data processing between many different servers. It is anticipated that a typical job can be completed about 30% faster, which not only reduces the time getting a report back to the client, but also increases the number of jobs that can be completed within the same period. It is projected that if the project is successful, an additional $30 million in revenue can be generated from the increase annually. This project is currently in alpha testing stage and is around 12 months away from completion. The company suspects that their primary competitor is also working on something very similar at the moment and believes that they (the competitor) are very close to having a fully functional product (within 2 months). This project will involve some infrastructure upgrade as additional network cables need to be laid to provide for the increased bandwidth required between existing servers as well as provide for additional servers. It is also anticipated that an additional 10 servers / workstations will be required as well as a new high-speed network switch.

5.0 Contractors and Vendors

The company uses sub-contractors to meet some of their work force needs as well as to provide contracted services.

Clean and Mean Pty Ltd

- Providers of cleaning services to the organization
- 2 cleaners during office hours to keep the environment clean, for example keeping the toilet clean through the day, cleaning the pantry or to provide general cleaning services as required
- 4 cleaners after office hours to keep the office clean, general cleaning, wipe tables, vacuum floor, clean meeting rooms, etc.

Computex Pty Ltd

- Contractors providing network infrastructure services, e.g. laying network cables, network points, etc.
- Work mainly after office hours or on weekends to minimise disruption to daily operations

Printmaster Pty Ltd

- Supplier of photocopier and printers to the organization
- Responsible for maintenance of copiers and printers
- Monthly maintenance of copiers and printers by technician every 1st Wednesday of the Month
- Ad hoc maintenance and repair as required

PeopleRus Human Resource Pty Ltd

- Employment agencies used by the organisation to provide permanent and temporary placement of staff within the organization
- The organisation used short-term contract staff extensively to meet temporary staffing requirements for the various departments. Example, to cater for staff going on extended leave or to meet temporary increase in workload.
- Contract staff will be assigned to various departments and given the same access as permanent staff in similar roles.

Hungerbuster Pty Ltd

- Vendor providing food and drinks to the vending machines located in various locations in the company.
- Also provide food and drinks for meetings and functions as required

6.0 Physical Security

Entry to the organisation is either via the main entrance on the ground level or via the car park entrance in the basement. There are 2 fire exits with one-way door (i.e. can only be opened from the inside) and these doors are armed to set off the fire alarm if they are open.

Access to the upper level of the company is via the passenger lifts, cargo lift or by climbing the stairs.

Signs near the main entrance as well as near the lifts in the basement direct all visitors to the reception desk on the ground level. All visitors are required to sign in and a visitor's badge

will be issued to them. Visitors will be escorted into the company premises by the person they are meeting, but are not escorted out when they leave. The passenger lifts operates 24/7 and the door to the stair well is not lock.

Vendors and contractors will use the cargo lift to gain access to the upper levels for deliveries. Vendors and contractors are required to obtain a contractor badge but are not escorted in or out.
The cargo lift normally only operates during normal office hours, but after hours use can be arranged with the security office if the need arises.

In the upper levels, there is a set of doors leading from the lift lobby (see layout) to the office area. These doors are kept open during office hours and the last person to leave at the end of the workday is responsible for locking them up.

The company uses an open plan office layout and staffs have their own cubicle. Upper management staff have their own individual offices.

7.0 IT Infrastructure

7.1 Server Room

There is a server room that houses the company's servers as well as networking equipments. The server room is air-conditioned and the temperature and humidity is monitored for optimal equipment performance. The server room is not locked during office hours, to facilitate easy access for IT staff. The last person to leave at the end of the day is responsible for locking up.

7.2 Wiring Closet

There is a wiring closet on each of the upper levels and contains router and switches. All computers, network printers and photocopiers are connected to the switch and routers on their level. The switches and routers on each level in turn connect to the core routers located in the server room via vertical cable runs that runs from the basement to the top most floor. For redundancy, there is a primary cable as well as a secondary (backup) cable connecting each floor to the server room.
The company uses Big Lake ISP as their Internet Service Provider and the cables from the ISP enters the building via a cable conduit on the ground level (see layout). The cable from the ISP then runs vertically up the conduit into the server room. Due to their size and location, the wiring closets are not air-conditioned. The wiring closets are normally left unlocked to allow easy access by IT staff.

7.3 Data Processing

The seismic data processing department runs their own servers and workstations. It is housed in the data processing room and is separate from the main server room. The data processing room is air-conditioned and the temperature and humidity monitored. Client data are backed up on tapes and the tapes are house inside the data processing room on open racks that line the walls.

Due to the sensitive nature of the client's data, the door to the data processing room is normally kept locked. Only authorised personnel are allowed into the data processing room.

8.0 IT Security

8.1 Client PC

All client computers (desktops and laptops) run off a standardised operating system image. All client computers have the same antivirus software installed and the operating system's firewall software is turned on by default. In addition, all clients' computers come complete with MsOutlook email client as well as MsOffice. Department specific software are installed separately as required. Automatic OS patching is turn off by default to prevent new patches from creating compatibility problem(s) with existing software.

Back office staff are issued with Dell Optiplex 360 desktop running the Windows 7 operating system. Sales and IT staff, as well as all managers are issued with Dell E4300 laptops running the Windows 7 operating system.

The software, R&D, support and training business unit uses a mixture of Dell Precision desktop and laptops. A variety of operating systems such as Windows 7, Windows 8.1, Server 2012 as well as Linux variants such as Ubuntu and Red Hat Enterprise. Virtual machines are used extensively in the R&D business unit for application development.

8.2 Servers

The Domain controller server runs on Windows 2012 R2 server while the File and Print server, and the Web server run on Windows 2012 server. The organisation uses HP ProLiant Gen7 and Gen8 servers, rack mounted with raid 5 hard drive redundancy.

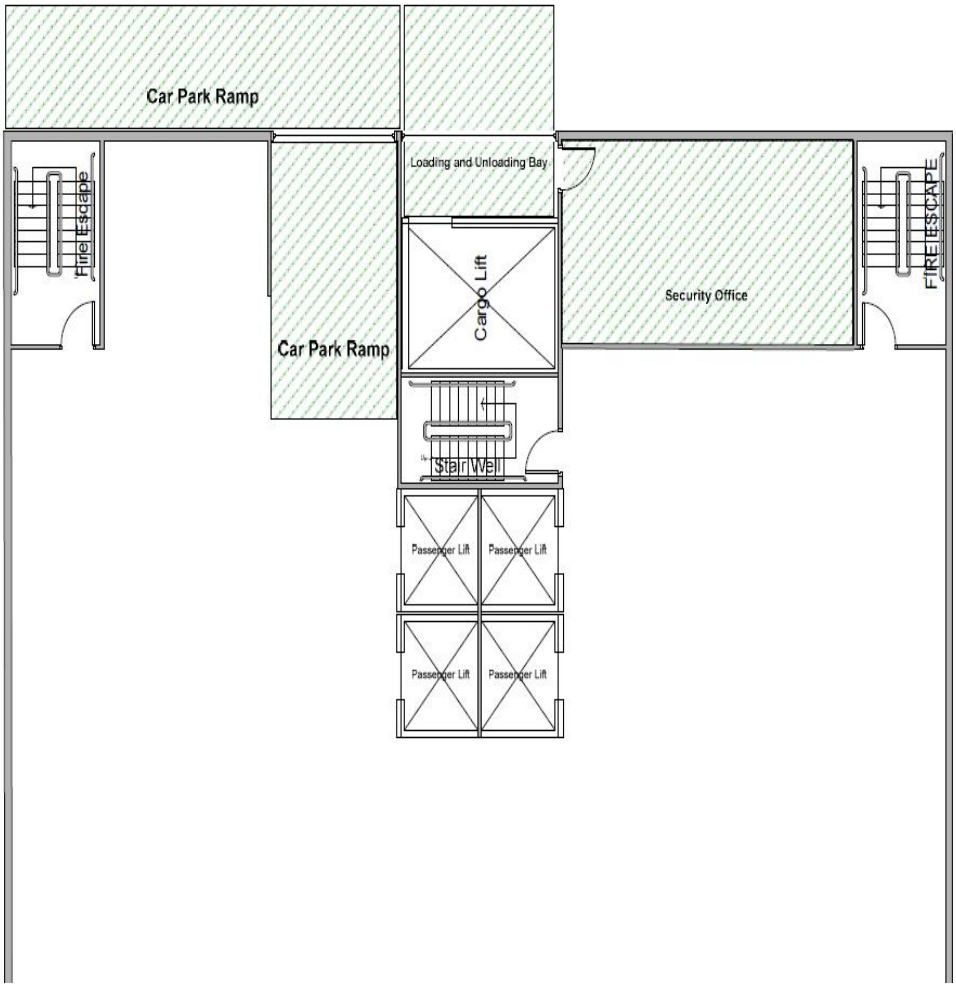
All servers are protected with the server version of the same antivirus software as well as the same firewall software. Automatic software patching is disabled and new patches are only applied after being tested for compatibility on a test server. All servers are also loaded with the Symantec Backup exec software that backup all data to a HP 1/8 G2 Tape Autoloader.

The data processing business unit uses IBM blade centres running a customised Linux based operating system for data processing. To ensure stability, the kernel and systems application are rarely updated. The data processing business unit runs their own separate backup on a HP 1/8 G2 Tape Loader.

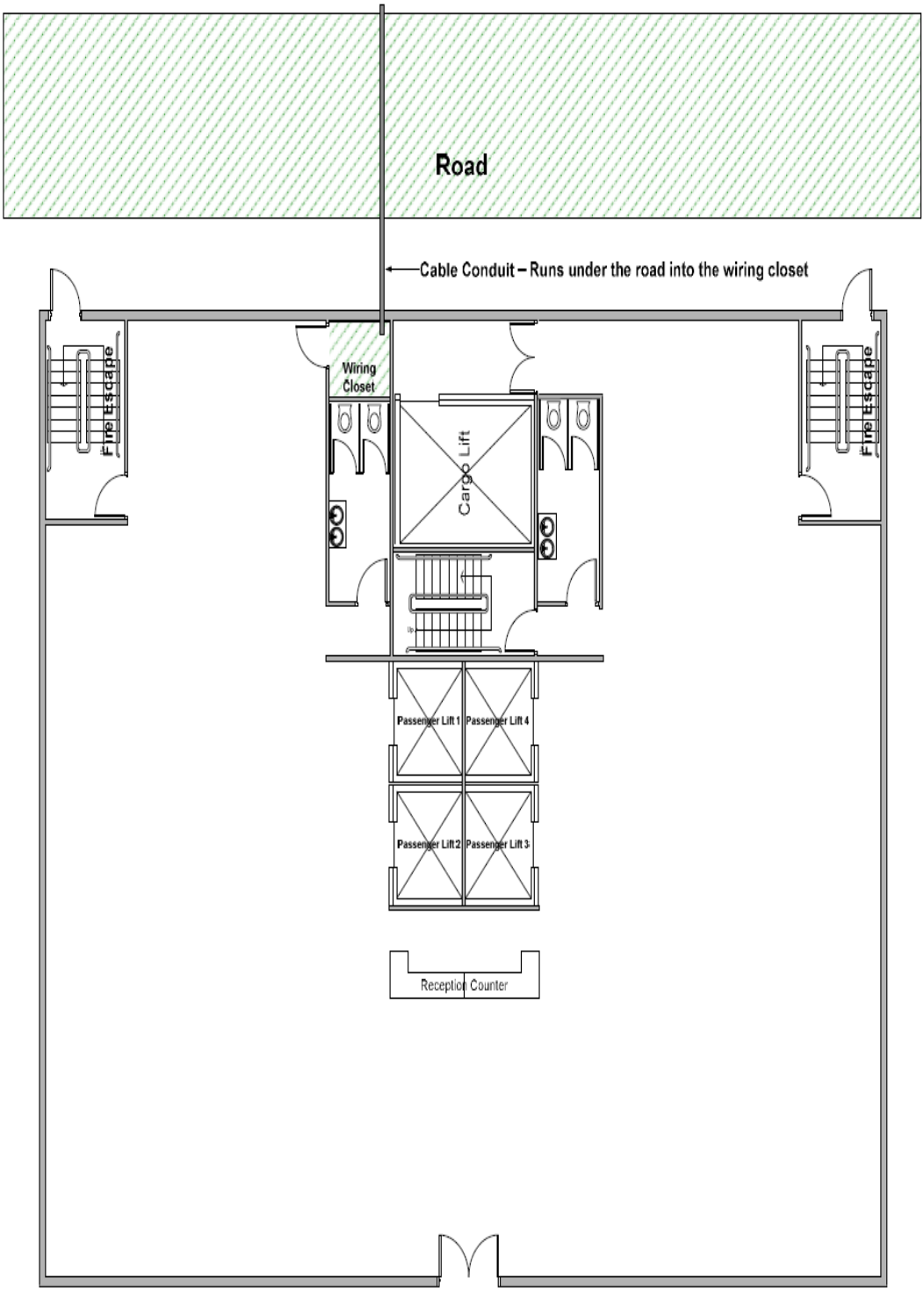
8.3 IT Policies

When new staff joins the company, a user account and password will be created for them. All new users are told that they should no share their user account and to keep their password secret. They are also encouraged not to write down their password in clear text and to change their password periodically.

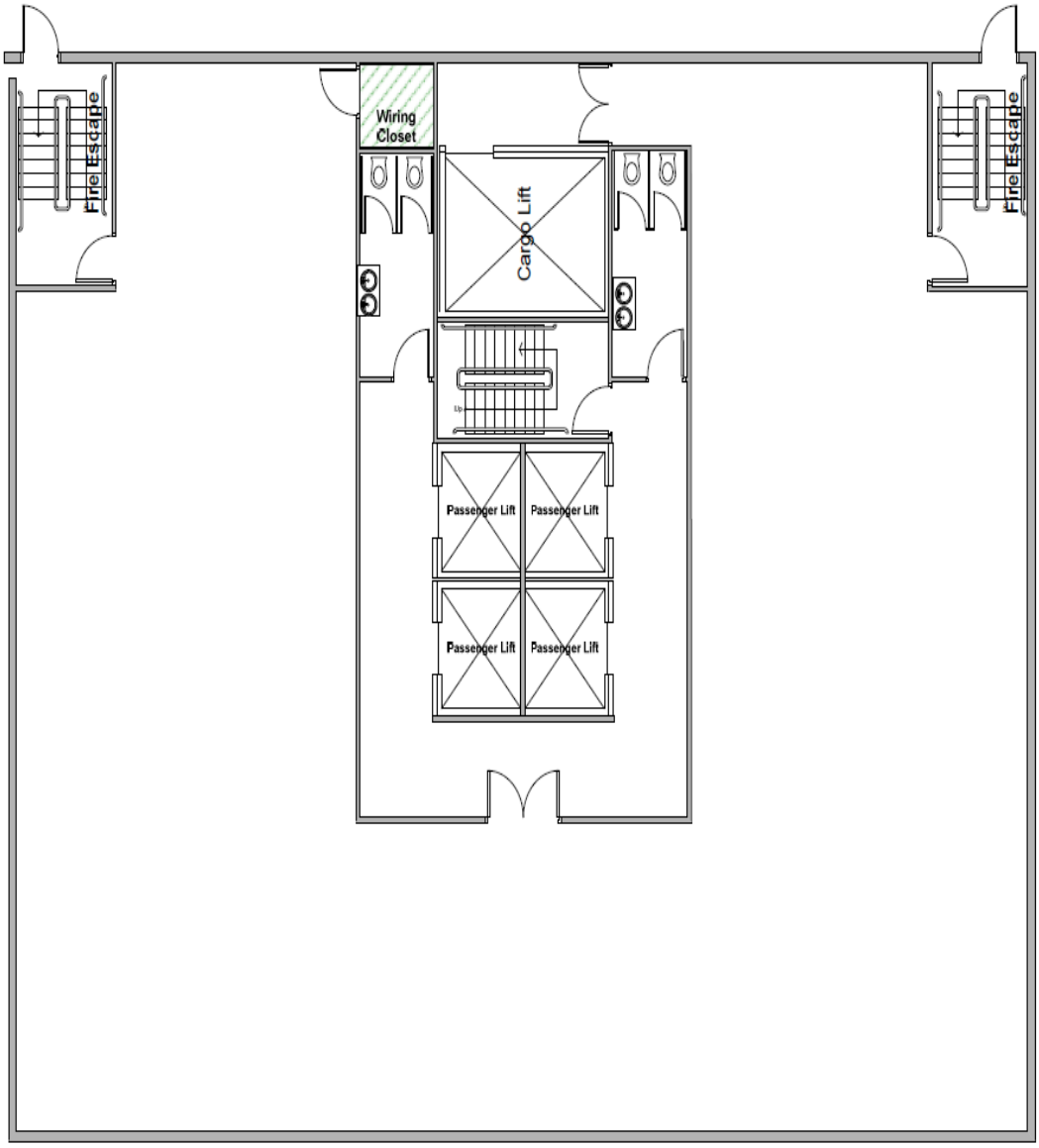
FLOOR PLAN - BASEMENT



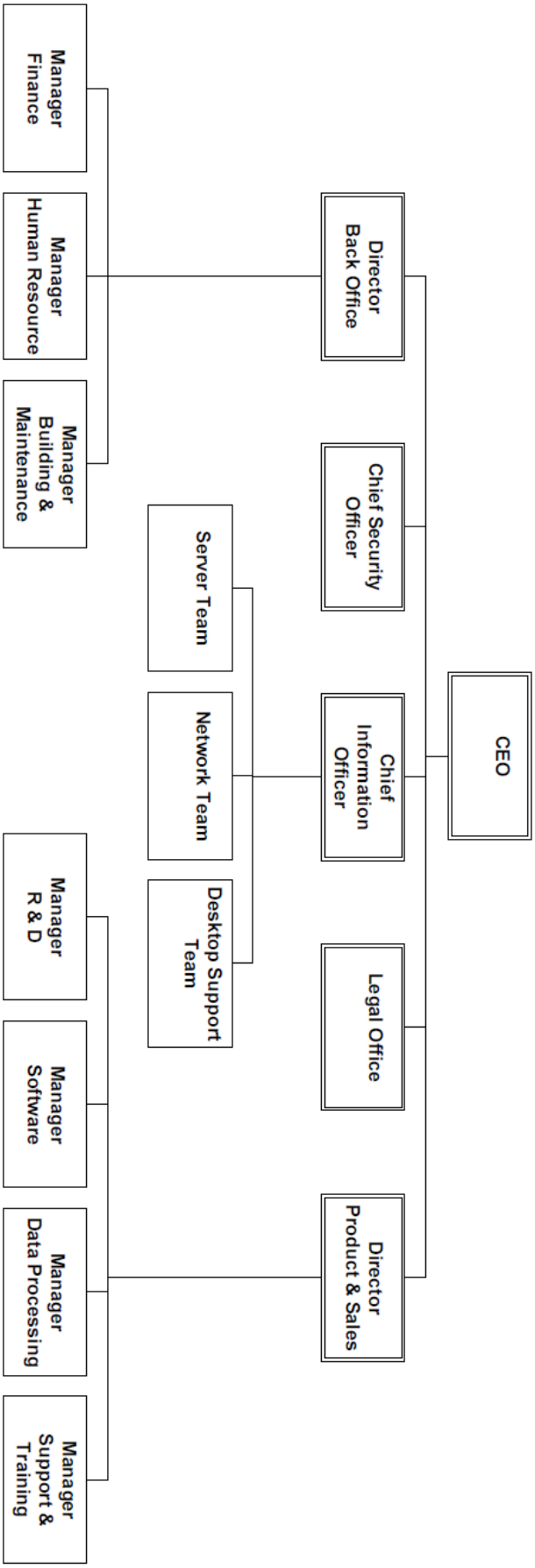
Floor Plan - Ground Level



Floor Plan - Upper Levels



Organisation Chart



Network Infrastructure