Yotsuba Network Design Brief

360CT - Advanced Network Management and Design

By
James Thomas - 9195071
Liam Smith - SID
Alexander Collins - SID

Contents

1. Introduction

This is to get references to appear (Heikkinen & Hamalainen, 2020)

2. Requirements and Assumptions

2.1 Expansion

Yotsuba Group is a company experiencing rapid growth, hence the need for their new office space. It is assumed that this rapid expansion is to be around 10-20 (May need to be more scaleable) new employees per year. Because of this, there is a strong requirement for scalability, so the network can cope with this growth and there are no detrimental effects on network performance. It should be kept in mind that the selection of devices and routing protocols should support this need for scalability.

2.2 Network Speeds and Bandwidth

Research showed that private internet for the greater Tokyo region had available speeds in the range of 10Mbps to 1Gbps. It is assumed that enterprise internet speeds will be within a similar range and that the Yotsuba Group will be purchasing at the top range. Therefor a 10Gbps connection will be used for the designs.

2.3 Employee breakdown

As no information on individual department employee count was provided it has been assumed based on departmental needs.

- Research and Technology - 50 employees
- Financial Planning - 20 employees
- Sales - 34 employees
- Material and Design - 50 employees
- Personnel - 10 employees
- Planning and Manufacturing - 60 employees
- Legal and Accounting - 10 employees
- Marketing - 20 employees
- IT - 16 employees
- Department Head and Assistants - 16 (8+8) employees

2.4 Cisco in Japan

The network will be using Cisco hardware, some of which will be transferred from the old building. Cisco (2021) press release demonstrates how the company plans to transition further into Japan through an agreement between the Japanese Government and Cisco on mass-scale digitalisation projects. need to cite (CISCO, 2021)

2.5 Physical Office Dimensions

Floors U1, U2, G, 1, 2, 3, 4, 5, 6: 30mx50m - 64, 7m2 pp
Floor 7: 50mx20m - 16
Floor7 Balcony: 50mx10m

2.6 Underground Carpark

We are assuming that the two-floor underground car park does not currently have a good mobile signal and therefore, Wi-Fi APs could be implemented underground. This does depend on the budget of the organisation though because it is not necessarily something that is needed but would be helpful for employees who have parked underground as they can still make calls, send emails or do other work from their cars.

2.7 Previous Devices

3. Physical Network Design

3.1 Devices

3.1.1 Workstations

It is assumed that all workstations in use have been bought over from the old branch. The only upgrade that would have to be made to each workstation is the installation of an SFP+ network adaptor. The recommended PCI expansion card is the ASUS 10GbE SFP+ PCIe 3.0 Network Adapter.

3.1.2 Wireless Access Points

Cisco Catalyst 9136

3.1.3 Layer 3 Switch

3.1.3.1 Chassis - C4506-E

3.1.3.2 Line Card - WS-X4712-SFP+E5

3.1.4 Layer 2 Switch

3.1.4.1 Chassis - C9404R

This chassis has been chosen as it is the correct size needed to fit two supervisor cards and two line cards. Going any larger would not be beneficial and cost more.

3.1.4.2 Line Card - C9400-LC-48XS

This line card has been chosen for the access layer switch as we can fit two of them in the chosen chassis. This will provide enough ports to cover the existing devices on each floor as well as any new devices bought in due to expansion.

SKU	Ports	Connector	Speed	Total Needed
C9400-LC-48XS	48	SFP+/SFP	1/10Gbps	2

3.1.4.3 Supervisor Card - C9400-SUP-1XL-Y

Allows for 10Gbps on each port.

3.1.5 Router

Cisco 4000 Series Integrated Services Router

3.2 Wiring

3.2.1 Fibre

A full fiber solution will be employed for this network to account for future proofing and to reduce noise on the network.

3.2.1.1 Multimode Fiber - OM4

Current network will be 10GBASE-SR, using OM4 fiber will give us options to expand to 40GBASE-SR or 100GBASE-SR in future. Could be used in and between core/access due to high data transfer rates (10Gbps) over a distance of 550m.
While the distance of 550m is overkill for a 7 story building, the allowance for higher distances at higher speeds (100m at 100Gbps) will be good for future-proofing our solution.
Cost of fiber is reducing as time passes, basically as cheap as ethernet at this point.
OM4 would be used due to the cost/benefit compared to OM5 which would be overkill for our setup.
Will incur an additional cost of installing fiber optic enabled network cards in workstations.

Type	Distance for a 10Gbps connection	Cost per meter
OM1	33m	
OM2	82m	
OM3	300m	
OM4	550m	
OM5	550m	

3.3 Device Placement

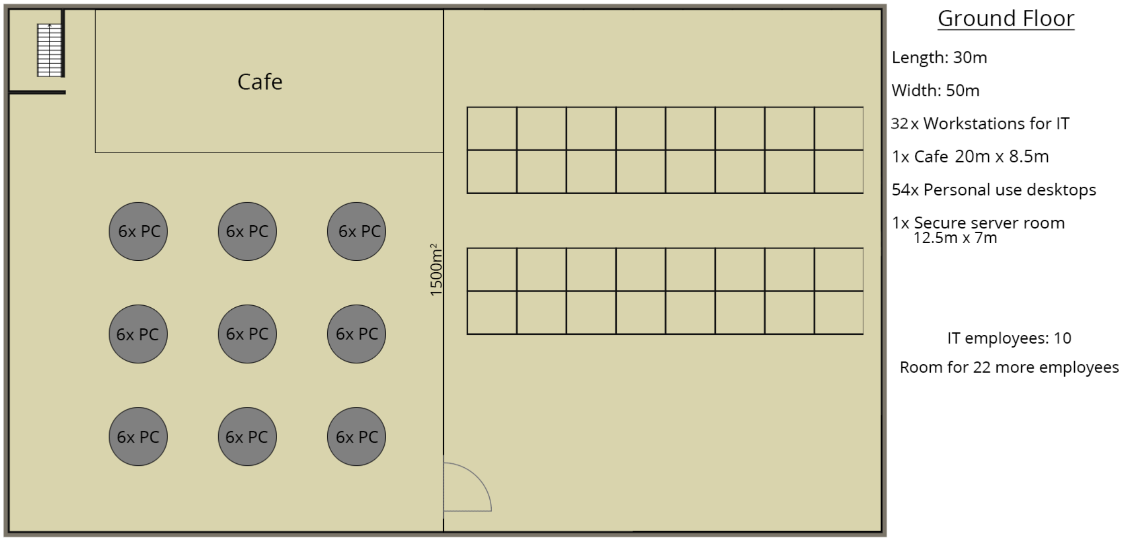
Change numbers of legal, marketing, finance and personnel to match google doc numbers.

3.3.1 Patch Pannels

Patch pannels could be placed on each floor to house access section L2 switches.

3.3.2 Ground Floor

Change this diagram 10 to 20



Ground Floor

Length: 30m

Width: 50m

32x Workstations for IT

1x Cafe 20m x 8.5m

54x Personal use desktops

1x Secure server room
12.5m x 7m

IT employees: 10

Room for 22 more employees

Figure 3.1: *Ground floor floor plan*

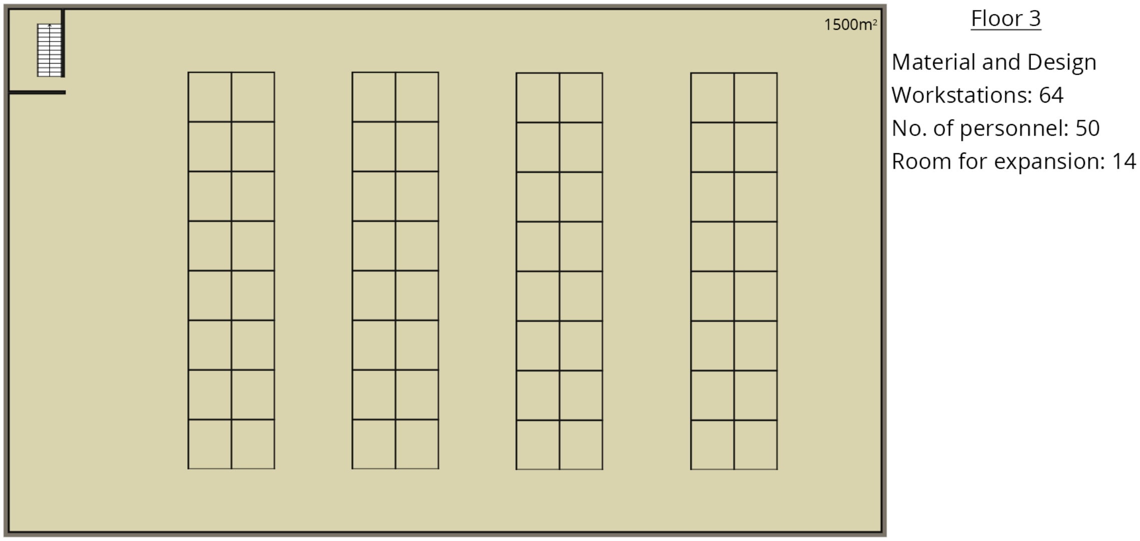
3.3.3 1st Floor

MAKE NEW 1ST FLOOR

3.3.4 2nd Floor

MAKE NEW 2ND FLOOR

3.3.5 3rd Floor



Floor 3

Material and Design

Workstations: 64

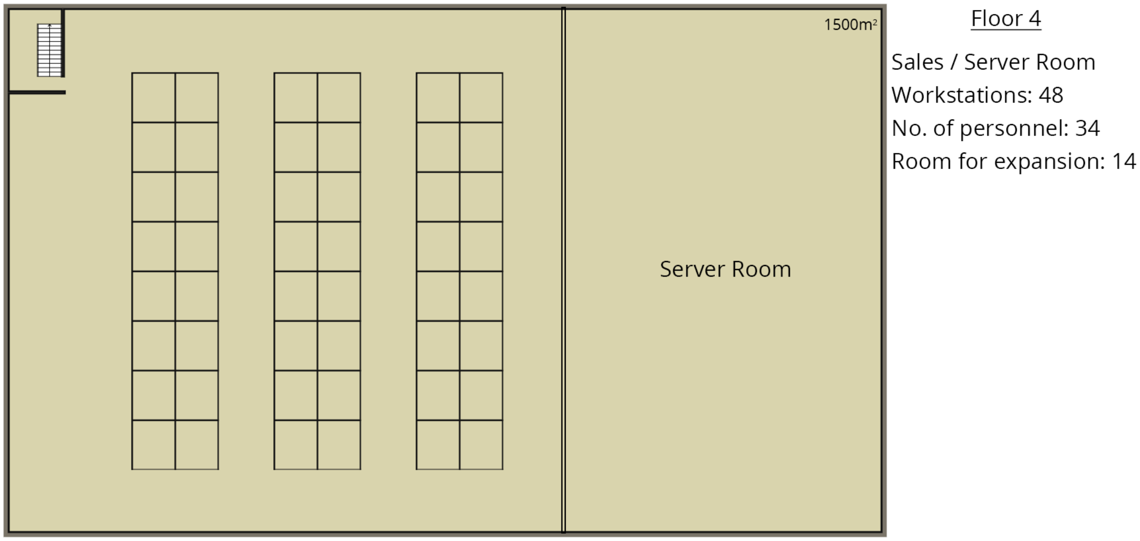
No. of personnel: 50

Room for expansion: 14

Figure 3.2: *3rd floor floor plan*

3.3.6 4th Floor

This is text and so is this



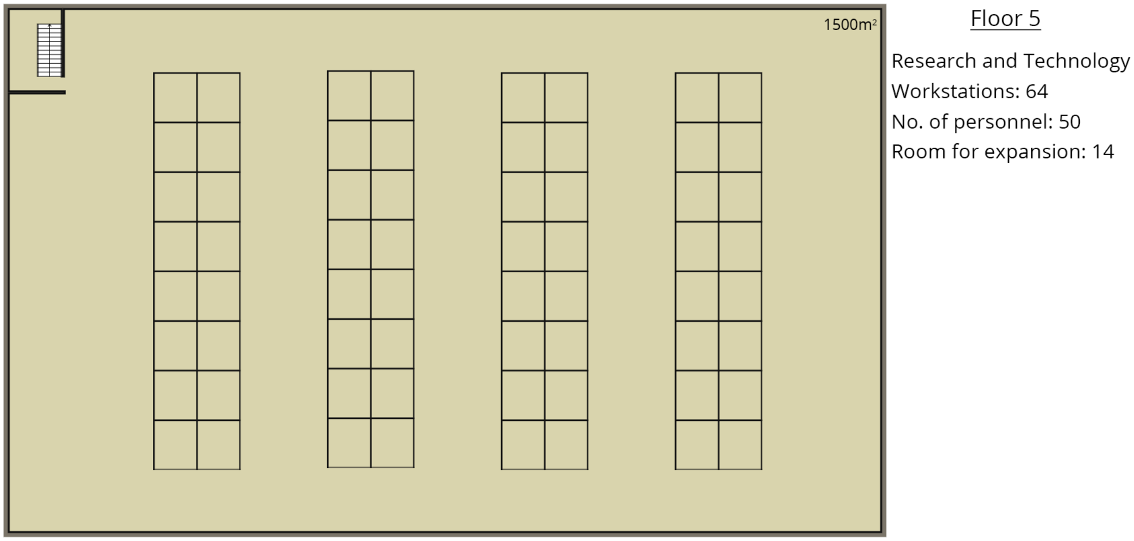
Floor 4

Sales / Server Room
Workstations: 48
No. of personnel: 34
Room for expansion: 14

Figure 3.3: *4th floor floor plan*

3.3.7 5th Floor

This is text



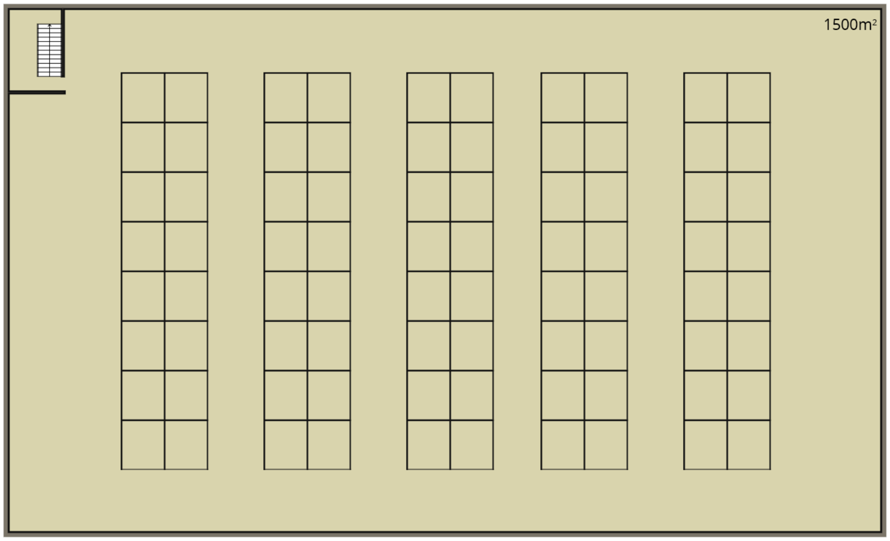
Floor 5

Research and Technology
Workstations: 64
No. of personnel: 50
Room for expansion: 14

Figure 3.4: *5th floor floor plan*

3.3.8 6th Floor

This is text



Floor 6

Planning and
Manufacturing

Workstations: 80
No. of personnel: 60
Room for expansion: 20

Figure 3.5: *6th floor floor plan*

3.3.9 7th Floor

MAKE NEW TOP FLOOR

3.3.10 Server Room

4. Logical Network Design

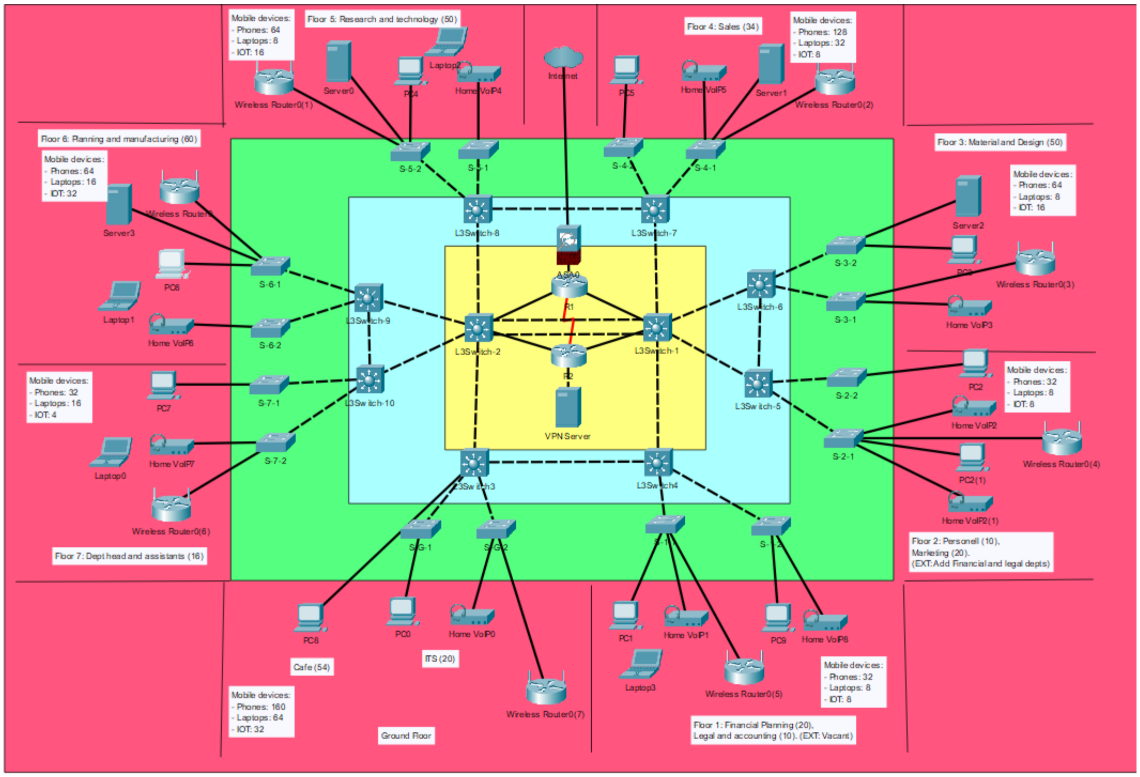


Figure 4.1: *A Network Design produced in PacketTracer.*

4.1 Justifications

5. Addressing Scheme

NAT/PAT enabled

Ground Floor:
IT Dept: 10.0.1.0
Cafe: 10.0.2.0
Wireless: 10.0.3.0
Phones: 10.0.4.0

Floor 1:
Financial Planning: 10.1.1.0
Legal & accounting: 10.1.2.0
Wireless: 10.1.3.0
Phones: 10.1.4.0

Floor 2:
Personell: 10.2.1.0
Marketing: 10.2.2.0
Wireless: 10.2.3.0
Phones: 10.2.4.0

Floor 3:
Material and Design: 10.3.1.0
Wireless: 10.3.2.0
Phones: 10.3.3.0

Floor 4:
Sales: 10.4.1.0
Wireless: 10.4.2.0
Phones: 10.4.3.0

Floor 5:
Research and Tech: 10.5.1.0
Wireless: 10.5.2.0
Phones: 10.5.3.0

Floor 6:
Planning and Manufacturing: 10.6.1.0
Wireless: 10.6.2.0

Phones: 10.6.3.0

Floor 7:

Dept Heads & Assistants: 10.7.1.0
Wireless: 10.7.2.0
Phones: 10.7.3.0

Underground:

Wireless

6. Network Policies

6.1 Issues

6.2 Resolutions

7. Security

7.1 Overview

Advancements in network technology has changed how employees work, even more drastically in recent years in response to COVID-19. This has led to employees possessing the ability to acquire, modify and distribute information more easily. Despite this being beneficial in terms of productivity, it is just as much of a threat to network security. As Yotsuba Group is a large manufacturing company leading the market in Asia, their assets and infrastructure are a prime target for cyber-attacks. The manufacturing industry is reported as the 2nd most targeted industry by cyber attackers, primarily due to COVID-19 (https://www.bitlyft.com/resources/cyber-threats-manufacturing-companies) so ensuring that Yotsuba Group can cope with these threats is crucial.

7.2 Identifying Network Security Threats

7.2.1 MAC Spoofing

Attacks occur in all layers, but level 2 and level 3 attacks are the primary concern in networks. MAC spoofing is a common layer 2 attack that forges a suspicious MAC address as a legitimate one. Due to this, a suspicious device can then bypass security controls to access the network.

7.2.2 ARP Cache Poisoning

Similarly, common layer 3 attacks include ARP cache poisoning. This attack exploits vulnerabilities in the ARP protocol that potentially leads to man-in-the-middle attacks. Since the ARP protocol doesn't verify identities, it can be easy for an attacker to trick a legitimate host into thinking its legitimate itself. Therefore, if an ARP poisoning attack is successful, the attacker can view all traffic sent between two hosts.

7.2.3 Distributed-Denial-of-Service (DDoS)

7.3 Solutions

7.3.1 Device Security

At the very least, YG should ensure that devices are made more secure by implementing a strong password policy and multi-factor authentication. This is basic level security but prevents even the simplest of attacks. Unnecessary services and applications should also be disabled on devices that do not need them to protect the network from vulnerabilities in certain applications. For example, employees in the manufacturing department will not need access to finance applications, so segregating them makes the network more robust.

7.3.2 IDS/IPS

Intrusion Detection/Prevention Systems can help to analyse traffic, detect attacks or even prevent them.

7.3.3 Firewalls

7.3.4 ACLs

Thorough Access Control Lists should be created to control network traffic. Using the logical network design created earlier, an example ACL has been created between two different departments of the network, ensuring that each department cannot access one another's resourceshaving ACLs limits the lateral movement an attacker can make within a network.

7.3.5 Network Segregation

7.4 Previous Security Threats

The Yotsuba Group reported a number of security incidents in the last 6 months. These have been assumed below.

7.4.1 IP Theft

The company had some intellectual property stolen from a physical attack on the servers within the company premises, the attackers were not found or apprehended as the security was not to standard. This attack was made possible by a lack of physical security measures on there network infrastructure.

7.4.2 Internal Breach

30% of attacks come from employee's within the companies, some data was accessed by departments who has access to other parts of the organisation that they should not have had. A lack of access control was the cause of this attack.

7.4.3 Identity Theft

An external attack left the customer database held by the company open and accessible to the attackers, this in turn was used to ciphon their data and initiate fraud through loan applications under customer names.

7.5 Possible Security Threats

In addition to the previous incidents, various other attacks could be possible against the group and their network. These have been outlined below.

7.5.1 Some new attack

8. Monitoring and Maintenance

Network Performance Monitoring and Maintenance The network performance and maintenance strategy will focus on maintaining specific network performance goals. Ongoing evaluation of this strategy should be performed routinely, to ensure that it helps achieve the objectives outlined below:

- Minimising network downtime
- Providing sufficient bandwidth
- Minimising latency
- Proactively identifying security or network issues
- Troubleshooting issues as quickly as possible

The tool of choice to help achieve this will be the Intermapper Network Monitoring Software, which provides mapping, monitoring and alerting solutions. It is an SNMPv3 enabled software, allowing for enhanced security and performance of monitoring network devices. Some key features include:

- Automatic network mapping - colour-coded statuses on network devices provide the IT team with a visual indication of how the network is performing.
- Proactive network monitoring - SNMP protocol allows for continuous status updates for all devices, servers and applications.
- Remote network monitoring - geographically scattered devices and offices can be monitored, allowing for problems to be diagnosed and addressed remotely.
- Network traffic analysis - provides insight into bandwidth usage, traffic statistics and suspicious spikes or dips.
- Network automation - reduces manual network activities by executing pre-defined responses to alerts.

Other solutions on the market included software such as SolarWinds and Datadog and although they are more popular, two of the main factors in choosing Intermapper was due to its remote network monitoring and network automation features. As Yotsuba Group expands rapidly, there will be more instances of devices being spread across a larger geographical area. Intermapper bridges the gap so that those devices can still be monitored, but also issues on these devices can be resolved with a degree of automation. The pricing of Intermapper also helps with the upscaling of Yotsuba

Group in line with expansion, with prices varying depending on the number of devices that need to be monitored. Intermapper also comes with a risk-free 30-day trial so if for whatever reason it does not meet the requirements of the network, another provider can be sourced.

9. Disaster Plan

9.1 Outline and Scope

This disaster management and contingency plan aims to identify risks and provide methods of mitigation. Certain issues can be treated with automation via the setup of executables using the Intermapper network management software. If manual intervention is required, the plan employs a systematic approach, which allows problems to be treated in a sufficient timeframe, but with enough knowledge so that it can be understood and corrected properly. We have been proactive with our network design, employing the Cisco 3-layer hierarchical model to prevent issues and help with troubleshooting. Our design makes it easier to isolate a section of the network where an issue may be found, makes scaling easier and ensures we have redundancy within the network.

9.2 Risks and Mitigation

9.3 Risk Assessment Matrix

Will take a screenshot of finalised table as image

The Risk Assessment Matrix provides visual indication of how likely a risk is to occur, as well as its impact on Yotsuba Group in such an event. Mitigation methods described in Table 9.1 will help overcome and reduce the consequences of these risks.

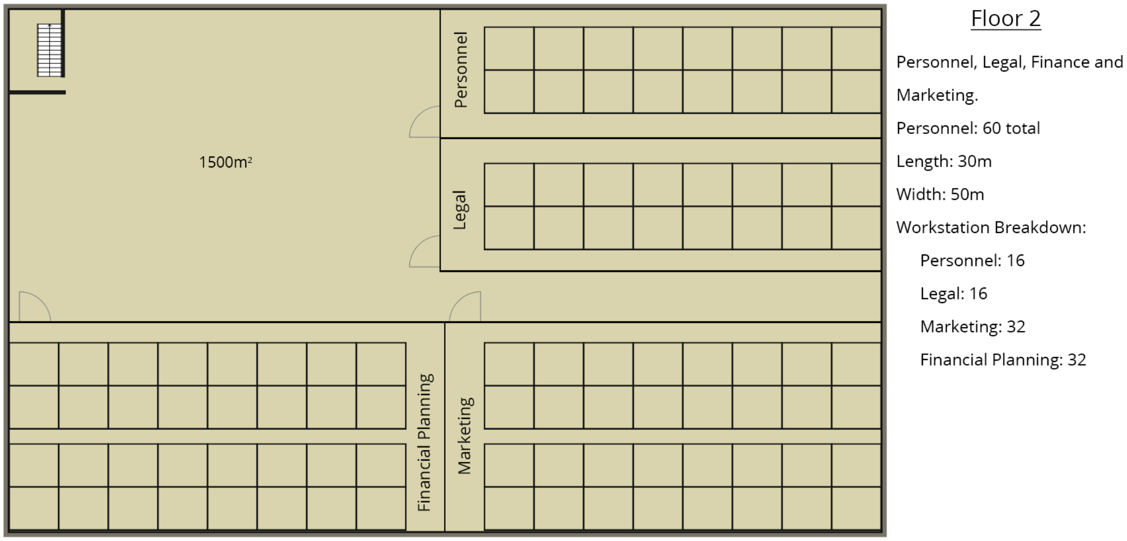
Risk	Potential Consequences	Mitigation
Natural Disaster i.e., flooding, earthquake, tsunami	Destruction of the building or critical IT infrastructure. Loss of critical personal and manufacturing data.	Seek cloud-based computing solutions for storage of critical data in geographical locations where natural disasters are less frequent.
Fire	Destruction or damage to critical IT infrastructure. Damage to company reputation	Conduct regular fire assessments, ensuring sockets are PAT tested and fire extinguishers are readily available.
Power Cut	Disrupt operations and potential loss of data.	Utilise the space in the underground car park for a temporary backup power supply. Ensure this power supply can handle normal business operations.
Network Issues	Loss of communications and disruption of operations.	Ensure adequate levels of redundancy are implemented into the network. Isolate network where the issue is and ensure there is enough backup equipment available to create a simple network should critical operations be required.
Theft	Loss of infrastructure or crucial data. Damage to reputation.	Ensure IT team performs regular checks on IT devices along with trackers and encrypted hardware.
Software Issues	Disruption of operations. Loss of access to data.	Perform backups regularly before updating software. If the latest versions of software cause issues, the IT team should roll back to the previous version if there is no significant vulnerability risk.
Hardware Issues	Disruption of operations. Loss of access to data.	Planned resolution methods for each network device, whether it is router, switch or computer. Isolate network where hardware issue is if needed and perform regular backups to prevent loss of data.
Employee Lost Device	Possible loss of data and/or exposure of sensitive company data.	Ensure password policies are enforced on employee devices, with multi-factor authentication and encrypted hard drives.

Table 9.1: *Risks and mitigations*

10. Additional Problems

10.1 Renting One Floor Out

The second floor will combine four different departments to allow for space in the first floor. The new layout can be seen in figure 10.1.



Floor 2

Personnel, Legal, Finance and Marketing.

Personnel: 60 total

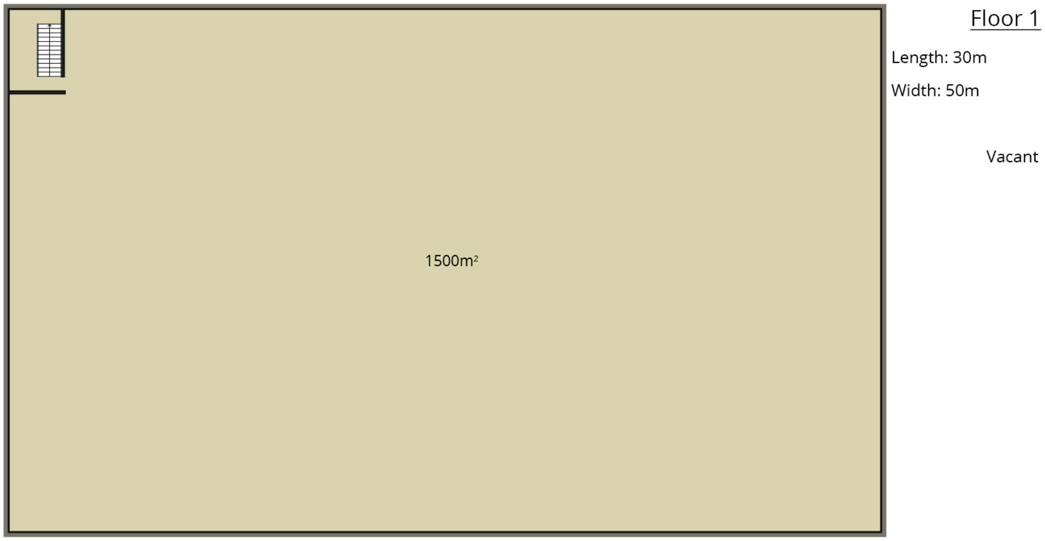
Length: 30m

Width: 50m

Workstation Breakdown:

- Personnel: 16
- Legal: 16
- Marketing: 32
- Financial Planning: 32

Figure 10.1: *2nd floor floor plan combining 4 different departments*



Floor 1

Length: 30m

Width: 50m

Vacant

Figure 10.2: *1st floor vacant plan*

10.2 Splitting Between Two Buildings

References

CISCO. (2021). Cisco launches digitization program in japan to support inclusive pandemic recovery. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2021/m02/cisco-launches-digitization-program-in-japan-to-support-inclusive-pandemic-recovery.html

Heikkinen, E., & Hamalainen, T. D. (2020). Deployment of batch processing for log file analysis. *2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS)*. https://doi.org/10.1109/icps48405.2020.9274712