Autohub Group of Companies

A Study and Assessment of ISD

Cruz, Fajardo, Federico, Luces, Simon

Table of Contents

[Executive Summary 3](#_Toc368994003)

[Company Overview 3](#_Toc368994004)

[Purpose of Investigation 5](#_Toc368994005)

[Investigation Proper 6](#_Toc368994006)

[Analysis 11](#_Toc368994007)

[Recommendations 14](#_Toc368994008)

[References 17](#_Toc368994009)

[Appendix 18](#_Toc368994010)

# Executive Summary

The team investigated Ford Dealer, otherwise known as Autohub, a company which is in the business of car dealership and distributorship. This paper will be focused on auditing the network and data center aspect of their IT department. The purpose of the investigation is to bring to light the IT's strengths and weaknesses in order to give an in-depth recommendation to improve the company's performance.

Over the course of the investigation, the team has found that the IS Department acts as a support unit, which implies that it handles a number of jobs across all departments. A downtime, even for a day, would be costly; however, the group has found the data center to be reliable enough due to the existence of redundant components. The main problem with their current setup with regards to the data center is its physical space. With regards to their network, Autohub lacks security. The current system and architecture is able to accommodate its users but, long-term, their plans aren’t viable.

In order to resolve the issues stated above, the group proposes incorporating a virtual server into their system and improving the physical space of the data center. The group also suggests it looks into long-term planning in order to support the growing needs of the company.

# Company Overview

The Autohub Group of Companies is a company which deals with automotive dealerships and distributorships. With Engr. Willy Q. Tee Ten (WQT) as its president, the company has been in business for 14 years, being known as the One-Stop-Auto-Shop.

In 1999, the WQT Group was awarded the automotive dealership by Ford Makati. The following year, Ford Dealer established the Ford Davao branch. The year after, they branched to another Ford Mindanao Dealer and established Ford Cagayan de Oro. In 2004, Ford Dealer expanded to Metro Manila but it was only on October 2005 that Ford Makati was transferred to The Fort (currently known as Global City). In 2005, Nissan Gallery in Ortigas and Nissan Gallery in Quezon Avenue were taken over in order to acquire new car brands. Hyundai Global City Hub was taken over the year after. The business expansion not only resulted to acquisition of car dealerships but also car and motorcycle distributorships: Vespa, Piaggio, Gilera, etc.

There was a point in time that the Autohub Group was a dealer of BMW automobiles under Klassik Motors Inc. which can be found in Araneta Avenue, Quezon City. Soon after, the company gave up their BMW dealership, they applied and successfully acquired the distributorship of MINI Coopers in 2010. A year after, another brand was added to the company, a Mazda Dealership in Cagayan de Oro.

In the first semester of 2013 the Autohub group launched their distributorship of Piaggio Ape (APE Inc.) along with the launching of the distributorship was the opening of the company-owned Piaggio dealerships which can be found in Otis, Greenhills, Quezon Avenue and Cavite. In addition Ford Bohol was added to the dealership family of the family which is a venture with AutoCentral Group, an automotive veteran in Cebu and Bohol.

June 2013, after 6 months of negotiations, the group successfully obtained the official distributorship of Rolls-Royce under British Bespoke Automobiles Inc., which is also known as Rolls-Royce Motor Cars Manila. It was a huge mark for the Philippines with the arrival of the of the ultra-luxury known car brand.

Autohub Group has other automotive-related businesses one of which is the Autohub CarCare Services (ACCS) in Otis which handles body, paint and car accessories. Another would be CLICK CarRental and Auto Leasing, Go LPG (a venture with GATES) which carries Tartarini and Lovato LPG Kits. They also have the official distributorship of V-KOOL spectrally-selective films here in the Philippines which inaugurated its first-ever Envirocare Showroom in the whole dealer network of V-KOOL International in 2012.

Future dealerships of the Autohub Group will be Ford General Santos, Ford Zamboanga, Mazda Davao. On the other hand, Piaggio Dealerships would be in Cebu, Zamboanga, Naga, Tacloban, Calamba, Cagayan De Oro, Urdaneta, Bohol, Cabanatuan, Davao, and Pampanga.

The company has now been more than 14 years in the automotive business; the Autohub Group of Companies has proven its worth and earned to be referred to as your One-Stop-Auto Shop.

Through the years of operation Autohub Group has constantly grown. They have acquired numerous companies and gained different distributorships in which different types and numerous data could be captured.

# Purpose of Investigation

**Scope**

The group will be investigating the data center structure and management, and the network administration of the company. After gathering the current data about the company’s implementation, processes, and structure of these topics, the group will determine the weaknesses, strengths and, if possible, the relation of these two areas in ISD to determine possible risks that their current ISD might exhibit. With an in-depth analysis of the whole system, the end-result should be a list of recommendations for the company in order to improve their IT department.

**Limits**

Due to security concerns, the group was not able to gather information on the following areas:

* Specific hardware details (i.e. Certain brands have their own security flaws, exposing the brand used such as the firewall incurs possible risk)
* Protocols and methods that the company deems as confidential to maintain competitive advantage or promote security measures
* Physical access to the data center

**Objectives**

* To determine if the company is able to accommodate all clients in an effective and efficient manner given their current data center setup
* To determine if the network setup is effective in its transmission and protection of its technologies
* To determine the company’s strengths and weaknesses in reference to their network and data center setup
* To provide proper recommendations that would improve the IT Department

# Investigation Proper

**Methodology**

The group accomplished the investigation through a personal interview with Mr. Arnel Endaya, the IT supervisor of Autohub Group. The interview was done in BGC, The Fort, on October 4, 2013 from 10:30am to 12:30pm. Further details needed to accomplish the investigation were acquired through internet research and consultation with professors from the Ateneo de Manila University.

**Network**

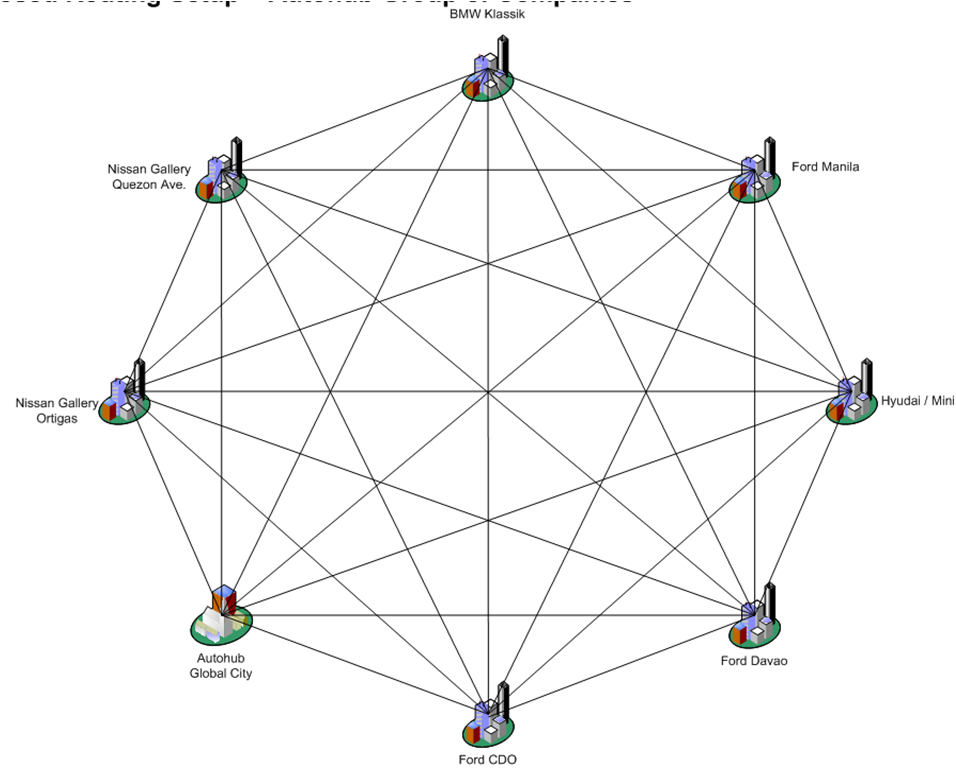
The type of network topology used by Autohub Group is a Mesh network. Since there are multiple branches, each branch must be capable of managing its own data and relaying these items to other branches. This type of system allows the company to easily collaborate despite the geographical distance. With regards to individual hardware, Autohub provides preconfigured devices that are connected to the organization’s servers. These preconfigured devices rely on their connection to the network and without it, any data processing cannot happen. This enables Autohub to ensure that all information remain secured in case any theft happens.

Figure 1 Autohub's Mesh

The company refuses to disclose the brand of the firewall they are currently using but they mentioned that the techniques used to implement the firewall is through proxy server, which makes use of the application layer, and through packet filtering. Additionally, the firewall is used to monitor traffic and utilize the ports.

Attacks on the company network happen on a regular basis. This year, there has been a report of 5000 attacks on the firewall alone. The company is invested in keeping their networks secure. Ideally, IT assistants and network administrators keep watch on the network security minute by minute, 24 hours a day. For the people who are monitoring the network, it’s not enough to know which ports are utilized. The software must be manually updated on a daily basis as new technologies to hack into systems are developed every day. By default, the network implements a hybrid of whitelisting and blacklisting, only allowing a number of items to enter their system and preventing specified items. Some however are bound for verification when not passing the whitelist and blacklist.

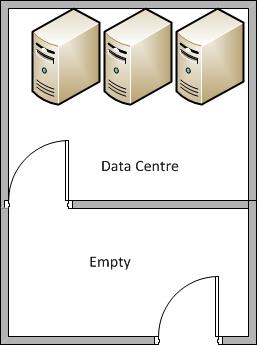
For User Management, the system makes use of an active directory exclusive to each branch. A specific user may have specific privileges depending on what the directory dictates. The one who is responsible in managing this directory is the network administrator. The system makes use of a login, implementing password aging (where the password expires after 90 days) and password rotation (where the user cannot repeat the last five passwords used). The password must be composed of at least seven alphanumeric characters while following a certain combination. The user may only attempt to login five times before the system rejects the user altogether.

For Software Management, all updates are managed by Mr. Endaya. Depending on the nature of the application, updates are either done manually or automatically through the central server. For automated updates, the application is simply loaded into the main server and it would automatically update all the users of the system. Manual updates, on the other hand, have to be done on each device. Software updates range from virus protection to application updates.

**Data Center**

Autohub’s data center is located within the Ford dealership in the Fort, Taguig. Currently, the data center takes up two rooms within the site. Being the only data center of the whole company, it is responsible for handling all the system processes and storage of the different sites. Currently, Autohub’s data center has the capacity to accommodate 700 employee users nationwide. Having been established more than a dozen years ago, Ford Autohub’s initial architecture contained plans for a data centre that has the capacity to ideally support up to 200 users. There have been no changes in the data center location and space since construction. All expansion involved a simple addition of hardware, and wires, that have to fit within the room.

In case of power outage, the company has a generator and an Uninterruptible Power Supply (UPS). The system automatically sends an email to the IT supervisor in order to rectify the situation. Switches also have backup power supply. The switches serve as a hub for all of the connections so if the switch loses power, it wouldn’t be able to communicate important information with the other system components.

As for physical security, there are two doors that need to be passed through which is protected by physical lock and key. There is also a CCTV to monitor the surrounding area. This is illustrated in Figure 2.

The Database Management Systems used for their databases are: DB2, MySQL, etc. The system applies heterogeneous computing, making use of multiple Operating Systems: Windows, Unix, etc.

Figure 2. Data Center

The company makes use of 2TB tape, costing around Php 2000, which contains a month’s worth of historical data. They manually perform an incremental GFS backup on a daily basis. They do this twice a day during these times: 12nn and 8pm. Full backups are done only at the end of the month. All of these backup data are then archived by year. The earliest records they have go back to as far as 2007 and are preserved. These backups are also copied and stored in an undisclosed offsite location. Finally, they employ a system backup although they also have measures of recovering both the system and the Operating System.

Data Center Topology

Currently, the data center consists of three switches: 1 main master switch and 2 redundant slaves. These switches can connect to several servers, and external memory. All of these consists the Storage Area Network which Autohub implements.

Protection utilizes Unified Threat Management (UTM) hardware that consists of several security measures such as a firewall, gateway, anti-virus, load balancing, content filtering, data leak prevention, VPN, gateway anti-spam and anti-virus, and network intrusion prevention.

They have several classifications of servers: file, name, backup and telephone servers which are also segregated depending on the subcompany. For example, MINI has a different mail server than Ford. All of these servers however are virtually implemented, which allows for easy deployment and expansion when the need arises. Physically however, there are three main servers located in the data center: 2 main servers and a redundant third server allocated to either of these 2 main servers.

Finally, there are also redundant lines for Internet Service with PLDT being the sole provider of internet connectivity. However, when a line is down, the data center is set to utilize a backup DSL line.

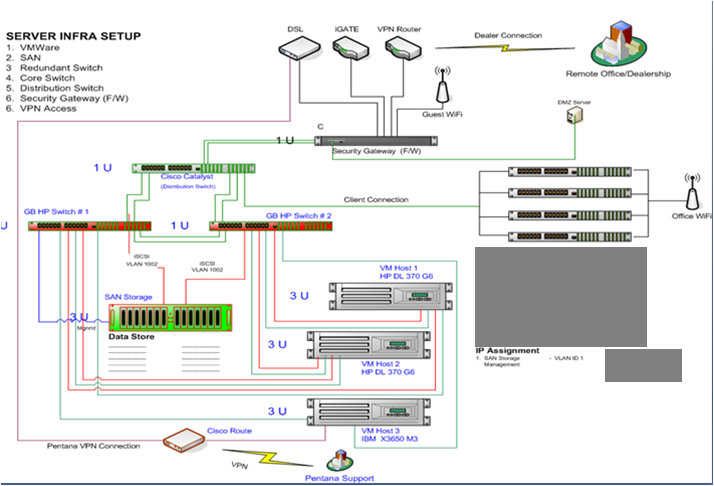
****

Figure 3 IT Infrastructure

**History of downtime**

There have been several critical events that happened since Autohub was established; the most recent one occurring on November 13, 2013. A virus was able to penetrate the security measures and ended up disabling the automated warning email notifications that were supposed to be sent by the server in case of such an attack. Due to this, a month’s worth of data was compromised and the said server was down for 24 hours.

Another critical instance has also happened due to internal procedure failure. One of the servers was compromised again due to a backlog of memory which in turn slowed down the server. This problem ideally should have been identified during regular maintenance; however, according to Mr. Endaya, lack of manpower caused the current staff to overlook and rush through maintenance.

# Analysis

In order to analyze the department, the team generated a set of criteria and evaluated each criteria accordingly. Featured in Table 1 is the result of the analysis.

Table 1. A Matrix-Based Analysis

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Network** | **Data center** |
| Chance of failure | Low | Low |
| Recovery time | Medium | Medium |
| Chance of infiltration | Medium | Medium |
| Potential for expansion/upgrade | Medium | High |
| Cost incurred during failure | High | Medium |
| Flexibility | Low | Medium |

**Data Center**

With Autohub’s ISD as a support unit and service provider, it is necessary that the data center functions around the clock. With their current data center containing several redundant components such as the switches, servers, and lines for internet service, the impact of failure among any of these redundant components is minimal in terms of business continuity. The presence of the UPS and generators, along with the notifications they give to the IS Supervisor when needed augment the continuity of the data center.

Even the push for virtualization of servers is beneficial due to a better way to manage disaster recovery. A virtual server combined with SAN means that a downed virtual server won’t necessarily translate to lost data. When disaster happens within a virtual server, another instance can easily be loaded and all data can be fetched from the SAN. Expansion would also be easier because instead of having to purchase an additional physical server for another instance of the server, Autohub would only have to purchase additional memory and processing power to create another instance of a virtual server and balance out the load it puts on the hardware.

An issue identified however within Autohub’s data center is the physical constraint present. As mentioned in the *Investigation Proper* of this paper, the data center was initially designed for a much smaller volume. However, growth and expansion wasn’t put into consideration and as such, physical crowding within the data center became apparent. According to the interview, the number of cables and wiring within the room is such that although it is organized, cramped up space is still detrimental. This also poses potential risk for fires due to choked wiring.

**Network**

Seeing that Autohub’s IT network infrastructure has only been implemented recently(2013), it is safe to say that the organization’s system is not as robust yet as compared to those who have for it longer years. Since Autohub’s sites are geographically dispersed, it was a good idea to implement the same kind of topography (mesh) to ensure easier expansion and modification as well as better reliability when it comes to data. Although one disadvantage in implementing this kind of topology is that it requires high investment and maintenance. Seeing that there are not enough people in the department, this could pose as a concern for the organization.

With regards to the external security of the system, the current network protection can be recognized as relevant and efficient since a lot of network components and concerns are already answered by a single hardware (UTM9). Having a good hardware, however, does not mean that the control measures are sufficient and accurate since threats grow and become more powerful by the day. Having experienced automated hackings, daily unauthorized access attempts, the organization seem to either lack a reliable procedure or the implementation of the security is lacking. This is to say that the network security should always be up to date and monitored exclusively and looked upon by certain people.

IT security should not only focus on the factors outside of the organization but also on the internal assets it holds whether small or not, since these things could lead to potential unwanted attacks. It was a good decision to prioritize the data assets more than its hardware because these data are not easily replaceable, may be confidential, or may not be easily translated to monetary value (i.e customer information, financial plans, etc.). While having the advantage of versatility, scalability, and connectivity, having a central storage system entails the high risk of the data being vulnerable when the system breaks down, thus it is only necessary that the organization pays a close attention to the maintenance and the security of the network at the individual level.

It should also be noted that the current configuration and software management of the organization is something that should be looked upon since it deals heavily with the technical details that might affect the sustainability, reliability, and quality of IT operations. Although it tackles more on the knowledge management side, it is noteworthy to take note of how knowledge is passed on from employee to employee. Having only a single employee (in this case, it’s Mr. Endaya) who performs technical recommendations, the training of the new IT hires, and the administration, can prove to be very risky. It is risky because the source of knowledge and technical specifics only belongs to one person. If that person leaves, he takes this information with him. It would be hard for another employee to take over the responsibilities since it takes time and money to learn the current system and the business goals.

As for the User Management of Autohub, the use of an exclusive active directory for each brand is a good idea. The implementation of the different password protocols plays an active part in controlling unauthorized system access. Autohub’s active directory also helps in minimizing the access of each user to the different parts of the system and at the same time providing the certain system accesses even outside the reach of the company network.

In conclusion, while it is commendable that Autohub is giving effort in implementing security measures for their assets and connecting and making available these information across the sites, there are still a lot of areas that needs to be fixed and improved upon. Autohub’s current system and infrastructure is able to provide support its current users but there will come a time when maintenance and capacity would become a problem if the system is not properly acted or planned upon. What Autohub failed to address in its design is that it did not consider long-term planning and it overlooked some processes that seemed to be trivial at the moment (i.e. job description, training, documentation, etc).

# Recommendations

**Data Center**

With Autohub continually growing and expanding, the value of their data center grows with it as well. However, one key finding within their data center is the apparent lack of room and investment for the expansion of the data center itself. The data center has been established and is already 14 years old as of 2013. However, there seems to be minimal attention paid to the data center facility itself. To prevent future risks, and to accommodate future expansion, plans must be drafted to expand the area for the data center. A 3-year plan for the data center would be optimal in upgrading it. As can be seen from *figure1*, there is a potential space for widening the center itself. This would however include costs for construction and additional modifications needed by the room.

It must be considered however that currently, the only physical security Autohub’s data center possesses is the double lock and key expanding into the second room would mean that the data center would have to be protected by only one door. With this in mind, arrangements must also have to be done upon renovation of the data center such that it would be more physically secure. Reinforcement of the door along with the addition of more secure verification methods such as biometric scanning is suggestible.

Efforts needed for the data center renovation would be as follows:

* Provisions made for continuous operations during data center renovation (possibly outsourced, or temporarily migrated operations)
* Complete refurbishing of current data center space to rid it of unnecessary cables, hardware, etc.
* Addition of further data center utilities such as a fire suppression system and structured cabling.
* Upgrading of current physical access controls to the data center.
* A 3-year plan for the future of the data computing needs of Autohub.

As the group assessed Autohub’s network, it showed that they can handle the company’s basic needs. However, weakness and room for improvement of the current network emerged as more and more data about the company was gathered. One of which that the group identified was related to the roles of each employee in the IT department. There must be enough employees with a clear distinction between the roles of the employees in the department. From the interview, it was mentioned by Mr. Endaya that they did have a clear structure in the IT department but the problem was that roles were intertwined with each other. Certain jobs overflowed to other employees even if it didn’t cover their job. This could cause redundancy with employees doing a certain job which could be a waste of effort.

It was also mentioned there was a single point person in doing technical recommendations, training of the new IT employees and administration, and system maintenance. The problem with having only one person responsible and accountable with critical processes in the company is that if that certain employee leaves or something happens all knowledge by the specific employee goes down with him. The group recommends having additional employees that would focus on specific area and roles. In addition, since multiple processes were handled by only one person, documentation policies should be implemented to promote a standard way of doing processes. With this, the company could replicate its internal processes without the worry of error.

**Network**

One of the main concerns of Mr. Endaya was the adding of a monitoring specialist in the IT department. Given their previous experience, the company was dependent on the Email notification before acting on certain jobs. The problem with this setup is that most employees are overworked or have too much workload to do to check the email and this is because of the lack of employees in the department. The addition of a monitoring specialist means that there is a single person dedicated to maintaining the server, storage, networks and the like. They would be avoiding their previous experience of incorrect implementation of updates and delayed reaction to monitoring notifications. A monitoring and maintenance protocol could be improved by making it more frequent. Also, the salary of a monitoring specialist is lower compared to the expense the company could incur if the system fails. Along with the addition of a monitoring specialist the company could set up better systems and software. This would enable the company to improve virus detection and intrusion.

Finally proper planning is needed by the company. In their current plans, future hardware and software addition was not identified. The group recommends the company to have an additional ISP because currently the company only has 1 ISP (PLDT). If the primary ISP fails, having a backup ISP would enable the company to continue its business processes while lessening costs from down times.

Efforts needed for network management improvement would be as follows:

* Set up policies for documentation
* Clarify separation of duties
* Establish a knowledge management system that would ensure proper and more efficient information handling and sharing with the organization.
* Hire additional employees that would focus on specific areas and roles.
* Improve virus and intrusion detection by setting up better systems and software.
* Improve monitoring protocol and maintenance by making it more frequent.
* Add additional ISP for backup purposes.

# References

**Works Cited List**

*Autohub Group* Family of Sites. Authohub Group. Web. 7 Oct. 2013.

Rouse, Margaret. *Storage Area Network*. Search Storage, Oct. 2007. Web. 7 Oct. 2013.

Pratt, Mary. *SAN Costs*. Computer World, 1 Jul. 2002. Web. 7 Oct. 2013.

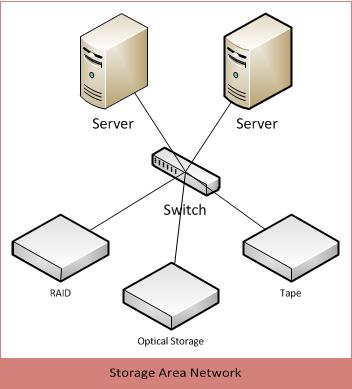
Wikipedia contributors. "Unified threat management." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 3 Oct. 2013. Web. 7 Oct. 2013.

# Appendix

**Storage Area Network (SAN) research:**

A SAN is a specialized network of storage devices. It makes these storage devices appear as locally attached to the servers in the network the SAN is attached to. SANs are usually integrated in enterprise networks.Fiber optics are usually the technology of choice for SANs, since they provide high speed data transmission capabilities, which is critical to SAN operations.

According to Margaret Rouse, SANs support disk mirroring, backup and restore, archival and retrieval of archived data, data migration from one storage device to another and the sharing of data among different servers in a network.



**Benefits**  
 The main benefit from implementing sa SAN is efficient disk utilization. All hard disks used for storage are available to all servers in the SAN, and these can be intelligently assigned per server. This means that unutilized disk space is not wasted, since the disks are not constrained per server.

Since SANs have centralized storage, storage administration is simplified and more flexible due to the fact that cables and storage devices do not have to be physically moved from one server to another.

SANs also make more effective disaster recovery processes possible. A secondary offsite storage location can be included in a SAN to serve as a backup source for emergency purposes. The backup source can be accessed immediately since it is part of the SAN.

**Limitations**

SANs in general are very expensive, costing around $100,000 for a small one consisting of 10 servers, 500GB of storage, and 16-port switches, and an additional $20,000 for software and $10,000 for labor, according to Computerworld.