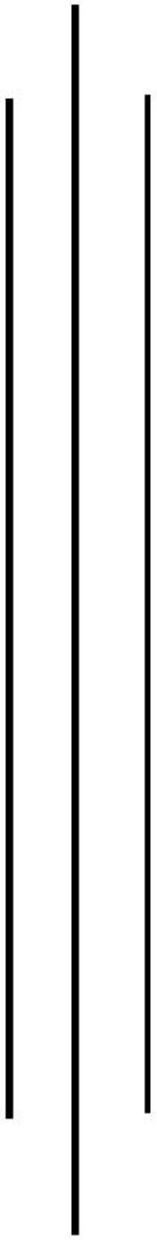
MOTORHEAD DISTRIBUTORS' INC.



Nawaraj Subedi, Shiv Bhushan Shah, Ayush Mainali

Executive Summary

A security audit for MotorHead Distributors Inc. was performed through October 28, 2016 through December 28, 2016.
MotorHead Distributors is the one of the largest automotive parts distributors in the USA, and around the world. The quality and reliability of its products have earned this company excellent brand recognition all over the world. This company has many foreign branches including one each in India, Australia, China, Germany and Japan. Based in Columbus, Ohio, this company employs about 1750 people.
After analyzing the company's business process, the audit reports, policies, and the network set up, a detailed report on the overall information setup for MotorHead Distributors Inc, which includes the analysis on current network setups and implementations on it was conducted. Furthermore, this report also provides the recommendations which can be followed to make the information technology setup more safe, effective, and secure.

Audit procedures:

1. Previous yearly audits
2. Network diagram analysis
3. General Business process/services

Problem Analysis:

The analysis of previous audit report, network diagrams, and business processes reveal the current situation of the software, hardware, information and personnel assets. When compared with best practices prevailed all over the world in the information technology sector, the strengths and weaknesses of the current information technology setup was effectively assessed.
After this assessment, the impacts of specific assets on the daily business operation was prioritized from most severe to insignificant.
Finally, specific recommendations for implementing solutions have been provided to make the information technology setup more secure for all processes, employees, contractors, and visitors.

Network asset identification.

The assets that enable the information technology services used within the company network were identified. These hardware, software, and information assets work hand in hand to keep the daily operation of the company running smoothly.

1. Data Center Asset

- IP Telephony Server

- File/Database Server
- Wireless Controller
- Network Area Storage
- Core Network Equipment

2. Network Equipment
- Router
- Switch
- Firewall

3. Information assets:
- Payroll data
- Employee Records
- Financial Data
- Inventory Records
- Customer Records

Network Diagram Analysis:

After analyzing the current setup of Network diagram of the company, all the routes available on the network can be analyzed. The network diagram of the company reveals the fact that the network is setup improperly. The data and information of the company is not completely secured. PSTN and IP telephony server can directly accessed by users and is susceptible to hacking. Ihe IP Surveillance Camera, Soft Phones, Personal Computers, Network Printers, IP phones, IP Video Conference machine, and Scanners can be accessed by anyone from the IP Telephony Server without any firewall protection. So, the company's assets are not secured appropriately.

It is evident that the company has not implemented a layered approach to the information security. According to a nonprofit website named sans.org, "Defense in depth is a concept of protecting a network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack or failure". Motorhead Inc's network does not have defence in depth layer. The network diagram reveals the fact that there is only one firewall protecting the entire network and there are no internal firewalls between the various departments. Therefore, if a hacker is able to bypass this firewall, then all the departments and the entire network could be compromised. It is highly likely that this vulnerability was exploited in the previous security breaches to compromise customer information.

All the zones/department are connected through the core switch, which means there is no proper data security of server and its directly accessible from users of different departments. One department of the company can easily be accessed from another department without any scanning because they are connected by the distribution switch without any authorization mechanism. The uses of layered defense approach was not found here. Defense in depth

mechanism is important to protect valuable data/information and to provide the backup for the company if in case one fails another will palce to thwart an attack.There is no proper device in place to handle in case of failure occurs and also there is no backup plans in case of an attack from the cybercriminals/ cyber-hackers.
Despite the fact that

Data Identification and Assessment

The critical business operations of Motorhead Distributors Inc. includes online order processing, payroll and warehouse management, order entry and managing financial systems. Additionally, it also provides health benefits, paid-time off, and travel benefits to its employees. These operations require the handling of following types of data:

- Customer's Personally Identifiable Information
- Employee's Personally Identifiable Information
- Employee's Payroll Information
- Customer's Credit/Debit card information
- Employee's Health Information
- Company's financial information
- Inventory data
- Retailer's and manufacturer's information

With these data at hand, Motorhead Distributor has to comply with some industry regulations to ensure the security and proper use of these data as well as to avoid being run into legal issues. Customer's Personal Information and Employee's Personal Information should be protected under the Privacy Act of 1974. Under this act, the customer's and employee's information should not be disclosed to any other individual other than owner without owner's consent. Employee's payroll information should also be kept private and confidential to comply with the Privacy Act of 1974. The handling of customer's credit/debit card information will require the company to abide by PCI DSS. It requires that the company host monetary information securely with a PCI compliant hosting provider to accept, store, process, and transmit cardholders' data. Also, since the customer order is also taken through phone or fax, any information regarding customer's telephone calls should be protected under CPNI. To record and process employee's health information, the company should comply to HIPAA, which ensures the protection of individual's medical records and other personal health information. Furthermore, while managing financial systems, SOX act should be taken into account. The financial reporting of the company should follow the rules and procedures described in the SOX.

The company should always maintain the confidentiality, integrity, and availability of the data it stores and processes. One of the most important data that company is working with is credit card information. So, the possibility of card information theft is one of the most important concern. The company is currently relying on the third-party vendor for processing online credit

card payments. Since, the vendor uses SSL encryption and is also compliant to PCI DSS, there is a minimal chance of card information theft during online transaction. However, the use of telephone calls and fax to accept credit card payments introduces a huge risk to such sensitive information. Hacker could potentially intercept the communication line between the customer and the company to steal the information. Also, while using fax, the information may be sent to wrong number.

To ensure the confidentiality, integrity, and availability of the data, the data should be protected at both the rest and transit state because the company's confidential and sensitive data stored at computer servers could be breached or customer's payment information transmitting over network could be intercepted by hackers. One of the best techniques for protecting data would be to use encryption technology. Data stored at servers could be encrypted so that even if the server is breached and data is stolen, it will remain encrypted and safe. On the other hand, data sent over network or telephones should be protected by encrypting the communication. Likewise, SSL encryption is being used for online payments, telephone lines should also be encrypted using effective encryption technology. The company's policy should ensure compliance to FIPS when implementing cryptographic algorithms. The policy should also ensure that the encryption techniques are re-accessed periodically and changed if outdated.

Additionally, company can consider moving its services to cloud platform as it can prove to be more cost-effective, reliable, efficient, and secure. Hosting all the data and resources in the cloud will eliminate the company's burden of maintaining and securing the physical data centers, computers, and network equipments, which will save company's time and resources. It will also completely eliminate threats like theft of hardware, natural disaster, or fire since there will be no physical server rooms and network equipments in the first place. Also, the cloud will offer employees a secure environment to work even from home. Cloud computing offers software as a service, which can be used as easily at home as they can in the office. It also provides tools to make it easy to collaborate between colleagues.

However, there are some risks related to cloud computing that company should consider. First, moving services to the cloud can cause the company to suffer downtime in its critical operations. Cloud service providers can become overwhelmed with large number of clients and may come up with technical outage. This can cause a huge loss to Motorhead, as it cannot expect downtime of more than 4 hours for order processing system and 7 hours for other critical operations. Second, security of data and resources hosted in the cloud cannot be guaranteed since it is handled by the third-party vendor. Other party has access to the company's sensitive information, which may be internally leaked or hacked by another user hosted on the same cloud server. Nonetheless, the security of data and resources on the cloud can be increased by ensuring that the vendor is compliant with the cloud industry standards and regulations such as FedRAMP.

Some of the ways to further strengthen the Information Security in the organization would be:

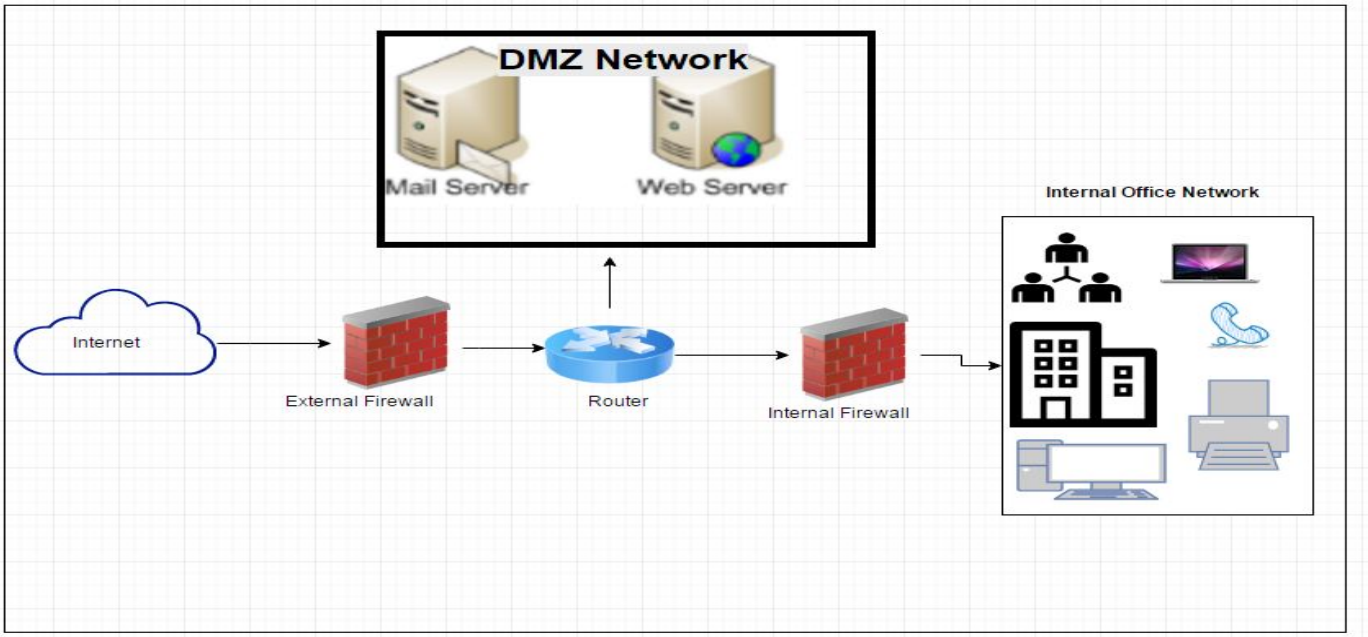
A. Create a DMZ in network:

DMZ stands for Demilitarized zone, which is basically a physical or logical subnetwork that contains any organization's external-facing services to a larger and untrusted network,usually the internet. In other words, DMZ is a physical/logical sub-network that separates an internal LAN (Local area network) form the untrusted network, usually the internet. All the public facing networks, services, resources are located in the DMZ and are accessible from the internet but the LAN remains unreachable. Hence, it provides an additional layer of security to the LAN, which ultimately restricts the ability of cyber-criminals to have direct access internal servers and data through the internet. This not only reduces the number of possible network attacks but also helps to secure the data and information of the company which could be worth huge.

After analyzing the network diagram of the company, we find a DMZ is not set up in the network. So, basically there are no backup plans if any case of breach or attack occurs. The assets like web, mail, FTP, DNS, VOIP etc are placed randomly in the network diagram, which actually needs to be setup inside the DMZ.

As stated above, for an organization, any service provided to the user such as web, mail, FTP etc. on the internet needs to be place in the DMZ in order to strengthen the information security. If a DMZ has not been set up in the company's network, there is a high probability of attack from the hackers, which will affect the service and the basic function of the company. Cybercriminals can easily hack the network if DMZ is not implemented in the network system. Once the attacker gains certain access into the network system of the company, the attacker can gain access to all the servers, and databases, which may compromise the data and valuable information of the company. If DMZ is implemented in the network system, then the malicious virus or spyware content on the internet does not get into the private network of the company. So, having DMZ in the network ensures that the critical functions such as company's email, annual account, audit data, and payroll information etc. is secured. This will save all the data and valuable information of company from breaches and malicious virus.

Finally, DMZ zone is needed to secure the internal network. DMZ helps to isolate the internal network, and is also able to connect to the web server that exposed to the public network. In the company's network, the DMZ and internal office network needs to be separated by the multiple firewall and all the critical function of the company need to be placed inside the internal office network.



Simple DMZ Setup

B. Company needs to create a incident response team to aware if any incident has occurred. Currently the IT staffing is inadequate, and to fix this, the company is advised to create a dedicated department for information security purposes. This department will be able to respond to threats more effectively.

C. Most important Implement a Defense in Depth approach. To effectively implement the defense in depth approach, the company need to use series of devices if in case of any failures occurs. Furthermore, to continue basic company function if in case of any attack, another data center can be built away from the company headquarters which can be used to backup all sensitive information and provide redundancy if the main server shuts down

D. Strong and effective acceptable use policy needs to be implemented.

E. Regular analysis of audit, compliances, and policies is necessary. Although the audits are performed yearly, the audits are not re-assessed regularly. In company must stop overlooking internal audits in order to ensure better policy framework.

F. Effective cybersecurity oriented awareness program for the employee and customer is need to organized.

G. Data center and the backup units need to be created that are located away from the headquarter of the company.

H. Regular patching and updates are not carried out in the company. To resolve this issue, the management should ensure that the IT department is able to roll out patches in a timely and

updated manner. They should also instruct the IT department to make sure that all the software, including the antivirus in up to date.

Risk, Threat and Vulnerability Analysis

There are many threats and vulnerabilities that can gravely hamper the day to day activities of the organization, if exploited by a threat. This is a great risk for the organization, and so, the best practices of identifying the possible threats and vulnerabilities must be carried out. Some of these threats and vulnerabilities for Motorhead DIstributors are as follows:

Threats	Vulnerabilities/Weaknesses
Hacking	- The Lack of a Demilitarized Zone (DMZ) - Lack of firewalls to protect the servers. - Weak security in network access point - Unpatched and outdated softwares and configurations
Unauthorized Remote Access	- Lack of encryption for data at rest and data in transit - Absence of DMZ for network equipments - Lack firewall protection for computer servers
System Intrusion	- Lack of IDS (Intrusion Detection System) - Outdated antiviruses - Weak/outdated configuration for network equipments
System Failure/Error	- Lack of system testing - Poor patch management
Unauthorized System Access/Use	- Ineffective access control mechanism
Internal Fraud/Theft	- Lack of physical security - Disgruntled employee
Data Error/Corruption/Loss	- Lack of data redundancy
Natural Disaster	- Location

	- Lack of alternate business sites
Third Party Vendor Failure	- Lack of policy assessment of the third party
Employee Blackmail	- Fired Employee who still has access to the company's services - Disgruntled employee
Operator Error	- Understaffing and lack of manpower - Lack of proper training

It is evident from the above table that many risks and vulnerabilities exist in this network. Therefore, there are a number of steps that can be taken to reduce or mitigate the impacts of these risks.

The management of Motorhead Distributors Inc. must identify these risks and vulnerabilities, and address them with appropriate actions. To mitigate the impacts of any risks, or to prevent these events from taking place altogether, all these risks must be handled with utmost care. Some ways of doing this are:

1. Ascertaining Risk Management Strategy (as done above)
2. Identifying the Management Structure Responsible for action (CISO)
3. Identifying Assets and Activities within Risk Assessment Boundaries.
4. Identifying and Evaluating Threats and Vulnerabilities.
5. Identifying and Evaluating Countermeasures.
6. Selecting a Methodology based on Assessment Needs.
7. Developing Mitigating Recommendations.

The most important aspect of Risk Assessment is the policy. The policy is the document that directs the entire company's action plan for information security. This also enables the company to keep up with the best practices and standards, in addition to maintaining compliance with federal laws.

The company ensures that the credit card payment uses SSL encryption and the third-party vendor that hosts the site is in compliance with security audits. This shows that the company has taken steps to protect customer information. However, this principle is not applied to the internal processes of the organization. To fix this problem, the company should put in proper authorization and authentication mechanisms that can clearly grant permissions only to people who are allowed to access certain servers. Additionally, the staffing of the company seems to be inadequate. The current IT employees are able to keep the existing systems and processes running, but are frequently inundated with new requests and have to juggle personnel resources. So, there must be a policy to keep IT employees for specific roles, instead of having them work for different processes.

On inspecting the network diagram and general overview of the company, it becomes evident that the policies of the company have not been fully effective in guaranteeing an acceptable level of information security. There are many areas that the company can improve to make their information security process coherent and effective. The company needs to create policies and procedures for applying redundant means of performing critical business functions. The company's transactions and business process make widespread use the internet, is is vulnerable to different types of online threats. These threats range from viruses, malware, and spyware, to cyber-attacks. Therefore, in such a risky environment, the company must be able to create alternative means of carrying out business processes, in case some of their critical systems do not work.

The policies of the company must also provide the procedures and steps for recovering in case of natural disasters. This company is located in the Midwestern US, which makes it vulnerable to natural disasters like tornados and blizzards. So, the company's management must have clear policy that details the steps that must be carried out in case of such an incident.

In addition to this, the company must have appropriate policy for notifying the company's procedures and policies to make sure that the company's downtimes are not extended. Every time a new technology or process is introduced, or if the existing process is altered in any way, the organization should have the policy to notify the employees, and to train them to use the new process. This aids the company by making the employees less prone to make errors, and helps the employees to do their job faster and more confidently. This should include the appropriate use of authentication (safe passwords, usernames, etc.), safe storage of data, acceptable use policies etc.

Hence, there are many improvements that can be made to improve Motorhead Distributors' information security. The company is capable of implementing a layered defence and should implement it to ensure better information security. Although the current network setup does feature some advanced defence mechanisms, there are still many more measures that the company can adopt to enhance its security situation.

Business Continuity Plans and Disaster Recovery Plans

A successful organizational information security should address business continuity plans. Motorhead Distributors can face any time of disruption or disaster like natural disaster or hacker's attack, in which case it might not be able to continue to perform its critical business operations. For example, if there is a fire in the server building and all the computer servers are compromised, the company might just have to wait for things to recover just because they did not know how to act in such emergency situations. Business Continuity Planning will provide a plan to the company so that it can continue to operate during and after such emergency situations.

To put an effective business continuity plan in place, the company should focus on its critical business operations which are order processing, payroll management, inventory management,

and financial systems management. BCP's purpose should be to protect these critical functions during disaster. It should also work with Disaster Recovery Plan(DRP) which is a part of BCP focusing on the more specific and technical elements of the organization. The organization should realize any type of disaster probable in the area, and understand the level of risks associated with it. The emergency situation should be responded by notification of personnel, damage assessment, plan activation, and implementation of specific steps and procedures.

Following are some steps/processes/technology that the IT department can use or take in order to ensure optimal recovery time during disruption or disaster:

- **Scoping and Prioritizing the business operations:**

- **Using Alternate Locations:** To carry out effective recovery process, Motorhead Distributors should consider to rent alternate locations for moving its business in case of an emergency. Since, the company is located at the Midwest US, it is exposed to the risks of natural disasters such as tornadoes and flood. In case of occurrence of any of such disasters, company could move to the alternate location far away and continue to able to function. Considering their recovery time objective of 7 hours, it will be better to rent either a hot site or warm site. Both of these locations will have part or all of the data, equipments and application necessary to resume critical operation. If budget is an issue, warm site could be more cost-effective.

- **Using Redundant Backup Strategies:** Order information, payroll information, payment information, and inventory data are among the most critical assets company has to save during disaster. So, they should select to implement an effective backup strategy. Considering the maximum tolerable downtimes for the critical operations, the company should consider using a combination of full backup and incremental backup as it will provide faster recovery time.

- **Organizing BCP and DR teams:** Planning and implementing recovery without a team is not possible. Staffs should be put together to help the process. There can be different teams such as emergency management team, damage management team, and technical recovery team. Members in each team should have the required expertise and skills to support the goal of the team. So, proper staffing is very important. Also, when picking staffs, it should be ensured that they have the ability to work together, since working as a team gets the job done more quickly and effectively.

- **Training about the disaster and recovery:** The company should provide necessary training to its employees and staffs about the steps they should take during emergent situations. They should be made aware about the natural disaster that are frequent in Company's location. They should be trained on evacuation procedures and safety drills. They should also be trained on reporting of emergency situation and on what steps they should take to activate the recovery procedures during emergency.

Basis for the Evaluation, Analysis and Findings

The audit suggestion for the company is based on the analysis of the overview and the IT structure of the company. The network setup of the company was also analyzed through which deeper insight of the information security comes out. After analyzing the all things , several effective policies such as Acceptable Use Policy, Security Response plan, Disaster Recovery plan, Remote Access policy, Router and Security policy were created for the company. Furthermore, after looking the current and possible issues, following steps need to taken to make information security effective.

Issues Identified and Addressed

In the analysis process, various problems regarding the information security were identified and to address those problems various alternative solution were introduced. Following are the problems that the MotorHead distributors company will need to resolve from this audit, and policies are:

1. Data security and encryption issues
2. Device backup issues
3. Data classification and retention issues
4. Information security awareness issue
5. Natural disasters and Environmental issues

Network Diagram