Name/id: Abdelkareem Yousef Mamdoh Soubar/19110022

Assignment Title: Delivato

Course Tutor: Eng. Moath Sulaiman

Submission Date: 17/6/2022

Table of Contents

Introduction

I have been hired as an “Information Security Risk Officer” in a the Delivato foundation. Delivato is a top leading company in the delivery section all around the world. In this document, I would like to evaluate and assess all the risks that we could face and to actually find a solution for such instances.

IT Security Risks

In this part of this report, I would like to talk about three main topics in IT security risks. These topics include:

- Identifying the IT security risks.
- Proposing a method to assess those IT security risks.
- Proposing a method to treat them.

Identifying the IT Security Risks

Since risks are bound to happen, we should consider every aspect in order to ensure the integrity and the security of all the data related in between the people in our company and our dear customers.

1. **Natural Causes**

   The best term that we can define natural causes is what instances caused by nature. These can include multiple of instances; I am going to count a few:

   - Floods
   - Earthquakes
   - Tornadoes
   - Hurricanes

2. **Human Causes**

Human causes are defined as what actions can the employees do, in which they can harm the foundation. Human causes can be split into two major points, intentional and unintentional

- **Intentional Human Causes:** This category defines what the employee can do to intentionally affect the company in a negative manner. This can include implementing malicious code to harm the contents of the servers to physically harming the servers and the essential equipment that contain all of the essential data that Delivato run on.
- **Unintentional Human Causes:** On the other hand, unintentional human causes are actions that what the employees do that can negatively affect the company, but the difference is that the employee did not intentionally want to do such an act. These can vary from tripping over a lose wire and turning off the server, to forgetting the doors of the server room unlocked, making it possible for unauthorized personnel access such rooms.

3. **Social Engineering**

Social engineering is a term that can be used in order to collect personal information that is sensitive for the victim that a hacker can use in order to harm the victim. This can be caused by manipulating that victim into thinking that he/she are doing something correctly, but false pages are presented to the victim.

4. **Man-in-the-Middle**

A man-in-the-middle attack is when a user thinks that he/she is directly communicating with another computer itself, but what happens is that there is a computer in the middle that collects the traffic from both ends, and both end devices are tricked thinking that they are directly communicating. This type of attack has two variations, an active attack and a passive attack. An active attack is simply transmitted message between the two end-devices being interrupted and altered before it reaches the other end. On the other hand, a passive attack is when the attacker gets the transmitted message without altering the message, in which the original content of the message is received to the intended end-user.

There are several methods for the man-in-the-middle attacks, I would like to talk about three common types.

- **ARP Poisoning**: Firstly, we need to define what is an ARP. An ARP (Address Resolution Protocol) it is a protocol that maps a dynamic IP address to a physical machine address in a LAN. ARP poisoning is an attack that involves sending false ARP packets on a LAN in order to change their pairings that are connected between the IP and MAC address tables.
- **ICMP Redirects**: An ICMP stands for Internet Control Message Protocol, its job is to convey error messages and operational information in which it signals success or failure when devices within a network communicate between other IP addresses. An ICMP redirects attack is an attack that "spoofs" the ICMP message of the router in between the victim and the client.
- **DNS Poisoning**: A DNS is Domain Name System that translates domain names to IP addresses, so browsers can access internet resources. A DNS poisoning is an attack that make the victims access legit-looking websites thinking that they accessed the actual website, but they accessed a fake website.

5. **TCP/IP Hijacking**

When having a compromised TCP/IP session, the attacker has the ability to access and alter transmitted messages over a network. The attacker can attempt to take the client's place by faking the genuine client's address and disconnecting the client's established and potentially already authenticated session with the server. It is possible for an attacker to redirect and receive information from a server by delivering bogus ARP information to the server.

6. **Viruses**

A computer virus is a type of malicious code or program that spreads in between the computer system. It can cause disruption of the computer system, as well as causing data loss.

7. **DDos**

A DDos stands for distributed denial-of-service attacks, its main task is to flood a computer network with instantaneous and repetitive HTTP requests and traffic over a network. It could cause disruption for the network infrastructure.

8. **Worms**

A computer worm is a type of malware that spreads malicious codes and makes copies of itself within a computer system. Without needing any human interaction, worms can replicate themselves. The main difference between worms and viruses is that viruses are often attached in between files, in which it requires an activation by the victim. However, once a worm enters a system it can itself without the host running the distribute file.

9. **Logic Bombs**

Logic bombs are malicious code that are stays inactive until specific criteria is met. Once this specific criterion is met, the logic bomb runs, in which it could cause a disruption in a computer system.

10. **Trojan Horses**

A trojan horse is a malicious code embedded in-between a computer program, once this computer program is ran, the trojan horse works and its main task is to disrupt the user experience and destroy user files.

Proposing a Method to Assess These Security Risks

In order to assess these security risks, we should fully plan and document the process of identifying these security risks. I would like to talk about the whole process of this procedure.

- **Identify the Threats:** In order to know what risks we could face; we should set out every risk that can obtained within our foundation. After setting these risks, we should find a solution to solve them.
- **Identify Vulnerabilities:** We should check out which systems are the most vulnerable and then progress through to the least vulnerable system.
- **Analyze Internal Controls:** Through the identification of the threats and vulnerabilities phase, we should set out certain control procedures to know how we could manage the occurrence of such security breaches and failures.
- **Determine the Likelihood of the Occurrence such an Incident:** After gathering all of the information needed and after making all the tests needed, we should determine the probability of likelihood of such an occurrence.
- **Assessing the Impact a Threat would Have:** During the testing phase, we should lookout and process the results that a threat would have.
- **Documenting the Results:** After we are done with all of the phases (identifying the threats and vulnerabilities, analyze internal controls, determining the likelihood of the occurrence, and assessing the impact a threat would have) we should document all the results for the future. The importance of a documentation is to improve the knowledge amongst different employees and to know if a security breach would occur in the future, we would know how we could solve it by looking back at previous steps and methods we have implemented.

Proposing a Method to Treat IT Security Risks

Whenever there is a threat, a solution must be found ASAP. Data security and integrity is one of the most important things that our foundation, Delivato, runs on. If any breach is to be found, it must be handled correctly and through certain procedures that are suitable enough. I would like to talk about some steps and procedures that we can solve these different types of risks.

Since the datacenters are located in different regions all around the globe, we could implement certain procedures that could help protect the datacenters in a physical manner. For example, in regions that are situated with high precipitation and the probability of high flooding rates, we can well insulate the buildings to make them waterproof. We can also raise equipment by a few centimeters to prevent water to get into them. On the other hand, in areas with high temperatures and extreme drought, we can focus on the cooling point of view. Cooling is a very important part, because servers and major network equipment generate a lot of heat, excessive heat can negatively affect the performance of these equipment and could also ruin these equipment in the long run. We can put powerful air conditioning units to help with the cooling procedures.

For the physical security of the facilities, we can put out certain measures that would help secure the server rooms. Only allow authorized personnel to enter the server rooms, this can be achieved with a high security protocols with using different biometric measures. Also, to prevent the issue of forgetting to lock the server room doors, once a door is closed, it will be locked automatically. To keep track of everyone who enters and gets out of any facility, we would implement CCTV cameras with making sure that no blind spots are compromised.

In terms for the security of our network, we should predefine certain rules to be enforced amongst the employees within Delivato. First of all, we should prevent the use of any unauthorized external storage mediums to be used. This is because certain malware from several types can be transferred from these external mediums to the end-devices of our employees. Also, our employees are required to change any passwords that they use within our foundation every three months. Finally, a strong firewall would be implemented that is tailored to our needs, this would filter out any malware, making the data transmitted clean, and a it would prevent DDos attacks.

Risk Assessment Procedures

Having a strong network for the processes and the information in such a foundation is extremely essential. If any misconfiguration occurred during the designing and implementation of our network, data might get corrupted and would be ruined. Frankly saying, there is no need to bother with corrupted data, since it would waste a lot of time trying to restore the data, and it would result in an unsuccessful reaction. Cold and hot backups are a must in our foundation. Cold backups are done when the all the users in the network are offline, they are safer than hot backups since no files can be changed during the backup. On the other hand, hot backups are done whilst the users are still logged into the system. They are used as making replicas for backups.

For our risk assessment procedures, I would like to point out certain points and techniques that would minimize the risks of any physical or networking failures.

- Physical security from natural disasters is mostly handled by the construction of the building.
- For standard building security, we would have a control room with complete connectivity to human security personnel, which would act as needed.
- A control room would have access to CCTV and security system to make sure only authorized people would access certain areas.
- Firewall is one of the most important security components in our system. It prevents any unauthorized connections, filters network connections, prevents social-engineering, and DDos attacks. If the firewall is misconfigured, it can drop and refuse connections that would allow any reading of data sent from other locations or leaked data.
- VPNs are programs that allow employees to establish a secure connection to a server. However, if the configuration is incorrect, we would have an unsecure connection. This would mean that a hacker/attacker would be able to sniff the data that is being transmitted within the network and the would be able to obtain passwords. Manipulation of the main servers would also occur.
- Each employee would have a PC that is secured and would have anything pre-installed by the IT department, which includes a VPC (Virtual Private Connection). A VPC is needed in case if the employee needs to work from home. In addition to a VPC, SSH keys and VPNs are used to provide an encrypted connection to make sure that no 3rd party programs are used to sniff the network.

ISO Risk Management

To secure our assets, such as people, hardware, and software, we must first identify and assess the dangers that we may encounter and how they may harm them. Risk assessment is a process for determining what might cause damage or injury to the Delivato Foundation and then doing analysis to better understand those risks so that we can devise a strategy to safeguard our equipment and assets from harm.

Risk Management has some essential steps that are followed to improve the flow of this process.

- Identify
- Analyze
- Evaluate
- Treat
- Monitor

I have been assigned by my manager as an “Information Security Risk Officer” and it is my responsibility to know what factors that would harm our network and find ways and solutions to minimize the risks of any failure that would occur.

ISO 31000 is a risk management is an internal standard that was founded in 2009. Its main goal is to provide guidelines for effective risk management.

There are a lot of benefits of using the ISO 31000 standard in our foundation, I would like to count a few:

- Strengthen operational effectiveness and governance.
- Increase stakeholder trust.
- Boost Delivato’s productivity, crisis management, and organizational resiliency.

ISO 31000 has some of the following points that are followed:

- **Risk identification:** This is the process of determining what we can do to keep our system from being damaged.
- **Risk analysis:** Examining the data around these dangers.
- **Risk assessment:** Compares the risk assessment to the risk criteria.
- **Risk treatment:** We would like to know how a risk would be handled, whether it's positive or negative.
- **Putting the situation in context:** This procedure entails establishing the scope of the risk management process as well as the company's goals.
- **Monitoring and review:** This step entails comparing the risk management framework to the risk management strategy and determining if the risk management framework is still appropriate.
- **Communication and consultation:** The goal is to determine the social effect as well as the interests and concerns of stakeholders.

ISO 31000 Application in IT Security

To follow the ISO 31000 standards in the UK, we need to identify the risks. This step is needed to locate, recognize, and explain any hazards that might aid or obstruct a successful outcome. After the step of identifying the risks, we would need to do some risk analysis, in which we need to understand the nature of risks and its characteristics. Risk analysis entails a thorough examination of unknowns, repercussions, and the likelihood of events and scenarios. After these steps are done, we need to report the risk and inform the people in charge of what instances occurred.

How Could We Improve Delivato's IT Security?

We can improve Delivato's IT security by following certain design methods and certain techniques that would enhance the general performance and security of our network.

Different Security Procedures

- **DMZ (Demilitarized Zone)**

  By definition, a DMZ is a physical or logical subnet that divides a LAN (Local Area Network) from external untrusted networks, such as the internet. Between the public internet and the private network, DMZs serve as a buffer zone. A DMZ subnet is setup between two firewalls, in which before reaching the servers in the DMZ, all in inbound network packets are checked using a firewall or other security appliances.

  The benefits of using a DMZ are as follows:

  - **Access Control:** A DMZ network controls access to services accessible via the internet outside of an organization's network perimeters. It also creates as a layer of network segmentation, which increases the amount of barriers a user must overcome before being granted access to an organization's private network.
  - **Network Reconnaissance Prevention:** If the network that is DMZ enabled is compromised, the internal firewall would still protect the private network. Even if the attackers get access to DMZ enabled servers, they will remain separated from the private network due to the DMZ's internal barrier.
  - **Blocking IP Spoofing:** Attackers may get access to an authorized IP address within the network and could in return "impersonate" the victim's IP address. The DMZ's job is to discover and stall such spoofing attempts.

- **Static IP**

  Simply, a static IP is an IP that does not change. Once this IP is allocated to a device, it would not change. There are many benefits I would like to present to you:

  - **It Gives Potential for Remote Access:** When having a static IP address, you are able to access you device from anywhere in the world. When you have a VPN also, it would allow to access your machine.
  - **Provide Stability:** Static IP addresses are known to provide stability unlike dynamic IP addresses, this is because it does not undergo frequent lapses.
  - **Provide Security:** When having a static IP address, it would provide a better level of security. This is because it would provide an extra layer of protection.

- **NAT (Network Address Translation)**

  It is a technique for translating numerous private local addresses to a public one before sending data. There are some advantages of using a NAT:

  - **Conserving Address:** NAT can prevent the consumption of IPv4 addresses.
  - **Network Security:** When using NAT schema, all the of the original sources and destination sources would be hidden. Without having the user's authorization, the hosts inside the LAN would not be able to be reached by other hosts.
  - **Improved Reliability**: NAT includes a number of features, including load balancing and backup options. These tools will aid in improving the network's overall resilience and flexibility. It will happen when we establish any link, whether public or private.

- **VLANs (Virtual Local Area Networks)**

  A VLAN is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group.

  - VLANs reduce the need to have router deployed on a network.
  - VLANs would ease administration in which it would enable the network administrators to group devices for administrative and nontechnical purposes.
  - Security would be tighter when using VLANS. This is because it would provide a higher degree of control over devices.

- **VPN (Virtual Private Network)**

  A VPN connects a private network to a public infrastructure, like the internet. There are multiple reasons to use a VPN:

  - **Encryption of the IP Address:** The main goal of using a VPN is to hide the IP address from the ISP and other third parties.
  - **Encryption of Protocols:** The VPN would prevent the user from leaving any traces, that could be used against a certain user. This includes cookies and search histories.
  - **Enable Remote Connectivity:** When the employee would like to connect to the Delivato's network remotely, the employee would be able to connect to it.

Different Security Procedures

There is a reason that we need to secure our network. Network security is one of the most important things that any company run on. This is because, this network is considered as the backbone of the company, if it is out of service for whatever reason, this can lead into major consequences. This is where an NMS (Network Monitoring System) comes in place.

An NMS is a standalone server that runs an application or multiple application to monitor a certain network. Network elements communicate with the NMS to transfer management and control information. The NMS acts as a logging system in which it has a backlog for every network device and software.

I would like to talk about the benefits of using an NMS:

- **Makes Documentation Easier**: NMS provides system administrators with up-to-date statistics and information about any failures in the instance of their existence. This can make documentation easier, because the system administrators would know what went wrong in the process of configuring the network.
- **Prevents Business Disruption**: Since our business relies on our network, having an NMS would detect and resolve any issues that are related to our network.
- **Minimizes Security Risks**: Since any worldwide company is bounded to have breaches from other competitors, hackers, and other organizations from breaching the network and implementing certain viruses that can make our network vulnerable.

Data Protection Processes and Regulations

All data is important! We must have some protocols and techniques that would help prevent any “leakage” of data. These protocols and techniques include:

- **Encryption Algorithms**
- **Data Integrity Checking**
- **SSL Protocols**
- **Usage of Firewalls**

Encryption Algorithms

Encryption is the process of transforming data into a format that can only be decrypted with the help of a decryption key. Encryption must identify all database communications as well as secure all the protocols entering the database. Some encryption algorithms include:

- **RSA**: It is an encryption cryptography algorithm, in which each session has its own secret key, which is produced at random, all network traffic is completely secured. RSA is an asymmetric algorithm, which has two different keys (a public key and a private key)
- **DES (Data Encryption Standard)**: Unlike RSA, DES is a symmetric type of encryption. A symmetric encryption type uses a single key that must be shared between all of the people who need to receive a message.
- **Triple DES**: Triple DES is based on the DSA algorithm, but the main difference is that a message must pass through three times on the DES algorithm.

Data Integrity Checking

Data integrity checking algorithms are added to a network to ensure the integrity of the data and to detect any corruption that would occur in the process of data transmission. I would like to talk about some techniques that can be used to ensure data integrity.

- **MD5 Checksum**: It is a data integrity approach that uses hashing and sequencing to ensure that data is not tampered with or stolen.
- **SHA (Secure Hash Algorithm)**: SHA is a modified version of the MD5 algorithm, in which it is more secure and produces a larger message digest for greater security.

SSL Protocol

An SSL stands for “Secure Socket Layer”. In a PKI (Public Key Infrastructure) format, SSL enables authentication, data encryption, and data integrity. SSL authenticates server-to-client and client-to-server communication. The SSL protocol uses the “handshake method” to establish a connection. It has four main phases:

- **Phase 1**: The client and the server send “hello packets” to each other. In this phase, protocol version and cipher suite is exchanged for security reasons.
- **Phase 2**: The server sends its certificate and “Server-Key-Exchange”, in which the server end phase 2 by sending the “Server-Hello-End” packet.
- **Phase 3**: Phase 3 is about the client replying to the server by sending its certificate and “Client-Exchange-Key”
- **Phase 4**: Change-Cipher suite occurs, and the handshake protocol ends.

Firewalls

Firewalls are used to transfer data from one protocol to another without the hassle of decryption and re-encryption. It eliminates any weak places in the network infrastructure. Installing a firewall between the public network and the intranet is one of many techniques that can be used to ensure data security.

Regulations

What is the European Union's General Data Protection Regulation (GDPR) and how does it affect the foundation?

GDPR is one of the most famous rules regarding data protection that is collected and processes from the people's personal lives. Users of EU websites must accept certain statistical disclosures under the GDPR. In addition, the web site must make measures to aid EU customers' rights, such as quick notice in the event that personal data is compromised.

GDPR's Customer Service Requirements

Depending on what the GDPR's regulations depend on, website visitors should be informed about the data that is collected from them and how they are used. An "Agree" button should be implemented to show the acceptance of the process of data collection of the website user.

Cookies are implemented. These "cookies" are small files that their job is to store private information, such as webpage settings and preferences. Also, websites must alert the website visitors if any of the personal information that is stored within the website is compromised.

A DPO (Data Protection Officer) should be employed in which he/she would review the website's data security. Contacting the DPO must be also available and his/her contact information should be made clear to the public, so that visitors may use their EU statistics.

Controversies Surrounding the GDPR

The GDPR has drawn criticism from a variety of quarters. Some believe that requiring enterprises to hire DPOs or virtually review their need for them creates an undue administrative burden on a few. Some people also argue that the directions aren't clear enough about how to deal with worker realities.

Furthermore, data cannot be sent beyond the EU unless the receiving firm meets the same security standards as the EU. As a result, high-priced corporate process interruptions have resulted in legal disputes.

Benefits of IT Security Audit and its Impact

A security audit is a series of checks on the settings, technologies, and infrastructure of an IT system.

You may ask yourself how a security audit function? I would like to point out certain steps that would enable us to have a successful security audit.

- First and foremost, we establish the evaluation criteria. To put it another way, we agree on the main goals that will be covered in the audit, as well as how the audit will be executed and tracked.
- Following that, we prepare a security audit. In this step, we choose the tools and procedures that will help us achieve our objectives.
- Another thing we would need to consider is to do an actual security audit. This implies we must be cautious and offer adequate documentation, as well as closely check audit progress and data points for correctness.
- Finally, we finish and present the results. This signifies that the results should be shared with all previously identified stakeholders, and a list of action items should be created based on the audit findings.

The benefits of using an IT security audit are as follows:

- Find any hardware or software that is not needed.
- Discovering hacker entry points that hackers would use to disrupt the functionality of the network.
- Demonstrate that the organization complies with international regulations.
- Shows how well-qualified are our network administrators, in which it would show how employees would react and communicate in case of any security or networking failure that might occur.

What Would Happen if a Security Misalignment Occurred?

In case of any failure in the security of our network, there are several consequences to have in mind.

- Data loss.
- Reputational damage. When we would have a network breach and some data got leaked or lost, this could cause to a reputational damage, even if our company is the best in its field.
- Financial Crisis. When our servers are down, we cannot keep track of the operations that are made, this could cause a confusion to appear in between the customers. It can get to the extent of customers deviating from using the same service from other competitors.

Designing and Implementing a Security Policy

As mentioned above, a simple security misalignment could result into a big financial loss. In this part of this documentation, I would like to talk about making our network more secure physically and in a software point-of-view.

Physical Security

Physical security is about securing the actual servers in place and prohibiting unauthorized personnel from having access to our rooms. Some physical security measures are as follows:

- Check that both internal teams and security system vendors are adhering to the best cybersecurity procedures.
- Access control and surveillance systems should be installed in each place that houses sensitive information.
- To provide teams a better means to communicate information, establish a formal cooperation.

Data Retention

The term "data retention" refers to the types of data that a corporation collects and stores. Where will it be stored, how will it be stored, and for how long will it be stored? Some requirements must be met to ensure that we have this policy!

- **Discard outdated and duplicated data:** We must frequently look through data and check whether these data are outdated to the point that there is no point of storing them and we can also check if some data is duplicated, there is also no point of storing duplicated data, in which if we the data at the first place, why do we need to have a duplicate of it?
- **Making room for more storage:** Deleting and removing data that is not used is essential, this allows us to store newer data without having the trouble of getting new storage mediums.
- **Compliance**: Businesses can use the data retention policy to manage their compliance with industry rules and legislation.

Data Encryption

Data encryption is a means of encrypting (scrambling) data so that only the user with the right decryption key may access it. Data encryption is implemented by following certain criteria:

- **Choosing the right encryption tools:** The right encryption tools would allow the network to perform as what how our foundation intended to perform.
- **Maintaining a culture of security after implementation:** It's a good idea to make sure that the staff in charge of data encryption is well-trained and up to date on the latest data encryption technology and practices.
- **Defining Delivato's security needs:** It's crucial to understand the encryption techniques' strength and processing needs.

Access Control

Access control is a fundamental aspect of data security that ensures who has access to and uses corporate resources and data. It's crucial who has access to the network devices since it prevents sensitive data from getting into the wrong hands. We should explore the choices accessible to us in order to adhere to this policy.

- **Mandatory Access Control (MAC):** In this strategy, resources are allocated depending on the sensitivity of the network's information and the authorization of the user who may access it, which is determined by different security levels.
- **Attribute-based Access Control (ABAC):** Because ABAC is a dynamic technique, access is determined by a collection of qualities and external factors.
- **Role-based Access Control (RBAC):** RBAC controls network access depending on a person's position in the company.
- **Discretionary Access Control (DAC):** The system administrator decides who has permission to view the data using this way.

Security Training

Because human mistakes are unavoidable, it is critical to educate staff who are in charge of data management. Keeping them informed and doing particular checks in specific time domains is one approach to assist them in maintaining a high degree of security.

Risk Management

The process of discovering, analyzing, and responding to possible hazards is known as risk management. Because risk management is a core requirement of many information security standards and frameworks, it is critical in such an organization. To ensure that the risk management policy operates well, there are various procedures that may be taken. We follow these following steps to optimize the usage of the risk management process.

- Identify the risks that might make Delivato's network vulnerable.
- Analyze the severity of each risk by determining how probable it is to occur and what the consequences would be if it did.
- Examine how each danger falls within the permissible risk range.
- Make a list of the dangers that need to be addressed first.
- Determine how each risk may be addressed:
    - **Treat**: Typically, this strategy entails adopting additional or updated security measures.
    - **Terminate**: Totally avoiding the danger by altering the action that is producing it.
    - **Tolerate:** Make a conscious decision to reduce the danger.
    - **Transfer:** Sharing the risk with another party.
- Keep an eye on the risk to make sure it's still acceptable (monitoring the risk).

Business Continuity

The process of developing preventative and recovery measures to deal with possible cyber risks to a company is known as business continuity. If a cyber-attack occurs, it is critical to have a business continuity strategy in place to get operations back up and running as quickly as possible. We follow the following point to have the optimum business continuity plan:

- **Conduct business impact analysis and risk assessment.**
- **Develop recovery strategies.**
- **Solution implementation.**
- **Testing and acceptance.**
- **Routine maintenance.**

The Avoidance of a Vulnerable Network

In order to avoid making the network susceptible in any secure network, some rules must be established.

- **Using Strong Passwords to Protect Any Sensitive Data**
  - Use specified character combinations to ensure that the password is strong.
  - Change passwords on a regular basis.
  - Make certain that staff do not exchange passwords with one another.
- **Keeping Up with Software Updates**
  - Upgrades to any security software can occur, making the program more competent of managing data, thus keeping an eye out for these updates is a smart idea.
  - Enable automatic updates to eliminate the possibility of forgetting to update your program.
- **Providing a Policy for Backups**
  - The foundation should create a system that meets the backup and recovery plan.
  - Creating a backup plan.
  - Documenting all secure data backup and restore methods.
  - Generating a matrix indicating how long backups should be kept for recovery.
  - Results of planned restoration tests.
- **Keeping External Media Away from any Computer**
  - Pen drives are a huge data and network security concern. Malware might be distributed through them in this way.
  - If the usage of removable media is required, it should be encrypted.
  - Only approved removable media must be used with their devices for work-related operations.

- **Being Cautious About What Is Downloaded**
    - Because it is a private machine, the employee is not permitted to download any files from the internet. Because there is a danger of vulnerability if this occurs.
- **Policy for Managing Portable Devices**
    - Since we live in a wireless world, data may be sent in a variety of ways. It's critical to keep track of which devices are allowed into the network.
    - It is critical to provide specific authentication on which devices are permitted entry.
    - Enabling fingerprint authentication on devices. In which the use of fingerprints is far more difficult than the use of a password.

Suitability of Tools Used in this Policy

To ensure the integrity of our network in the planning and the implementation plan, I tended to use some software and tools that made it capable to ease securing our network and to show what backdoors are available for hackers and penetrators that can enter our network.

In this following section, I would like to talk about three main tools that were used during this process.

Nmap

Nmap is a service that looks for hosts and services on a network in order to assess the network's security. Nmap works by analyzing raw IP packets in certain ways to determine which hosts are present on the network. Nmap scans the network and interprets the responses it receives, then utilizes the data to generate a "map" of the network. This is a map that is produced provides all of the details on what each port is doing. There are several explanations for this.

I am going to enumerate a few reasons why we chose to use Nmap:

- **Network Mapping:** The sorts of devices actively using scanned ports will be identified by Nmap. Servers, routers, switches, and other equipment fall under this category. Users may also examine how those devices are linked and generate a network map.
- **Vulnerability Scanning:** Nmap may be used by businesses who frequently consume security information from threat feeds or other sources to assess their vulnerability to specific threats.
- **Portable to Use:** It can be used in many operating systems, so it is favorable to be used by multiple organizations.

Nessus

Nessus is a security scanning tool that may be used remotely. It keeps an eye out for any dangers that an unauthorized user could obtain access to the data. Nessus identifies which service is running by evaluating each on a machine. This service is tested to ensure that no liabilities are discovered that may be used against you.

The reasons that we use Nessus are the following:

- It is a user-friendly tool, since modules are set for usage in the tool
- It is often updated, ensuring that the customer is searching for accurate data
- It offers a lot of configuration choices; because it enables testing on all domains, any configuration may be specified in Nessus. It may be used in a variety of ways as a result of this.

Wireshark

Wireshark is a network monitoring tool that allows the network administrator to keep an eye on what's going on in the network. The way it works is that it allows the user to filter the logs either before or after the analysis.

We use Wireshark for these following reasons:

- Versatile to use, since it can be used in many platforms.
- Information about packets can be shown in detail in between the network.
- Filtering is enabled, we can filter out specific data that we need to see and observe.

The Roles of Stakeholders in the Delivato Foundation

A stakeholder is a person or organization who may have an influence on or be affected by the project.

Reviewing the cybersecurity goals and existing position is a smart idea. This necessitates an evaluation of the organization's aims and surroundings. Another thing to think about is starting effective cybersecurity talks. This necessitates an assessment of the environment and a check around corners for potential hazards. These risks are solved by:

- **Leading With a Risk**
    - Demonstrating the foundation's commitment to safeguard and guarantee its success
    - Show the significance of the steps required. Because if there is a breach, the cost will be much higher.
- **Communicating With the Same Language**
    - Because stakeholders are not security experts, it is critical to simplify the general topic and ensure that the stakeholder is interested in being a part of this foundation during the discussion process.

A Disaster Recovery Plan

A disaster recovery strategy must be established in advance to avoid any potential implications of a cyber catastrophe.

To begin, let's clarify what a disaster recovery strategy is (DRP). A DRP is a written document that contains instructions on how to respond to any unpleasant unexpected events. Following that, there are various actions we can take to ensure that the DRP operates as efficiently as possible with the fewest possible side effects.

- **Identify the Most Significant Potential Threats**

  We must check out the threats that are probable to occur. This is where we should pay the most attention to. These significant risks might negatively impact our organization.

- **Establsishing a Monitoring Plan**

  We should find a way on how we would monitor these risks. Monitoring the risks is a crucial point to consequences that would lead into something major to the integrity of the data held.

- **Define Roles and Responsibilities**

  Not all people are suitable to have a leading job, in which this has specific criteria that has to be met. In the contrary, our employees must have the best skills available and periodically check on what updates are available to improve their knowledge in this field.

- **Creating a Communication Plan**

  Creating a communication strategy entail sketching out how communication protocols will work in the event of a calamity.

References

- www.radware.com. (n.d.). *ARP Poisoning*. [online] Available at: https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning/.
- SearchNetworking. 2022. *What is Address Resolution Protocol (ARP)? Definition from SearchNetworking*. [online] Available at: <https://www.techtarget.com/searchnetworking/definition/Address-Resolution-Protocol-ARP> [Accessed 13 June 2022].
- Secret Double Octopus. (n.d.). *What is a Man In The Middle Attack? - Security Wiki*. [online] Available at: https://doubleoctopus.com/security-wiki/threats-and-tools/man-in-the-middle-attack/ [Accessed 13 Jun. 2022].
- Cloudflare (2019). *Cloudflare*. [online] Cloudflare. Available at: https://www.cloudflare.com/learning/dns/what-is-dns/.
- Keyfactor. (n.d.). *What is DNS Poisoning? (aka DNS Spoofing)*. [online] Available at: https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/#:~:text=DNS%20poisoning%2C%20also%20known%20as.
- Fortinet. (n.d.). *What are Computer Viruses? | Definition & Types of Computer Viruses*. [online] Available at: https://www.fortinet.com/resources/cyberglossary/computer-virus#:~:text=A%20computer%20virus%20is%20a.
- Cloudflare (2022). *Cloudflare*. [online] Cloudflare. Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.
- Kaspersky.com. (2020). *What's the Difference between a Virus and a Worm?* [online] Available at: https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms.
- HYPR. (2020). *What is a Logic Bomb? | Security Encyclopedia*. [online] Available at: https://www.hypr.com/logic-bomb/#:~:text=A%20Logic%20Bomb%20is%20a.
- Norton (2017). *Norton*. [online] Norton.com. Available at: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html.

- ZHAO, J. (2021). *How to Perform a Successful IT Risk Assessment*. [online] Hyperproof. Available at: https://hyperproof.io/resource/it-risk-assessment/.
- Vitanium. (2020). *What is the difference between hot backup and cold backup?* [online] Available at: https://vitanium.com/what-is-the-difference-between-hot-backup-and-cold-backup/#:~:text=A%20hot%20backup%20is%20performed.
- Norwich, Q.D.W.D. (n.d.). *ISO 31000*. [online] QMS. Available at: https://www.qmsuk.com/iso-standards/iso-31000.
- PECB (2019). *ISO 31000 Risk Management – Principles and Guidelines*. [online] Pecb.com. Available at: https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines.
- BSI Standards Publication Risk management -Guidelines BS ISO 31000:2018. (n.d.). [online] Available at: https://www.ashnasecure.com/uploads/standards/BS%20ISO%2031000-2018.pdf.
- SearchSecurity. (n.d.). *What is a DMZ in Networking?* [online] Available at: https://www.techtarget.com/searchsecurity/definition/DMZ.
- www.hitechwhizz.com. (n.d.). *7 Advantages and Disadvantages of Static IP Address | Drawbacks & Benefits of Static IP Address*. [online] Available at: https://www.hitechwhizz.com/2021/09/advantages-and-disadvantages-drawbacks-benefits-of-static-ip-address.html.html.html.
- GeeksforGeeks. (2021). *Advantages and Disadvantages of NAT*. [online] Available at: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-nat/.
- radhikat (n.d.). *Advantages of VLANs*. [online] library.netapp.com. Available at: https://library.netapp.com/ecmdocs/ECMP1401193/html/GUID-C9DA920B-F414-4017-8DD1-D77D7FD3CC8C.html#:~:text=VLANs%20provide%20a%20number%20of.

- Slattery, T. and Burke, J. (2021). *What is a VLAN (Virtual LAN)?* [online] SearchNetworking. Available at: https://www.techtarget.com/searchnetworking/definition/virtual-LAN.
- Kaspersky (2020). *What is a VPN and how does it work?* [online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn.
- Online Security News, Reviews, How To and Hacks. (2021). *What are the Advantages and Disadvantages of VPN?* [online] Available at: https://securitygladiators.com/vpn/advantages-disadvantages/.
- INS (2016). *How an effective Network Management System benefits your business*. [online] Iris Network Systems. Available at: https://irisns.com/2016/04/14/how-an-effective-network-management-system-benefits-your-business/.
- SearchNetworking. (n.d.). *What is network management system? - Definition from WhatIs.com*. [online] Available at: https://www.techtarget.com/searchnetworking/definition/network-management-system.
- GeeksforGeeks. (2018). *RSA Algorithm in Cryptography - GeeksforGeeks*. [online] Available at: https://www.geeksforgeeks.org/rsa-algorithm-cryptography/.
- Tutorialspoint.com. (2019). *Data Encryption Standard - Tutorialspoint*. [online] Available at: https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm.
- GeeksforGeeks. (2018). *Data encryption standard (DES) | Set 1*. [online] Available at: https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/.
- www.tutorialspoint.com. (n.d.). *Triple DES - Tutorialspoint*. [online] Available at: https://www.tutorialspoint.com/cryptography/triple_des.htm.

- What Is the MD5 Hashing Algorithm and How Does It Work? (n.d.). *What Is the MD5 Hashing Algorithm and How Does It Work?* [online] Available at: https://www.avast.com/c-md5-hashing-algorithm#:~:text=What%20is%20MD5%3F.
- Cloudflare (2021). What is SSL (Secure Sockets Layer)? | Cloudflare. *Cloudflare*. [online] Available at: https://www.cloudflare.com/learning/ssl/what-is-ssl/.
- GeeksforGeeks. (2019). *Secure Socket Layer (SSL) - GeeksforGeeks*. [online] Available at: https://www.geeksforgeeks.org/secure-socket-layer-ssl/.
- Cisco (2008). *What Is a Firewall?* [online] Cisco. Available at: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.
- Astra Security Blog. (2020). *IT Security Audit: Types, Importance and Methodology*. [online] Available at: https://www.getastra.com/blog/security-audit/it-security-audit/.
- Updated: 3/29/2020, J.P. (2020). *What is an IT Security Audit? The Basics | Varonis*. [online] Inside Out Security. Available at: https://www.varonis.com/blog/security-audit.
- segment.com. (n.d.). *What is Data Retention? How to Create a Policy that Protects Privacy*. [online] Available at: https://segment.com/blog/data-retention/.
- SearchDataBackup. (n.d.). *Data Retention Policy: What Is It and How to Build One*. [online] Available at: https://www.techtarget.com/searchdatabackup/definition/data-retention-policy.
- Townsend, R. (2018). *Access Control Models – UHWO Cyber Security*. [online] westoahu.hawaii.edu. Available at: https://westoahu.hawaii.edu/cyber/best-practices/best-practices-weekly-summaries/access-control/.

- Rapid7. (n.d.). *Information Security Risk Management (ISRI)*. [online] Available at: https://www.rapid7.com/fundamentals/information-security-risk-management/#:~:text=What%20is%20Information%20Security%20Risk.
- www.tutorialspoint.com. (n.d.). *What is Risk Management in Information Security?* [online] Available at: https://www.tutorialspoint.com/what-is-risk-management-in-information-security [Accessed 13 Jun. 2022].
- securityscorecard.com. (n.d.). *Integrating Cybersecurity into Business Continuity Planning*. [online] Available at: https://securityscorecard.com/blog/integrating-cybersecurity-into-business-continuity-planning.
- Information Security & Policy. (n.d.). *Business continuity management: Safeguards: Information Security & Privacy Program: Information Security & Policy: Indiana University*. [online] Available at: https://informationsecurity.iu.edu/program/safeguards/managing-business-continuity.html.
- SearchNetworking. (n.d.). *Common network vulnerabilities and how to prevent them*. [online] Available at: https://www.techtarget.com/searchnetworking/tip/Common-network-vulnerabilities-and-how-to-prevent-them.
- Kalman, G. (2014). *10 Most Common Web Security Vulnerabilities*. [online] Toptal Engineering Blog. Available at: https://www.toptal.com/security/10-most-common-web-security-vulnerabilities.
- Firch, J. (2019). *What Are The Common Types Of Network Vulnerabilities?* [online] PurpleSec. Available at: https://purplesec.us/common-network-vulnerabilities/.
- Hackingloops (2020). *Nessus VS OpenVAS Advantages and Disadvantages Explained*. [online] Hackingloops.com. Available at: https://www.hackingloops.com/nessus-vs-openvas/.

- UKEssays.com. (n.d.). *Cisco Prime and Wireshark Advantages and Disadvantages*. [online] Available at: https://www.ukessays.com/essays/information-technology/cisco-prime-wireshark-advantages-7229.php.
- Comptia (2020). *What Is Wireshark and How to Use It | Cybersecurity | CompTIA*. [online] Default. Available at: https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it.
- ReadWrite. (2022). *How to Create a Cybersecurity Disaster Recovery Plan*. [online] Available at: https://readwrite.com/cybersecurity-disaster-recovery-plan/#:~:text=What%20is%20a%20cybersecurity%20disaster.
- Snoweb (n.d.). *DRP: all you need to know about the IT recovery plan*. [online] www.c-risk.com. Available at: https://www.c-risk.com/en/blog/drp-disaster-recovery-plan/.
- Burgess, M. (2020). *What is GDPR? The summary guide to GDPR compliance in the UK*. [online] Wired.co.uk. Available at: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.
- GDPR. (2017). *GDPR*. [online] Available at: https://gdprinfo.eu/.