**Final Security Summative**

**Endpoints**

**CEO**: Endpoints are one of the most important risks that the company might face, when working in a large environment, the lack of system protection can affect the company’s work and our employees in a big way since they can easily be attacked by hackers and by any type of viruses or threats related to security flaws. Furthermore, it could take two business days on fixing the vulnerability and all the down systems that the company might face if it is not well secured. In addition, the reputation of the company will be affected if the workflow is too.

**CFO**: If any hacker got into any PC in the company that is because of the weakness of the security on the endpoints that our company has, so that means the loss we are going to have is about 200k$ contains data and information related to our company and our employees, and it would take 2-3 business days to fix it, and in that time the company will face another risk and it is time loss, and that will affect the competition in our company. On the other hand, we are going to lose customers which will affect the income of the company too.

**COO**: As we can see that the risk here is the endpoints so we have to secure them in order not to get hacked easily and that’s because of the daily goals that our company would face. The two business workdays will affect the operations of our work, and if three or more computers are down then it will affect our company’s goals in the long term.

**Endpoint risk assessment:**

1. The vulnerability: The unsecured endpoints must have Anti-virus in order to catch any unknown virus, and it must be on its latest update.
2. The threat: Downloading any unknown files from the internet, inserting a USB on any PC because that might be accessible to external hackers.
3. The magnitude might arrive up to 40% because the expectancy arrived at 30%, the frequency at 15%, and its harm to the company’s data and information is 15%.

**Controls to avoid the risk:**

1. Server Security
2. Using HTTPS malware detection
3. A protocol to scan every email to avoid phishing.
4. Using SFTP instead of FTP to transferee files

**Using one subnet for all devices**

**CEO**: One of the biggest threats for our company is having one subnet because that would put us and our privacy, in a bad situation and its reputation because of the many branches, the use of one subnet for all devices can leave a security threat in which anyone from any branch can access the data. In addition, having all the devices become infected would cost us 3-4 business workdays to fix this vulnerability in case of a hacker or a virus on the network since they are all on the same network and subnet and that would delay out business continuity.

**CFO**: This risk would cost us a lot due to its vulnerability and that is because the one subnet that is used for all the devices, if a hacker or a virus got into our subnet all of our data and information would be taken away, and if the hacker or the virus had reached the main subnet, all of the systems would be down, and that would cost nearly 250k$ due to the off days that our company wouldn’t be able to work, with a 3-4 business workdays to fix this risk. On the other hand, if the hacker got all the data of the company, he might ask for a ransom in order to give us back the data needed for our company.

**COO**: This risk would affect our company’s day-to-day operations, and our employees and customers will not have any access to the database due to the fix days, which will affect badly the company’s operation, which would let us lose our customers and employees to go and search for other competitors.

**Risk assessment for one subnet for all devices:**

1. The vulnerability: Not having a single authentication, weak passwords, outdated software applications, and poor firewall configurations.
2. The threat: If a virus or a hacker got access to the subnet, the system will do down.
3. The magnitude would arrive up to 50% because the expectancy would arrive up to 20%, so the frequency is going to arrive up to 10% and the harm to the company would arrive up to 20%

**Controls to avoid using one subnet:**

1. Creating virtual LANs and VPNs for each one of them and disconnecting all from each other.
2. Make each branch or department separate from another.
3. Create a different subnet for each branch and location, which can help in different manners such as organizing and differentiating between branches and departments.

**Data processed by a conveyor system**

**CEO**: Any private data information for the company must not be accessible by any unauthorized person. Thus, it will affect the business continuity if that data was shown to everyone; anyone coming over that webpage can view or find our data. When dealing with sensitive data for customers and shipments, it is very important to have a well-secured database and webpage with a secure connection and logging reports.

**CFO**: The accessibility to such sensitive data would lead to serious threats from hackers as it will be easier for them to hack into our network and blackmail us by publishing our data which would cost our company lots of money. On the other hand, any type of viruses can get into our cloud server or database and kill some systems which would cost us 100k$+ in law firms fees and compensations for damaged customers.

**COO**: The publicity of the data would harm the customers, in which by laws and regulations would give customers enough motivation to sue our company, which would harm the company’s reputation and operation in the short-term and might to long-term damage. That is why we need to stay on the safe side and not to put ourselves in a situation to be in court.

**Risk assessment on data processed by conveyer system:**

1. The vulnerability: publishing it in the cloud, publishing using the internet
2. The threat: Complete cloud visibility and zero day-to-day threat detection
3. The magnitude would arrive at 60%

**Controls to avoid data processed by conveyer system:**

1. terrorist or a Microsoft SQL and Azure solution for that data
2. secured with a username and password for each employee
3. to create a rule on the server which allows the customers to access a specific link just for them for that certain shipment for tracking and complaints
4. have a good type of server and web protection installed on your cloud server in addition to a backup to make sure that no threats can reach, as well as an additional backup to make sure that if anything happens to the main cloud server or database, everything can be easily restored to within no time and can help with data loss cases

**Customers are able to create profiles**

**CEO:** If the website were not secure enough it would affect the customers when creating their personal profiles, which would affect the company’s reputation because the customers would not allow their personal information to get hacked easily and not get lost by any virus like malware, and to be in hand for everyone. In addition, it would take me four business days to fix that problem and restore all customers’ personal information.

**CFO:** One of the biggest risks is creating a personal profile for customers and not being secured, because that would affect us losing customers if their personal information got hacked, and we as a company will lose nearly 320k$ because it will take me 4 business days to restore all the customers information.

**COO:** In the long and short term, customers will opt for other companies because of the lack that would happen due to the customers that we might lose, and our company’s reputation. In their private information, and they will lose interest and trust in our company, so we have to secure their personal information in order to gain more customers and not to let them down.

**Risk assessment creating profiles:**

1. The vulnerabilities: Using HTTPS instead of HTTP to secure the customers’ information.
2. The threat: of losing customers’ personal information.
3. The magnitude would arrive up to 55%.

**Controls to avoid the risk:**

1. Customers should have a specific user or link just for them, which should be protected with a username and password to make sure nobody can access their data except for them.
2. The server should also have daily backups scheduled with good protection in case of disaster recovery.
3. There should be a cloud solution installed and set up on the main server which can make sure that all the data is uploaded as soon as it’s created which can also help as a mirroring solution in case something happens.

**Datacenter**

**CEO:** In our company, the server room is one of the most important rooms in it, because there are many essentials that we need to keep in mind such as physical center security, correct environment, the perfect temperature and sever control, other than that the business continuity might be affected due to any natural factors and unauthorized people entering the room.

**CFO**: In this situation, our loss would be very big, due to the servers that we need to protect from anything that would affect it like fire, water and unauthorized people entering the room, because any damage on the servers will not just cost us the data we have for our company, it would also cost 410$ due to its importance in the company. Furthermore, our company could stop its work for 5 days to fix the problem we might have.

**COO:** we should really take care of our servers and protect them from anything that might affect them like natural disasters, because anything that would happen on the cabinets will reduce our workflow and would delay the long-term goals and the daily operation due to the data we might lose.

**Risk assessments on the data center:**

1. The vulnerabilities: unauthorized access, climate for the cabinet.
2. The threat: Fire disaster, unauthorized
3. The magnitude will arrive at 70%.

**Controls to avoid the risk:**

1. fire resistant glass, which can help in case of a fire happening to make sure that the room is protected, and fire won’t reach it
2. the raised floor is also an important fact, which means that there has to be alcubond or a wood floor raised about 5-10cm to protect the room from any disaster that happens on the main floor or can help in case of cleaning, water flood and other cases that might happen.
3. people who can enter the server room are only the IT department or people who are qualified to work in the server room, which can help in protection as well as making sure that no one who is unqualified or untrusted can enter without unlocking the door remotely from their smartphone before entering.
4. All cabinets should be locked as well to make sure for extra security.

**VPN**

**CEO:** It will negatively affect the reputation of our company because employees are using VPN in the wrong way and entering places on the data server with no certificates. Therefore, our ratings will suffer massively leading to a decrease in the number of consumers and the company’s business performance.

**CFO:** The rules and regulations that we are going to implement will affect employee salary’s due to their bad consumption of VPN access, and that will affect the company’s income due to the customers that we might lose, and viruses could have access from using the internet in a wrong way using VPN and that could cost us 260k$.

**COO:** The day-to-day goals will affect the productivity because employees are using VPN in the wrong way and they could open anything that might be danger to be open on our servers, so the customers will mistrust working with our company due to its bad operations.

**VPN risk assessment**

1. The vulnerability: If its security implementation process is not done properly
2. The threat: lack of accountability creates third-party VPN risks.
3. The magnitude will arrive up to 80%

**Controls to avoid the risk:**

1. User accounts should be created for each user in addition to a policy, which can control what each user is allowed to access through the connection.
2. The employees should only be able to run specific applications or webpages that they are allowed to access through the VPN configuration policy.

**Third parties**

**CEO**: If third parties started using VPN, they can easily have access to our records and private data and that will create a single shared network between multiple office locations, and that will affect Bombino’s workflow as well as the customers trust.

**CFO:** with our trusted VPN provider, they will keep our data private and secure without exploiting the users, which will lead to an increase in the consumption of the VPN by new consumers leading to an increase in profits. In addition, that would make us pay more nearly 277k$ to have a secure VPN

**COO**: we have to make sure that the VPN does not suffer from any leaks that might lead to exploiting our users and making sure that their data and private information remain secure, intact, and in safe hands, because other than that it will affect our daily operation due to the customers private information, and tout private data.

**VPN access for support risk assessment**

The vulnerability: enhance the employees’ security by keeping their private information and data safe

The threat: Potential hackers might leak the data, leading to the exploitation of the employees’ private information for money.

The mitigation will arrive at 78%

**Controls to avoid the risk:**

1. The support team for any company should be granted access to the VPN only in case support is needed
2. the user should be monitored in case they have done something wrong to make sure everything is recorded

**Minor security procedures**

**CEO:** This can affect any business in a large way since employees and systems on the network are prone to getting any type of virus or threat or their data stolen. There have to be different methods used to protect and monitor such issues that might occur. Moreover, our reputation would get harm since the network are prone of getting any type of virus.

**CFO:** Better security requires more resources. However, having low-grade security will damage the company more in the long run. Therefore, spending resources on security will benefit the company in the long run. On the hand, that would cost us 310k$ since we do not want to lose any data or employees.

**COO:** To achieve better security, the company requires better error and bug handling from professionals, and up-to-date tracking of the company’s data whilst making sure that there are not any undetected leaks that may result in the exploitation of employees or the company’s data and the daily reputation.

**Minor security procedures risk assessment:**

The vulnerability: anyone could have access to the VPN.

The threat: an unauthorized person having control of the network.

The mitigation might arrive at up to 58%

**Controls to avoid the risk:**

1. Install security software on each system, this is to make sure that it’s monitored and secured by a trusted solution.
2. There has to be a rule specific for VPNs that allows only trusted users to access at a specific time, as well as good IP arrangement and grouping for VPN users.

**Risk assessment procedures**

1. **Establish the context:** Establishing the context specifies the scope of the risk management process and establishes the criteria for assessing risks. The scope should be chosen in light of the firm's organizational goals. Because risks are uncertainties that impact the attainment of corporate objectives, they cannot be adequately identified if the objectives and strategies are unclear.
2. **Identify the risks:** classifying risks is to realize what must be controlled in a building project Risk identification is the first phase in the risk management process since potential problems must be detected before risk assessment, response, and control can occur.
3. Analyzing the risks helps to identify potential problems that could arise during a project or process, for example reducing the impact of a negative event, eliminating risks during a process, and evaluating whether there are more benefits to a project than risks before the intention.
4. **Evaluate the risks:** Prioritization is a way to deal with competing demands. This aids in determining where you will spend your limited time and effort. It has the greatest impact.
5. **Treat the risks:** It is the process of selecting and implementing measures to appropriately deal with the threat and manage it in a possibly profitable way. In addition, It is a collective term for all the tactics, options, and strategies chosen to respond to a specific risk and it is mandatorily a part of an effective risk management plan.

Qualitative and quantitative risk assessment:

1. Qualitative approach is used to quickly identify risk areas related to normal business functions and is generally performed on all business risks.
2. Quantitative risk analysis provides more objective information and accurate data than qualitative analysis because quantitative risk assessment is based on realistic and measurable data used to calculate the impact values that the risk will create with the probability of occurrence.
3. Qualitative risk analysis is quick but subjective.
4. Quantitative risk analysis is objective and has more detail, contingency reserves, and go/no-go decisions.

**ISO 31000**

What is ISO 13000: ISO 31000, Risk management - Guidelines, specifies risk management concepts, a framework, and a procedure. It is applicable to every organization, regardless of size, activity, or sector.

Using ISO 31000 may assist businesses in increasing the possibility of accomplishing objectives, improving the identification of opportunities and risks, and effectively allocating and using risk treatment resources.

ISO 31000, on the other hand, cannot be used for certification but can give guidelines for internal or external audit programs. It allows organizations to evaluate their risk management methods to a globally recognized benchmark, therefore offering good principles for successful management and corporate governance.

**Terminology** has four main things, which are the **asset,** and it is anything value that can be impacted in a manner that results in a loss. In addition, any agent capable of acting against an asset in a manner that could result in loss is a **Threat.** Moreover**,** a **vulnerability** is a probability that the threat agent’s action will result in loss. In conclusion, the **risk** is a measurement of the probable frequency and probable magnitude of future loss.

Most risk assessment approaches have some form of these terms.

We seek to find and use objective methods to provide a responsible estimation of risk and the associated potential loss.

There are two types of risk, which are the **initial risk** which is the risk remaining after mitigating actions are taken. And the second is the **residual risk** which is the risk remaining after mitigating actions have been taken, and their mitigating actions are called **controls**.

The four approaches to managing risk and it is risk treatment are:

* **Avoid**: and it is the surest way to prevent the potential loss arising from a certain activity is to completely avoid it.
* **Mitigate**: if we are unable or unwilling to avoid an activity, we can take steps to reduce the probability and potential severity of loss associated with the activity.
* **Transfer**: Is another way to deal with risks we are unable or unwilling to completely avoid is to transfer them to a third party.
* **Accept**: Accepting full responsibility for the potential loss.

**What is the difference between probability and possibility?**

A possibility is as being binary, something is possible to happen or it is not, in other words, a chance that something might exist, happen, or be true.

1. It is possible it could rain today.

Probability is a continuum that addresses the area between certainty and impossibility, in other words, something that has a chance of happening.

1. There is a 50% chance of precipitation between 10 am and 2 pm today.
   * Prediction: The word prediction implies a level of certainty that rarely exists in the real world and does not help people understand the probabilistic nature of the analysis. Furthermore, risk Analyses are not reliable predictions of future events.
   * The Monte Carlo Fallacy: The mistaken belief that if something happens more frequently than normal during some period, then it will happen less frequently in the future

**What is the risk of the management stack?**

It is showing the relationship between these elements. Moreover, as with similar relational constructs, it becomes immediately apparent that failures at lower levels of the stack impair the ability to achieve effectiveness at higher levels.

* Effective management
* Well-informed decisions
* Effective comparisons
* Meaningful measurements
* Accurate risk model

**Taxonomy**: Taxonomies are organized methods of decomposing complex systems to explain how they work. However, taxonomy definition is the practice and science (study) of classification of things or concepts, including the principles that underlie such classification.

The main purpose of it is that without a logical, tightly defined taxonomy, risk assessment approaches will be significantly impaired by an inability to measure and/or estimate risk factor variables. This, in turn, means that management will not have the necessary information for making well-informed comparisons and choices, which will lead to inconsistent and often cost-ineffective risk management decisions.

**There are two types of element risk**

1. Risk that is considered as loss event frequency, which is not added or multiplied with each other to form a new expression related to risk.
2. Loss magnitude and loss event frequency both have multiple unique factors beneath them in the taxonomy.

Loss magnitude has two loss types, which are primary loss and secondary loss.

Primary Loss occurs directly because of the threat agent’s action upon the asset, and the losing side of the taxonomy is expressed in monetary terms.

Primary Loss has Forms

* Productivity
* Response
* Replacement

Secondary loss can be thought of as “fallout” from a primary loss event in which its Frequency allows the analyst to estimate the percentage of time a scenario is expected to have secondary effects.

* Secondary loss Forms
* Fines and Judgments
* Competitive Advantage loss

Talking the loss forms, there are six loss forms, which are:

* Productivity loss has a unique dual loss component, Revenue Loss and Employee Productivity Loss, which may also include sunk costs associated with personnel who are unable to perform their duties but who continue to collect their paycheck.
* Response Losses are expenses associated with managing a loss event.
* Replacement Loss is the intrinsic value of an asset. loss is typically represented as the capital expense associated with replacing lost or damaged assets
* Fines and Judgments
* Competitive Advantage The loss of Competitive Advantage can exist in the private sector, public sector, and even the military.
* Reputation Losses are losses associated with an external stakeholder’s perception that an organization’s value proposition is diminished and/or that the organization represents a liability to the stakeholder.

**Risk identification**

Theft and data breaches are examples of risks, and the act of recording risks is what could prevent an organization from achieving its goal. As the initial phase in the risk management process, it is intended to assist businesses in understanding and preparing for potential hazards.

The purpose of risk identification is to enable firms to foresee potentially detrimental occurrences and take steps to lessen their effects. Furthermore, it involves not only identifying potential risks but also documenting them and communicating them to relevant parties.

The risk origin can be projected itself for an external source, in which there are several solutions for what you might need to identify risks, including:

* Support investment decision
* Assess cost uncertainty/operational costs
* Test program before acquisition
* Analyze multiple alternatives

**Risk evaluation**

1. Identify and prioritize assets: Take into account all the various data, software, server, and other asset kinds that are controlled.
2. Locate assets: Find the source of the assets and list it. You should be able to identify the origin of any asset, whether they are internal servers, mobile devices, desktop office PCs,
3. Classify assets: Decide if each asset belongs in the categories of public information, sensitive internal information, non-sensitive internal information, compartmentalized internal information, or controlled internal information.
4. Finalize data and make a plan.

**Recording & Reporting**

It is a system that allows for individualized follow-up in helping patients who do not make satisfactory progress. In addition, they have some responsibilities like establishing national procedures for reporting incidents.

Moreover, their procedure is to protect the integrity of the report by insisting that the statement report is being done.

**What are controls?**

Controls are defined as any person, policy, process, or technology that has the potential to reduce the Loss Event Frequency (LEF) and/or Loss Magnitude (LM). Thus, there are control types, which are:

* Avoidance: that reduce the potential for contact with threat agents are called Avoidance Controls and they include:

1. Firewall filters
2. Physical barriers
3. The relocation of assets
4. The reduction of threat populations

* Deterrence: Controls include hardening assets because many threat actors are opportunistic in nature and will gravitate toward easier targets.

1. Physical obstacles like external lights on buildings or barb-wire fencing

* Resistance :

1. Authentication
2. Access privileges
3. Patching
4. Some configuration settings

* Responsive : Responsive/Response Control

1. Backup and restore media and processes
2. Forensics capabilities
3. Incident response processes
4. Credit monitoring for persons whose private information has been compromised
5. **Describing different security procedures**

**Physical:**

1. CCTV cameras: a closed system that enables the transfer of pictures from video cameras to displays through wired or wireless data networks, video cameras, and display devices (monitors).
2. Thermal sensor: Thermal sensors use changes in the electrical characteristics of the sensor materials to monitor temperature changes specially used where all the servers are.

**Virtual:**

1. Firewall: A firewall is a software program that is installed on each computer that restricts traffic via port numbers and programs, whereas a physical firewall is a piece of hardware that is situated between your network and the gateway.
2. Anti-Virus: this is a tool that detects and removes viruses and other types of unwanted software from your computer or laptop. Malicious software, sometimes known as malware, is a type of code that may destroy your computers and laptops, as well as the data on them.
3. **data protection processes and regulations**

**Encryption**: data must have a specific system in it because the network is the most important due to any business data transition and it is the most likely to be targeted by hackers. Thus, we use encryption to make sure that if data was stolen, encryption will prevent unauthorized access to read it.

* + - 1. **Back up**: back up is used to restore any missing data if the company’s devices got lost or the device’s system was down. Thus, Backups should be kept as safe and up to date as feasible. If your company's data is frequently changing, you should update the backup every day, if not every hour.

**IT security audit**: Security auditing helps businesses identify and assess vulnerabilities in their IT networks, connected devices, and apps. As a result, it benefits from a thorough examination of an organization's security posture and IT infrastructure.

**Benefits of IT security audit**: It identifies gaps in the company's security and awareness; moreover, it assists in making educated decisions toward its improvement. Furthermore, it reduces hacker risks by identifying probable hacker access points and security holes ahead of time.

1. **The security impact of any misalignment of IT security**

Bombino Company must be guided by corporate strategies, which shape and inform the business in the long and short term because any effective strategy could make a big difference to the company’s outcomes and its business continuity. Furth more, the employees should be aligned with all policies set by the company.

In addition, if a misalignment occurs in Bombino’s policy and its employees, it will leave them without any momentum and they will be unable to achieve any progress, because if any employee does not follow the Bambino policy, some private data may be leaked. If the employee installed an untrusted link from the internet and plugged in a USB on the computer, it could be an external hacker or malware that could possibly have access to the system by the user’s PC.

Moreover, if a hacker got access to the company’s system it will affect Bombino’s reputation because the personal information of the customers and the employees could be in a hacker’s hands, or it could be attacked and deleted from a ransomware virus, and that should not happen due to the company’s private information that no one should have access to but the managers.

If an employee repeatedly breaks Bambino’s security policies, it will compromise Bambino’s security measures, and this will affect its customer’s trust leading to almost no market credibility. Not following company policy could lead to incomplete data sets, which could hinder business operations and the data analytics initiatives that support them. Data silos may damage an organization in many ways; some of them are inconsistent data, duplicate data and less collaboration between users.

1. **Security policy for Bambino**

Designing a security policy for all the networks in Bambino is the most important thing because everything needs to be under control, in which the managers must have access to all items, but the employees must only have access to specific items on their PCs.

|  |  |
| --- | --- |
| Password policy | - Do not talk about a password in front of others  - Do not reveal a password in a mail message  - Do use a strong password that contains 8 characters with numbers. |
| VPN | It allows the users to only have access to certain programs that is related to the workplace. |
| Backup | Bombino’s data must be backed up at the end of every day because Bambino’s data must be in a safe place in case of any disaster happen. |
| Recovery disaster | It is to have a recovery plan in another building or in another station in case of a disaster could happen |
| Data servers | The cabinets must have a security code that only authorized people can enter. |
| Firewall | Security systems that manage and impose restrictions on network connectivity. Firewalls create a point of control where access controls may be applied. |

1. **Evaluate the suitability of the tools used in this policy**
2. **Password policy** is important for the employees and the company’s private information about the work. Moreover, it provides protection against unauthorized access to the employees’ and companies’ personal information.
3. **VPN** is important for the workflow because I can control what the employee can have access to while working. So that the employees cannot open anything that is not related to work.
4. **Backup** is one of the most used tools in any company because it can back up all the data that Bambino has and protect the company from data loss from any disaster that might happen.
5. **Recovery disaster**: Bambino must have this recovery type because if anything happened like a fire or if the company got into an earthquake, Bambino’s data will be in a safe place outside the main company.
6. **Data server**: All the cabinets in the company must have a high-security policy because If an unauthorized person got into it, the data could get destroyed and stolen.

**Firewall**: It can secure our machine and information by controlling network traffic. It accomplishes this by filtering undesirable and unwelcome network traffic.

1. **A discussion of the roles of stakeholders in the Bombino to implement security audit recommendations.**

CEO: Any risk that might happen in the firm that would definitely affect the company in many ways, some in the company’s reputation because the risk might be huge, high and that would make the customers lose their trust in our company, and that would make it enough to hit Bambino’s reputation. Moreover, Bambino’s business continuity could be affected by the vulnerabilities and threats it might get from its weak key information.

CFO: The money that Bambino might lose from the security for the organization loss is big and high, so we have to evaluate the existing information security and focus on the controls, and what we would do in the event of the administrator functions and not to lose customers as well as an delay in our financial income. In addition, it will protect us from a huge loss and in return, it will save a lot of money that the company can use for other security items.

COO: We are going to lose balance on the company’s daily operations because it will affect the customers and the employees in many ways as well as our company’s reputation, and not only the customers, but the other companies also that we are dealing with, and that will effect on the trust they have for us, and that what would affect the long and the short term operation.

1. **Organizational disaster recovery plan**

**Determine critical applications, documents, and resources**: the process of the organization must evaluate to determine which are critical to the operations of the company. It should focus on the short term in case we had to restore any data flows and revenues, rather than the long-term solution of restoring the company’s full data capacity.

* + - * 1. **Recovery time objective**: It is the goal the company has for the maximum length of time it should take to restore normal operations following an outage or data loss.
  1. **PRO**: it refers to how much data loss the company can tolerate at its maximum.

**Specify back and off-site storage procedures**: These protocols ought to specify what has to be backed up, who should do it, how to do it, where to do it, and how regularly. Backing up all essential software, hardware, and documents are advised. In addition to backing up the current list of employee data information they have.

**Identify and assess disaster risks**: our disaster recovery should be identifying and assessing the risks to the company; this step should include items related to natural disasters because this will identify the recovery strategies within an acceptable timeframe.

**References**

(Team, n.d.)

(Sergio Loureiro, 2020)

(Defense, 2020)

(Security policy, 2022)

(Grimmick, 2022)

(Security Policy, n.d.)

(Team I. E., 2021)

(n-able, n.d.)

(National Library Of Medicine, n.d.)

(JACOBSON, 2021)

(researchgate, 2014)

