School of Computing and Informatics

Security

Subject :Delivato Security

Name --> Hamza Mohammad Muhsen
ID--> 20110044
[Date]
*Note: References list in the last page

Semester 2, Year 2022

Security in Delivato Company

Risks , how to asses them, treatment :

From my tour in the organization, I found many risks that may affect the work of the organization and I recommend to overcome these risks:

-Risks that related to the physical security:

I found that the doors of the offices and warehouse are easy to open and that's not good because that's make the shipments and important rooms under the danger of unauthorized access and that's caused theft of the shipments and equipment and decrease the repetition of the organization in job market.(R1)
(Solution):I recommend to put a signs that tell the employees to not enter the room (not all the employees just authorized personnel) and put lock in the doors of warehouse and in the important places in the organization such as: server rooms and network and I recommend to put one of these locks:

Biometric
(number)

Proximity card
(special card from the employer to open doors)

Biometric
(using the finger)

By using any kind of these locks, the important rooms will be more secured from any unauthorized access than before .(and the organization managers can hiring some employee to enter these rooms and the others can't enter) and I also recommend to put more than one camera in the organization.

-Risks that related to the human (All the persons in the organization) :

that many employees devices are not good protected and that cause dangerous in the data related to the organization and employees can faced from hacked and Unauthorized access and phishing.(R2)
(Solution):First, we must set policies and the employees should implement it very well, for example the employees devices must have a anti virus and they should update their devices periodically to protect their devices from any malicious intent.

I noticed that the security procedures are not enough and need more security procedures or policies to implement it in the organization because more polices means more security and awareness in organization environment for the employees and third parties.(R3)
(solution): Set more about policies in the organization such as :discuss more about security awareness which is make the employees know more about cyber security risks and get away from social engineering mistakes. Also make a polices to employees and the third parties of how and the procedures to connect remotely and others.

Mistakes about configuration on DNS and firewall which make it easy to attackers to access the network and steal the data related to organization because firewall protect the organization network from any malicious intent that comes from the internet because fire wall can block the information that comes from the internet and the organization doesn't need it. And examples of the attack that the organization can face are DNS poisoning, ddos, zero day malware and middle attack.(R4)
(Solution):About the mistakes of configuration (DNS and firewall), I recommend to replace the employees who work on DNS and firewall and hiring new employees with a high experience of configuration DNS or firewall, set more policies on each one .

-Risks that related to the environment:

I found the servers and networks rooms are not good in temperature and humidity and that's not good to the organization because the overheat make the equipment, server, devices failure and doesn't work and that is make loss of data and the organization needs more budget.(R5)
(Solution):Put air conditioner in the network and server rooms and worked 24 hours and ensure that will not stop working, and these rooms must has temperature between (18-22) and the percentage of humidity must be between (20 % - 70 %) to work perfectly and ensure that the every thing work well.

-Risks that related to the natural disaster:

We should count a natural cases as a risks because it's played an important role in security and natural cases such as burning fire in a branch and causes failure in the devices and important rooms that save or manage the data. Not only fire, there are many such as : flood, earthquack or storm.(R6)
(Solution):I also recommend to backup the data every period of time to decrease the percentage of the data loss and ensure that there is another copy of the data to restored it when needed. For example if the organization face any form of natural causes and the data removed, then the organization has a copy of the data and will recover it and continue the work to serve the customers.

-Risks that related to the organization network:
Let some employees have the access to VPN data center, I don't recommend the VPN because it's not safe and the probability to face the attacks is high, for example of the attack that the employee can face like spoofing, ddos, malware and others.(R7)
(solution): maybe if the VPN is important or necessary to the organization, we can train the employee about the VPN and what are the risks and how to avoid the risks and also make some guidelines to let know the employee who is using the VPN the safe steps.

- use same subnet

Using the same subnet is dangerous to the organization because it's make the LAN of the delivato in danger and easy to access it and also congestion and slow down in the company and that's not good to the organization.(R8)
(Solution): I recommend to implement many things that will help to treat this problem such as : implement user zone, DMZ .

***Risk matrix approach:**

I will use this method to assess these risks to let the delivato know what is the risks that is dangerous and need to get away from them and the risks that not damaged hard to the delivato. This method is described as a table contains the impact and the frequency of each risk and I used this method because I am familiar with this method and used it in many projects.
>> **Assessment**:

(Risks)		**Impact**		
		Low	Medium	High
Frequency	Very high		R8	R1 ,R2,R4
	High		R3	R5
	Medium		R7	R6
	Low			

--> **(User, 2022)**

B.What is risk assessment procedures :
First before talking about procedures, I want to talk more about the risk and risk management and what is the impact to the delivato so the risk is the percentage of the threat happened and cause damage to the delivato and the management is the steps that can help delivato to define the vulnerability that in the delivato and also making a response process to defend the CIA (confidently, integrity, availability) of the delivato.

Let deep in this management and talk what it contains, it must divided : what the delivato define group of (vulnerability) and rank of each of them and delivato must not look to another risk management of another organization because this management affected by the size of the company, resources ans so on.

Processes:
-**Find the risks->**
the steps that can help delivato to define the vulnerability that in the delivato.It also can describe about each vulnerability that help the delivato and reach all the goals of the security objectives in delivato.
-**Analysis the risks->**
This is the second step and the delivato must know more about risk and learn the nature of the risk , impact and how it will affect the controls of the delivato the probability to happen.In this stage the employees can used, documentation, techniques during this step.
-**Evaluate the risks->**
After know the every nature of each risk and the impact, the delivato must evaluate these risk to which one is the most important and the delivato need to treat them to which risk that can not impact very much to the delivato. There are many **concepts that will help to evaluate such as :**
-**Avoidence:**
In short, it is describe to get away from any investment of the vulnerability in delivato by using many things like the organization can add more security safe guards and so on.
-**transference:**
Delivato can take benefit from another companies that specialized in implement the security and assets the risks to over come the vulnerability that in the delivato In exchange for money or delivato can hire some persons that have a lot of experience on security.

-**mitigation:**
As discussed before delivato need to identify the impact of the risks, so in this phase the delivato needs at least to reduce these impact of the risk to the delivato ,and there are many plans that delivato can reduce the impact like DRP or BCP or IRP as discussed in the previous task.

-**acceptable:**
To discuss this briefly, the delivato forget the risk because it will not affect much to the delivato and the risk want much money to cover it so it's wisdom to forget this risk in the organization.This option is not fit with any risk and it should be studied the risk before select this option. For example the organization can implement this risk if the risk determined it impact, what is the probability to the risk will happen, review the risk from cost plan in the organization and other factors.

--> **(Five Steps of Risk Management Process - 360factors, 2022)**

C.Information about ISO (31000) and application :

It's a system used in risk management, and it established in 2009 of it's first version and it developed every period of time until 2018 . In 2009, it has 11 main principles of risk management and in 2018 it became 8 instead of 11.

ISO 31000:
It's a system that used to help the organizations to analysis and assessment the risks by using rules and guidelines that are in the organization, it's used for all organization because it's fit with all the functionalities. If you implement ISO in your organization, your organization will improve in the security and become more popular and confident in making decisions.

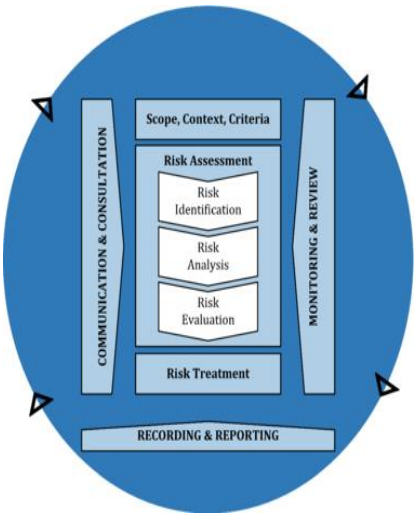
principles :
There is something called principles in the system and it's 8 principles, first which is the risk management is completely implement the system on all the process and combine them with the procedures that related to the activities of the organization and that's called (integrated), management must structure with the guidelines to continue to save the productivity and creativity and that's called (structured and comprehensive), it also must be customized with all the activities in the organization to reach the goals that related to the organization and that's called (customized),it also should be to all the people who involvement in the organization such as : employee or stakeholders and it must be clear to read and understand (inclusive), inside every organization the knowledge will change and increase every period time so, the risk management should fits with all these knowledge every time to get the best result and productivity (Dynamic), also in every organization, they will never get the required data all time, so they should benefit from the best information believable and the information means the information in the past and current information and it should be available to the stakeholders (Best available information), also these management is affected with the human and their actions and culture and the organization characteristics and people goals in the organization should be in the risk management to reach the goals of the organization (Human & culture factors), and finally the organization should improve more and more by using experiences and using many methods and tools to continue the improving (like: PDCA) and deals with the results of risk management to grow (Continual Improvement).

Frame works:

It's considered one of three main categories in management(risk) and help the organization to make the perfect decision. This category consists of six sections which : Leadership -->Integration--> designing --->implementation---> evaluation and improvement .

-Leadership:
This the first step where all the leaders of the organization needs to choose and discuss if they want to implement the risk management in their organization according to their goals and business culture.
-Integration:
It's part of the frameworks when it is depends on the structure of the selected organization (note that the structure is not the same in all organization and very organization has the unique structure) and the risk management manage all the risks in all the structure of the organization. Integration risk management is a loop process so it's repeated over and over according to the organization needs and rules in the organization and it should be a part of risk management.
-designing:
It's also part of frameworks when the organization needs to design their management and fits with all their goals and business culture based on their needs .
-implementation:
This step after designing when the organization wants to implement the risk management on their organization and it always a officially step with identified goals and final date and needs reports.
-Evaluation:
It's used to rate the design and know what is good and what are the things that need more develop and improvement.
-Improvement:
Every organization that implemented ISO in their organization should not stop and continue improve their ISO to achieve more goals in the organization.

Processes:



After we discussed about the principles and frame works, we must mention the third category which is processes of ISO, and these process are:

-establish the context: Every organization should put their context risk assessment according to their relation ships inside and outside the organization and every organization should focus on the goals and the scope of the assessment and also focus on the factors that affect the risk assessment.

-identify the risk:
The organization should put the risks that can affect the work of the organization and also they should focus about natural risks and zero day malware because to ensure that every thing in the safe side and if one risk happened , the organization can treat it.
-analysis the risk
It is important that the organization analysis the risk and potential risk to completely identify the risk and the methods to treat them.
-evaluate the risk
After that the organization needs to asses every risk and rate them into (high damage, average or low) and the rate depends on : the amount of the damage and finical of the treat the damage.
-treat the risk
If one of the risks happens, the organization should know how to treat the risk depends on the risk management so after identify and asses the risk, the organization should know how to treat the risk and with the help of team of the risk managers.
-communication and consultation:
It's important because for example the organization can put the warning signs to tell the employees about risk for example we should put warning signs on the fuel tank to warn the employees about the risk that can affect the work of the organization.
-monitor and review
Every organization should review the risk management every period of time to ensure that still work and perfectly treat the risks.

--> **(ISO 31000, 2022)**

From all these characteristics of ISO , we can implement it and help us and the organization for many things that related to the risk that the delivato can face it in the present or future and as we know iso can manage and give us the impact of the risks but we need to implement the process perfectly and understand every concept of it to know every risk and how it will impact the system or services of delivato and discuss about if the organization accept the risk or mitigate it an so on.
So the iso the organization can:
- Know what are the risks and impact every risk on system or services.
- From know the impact , we will know the potential financial loss that will happen to the organization.
- Delivato and it's employees can handle the risk more efficiency.
- Decrease the data loss.

D.1 Security Procedures to implement in Delivato:

From my tour I recommend these procedures to implement it in the organization :

-Implement the back up to the data in the organization which is make the copy of the data and recover it when the organization needs to solve the data loss risk.
-Implement more policies in the organization so the employees and stakeholders know the guidelines and the instruction of the organization and make the information and equipment of the organization more secure, also put more polices about remote access and polices about identification, authentication and authorization.
-Some employees are not ready to hand over the responsibility of secure the data of the organization so they need training to teach them the basics of the security such as : beware of social

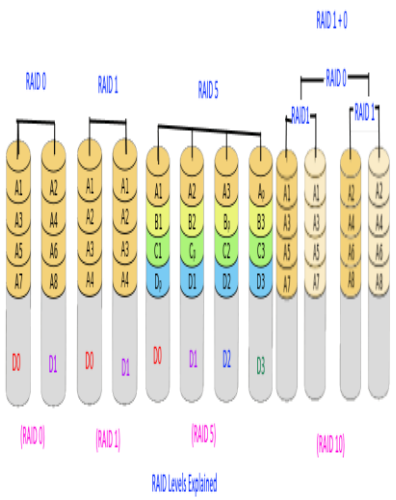
engineering ,know more about the malware, viruses, how to set strong password and secure their laptop and phones .
-Implement incident response plan which is the plan that the methods of how the organization identify and response to incident and it contains of (formating and content, storage of this plan and testing).
-Implement disaster recovery plan in the organization and it's focus on how to recover the business process that has been damaged from a disaster and make a document of the plan that contains of (disasters that the organization covered, team members and their contact of each member, business impact and continuity plan, backup and restore documentation).
-The perfectly implement a firewall to protect the organization network from any malicious intent that comes from the internet because fire wall can block the information that comes from the internet and the organization doesn't need it.

-The important information about the password and how to make a strong password that won't let any person access the employees accounts or others by knowing the characteristics of strong password , also update the password every period of time is important. And from the password, employees and users can access to the delivato system(organization system) or delivato services (organization service).
-Employees must know about physical security which is protect their devices from any theft and notice them to not write their passwords and put it in the desk, when they finish from using the laptop notice them to turn off the laptop, update their device as soon as possible and download anti-virus.

-->(10 Must Have IT Security Policies for Every Organization, 2022)

D.2 Data protection and regulation in Delivato:

First let's talk about data protection, it's the way that the organization can save their data or information from any theft or lose or any reason that can affect the data and the organization and it's divided into three categories:
-**Data protection:**
It's one of the three categories, to discuss more about it let's take an example of data protection such as:cloud backups that is really important to the organization to make a copy of their data and prevent the data loose and we should back up our data every period of time. Another example of data protection is :
Implement RAID in the organization :
Abbreviation of (Redundant array of independent disks) and it's the method that the organization store the same information in a multiple hard disks and it can be for many type .I recommended to implement hardware RAID because it's give the availability and fault tolerance because for example if one disk failure, there are another disks that have the same data.
And as mentioned above there are many types of it such as:
1.1 Raid 0-->It has at least two hard disks and the characteristics of this type is the organization can extend the size of the hard disks. But the cons of this type is there is no redundancy so of one of the two disks failure , the organization can't get the data.
1.2 Raid 1-->It has at least two disks and the characteristics of this type is redundancy so the organization can have the same



information as in the original(main) disk and the copy disk can't write it's just for read.
1.3 Raid 5-->It has at least three disks and the characteristics of this type is one of the disks must be parity so if one of the disks failure, from the parity and the exist disk the organization can get the disk failure but if if two disks failure, the organization will loss the data.
1.4 Raid 6-->It has at least four disks and it is the same as type 5 but with two parities and the organization can loose maximum 2 disks to keep working.
1.5 Raid 10-->Even number disks and the characteristics of this type is this type is combines from (0 and 1) so this type can extend the size of the hard disk and mirroring the data.

--> (What is RAID?, 2022)

- **Data security:**

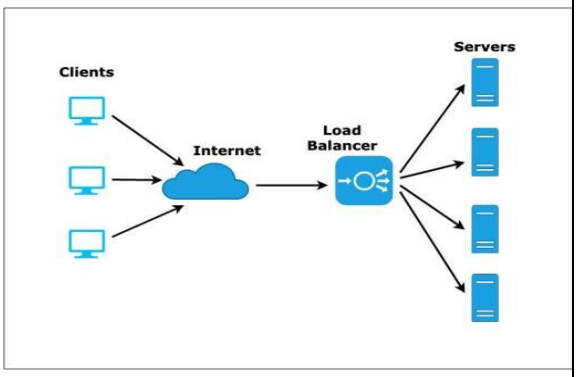
Such as : Always encrypts the data, and that's mean the data will be unreadable and any person will not understand the characters so it's will help the organization to save their data and save their customers information from the hackers or theft and make the data not benefit to the hackers and thieves because it is unreadable and in addition the delivato must encrypts all their data states (stored, transfer, use). The only thing that can decrypt the data is the key that specialized to decrypt the data so it is important to save and protect it.

-->(What is data encryption? Definition and related FAQs | Druva, 2022).

-**Data privacy** such as the policies of the organization that discussed previously.

Recommended:

Also I recommend to implement Load balancer in the organization



It's specialized and worked in the front end (user interfaces) and it's function to divides the users that want to access the organization web site to several servers have the same content and it helped to decrease the pressure of the servers and to satisfy the customer that access the organization website because it gives the speed of the website.

--> (Load balancing (computing) - Wikipedia, 2022)

If we are talk about data protection, we must mention something called GDPR which abbreviation of general data protection regulation ,and it is a law that contains of rules to protect the data of the company and users and it approved by the Europe parliament in 2016. In this law there are requirements and every country in the Europe must implement these requirements because it benefit to protect all the information about users and organization, some examples of the requirements: hide the collected data to provide the best privacy, some organization need to hire a employee that will track this law compliance and more requirements.

So from this law, delivato needs to hire a employee to track the compliance and that's called "data protection officer ", notified and trained the employees to the importance of the data and the steps to protect it, implement all the policies and procedures and make a punishment to the employees who ignore the policies, the steps of how to provide the best security to the most important data (users, delivato) and ensure that these data are not easy to reach by any employees who want to steal it or attackers. Also, the organization must know every update of this law because every time the law updated and put new requirements.

By implementing processes and regulations, delivato will become more secured and more reachable to it's goals so it's important to know and implement these two concepts and know what are the roles of it to secure the data.

--> **(What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019, 2022)**

D.3 Audit and it's impact to delivato :

I don't think that any organization doesn't have a security audit in this century because it's played an important role in the organization for many things like : help your organization to defend your data in the organization and prevent any kind of unauthorized access and theft the data, detect more about your organization and what is the strong security and weaknesses security in your organization and make a solution to overcome these risks by many methods such as ask for increasing the policies and it also help your organization by monitor the work of the strategies that are in your organization.

It's important in the organization because :

-The organization can know what is the current situation of it's security and if it's security still safe or needs more procedures or tools to treat the risks and attackers and from the audit the organization can see the audit report and know what is the weaknesses of the security and absolute treat them and also know the strong security to develop more and prevent the new risks or malicious that might be found after period of time.
-Know more about the results of the polices and procedures in the organization and know if it's useful and enough to the organization or needs more or maybe needs some changes.

-Also let the organization know if the employees has trained and have the awareness of the security process and polices and also know if the practice awareness that the organization gives to the employees are helpful enough or need more changes.

-Also to let the organization know if the plans of the organization (incident, DRP, BCP) are work and know if the organization are really ready to any attacks against any kind of the attackers and ready to protect the organization.

-Also the organization can improve more an more not only in the detect the risk , it also help to improve the the policies and more than one aspect in your organization.

--> **(10 Importance of Information Security Audit | ZEVENET, 2022)**

So I recommend to auditing the security in Delivato organization for many reasons:
-Ensure that the devices, rooms, network devices of the delivato are more secured than before.
-Find a new risks that make the organization in danger and over come it.
-Ensure from the policies in the organization if it good or need more.
-Ensure form the work of the strategies that are in your organization (DRP,IRP,BCP).

F- Design policies for Delivato :-

As I discussed before, Delivato needs more policies to implement it in their organization to avoid any threats that can affect the organization, so I decided to make a groups and each group has some policies, and I warning that the polices must be up to date to be valid in the company.

-**Group 1 :**
Policies that **related to the employees in the Delivato**, and as we know in delivato there are many risks that the employees do and we need to reduce these risk. This group is scoped for all the employees worked in the organization

* We know that most of the employees have a disk, so it's important to not put any important data that related to the organization or employee in the desk or put any data in the trash.For example of important data : password of every employee.
* After all the employees finish their work time, the doors must close
* Turn off all employees devices after they finish work.
* I recommend to use the locks on the organization devices.
* Employee must not used any CD, DVD.
* Employees must update their device and the auditor must check.
* Install anti-viruses and update it every period of time.
* Not access to unsure wifi such as the open wifi.
* No smoke in the area of the organization.

-**Group 2:**
Policies that the **Delivato should do and implement it in the organization** to prevent any kind of risks.This group is scoped to all the managers of the organization and every manager should know these policies.

* Put the best locks as shown in the previous sections on the important rooms such as: server, network, data center, shipments, and so on.
* Put the cameras on the delivato corridors to monitor all the employees moves and know all the unfamiliar faces that enter the organization.
* The auditor must check the system and services of the organization every time such as : the temperature in the server room and network rooms.
* Delivato must monitor the VPN and the employees that have access to the VPN .
* Delivato must always do a backup to save all the delivato data such as the data that in the cloud.
* If Delivato use DVD , CD , and USB, Delivato must store them in a secured way.
* Delivato must train their employees to avoid any social engineering.
* Delivato must encrypts their data,employees data, customers data that are in the cloud or in the organization and encrypts all the data states (stored,transfer,use).
* Managers should monitor the employees in the work.
* Delivato must put passwords on networking devices such as router, switch and others.

* Delivato must provide a maintenance schedule of the network devices, equipment, their website and so on.
* Use security tools in DNS to protect from any attacks such as man of the middle and others.

- **Group 3**

This policies are **related to the password policies in the Delivato** and how the password must be. This group is scoped for all the employees, managers and all the individuals that worked in the delivato. The characteristics of strong password are:

* The length of the password must be at least 8 char,numbers,and others.
* It must have a capital,small letters, numbers and symbols.
* Avoid any common password such as : 123456789, password , and others.
* Try to make a strong password that can't for everyone to access the account.
* Update password after every period of time.
* Implement multi factor authorization to ensure that the employee or users access his account not any one else.
* Prefer not to use the personal information to put a password.
* Employees must not share their passwords to any person even if it was manager.

-**Group 4**

This group **is related to the VPN access** and . This group is scoped for all the employees in the delivato , third parties to know the policies and instructions of VPN access of Delivato.

* Implement firewall and must be up to dates.
* Required Anti virus and must be up to date.
* Required Windows up to date or any operating system.
* Required Secured VPN application and must be up to date to connect the VPN .
* Implement username and password to access the VPN and after the employees or third parties access, the system will ask about 2FA (two factor authentication).
* Encrypts any VPN connection to avoid any attacks.

-**Group 5**

This group **is related to the firewall**, and know how firewall must work and manage the traffic and the help the organization to prevent any attacks.

* It must be block any private IP address that comes from the internet such as 192.168.N.N , 172.16.N.N ,10.N.N.N .
* Allow the most common IP protocols to enter such as : TCP,ICMP, UDP and others.
* It must block any traffic that has a wrong source and destination because it maybe caused malware, spoofing and others attacks.
* Also block the traffic that have the ip source routing information.
* It must block the traffic that has broadcast address to directed inside the network.
* Make the security employees to put the specific rules when they configured the firewall.
* Firewall must also has the ability to use and handle IPv6 address in the Delivato.
* Also it must block any unwanted and malicious traffic .
* Prefer to implement firewall technologies to become more advanced such as allow or deny the traffic based on user identities.

- **Group 6**

This group is related to the website that the delivato has. These policies help the website to prevent any attacks or errors.

* Every period of time, the website must be developed and maintenance it perfectly to avoid any attacks.
* The information of the users must be encrypted and away from any unauthorized access.
* If identified any unauthorized access to steal the customers information, the attacker will punish under relevant cyber security laws.
* The user must communicate with the customers support if any one accessed his account to prevent any steal and to change the password.
* If any document or data upload to the website, it must be authorized by the officials in the Delivato.

--> (Biswas and Biswas, 2022)

F. Security impact of misalignment polices:

So this is an important section to talk about, polices are important and compulsory to implement it to all the people in the organization if he an employee or manager or user because if there is any kind of misalignment in the organization by the user or employee, this will affect the organization by many things such as :

-First the data of the delivato may be under the danger because if any employee didn't follow the policies , he might send the users data or sensitive information of the organization to others people or organizations and make the delivato under legal threats because of disclosure of users information.

-If the employees didn't follow the policies it will decrease the security system in the delivato and become more easier to the attackers to access the delivato and steal the data because from the policies cover all the aspect of the organization to keep it safe.

-So in general of the previous examples , it impact--> weaknesses in the CIA in the organization (By the way CIA are confidentiality (prevent the unauthorized access), integrity (check if the data not changed), availability (trying to make the computer system more protect from any attacks)).

-Also it cause weaknesses in handle the process of the plans such as : DRP, IRP and others when any risks or attacks come to the organization and that's will make the organization in danger of continue the work and damage in financial situation .

- Decrease the percentage of the organization that can achieve the security goals of the organization for example of the security goals: the organization set a goal that is decrease the percentage of the identifying the risks in the organization system, so if the employees didn't follow the polices, the organization can't improve and develop and achieve the goals and also it decrease the reputation in the labor market.

After all these impacts, I recommend to put punishment to all the employees who didn't follow the polices and punishment should calculated according to the polices that the employee didn't follow and in many cases the employee should kicked out of the organization because any mistake or not following could harm the organization in many factors (finical, government, security , economic and others).

--> (Sisney, 2022)

G. Tools that help delivato :

There are many tools that helped in the security in the organization and delivato needs to implement it to protect the organization from any attacks or risks that may make the organization In danger, I will recommend some tools that will help:

- Network access control (NAC)

In the policies above, I mentioned that the organization should protect their network from any attacks, and this tools will help the organization by the organization will allow the security policies to the users and that's will make the organization knows from where and who is the user that login to the system and also know if the user device is protected well or need for example antivirus and so on by the user give the permission to the organization to know.

For examples of these products: **Aruba clear pass policy manager and fore scout.**

-DNS protection

Also we should focus on DNS and make sure that every thing is doing well because there are many attacks that aimed on DNS and weak configuration on it. These tools will protect the organization and users by making sure that the users are not connecting with any bad actors or any malware websites and his faith is connecting with the organization website and steal his information and make the user in danger.

For example of these protections and do the function: **Cisco umbrella**.

-End point protect

As I discussed before about the devices of the employees in the organization and the impact of it to the organization. These tools are usually combine between antivirus, malware, IPS to protect all kinds of attacks and make the files or employees information in danger .

For example of these protections:**ESET security** (contains some features: antivirus, malware, filtering web, firewall and others).

-IPS
Often it used behind the firewall because it used to filter the traffic and prevent all the malicious data. Also it contains of the work of IDSs and it's function to check the networks and providing reports of the risks.

Examples of these protections: **cisco next generation Ips**

--> (Vijayan, 2022)

H.Roles of stakeholders (implement security audit) :

After the delivato take the recommendation about the security of the organization and the evaluation all about the security such as the the security components of delivato from the auditors, the delivato need to implement these recommendation and take his evaluation to improve the security.

Also I should mention more about stakeholders and they are the persons that contribute to the delivato and it's performance.For example: employees in the delivato,users , investors and so on.

There are many stakeholders that are contribute to implement the security audit that come from security auditors such as:

-Employees in the delivato are responsible to implement the orders that comes from CEO of the delivato that related to the security audit to prevent any security issues that may happened to delivato. Employees are divided into many types:
***General employees**:
I called them general employees and it's the kind of the employees that are not related to the security of the delivato and their responsibilities in the implementation the audit is to implement the recommendation and policies that related to the physical security such as close the doors of the delivato if there isn't any body in the room and so on.
***Employees that related to the security**:
There are the group that specialized in the security field of the delivato and their responsibility is to implement the recommendations that related to the security field such as : networks rooms , servers, datacenter, network equipment that come from the auditor to prevent the attacks or security issues ,also another responsibility is to do the delivato policies recommendation like every body in the delivato.
***Administrators**
Also they must implement every things very efficiency because they responsibility to make the network devices, network security in the organization, systems, solve all the errors that happened in the organization services such as website and so on to best secure to reduce the risks and impact of it. So they must do every thing that the auditor tell to be on the safe side and make the organization secured from any attacks.
-Managers of the delivato
Manager played an important role in the security fields because one of the their jobs is to monitor and track the employees work and noticed if any suspicious in the work, so managers will give the security recommendations from the auditor and make the employees to implement it in the

organization.Without the managers,maybe the employees will implement the recommendations but not very efficiency and well secured and with managers, the employees will implement it very efficiency because the managers will always track their work and moves.Also managers considered as the decisions maker and responsibility in delivato.
-Other organizations
I mean here, if the delivato appoint other organization to do something that will help the delivato such as maintenance of the organization and others. The other organization should implement the recommendation from the auditor to get away from any mistakes and do the job in perfect way.

--> **(Stakeholders, 2022)**

I . Disaster recovery plan :

First let's know thee concept of DRP, it's a plan contains of many components and it's function to help the organization how to continue the work after faced a unplanned risk and return the functionalities of the system in the organization, and it's considered a part of BCP (business continuity plan) in the organization. DRP has many types to use it in any organization such as : cloud recovery plan , datacenter recovery plan and others.

To discuss more about DRP, we must mention components of it:
-**Assets of the organization:**
It's the first step to make it, and the delivato must make a map of all the assets of the organization to see what are the things that needs more protection and also can assets the potential risks. This component is important because it's give the overview of the situation of the delivato.
-**Scoop**:
Every organization in the world are threatening to face multiple of risks that may affect the organization so for this reason the organizations made this plan and the first step is the scoop where every organization need to identify the scope of the DRP to cover the incidents. So delivato must identify it's scoop and I recommend to cover cyber security attacks and natural disaster to focus on these risks to educe the affect of these risks if it happened in the delivato.
-**Team that is responsible in DRP:**
It's the team that are trained in this cases and situation and the team is responsible to return the key services of delivato and return the work of the system of the organization after the incident to return delivato to it's natural situation.Team will help the delivato to try to overcome the risks if happened and prevent any data lose.
-**Specific training:**
Delivato must training the employees before any incident happened to know their responsibility and what they should do when the risks happened to overcome and return to the natural situation so it's important to train the employees.
-**Secondary location**:
The delivato need to put the copy of the data in another location and restore it when it needed to ensure that there is a copy if something happen to delivato such as : big fire in the organization, so in this case the organization must put copy of their data on another place to continue the work.
-**RTO and RPO**:
It's important to talk about the two concepts in DRP, for the first concept means the time that the organization wants to recover and return to the natural situation (RTO), and the second concept means how much data does the organization lose when the risk happened (RPO). So the delivato must needs less amount of RTO and RPO to prevent any big issue so the organization must know about these two concept.
-**Back up:**

It’s important that the delivato must check the back up every time to ensure that every thing is good and put the backup in place that are away from any kind of corruption or theft.

-**Testing:**

After all the process of making the plan, also must tested it and review to check if the plan is really work and helpful to the organization or needs to some changes and ensure that every employee in the delivato needs to know what to do and the role and responsibility if something happened to the organization.

After all these components in the DRP, the organization will increase the probability of the protect data by be ready to overcome any thing that will affect the data or company.

--> **(What is a Disaster Recovery Plan (DRP) and How Do You Write One?, 2022)**

References:

User, S., 2022. *5.5 Methods for risk assessment*. [online] Cdema.org. Available at: <https://www.cdema.org/virtuallibrary/index.php/charim-hbook/methodology/5-risk-assessment/5-5-risk-assessment-methods> [Accessed 12 June 2022].

360factors.com. 2022. *Five Steps of Risk Management Process - 360factors*. [online] Available at: <https://www.360factors.com/blog/five-steps-of-risk-management-process/> [Accessed 12 June 2022].

Iso.org. 2022. *ISO 31000*. [online] Available at: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en> [Accessed 12 June 2022].

Adsero Security. 2022. *10 Must Have IT Security Policies for Every Organization*. [online] Available at: <https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/> [Accessed 12 June 2022].

SearchStorage. 2022. *What is RAID?*. [online] Available at: <https://www.techtarget.com/searchstorage/definition/RAID> [Accessed 12 June 2022].

Druva. 2022. *What is data encryption? Definition and related FAQs | Druva*. [online] Available at: <https://www.druva.com/glossary/what-is-data-encryption-definition-and-related-faqs/> [Accessed 12 June 2022].

En.wikipedia.org. 2022. *Load balancing (computing) - Wikipedia*. [online] Available at: <https://en.wikipedia.org/wiki/Load_balancing_(computing)> [Accessed 12 June 2022].

Digital Guardian. 2022. *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*. [online] Available at: <https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection> [Accessed 12 June 2022].

ZEVENET. 2022. *10 Importance of Information Security Audit | ZEVENET*. [online] Available at: <https://www.zevenet.com/blog/10-importance-of-information-security-audit/> [Accessed 12 June 2022].

Biswas, P. and Biswas, V., 2022. *Example of Website Security Policy*. [online] PRETESH BISWAS. Available at: <https://preteshbiswas.com/2020/02/06/example-of-website-security-policy/> [Accessed 12 June 2022].

Sisney, L., 2022. *The Misaligned Organization and What to Do About It - Organizational Physics by Lex Sisney*. [online] Organizational Physics by Lex Sisney. Available at: <https://organizationalphysics.com/2012/02/10/the-misaligned-organization-and-what-to-do-about-it/> [Accessed 12 June 2022].

Vijayan, J., 2022. *10 essential enterprise security tools (and 11 nice-to-haves)*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3310247/10-essential-enterprise-security-tools-and-11-nice-to-haves.html> [Accessed 12 June 2022].

Wgtn.ac.nz. 2022. *Stakeholders*. [online] Available at: <https://www.wgtn.ac.nz/cagtr/occasional-papers/documents/investigation-3.pdf> [Accessed 12 June 2022].

SearchDisasterRecovery. 2022. *What is a Disaster Recovery Plan (DRP) and How Do You Write One?*. [online] Available at: <https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan> [Accessed 12 June 2022].

THE END

Made by : Hamza Muhsen