Reduce damage to organisations essay sample

Stealing intellectual property is basically when someone steals images from your website or other information and uses it on their own site without your permission.

This is known as breaking the copyright law and works with logos as well and new ideas for new products as well.

This can for example include; patents and trademarks as well as domain names. If a person is caught they can be given a significant amount of fine and eventually a prison sentence as well.

The fine is £5000 for access and unlimited fine for modifying data.

Denial Of Service Attack

Denial of service attacks is basically when a particular person restricts access to a web page or network.

It basically stops legitimate information to get through to the server and stop legitimate service to respond.

This will make customers go to other websites and the company that has been attacked by this lose crucial customers and a significant amount of money as their website is not responding.

This is done by a particular person sending lots of blank server request which overloads the server/system and it stops getting a request.

Halting E-commerce Transactions

If for instance a particular person hacks into a website they can basically stop transactions so that the organisations lose customers and money.

They can also play around with the website and remove products that are on for sale by a particular organisation or even re-price them to ridiculously high price or even lower price.

This can cause a lot of problems for both organisation and customers.

If the security is removed or changed the hackers will be able to intercept customers card details.

If the card details were to be intercepted by a hacker they will be able to commit fraud crimes which can cause a lot of problems for both the organisation and the customers.

Preventing Technologies

One of the technologies that can be used to protect an organisations' computers is by simply using firewalls.

By using firewalls it will prevent intruders from getting into the organisations' computers.

It works by checking the filters that are coming through the network or internet and if they are malicious it will block them from entering your computer but if they aren't dangerous it will let it through to the computers.

Another technology that can be implemented by an organisation is antivirus, malware removal tools and spywares.

By using the above software’s an organisation can prevent viruses from getting into the computers, as viruses are used by people to hack into the computers and are used more to cause damage to the computers.

By using antivirus software such as Norton Anti-Virus and scanning regular the organisation can catch and remove viruses from the computers.

Malware can basically corrupt files on the computer so if the organisation don’t have a malware remover it will lose important files and if they are not backed up the organisation can lose money and customers as well.

By using malware remover and scanning regularly, a company can simply search for dangerous files on the computers that will corrupt the file and remove them.

Spyware is used to steal personal details such as online shopping details (credit/debit card, online email username and password details. Spyware can also log people’s password and send them to the hackers.

By using spyware remover and scanning regularly the company can remove spyware from the computers and keep it safe from being controlled by the hackers.

As for website protection a particular company can make their website read-only and disable right clicks on their website so no one can steal information and images from the website. Another way is to put copyright marks on the website as well as implementing the Hypertext Transfer Protocol Secure (HTTPS)

A company can also implement a CCTV in the server from where all the crucial information is stored. And perhaps have security locks on the doors. Only authorized staff should have permission to enter the zone.

Another technology an organisation can implement is swipe card door technology.

An exception is Microsoft Vista which is designed to prevent external attacks and is self-protecting and healing.

Disaster Recovery

Disaster recoveries are basically methods which can be put in place to recover from any disaster such as virus attack, fire, earth quakes, explosions, flood, hardware failure, power failure and sabotage.

As you can see below are the main ways to recover from disasters:-

It is crucial to make regular backup of the work and place the backups in a remote location where no one knows where it is and it is far away from the building so if the building goes on fire nothing harm will happen to the data. A good alternative is to upload the data to an external server which is located in a different place/building.

Data should be backed up regularly and normally at the end of the working day.

A particular organisation can invest in a backup server which could be located in a different country. All the data could then be backed up electronically.

One backup a day is not enough. It would be too risky for a company to backup once. So twice or more a day is necessary.

Another alternative is investing in some special designed CDs for backups or special made storage devices. A lot of data can be backed up with CDs and storage devices. Depending on how many of these the company invest in, they could save a lot of money by using this method.

If all of the steps above are taken into consideration the company will save itself from disasters recover as recovering data can cost a significant amount of money. It would cost around £600 for the data to be recovered which not 100% guaranteed.

A company can set up a system which allows real time copy which can be swapped if necessary.