LEADERS WHO MAKE A DIFFERENCE: JOEL KLEIN BRINGS ACCOUNTABILITY TO NYC DOE: DAY 1
LEADERS WHO MAKE A DIFFERENCE: JOEL KLEIN BRINGS ACCOUNTABILITY TO NYC DOE: DAY 1
P1 and M1

In this assignment I will be explaining security threats which could impose on IT systems and how it could impact organizations. As well as this I will be explaining how organizations can also keep their systems and data secure.

TheCaseSolutions.com
P1- Malicious Damage

TheCaseSolutions.com
Internal malicious damage can be both from accidents and attacks. Internal malicious damages happen within the business/company. Internal accidents that could occur could be employees within an E-Commerce site copying important information from a database table into an email for troubleshooting purposes and accidentally include external email addresses in the recipient list. To support this a 2012 study has showed that 51% of employees duplicate confidential information with a company printer.

However, sometimes employees don't make a mistake. Employees use their access and privilege to damage their company they work within, they often can sell the information on the black market to infiltrators who work for outside intelligence.

This is a news article which shows how a Starbucks employee takes advantage of personal customer information. She uses the advantage to make a copy of a customers card which she later on uses to buy groceries.
External

External malicious damage can also be both from accidents and attacks. External damage happens outside of the business/company. An example of an external accident is a power cut of a server that stores software licenses for other servers. Without licenses, data backup software may not function at its scheduled time meaning the database open to irreversible corruption.

The most common and worst external attack is from skilled hackers. Computer hackers are able to find network vulnerabilities or socially manipulate insiders to get past a number of outer network defenses. Once they get past the network defenses hackers are able to steal important information which makes the business lose information and data.

This is an example of an external malicious damage. Hackers were able to gain access within the phone company Orange and steal 1.3 million of orange customers personal mobile data.

TheCaseSolutions.com
Access Causing Damage-VirusesTheCaseSolutions.com

Access causing damage is where a computer virus has been targeted at specific computer programs. Because it has targeted specific programs this prevents them from downloading/opening up and it sometimes even directs a user to another service. This type of attack is commonly done on users internet browsers.

The most common way to prevent a virus is using an anti-virus software. These are used to find any viruses and try to get rid of them. Before doing this, the software tries to detect if there any there first, if the software does find one it will notify the user to ask what you would want to happen to it. It is important for users to keep updating and checking for viruses because they could occur very quickly.
**Access Without Damage**

**Phishing**
Phishing is where someone tries to obtain another person's personal information such as website details, bank details and many more. Users are likely to get an email in their junk mail asking for bank details which users should not give out. Because these emails look like legitimate company emails users are likely to trust them and enter their personal information.

[Image: Example of a phishing email]

**Piggy Backing**
Piggy backing is the name used for when an intruder tries to use someone's wireless without them knowing. If a user is wireless is secured with a weak password it is very likely and easy to break into. From this it slows down a user's internet and the person 'piggy backing' on the wireless can download illegal software so that it cannot be traced back to them.

**Hacking**
Hacking is where a person is able to break codes and passwords to gain unauthorized entry to computer systems. A lot of hacking cases have no specific fraud intent yet just enjoy the challenge. Yet, a lot of hackers do have the intent to commit fraud, steal personal data/information. Passwords are a popular way to prevent any hacking. Companies should make sure that their staff have their own User ID and password to gain access to the system. This reduces the risk of outsiders being able to get onto the system and damage any data. It also allows different employees to access different data.

**Identity Theft**
Identity theft is where a person steals another person's personal information and uses it. For example they could obtain someone's home address, name, phone number to be able to do multiple things such as open bank accounts etc. In big companies it is very important to lock all the doors where the servers are stored to prevent intruders from accessing the server and causing damage to it.

Identity theft is tackled under a number of related acts. These are: Theft Act 1968 such as a presumption, Data Protection Act 1998 which protects personal data, Identity Cards Act 2006 which describes identity theft, crimes and identity fraud relating to ID cards and the Fraud Act 2006 which makes it illegal to assume another person's identity.
Phishing

Phishing is where someone tries to obtain another person's personal information such as website details, bank details and many more. Users are likely to get an email in their junk mail asking for bank details which users should not give out. Because these emails look like legitimate company emails users are likely to trust them and enter their personal information.

This is an example of a phishing email, it shows how the 'bank' requires some personal information from the user in order to continue with their bank account.

http://www.freecomputerzone.com/phishing/hsicphishing-example1.gif

TheCaseSolutions.com