9/26/2016

Unit 7

Assignment 1

Simon Light

UTC Reading

Contents

[Contents 1](#_Toc462643743)

[P1 - Explain the impact of different types of threat on an organisation 2](#_Toc462643744)

[Planes taken off radar – External Threat 2](#_Toc462643745)

[Plane hijack - Physical threat 2](#_Toc462643746)

[Personal information – Social Engineering 3](#_Toc462643747)

[Profit skimming – Internal Threat 4](#_Toc462643748)

[M1 – Discuss information security 5](#_Toc462643749)

[Information Security (Discuss) 5](#_Toc462643750)

[Threats to IT Systems and how to keep data and systems secure 5](#_Toc462643751)

[Organisational issues affecting security of systems 7](#_Toc462643752)

# P1 - Explain the impact of different types of threat on an organisation

In this section I will be explaining some threats to a particular industry and the impact that that could have on the business/industry. An organisation that would be massively affected by an attack would be the aerospace industry. In particular, I will be looking at the commercial, people carrying flights and the businesses surrounding them.

## Planes taken off radar – External Threat

Planes being taken off of the radar is a very real and common threat to this industry. One example of this is the Malaysian Airways flight 370 (MH370/MAS370) which went missing March 2004. It lost all communication after issuing a state of emergency. Only parts were found and to date, no conclusion was drawn from the event. It may have been that the flight was hacked, removing its communication and therefore its known position. This could be taken a step further by not only removing the ability to send information from the plane, but also sending false information so that no alarms will be raised.

As you can tell from the examples given above, communication both to and from the ground is vital for a flight to go to plan. If either of these is taken down it can be detrimental. Some of the effects that could come from this could be a large cost to the company. These could include (in the case of the Malaysian Airways flight 370):

* **Plane** – there will be a large cost behind losing the plane. The price of an a380 (the plane that went missing) is around £305 million. There would then be the additional cost of all of the fuel and extra navigational equipment that would be on board.
* **Insurance pay outs** – the company responsible for the plane going missing will have to pay out for everything and everyone that went missing. This will be for reasons such and reimbursing the families of the people that went missing. This will more than likely total to a massive sum
* **Government investigations** – often after a large disaster, governments and 3rd party surveyors will look at the incident and the company involved to try to find the cause (to prevent it from happening again). If the company involved is seen to be the cause of the problem, such as an unfixed security risk then they could be fined a very large sum.
* **Bad press** – this type of incident will bring a lot of press along with it, often looking for drama and someone to blame. This will most likely fall onto the company involved opposed to an individual. This will the build a large stigma against the company, therefore, damaging business for the future.

This type of threat could be an external threat. This is one that is done from outside that forces privileges to people who shouldn’t have it. This type of attack often uses things such as brute force attacks and escalating privileges. This is one of the most common types of attack and requires little setup.

## Plane hijack - Physical threat

Plane hijacking is more of a physical threat to an airline. This however can be made more effective by the use of technology. This may be done by using the method above and removing communication between ground and air. This would remove the possibility of a staff member of the plane telling ground control about the threat. This would then be a more effective attack on the airline as it wouldn’t be as noticeable.

Airlines have however made this more difficult to do. Due to the fact that the threat of attacks on airlines have become more prevalent airlines often have a location reporting system in place. This is where the plane reports its position and status about the engines, fuel level etc. after a set period of time. Removing all communication to the ground would then be quite obvious to ground control as that the plane would have been tampered with in some way. They would then have some kind of backup system to communicate and retake control of the plane.

A method that could be used to stop this is spoofing. This is where one computer acts like another. This could be used to help with the hijacking of a plane. If another computer that the hackers own keeps sending the ground control fake messages about where the plane is and that it is ok, then it would be very hard to spot.

This would cause a massive impact on the airline if this happened. This would bring a lot of costs onto the company. Some of these costs would be:

* **Tighter airport security** – Tighter airport security would be required after this kind of attack. This would include the cost of X-rays, security personal, passport and visa control etc. Not only would this be a large monetary cost for the airport but it would also take longer to get onto the plane, creating a less satisfactory experience for customers, making them less likely to want to fly from that airport. Although the brunt of this cost would come from the airport, this is likely to result in an increase of cost for the airline to use the airport.
* **Tighter security on the plane** – due to the prevalent threats of a plane hijacking, there will need to be tighter security while on the plane. In the past it was quite common that children and their parents would be allowed into the cockpit of the plane to have a look around. His would have to stop due to security risks. There would also need to be a greater number of staff on the plane to help diffuse the situation on the plane. This would give a greater cost but also a worse customer system.
* **Secret flyers** – It is more common nowadays that airlines hire ‘secret flyers’. These are people that are trained in martial arts and counter terrorism that are paid to be on flights around the world. They are there to help air stewards defend against any serious threats that occur (such as hijacking). These people would be plane clothed so that they cannot be identified by the public. This would give great cost to the airlines as they would have to pay these people to fly around the world, most of the time not giving any effect. It would also mean that the airline would have to save a seat for this person meaning that they wouldn’t make the money from it. This also wouldn’t give 100% effectiveness as these ‘secret flyers’ aren’t on every plane flying.

This type of attack may be a physical attack. This is one that is done face to face or with physical force. This could be things such as forcing a network administrator to type in a password or allow access. It could also be breaking hardware so that the system is vulnerable to an attack. This type of attack is obviously very easy to track however if it is coupled with another type of attack (e.g. social engineering) then it could be made very effective.

## Personal information – Social Engineering

A massive target for hackers is personal information. This includes things such as credit card details all the way to name and address. These are all things that the airline will have to hold to complete transactions. This would mean that the airlines would have to have a large amount of security. If they don’t then it could cause a mass of effects. These effects could include:

* **Misuse of personal information** – an airline could be prosecuted due to the fact that the information would have been released to the general public. This would be done by the government and would bring a large cost. This could be both monetary cost and also restrictions on the company. This would have a long term effect and could cause many problems in the future.
* **Refunding and charges** – due to the leak of information, many people will be angry about this. A lot of them will ask for compensation and insurance as well as expecting you to try to fix the problem caused. This will almost definitely result in a large monetary outgoing from the airline which will have a large knock-on effect. This may mean that in the future the company doesn’t have enough money to complete certain developments.
* **Bad stigma** – the loss of personal information is likely to hit the headlines. This may mean that people could want to revoke their accounts with the airlines. This will make it harder to advertise to the personals making repeat custom less likely. People that have flight coming up may also cancel these in fear of loss of information.

This type of information could be used in social engineering. This type of attack is very common and often comes in the form of fake emails or phone calls. This type of attack can however be a lot more sophisticated. One example of this would be leaking fake information to a company (maybe of one of their suppliers being hacked) via newspapers/TV’s in the area of the office. This may prompt the company to make an action (i.e. change a password). This would then trigger another type of attack, maybe a key logger. This then makes very powerful attack that the company is oblivious to.

## Profit skimming – Internal Threat

Profit skimming is where a hacker redirects a small proportion of every transaction to themselves or another account. This is quite hard to spot and can create a lot of income depending on the frequency of transactions made by the company. This is quite hard to track, especially if it is sent through multiple accounts before reaching its final account.

This will often have to be spotted by an accountant as security engineers wont usually have access to transaction details of a company as it is deemed unnecessary. This leaves the company very vulnerable if the accountant is not trained to spot this kind of attack. If this happens then it will cause a lot of problems and knock-on effect for the company. These effects include:

* **Loss of money** – depending on how long it takes for the attack to be spotted, lots of money could be taken. This will then obviously have knock-on effects for the company. This may include firing/lowering pay of staff creating a less happy and therefore productive workforce resulting in a decline of business for the airline company.
* **Having to cancel plans and developments** – another long term effect on the company of having less money is that they wouldn’t be able to follow through with some of their plans. This would mean that they would let down the industry and lose custom. This would again mean that they would inevitably run into the ground or at least take a massive fall in the market.
* **Lowering standard** - due to the loss of money the standard of the company would be lowered. This may also be down to a knock-on effect from firing staff and cancelling future plans. This would inevitably lower the customers experience therefore lowering the chance of repeat custom and new custom (as un-satisfied customers would deter friends and family from shopping/flying with you).

This type of an attack could be an internal threat. This is where a staff member/someone inside the trust circle of a company either completes the attack or helps others do it. This is very powerful as they may have extra information or power that an outsider may not have. They also have the ability to complete a physical attack more effectively.

# M1 – Discuss information security

## Information Security (Discuss)

*I am going to complete this section as if setting up an IT system.*

Every company has data that they need to store. The first important decision to do with security is how highly they regard this data, in other words, how secure they want to store it. Arguably this is the most important step in information security. It is no use if you have the most secure system in the world, but all of your important data is on stored on Twitter.

The next thing to remember when setting up a secure system is the purpose of security. That is to obscure data and information from those that shouldn’t see it. This means that completely locking away the data and throwing away the key is no use to anyone. Information should be freely accessible by those who need to use it and not bale to be accessed by those who do not.

The other thing to remember is that a system’s requirements willchange. This may be due to changes in staff/positons or even due to previous attacks in certain areas. This is why it is important to have someone (a network administrator) constantly updating and monitoring the system as and when it needs to be. They should also be checking the integrity of the data and whether it is still accessible.

Constant checking of the system should be done. This can be done in methods from the network administrator checking that the password system is still in place to hiring a penetration tester to find vulnerabilities of the system. This then needs to fixed/updated so that it is no longer a risk.

The network may change hands down the line and it still should be secure when this happens. This means that there should be constant documentation of issues and upkeep of the system (similar to a car log book). This is so that if there is a new system administrator that has a new security issue, he can look it up in the system to check if it has happened before and check how it was dealt with before.

It is not enough to have a secure IT system if staff are going out on a Friday night and telling people things that they shouldn’t. This I why it is important that you keep staff fully briefed about the procedures to go through when finding risks and the new types of threats and attacks available. It is also common that employees have two mobile phones. One that stays at work that has all of the work information and details, and one that they can take home and has no company information on it. This is so that if an employee does lose their phone then they haven’t lost any secret company information that could be used to exploit the system.

## Threats to IT Systems and how to keep data and systems secure

*For each of the below threats I will explain the threats to the IT system and also give advice on how to prevent each kind of attack*

#### External Attack

**Threat to the IT system** - One of the most common types of external attacks is privilege escalation. This is where a hacker manages to log onto the system and then force his way to the top to gain root access. This then means that they have full control over the system. From there they can do anything that they want to the system including copying, deleting or damaging data on the system. This would then make the systems information open and would cause major problems for the company.

Another very common type of external attack is called ransomware. This is where a hacker would make the system unusable in some way (anything from changing login details to encrypting the entire system with high level encryption). When done via external attack, it is often forced onto the system by someone who does not already have access to the system. This could be done through a variety of external attacks from a man in the middle attack to an upload on a webpage run by the system. This would mean that the system is unusable until the requirements of the hackers are met. This may take a few weeks, ruining the validity of the storage on the system and would make those weeks of work pointless.

**How to prevent this type of attack –** This type of attack can be prevented by having a properly configured external wall and system. This include things like a firewall and making any services (such as websites or ssh/vnc) systems properly secured so no one can enter without proper permissions. This can be tested a number of ways from getting an employee to try to log in with invalid details to hiring a penetration tester.

#### Physical Attack

**Threat to the IT system** - Physical attacks, as stated above, can damage hardware. This means that there may be a downtime for either the IT system involved or just the security devices for the system. This means that the system could be infiltrated while this is happening, placing some kind of malware onto the system, damaging the integrity of the system.

Another threat associated with a physical attack is stealing of physical information. This could be in the form of company devices to the hardware that the systems actually run off. This will may give some kind of downtime to the system, however, if the hackers inspect hardware and devices stolen, they could find much more information out about the system than an external attack would.

If a system administrator is forced to give a hacker entry to the system, it is immediately at risk. This could be in the form of deleting/stealing data. There is also a chance that the hacker would leave some kind of malware on the system to keep feeding information back to the hacker.

**How to prevent this type of attack –** Preventing a physical attack requires physical security. This is things such as security guards or turnstiles at the entrance to a building. Another counter measure could also be physically securing hardware on the premises of the building. This means things such as Kensington locks. These are cables that lock a laptop to a desk so that people cannot steal them.

Another way to prevent this type of attack is forcing employees to have a work phone that they do not take home. This I so that if they lose a phone outside of work, they will not lose any company data that could be used to better create an attack on the company.

#### Social Engineering

**Threat to the IT system** - One of the most common social engineering attacks is phishing. This is where an email or phone call is sent to a person or company pretending to be another person or company. The recipient will then click a link or go to a web address. They would then give over information about the company or themselves. This would be very bad for an IT system as it would completely bypass all security systems in place to protect their passwords. This means that hackers could have full access to a company’s accounts without them realising.

Another social engineering attack is called baiting. This is where a hacker leaves a usb drive near the premises of the company they are trying to attack. An employee of the company may then pick up the usb and try to find out who it belongs to. This might be done by plugging it into a computer and looking through it. This would then trigger some malware to move onto the system and then throughout the network. This can then perform a range of problems on the system, from a small worm, to a full scale system lockdown.

**How to prevent this type of attack –** The way to prevent this kind of attack is to train your staff to spot it. They can then report it to a senior authority who can then send it through a firewall. This can then mean that no other staff members will get that email, lowering the likely hood of an attack. It is also very important to keep staff up to date on some of the newer attacks so that they are also aware of them.

#### Internal Attack

**Threat to the IT system** - A common reason for an internal is revenge. This could bring any kind of attack and could involve more highly skilled accomplishes. This could cause great consequences for the company. This could range from DOS attacks all the way up to encrypting an entire system. This could give effects from a few hours’ loss of internet connection to an unusable system that would take years to unlock. This would be devastating for the system and depending on what kind of backup system I in place, all data could be lost.

**How to prevent this type of attack –** There are two ways of stopping this kind of attack. The first is by having full profiling of staff members before they get the job. This means that you first of all lower the possibility of having an attack (as they haven’t shown any sign of it in the past) and also if three is an attack, it will be easier to stop the person doing it.

The second way is by keeping the security system up to date. This means that when people leave, you remove their account from the system as well as all of their privileges. This means that if an ex-employee decide that they want to make an attack, it will be harder for them. This may make them decide that they not want to commit the attack anymore.

## Organisational issues affecting security of systems

In this section I will explain some problems that organisations give to security.

#### Management not understanding threats

One problem is if management does not have full understanding on problems that face the company. If there is an attack occurring management may decide to place people on non-important tasks that will not stop the attack. This may mean that the attack is successful. This may then cause more work for the network manager and may cost them their job.

#### Understaffing

If there are not enough staff to control an attack it may be a problem. This could then cause the attack to be successful and therefore take down the system. There then may not be very many staff to fix the damage made by hackers in a reasonable amount of time. This then may cause knock on effects that users may not be able to use the system until it is fixed.