9/26/2016

Simon Light

UTC Reading

Unit 7

Assignment 1

Contents

[P1 - Explain the impact of different types of threat on an organisation 2](#_Toc462231842)

[Planes taken off radar – External Threat 2](#_Toc462231843)

[Plane hijack - Physical threat 2](#_Toc462231844)

[Personal information – Social Engineering 3](#_Toc462231845)

[Profit skimming – Internal Threat 3](#_Toc462231846)

# 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.

## 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.

## 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.

## 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 to spot this attack; lots of money could be taken. This would have been expected by the hackers and so would be made hard to track by passing through many accounts.

**Having to cancel plans and developments** –

**Lowering standard** -