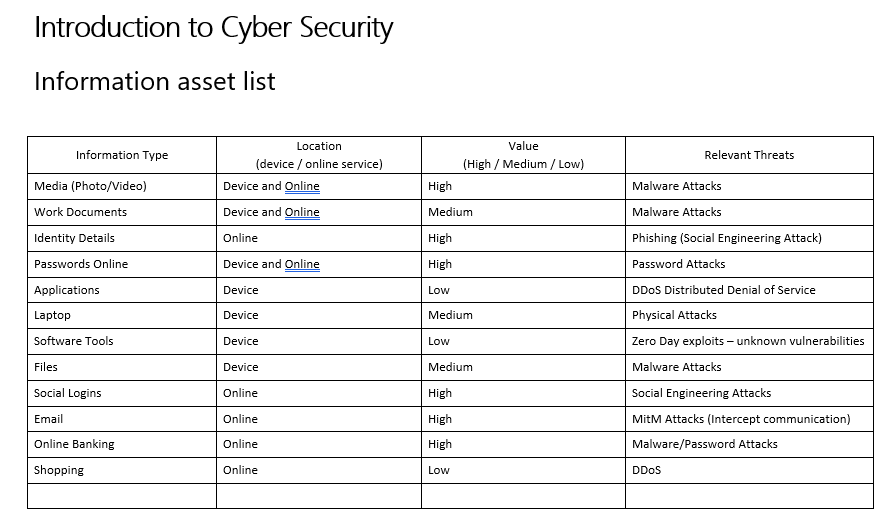
**CS6501: Risk Management Exercise**

Qualitative Risk Management

Compile a list of information you store on your personal computer or online using the provided information asset template from the Open University, which I will make available as a separate document. For example, you may have personal correspondence, photographs, work documents or personal details such as an identity document, insurance policy details and passwords for online services.



For each type of information, think of its value to you. Label the most valuable types of information as ‘High’, the least valuable as ‘Low’ and those that are in between as ‘Medium’.

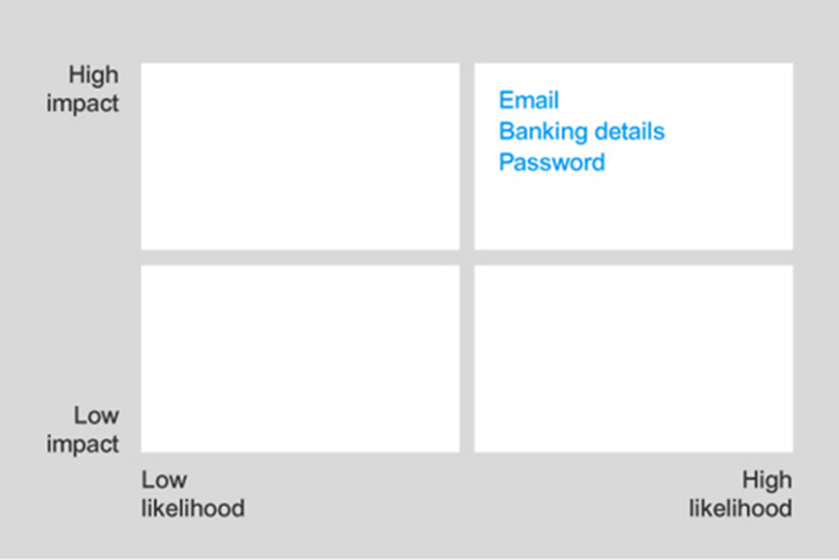
The value could be the cost to replace the information, in time or money, or the impact of its loss on your reputation, for example, all your emails or photographs could all be published online.

Do the same exercise for the online activities you engage in. For example, you might use online banking, shopping or social media. This time, label each one with a value based on the potential cost of an unauthorised person gaining access to it.

The main technique for a qualitative analysis of risk is to construct a likelihood–impact matrix in which the likelihood and impact of each risk event are assessed against a defined scale and then plotted on a two-dimensional grid. The position on the grid represents the relative significance of each risk. The simplest matrix is formed by classifying both likelihood and impact as either high or low, which leads to a 2 by 2 grid. This basic classification of a high or low value leads to the following rank order for tackling risks:

1. high-impact, high-likelihood risks  
2. high-impact, low-likelihood risks  
3. low-impact, high-likelihood risks  
4. low impact, low-likelihood risks.

By way of an example, assume that when you compiled a list of information stored on your personal computer or online, you identified email correspondence, banking details, and password information as information assets. Any successful attack on email, banking details and password information likely will have high impact and there is a high likelihood that these attacks will be targeted due to their high value. So, they should go in the high impact-high likelihood box.



Media (Photo/Video)

Identity Details

Social Logins

Online Banking

Shopping

Work Documents

Files

Applications

Software Tools

Laptop

Populate the impact-likelihood matrix with your identified e information assets.

Low-impact, low-likelihood risks are probably not worth expending much effort on. You can then look at the high-impact or high-likelihood risks one by one to determine whether there are ways either to reduce the impact if the risk occurs or to reduce the likelihood of the risk occurring, or both.

Quantitative Risk Management

1. The following threat statistics have been gathered by a risk manager. Based on these calculate the ALE for each threat:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat** | **Cost per Incident** | **Occurrence Frequency** | **SLE\*ARO** | **ALE** |
| Software piracy | $600 | 1 per month | 600 \* 12 | $7200 |
| Computer virus / worm | $2,500 | 1 per month | 2500\*12 | $30,000 |
| Information theft (hacker) | $3,500 | 1 per 3 months | 3500\*4 | $14,000 |
| Information theft (employee) | $6,000 | 1 per 4 months | 6000\*3 | $18,000 |
| Denial-of-service attack | $11,000 | 1 per 2 years | 11000\*0.5 | $5,500 |
| Laptop theft | $4,000 | 1 per 5 years | 4000\*0.2 | $800 |
| Web defacement | $1,500 | 1 per 2 years | 1500\*0.5 | $750 |
| Fire | $500,000 | 1 per 10 years | 500000\*0.1 | $50,000 |
| Flood | $300,000 | 1 per 15 years | 300000\*0.066 | $20,000 |

2. Using the figures you calculated above, determine the relative ROSI (return on security investment) for each of the same threats with the following controls in place. Copy the values in the ALE column in the table above to the ALE1 column below.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Threat** | **Cost per Incident** | **Occurrence Frequency** | **Control** | **ALE1** | **ALE2** | **Control Cost** | **ROSI** |
| Software piracy | $500 | 1 per 4 months | Anti-piracy protection hardware | $7,200 | $1,500 | $15,000 | -$9,300 |
| Computer virus / worm | $1,300 | 1 per 5 months | Anti-virus | $30,000 | $3120 | $5,000 | $21880 |
| Information theft (hacker) | $2,000 | 1 per 3 months | IDS | $14,000 | $8000 | $30,000 | $1000 |
| Information theft (employee) | $7,000 | 1 per 18 months | Access Controls | $18,000 | $4666.66 | $10,000 | $3333.3 |
| Denial-of-service attack | $4,000 | 1 per 10 years | Firewall | $5,500 | $400 | $15,000 | -$9900 |
| Laptop theft | $5,000 | 1 per 10 years | Physical security | $800 | $500 | $25,000 | -$24700 |
| Web defacement | $1,500 | 1 per 5 years | Firewall | $750 | $300 | $15,000 | -$14550 |
| Fire | $75,000 | 1 per 10 years | Insurance | $50,000 | $7500 | $30,000 | $12,500 |
| Flood | $50,000 | 1 per 15 years | Insurance | $20,000 | $3300 | $30,000 | -$13,300 |

Grouping Controls

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control** | **Threat(s)** | **Savings ALE1 – ALE2** | **Cost of Control** | **ROSI** |
| Firewall | DoS, Web defacement | 5100-450: $4,650 | $15,000 | -$10350 |
| Insurance | Fire, flood | 42500-16700: $25,800 | $30,000 | -$4200 |

3. Remember that a single control may affect more than one threat, and you need to take this into account when calculating the ROSI. Based on your calculations, which controls should you recommend be purchased? Briefly justify your answer.

*Controls to be purchased:*

*Purchasing the below controls will mean the company’s net profit will be higher than sales revenue. Indicating the company is operating at a profit covering expenses for these controls. Where the cost of the other controls will lose profit.*

**Computer virus / worm**

**Information theft (hacker)**

**Information theft (employee)**

**Fire**