Week 3: Approaches and Procedures for Risk Assessment

Welcome to this lecture (slides with voiceover) on approaches and procedures for risk assessment. These are the two main approaches to be taken in the process of security and risk management. In this lecture we will be looking at these approaches as well as assets and their value, and identifying best practices for risk assessment. In this first lecture on approaches and procedures, we will focus on the 'quantitative' approach and asset values and the second lecturer to follow on later will cover 'qualitative' approaches.

Let us re-cap on the previous lecture where we highlighted the purpose of risk analysis and assessment – that it is a process for measuring and quantifying risks to assist with security and risk management. The process includes an investigation of an environment to identify any risks and then evaluate each of the threats for the likelihood of them occurring and the potential impact both financial and reputational for an organisation. This process is focussed on understanding the risk in order to then evaluate any potential countermeasures/safeguards for the cost benefit analysis; the likelihood of the countermeasures being a success as well as the implementation requirements that are needed for the countermeasures.

In order to understand risk, it is essential to be able to identify and evaluate potential threats to assets and we have seen previously that this is not an easy task as many of these are difficult to identify. We also know that an asset is something that has any value to the organisation and the cost versus benefit in the provision of countermeasures is an essential part of the risk analysis and assessment processes. To identify threats and vulnerabilities, it involves creating an exhaustive list of all the organisation's assets and these are recorded in an 'Asset Register', and this will include both the 'Physical' and 'Data' assets. Following this, a list is drawn up of all possible threats for each of the assets within the organisation and this is a lengthy and arduous process. This list should also include threat agents as well as threat events. These details and findings may all be recorded in a single document although quite often the asset registers tend to be kept separately.

According to Darril Gibson (the author of the core module text), the steps to take in a risk assessment are as follows.

Firstly, it is important to select the appropriate risk assessment methodology and before progressing, two preliminary actions should be taken; firstly '*to define the assessment'* and secondly *'review any previous findings'*.

So here are the steps to be taken:

- Identify assets and activities to address
- Identify and evaluate relevant threats
- Identify and evaluate relevant vulnerabilities
- Identify and evaluate relevant countermeasures
- Assess threats, vulnerabilities, and exploits
- Evaluate risks
- Develop recommendations to mitigate risks
- Present recommendations to management

We will now look at the different approaches to risk assessment; 'Quantitative' and 'Qualitative'.

The main approaches to risk assessment are 'quantitative' and 'qualitative'. Quantitative risk assessment assigns real monetary figures to the loss of an asset. The process starts with asset valuation and threat identification, then the potential and frequency of each risk is estimated. All this information is then used to calculate various cost functions to evaluate safeguards. Qualitative risk analysis assigns subjective and intangible values to the loss of an asset and it is scenario based and then calculator based. Threats are ranked on a scale to evaluate their risks, costs, and effects. The process involves judgment, intuition, and experience. We will be looking at 'quantitative' risk analysis in detail in this lecture. Qualitative risk analysis will be looked at in greater detail in the next lecture.
Both approaches are essential for a complete risk analysis.

The process of quantitative risk analysis starts with asset valuation and threat identification. The next step is to estimate the potential and frequency of each risk to gain an understanding of countermeasures that could be needed. This information is then used to calculate various cost functions that are used to evaluate safeguards/countermeasures for the organisation.

We saw in the previous lecture where there was the creation of an asset register and the identification of potential threats, and we know this is the start of the risk assessment process. In this slide there is a list of possible asset values that could be in an organisation. These include: purchase cost, administrative cost, acquisition cost, value to competitors, market valuation, operational cost if lost, development cost, maintenance cost, value to owners and users, intellectual property value, replacement cost and liability. Identifying assets and activities to be protected can be seen in greater detail in Chapter 7 of the core module text.

Now, please pause/stop the video before continuing to listen to the rest of the lecture, and let us take a short break and reflect on the issues highlighted so far before moving on to the rest of the lecture presentation where we will look at the quantitative risk analysis in more detail.

Welcome back after taking that break, we can now continue with looking at the potential and frequency of how each risk is estimated in the quantitative risk analysis. The information from this can then be used to calculate or estimate various cost functions that are used to evaluate safeguards/countermeasures. The diagram in this slide, shows us the steps that are taken in the process for carrying out a quantitative risk analysis. Assets are assigned a value (AV), and then research is carried out on each individual asset in order to produce a list of all possible threats to calculate the exposure factor (EF), and single loss expectancy (SLE). The next step is to perform a threat analysis to calculate the likelihood of each threat being realised within a single year - that is the annualised rate of occurrence (ARO). Following on from this, the overall loss potential per threat is derived by calculating the annualised loss expectancy (ALE). The EFs, SLEs, AROs, and ALEs, are all cost functions. Research is then carried out regarding countermeasures for each threat, the changes to the ARO and ALE are then calculated based on an applied countermeasure. The final step is to perform a cost/benefit analysis of each countermeasure. Factors to consider in the cost/benefit analysis are security budget, compatibility with existing systems, skill and knowledge base of IT staff, availability of product, political issues, and partnerships. With regard to countermeasure selection and implementation these include, **Controls** put in place can be **Technica**l in nature eg. firewalls, intrusion protection. **Physical** for example door locks and gates and biometrics. **Administrative**: improved password policies, robust background checks on employees.

We know that we will begin with assigning an asset value (AV), and in this slide we see more information on the exposure factor (EF). It represents the percentage if a specific asset is violated by a single realised risk and indicates the expected overall asset value loss that is due to a single realised risk. The exposure factor is usually small for easily replaceable asset for example hardware and on the other hand it can be large for irreplaceable proprietary assets for example product designs. The exposure factor is expressed as a percentage.

The exposure factor is used when calculating the single loss expectancy (SLE), and this is cost associated with a single realised risk against a specific asset and indicated the exact amount of loss experienced if the assets are harmed by a specific threat. The SLE is expressed as a monetary value and is calculated using the formula on this slide. The single loss expectancy equals the asset value time the exposure factor. For example, is an asset is valued at £100,000 and it has an exposure factor of 50%, the single loss expectancy is calculated as SLE equals 100,000 times 50% which equals £50.000.

The next stage in the quantitative analysis is the annualised rate of occurrence (ARO), which is the expected frequency a threat or risk will occur in a single year. This calculation is also known as the *probability determination.* This is a more complex calculation and the examples we see on the slide that the ARO is equal to the number of known events and number of years or ARO is equal to the number of users times the likelihood of each threat per user. The ARO can also be derived from historical records, statistical

analysis or even guesswork, but would require the guesswork of an expert. For example, the ARO of an earthquake may be .00001, whereas the ARO of an email virus in an office could be 5000.

The annualised loss expectancy (ALE), is the possible yearly cost for all instances of specific realised threats against specific assets. This is calculate using the formula on this slide. The annualised rate of occurrence is equal to the number of known events for the said number of years or the annualised rate of occurrence is equal to the number of user's times by the likelihood of threats per user. To gain a better understanding, the example is if the single loss expectancy of an asset is say £30,000 and the annualised rate of occurrence for a specific threat such as the total power loss, is .0192 (5 days power outage in one working year (261 days), then the annualised loss expectancy is £576. However, on the other hand, if the annualised rate of occurrence for this specific threat such as the asset being unreachable due to a compromised use account, were 15, then the ALE would be £450,000.

Looking at exposure factors and annualised rate of occurrences, if the exposure factor safeguard fails, the exposure is the same as without it which is like having a bullet proof vest that can't stop bullets! A safeguard can also reduce damage made by the exposure factor but is similar to sprinklers used in a fire where the building still burns but not as bad!

IN addition to determining the annual cost of the safeguard or countermeasure, the annualised loss expectancy for the asset hast to be calculated if the safeguard is implemented and to do this requires a new exposure factor which might stay the same, but also a new annualised rate of occurrence has to be calculated specific to this safeguard.

When looking at the annualised rate of occurrence, a safeguard should be able to reduce the number of times attacks are successful in causing damage to an asset. Perfect safeguards would reduce the annualised rate of occurrence to zero, but many are not!

Now let's take a look at safeguard costs. For each risk, one or more safeguards should be evaluated on cost/benefit and for this a list of safeguards should be compiled for each threat. Each safeguard is then assigned a deployment value, the deployment value or cost of a safeguard should be measured against the value of the protected asset. The value of the protected asset then determines the maximum expenditures for the protection mechanisms to be put in place. Obviously, the security should be cost effective and the amount spent in terms of cash or resources protecting assets should not exceed its value to the organisation. If the cost of the safeguard is greater than the value of the asset, which is the cost of the risk, then the risk should be accepted.

In summary, the preceding slides cover the approaches to risk assessment and focus on 'quantitative' analysis. Now take a break and reflect on what we have learned so far before moving on to the next task which is to read Chapter 7 of the core text 'Identifying assets and Activities to be protected', to gain a more in-depth understanding of data and information assets.