Week 3: Approaches and Procedures for Risk Assessment (b)

Welcome to this third lecture (slides with voiceover) on approaches and procedures for risk assessment. In the previous lecture, we looked at 'quantitative' approaches and now we will focus on 'qualitative' approaches to risk management.
Qualitative risk analysis is more scenario based rather than calculator based. Threats are ranked on a scale to evaluate their risks, costs, and effects rather than on a purely monetary basis for example reputational impacts. The best approach is to balance both quantitative and qualitative risk assessments in order to get a successful result. The qualitative approach is known as a 'hybrid assessment' or 'hybrid' analysis and this process involves judgement, intuition, and experience.
The approach to qualitative analysis depends very much on the organisation and its culture. Normally, the threats will be viewed as either low, medium or high risk. Responses to risks might be risk mitigation, risk assignment where it is assigned and transferred to a third party (insurance). The risk might be accepted on the basis of cost benefit analysis, in which case it is accepted and not mitigated. Risk deterrence is another response where deterrents are implemented with regular auditing for example. There is also risk avoidance where the risk is removed and that might be for example a hurricane of act of God. Risk rejection is where the risk is ignored and this can lead to serious non-compliance if the risk is actually realised.
There are a number of qualitative techniques that can be used such as brain storming, storyboarding and focus groups to gain a wide range of ideas. Surveys and questionnaires are also used as well as checklists, one to one meetings and interviews to contribute to the analysis.
The creation of scenarios is another technique that is employed in qualitative analysis, where a single major threat is described. The scenario then focuses on how the threat would be instigated and what effects its occurrence could have on the organisation, the IT infrastructure, and specific assets. One or more safeguards are then described for each of the scenarios that might completely or partially protect against the threat that is discussed in the scenario.
After the safeguards have been described for each scenario, the analysts involved in the scenario then assign a threat level to the scenario outlining the loss potential as well as the advantages of each safeguard. These might be recorded as being either high, medium or low, or assessed on a scale of one to ten or the other alternative is to be detailed in an essay type from of response. The final outcome from the scenario exercise is then has all the responses from all the participants in the scenario written up in a report and then sent to senior management for decision-making.
Matrices are used for qualitative analysis and this slide shows one type of matrix that might be used. On the top of the diagram we have the heading 'impact' that is the impact of the threat, and on the left hand side we have the likelihood of the impact occurring with whether it is high, medium or low and then beneath the heading, we have the ranking of the threat being high, medium or low with colour coded levels of risk beneath each heading.
This slide shows us a matrix using arbitrary values to assign the likelihood and impact of a threat occurring with values assigned to scores on the first section under headings of 'Score', 'Likelihood' and 'Score' and 'Impact', and the bottom section with headings of 'Risk', 'Likelihood', 'Impact' and 'Overall Score', where scores are assigned to the risk and a calculation of the overall risk score.

The results of any risk analysis are many, they consist of a complete and detailed valuation of all assets, an exhaustive list of all the threats and risks as well as the rate of their occurrence, and extent of loss if the threat is realised. There will also be a list of specific threat safeguards and countermeasures that identify their effectiveness and annual loss evaluation (ALE), as well as a cost/benefit analysis for each safeguard. All this information is essential for senior management in their decision making regarding safeguard implementation and security policy alterations etc. Once the risk analysis is complete, management must address and assess each specific risk.
If senior management accept the risk, this is evaluated by the cost/benefit analysis of possible safeguards being put in place and the determination that the cost of this outweighs the possible cost of loss due to the risk. This also means that management accept any consequences of the loss if the risk is realised. In this case, it is normal practice to have a clearly written statement that indicates why a safeguard was not implemented, who is accountable for the decision and who will be responsible for the loss if the risk is realised, and this is usually in the form of a sign-off letter. If an organisation decides to accept the risk, it is based on its risk tolerance and this is the ability of the organisation to absorb any losses incurred with any risks that are realised. This may also be known as risk tolerance or risk appetite.
In summary, this lecture has given an overview of qualitative risk assessment, risk assignment and risk acceptance. Now, please take a break and reflect on what we have learned so far before moving on to the next task which is to read Chapter 6 of the core module text; this will enable you to gain a more in-depth understanding of performing a risk assessment.