LECTURE 11
RISK EVALUATION

Dr Warusia Mohamed Yassin

Topics

- Risk Analysis Result
- Evaluation Of Risk Level
- Risk Aggregation
- Risk Grouping

Introduction to Risk Evaluation

- ✓ At this point we have identified the risks and analysed their likelihood and consequence.
- ✓ From this we can establish the risk level and compare it to the risk evaluation criteria.
- ✓ We also need to consider whether some risks that we have regarded as separate are actually instances of the same risk and therefore should be aggregated and evaluated as one risk.
- ✓ Furthermore, as preparation for the risk treatment, we group risks according to relationships such as shared vulnerabilities or threats.

Risk Analysis Result

- ✓ The goal of the consolidation of risk analysis results is to make sure that the correct risk level is assigned to each risk.
- ✓ This is important because the risk levels direct the identification of treatments and provide essential decision support for the management.
- ✓ The results of the consolidation are documented in the same place as the risk analysis results simply by making the necessary corrections and updates, and also adding references if new information sources have been used.

Evaluation of Risk Level

- ✓ Having consolidated the risk analysis results, we are ready to evaluate the risks.
- ✓ The risk level of each risk is determined by its likelihood and consequence according to the risk matrix.
- ✓ The risk evaluation is performed simply by plotting each risk in the risk matrix defined as in figure below.

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical		2			
	Major	6				
	Moderate	4,5	8		1	
	Minor				3	
	Insignificant	7				

Risk Aggregation

- During the evaluation we need to take into account that some risks may “pull in the same direction” to the degree that they should actually be evaluated as a single risk. There are basically two cases where this may hold.

The first case, which is illustrated by Fig. 9.3, concerns incidents that harm more than one asset of the same party, thereby giving rise to more than one risk for the party in question. Even if the risk of incident *X* harming asset *A* and the risk of incident *X* harming asset *B* are both low, it may be that the combined effect of harm to *A* and *B* warrants a higher risk level for the aggregation of these risks. In this case the likelihood of the aggregated risks remains the same, while the consequence is the joint consequence of the two risks.

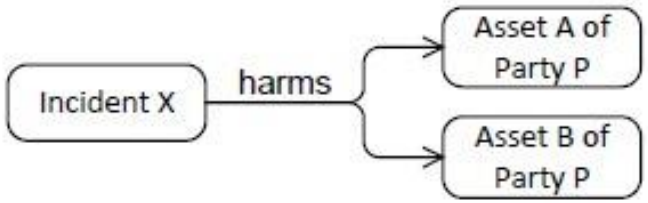

Fig. 9.3 Aggregation of risks where one incident harms more than one asset of the same party

Risk Aggregation

The second case is illustrated by Fig. 9.4 and concerns a single asset being harmed by more than one incident. Even if the risk of each individual incident harming the asset in question is low, it may be that the combined effect on the asset yields a higher risk. A typical situation in which we might aggregate is when the incidents are of the same nature, as is the case for Y_1 and Y_2 in Fig. 9.4 a), or when the occurrences of the incidents are triggered by the same threat, as is the case for U and V in Fig. 9.4 b). Notice that this also needs to be taken into account in cases where one of the incidents is malicious and the other is non-malicious.

Risk Aggregation

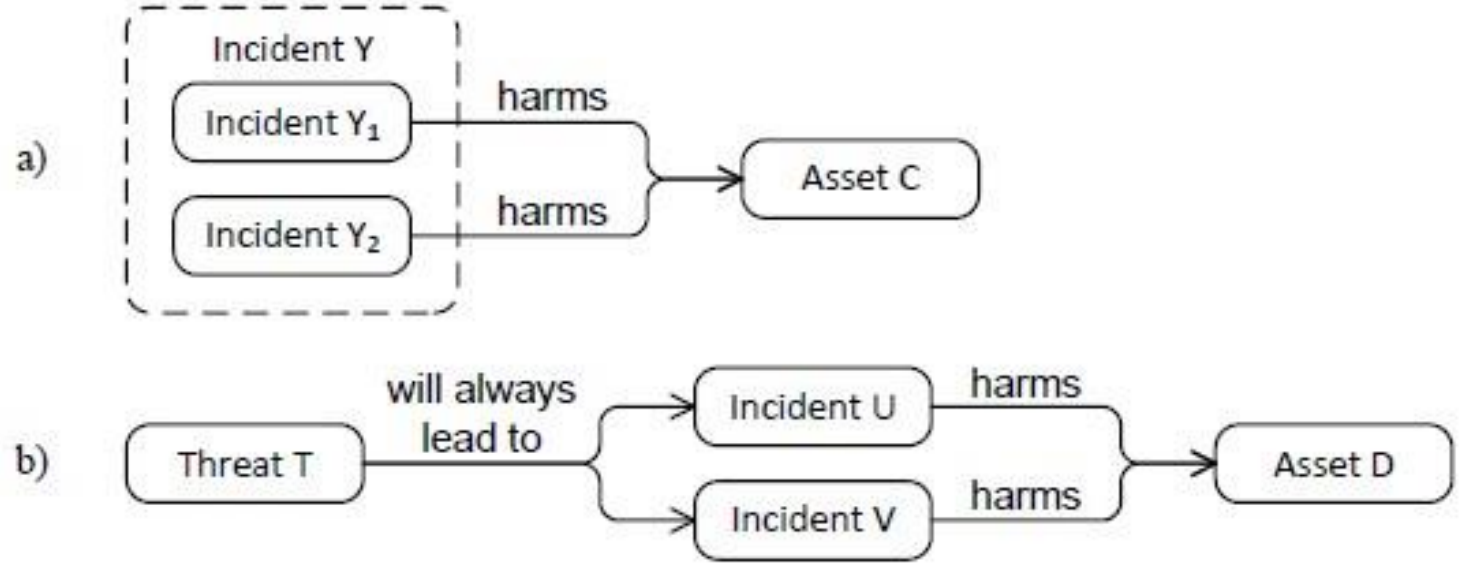

Fig. 9.4 Aggregation of risk where a) two incidents are special instances of a common, more abstract instance, or b) two incidents are triggered by the same threat

Risk Grouping

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical		2			
	Major	6,13	6+13			
	Moderate	4,5	8,11,12,14	4+11,5+12	1	
	Minor			15	3	9
	Insignificant	7			16,17	10

Fig. 9.5 Risk matrix after aggregation

- ✓ Overviews like the one provided by Fig. 9.5 give an indication of which risks need treatment.
- ✓ However, as preparation for the risk treatment, we also want to take into consideration the fact that treatments may have an effect on several risks, thereby justifying higher cost than if we only consider individual risks. It can therefore be useful to group risks with this is in mind.

Risk Grouping

- ✓ The distinction between malicious and non-malicious risks earlier in the assessment has given us two groups.
- ✓ This is already useful, as some treatments will only have an effect on one of these groups.
- ✓ For example, data encryption, firewalls, and intrusion detection systems will usually reduce the likelihood or consequence of (some) malicious risks, without having any effect on non-malicious risks.

Risk Grouping

- ✓ In addition to distinguishing between malicious and non-malicious risks, we may typically group risks according to shared vulnerabilities, threats, threat sources, or assets.

- ✓ The purpose of the grouping is to facilitate identification of the treatments that give the best effect for the least cost by placing together risks that may benefit from a common treatment.

Roadmap/Mind Map