Chapter 11
Which Measure of Risk Level to Use?

So far in this book we have measured the risk level of incidents in terms of consequence for assets and likelihood of occurrence. In other words, we have measured risk level based on two factors, namely loss of asset value when a potential incident occurs and how often this happens. In this chapter we present and discuss alternative ways of measuring risk level using two, three, or even more factors.

11.1 Two-factor Measure

A risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence, where consequence is the outcome of an event affecting assets. This is the classical two-factor measure of risk.

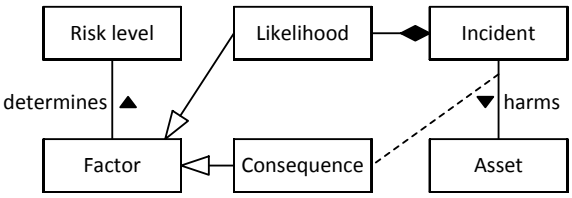

Fig. 11.1 Summary of two-factor approach

Figure 11.1 illustrates the two-factor approach using the UML [58] class diagram notation. Each line connecting two boxes represents a relation. The white-headed arrows pointing from likelihood and consequence to factor imply that the concepts likelihood and consequence should be understood as instances of the more general concept factor. In other words, they are both factors. Moreover, the factors determine the risk level.

A. Refsdal et al., *Cyber-Risk Management*, SpringerBriefs
in Computer Science, DOI 10.1007/978-3-319-23570-7_11

The relation with a black diamond connecting incident and likelihood captures that likelihood is an attribute of incident. This is because likelihood is a measure of incident occurrence. On the other hand, consequence is connected to the relation between incident and asset since it is a measure of the former's potential to affect the latter.

11.2 Three-factor Measure

In the field of security, three-factor risk measures are popular. For example, NIACAP [57] defines risk as "a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact."

The "likelihood that a threat will occur" is a measure of the extent to which the target is subject to a certain threat, while the "likelihood that a threat occurrence will result in an adverse impact" is a measure of the vulnerability of the target with respect to the threat in question. These two factors may be understood as a decomposition of likelihood from the two-factor approach since the likelihood of a threat occurring and the likelihood of it resulting in an adverse impact may be used to deduce the likelihood of a risk in the two-factor sense. The third factor "severity of resulting impact" corresponds to consequence in the two-factor case. The meaning of "combination" is not further defined. Hence, we may think of the risk level as a triple of factors whose relative weighting is left open.

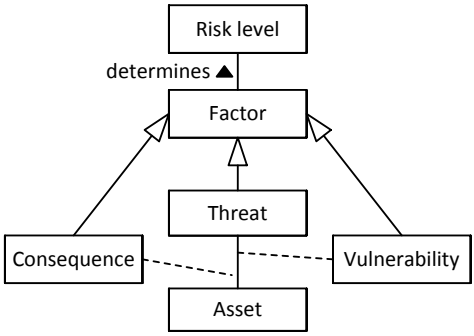

Fig. 11.2 Summary of three-factor approach

The definition is summarized in Figure 11.2, again using a UML class diagram. We now distinguish between three factors, namely threat, vulnerability, and consequence. As in the case of consequence, vulnerability is connected to the relation between threat and asset since it is a measure of the threat's potential to harm the asset.

11.3 Many-factor Measure

In some situations it may be beneficial to use even more factors. OWASP [64], for example, which is concerned with the security of web applications, recommends an approach where the likelihood of the two-factor approach is decomposed into threat agent factors and vulnerability factors. Similarly, consequence is represented by technical impact factors and business impact factors. The proposed vulnerability factors with respect to a group of attackers are, for example:

- Ease of discovery: How easy is it for this group of attackers to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9).
- Ease of exploit: How easy is it for this group of attackers to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (7), automated tools available (9).
- Awareness: How well known is this vulnerability to this group of attackers? Unknown (1), hidden (4), obvious (6), public knowledge (9).
- Intrusion detection: How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9).

According to OWASP, in the case of threat agent and vulnerability factors, the numbering from 0 to 9 is a likelihood rating. The overall likelihood is formally defined as the average of the likelihood factors. Similarly, the overall consequence is equal to the average of the technical impact and business impact factors. The risk level is then defined via a risk matrix as in the two-factor case.

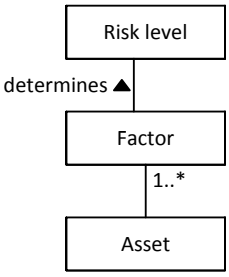

Fig. 11.3 Summary of many-factor approach

Figure 11.3 illustrates a many-factor measure, again as a UML class diagram. The factors, of which there may be any finite number, are all of relevance for the asset, and for representing and measuring risk level with respect to the asset.

11.4 Which Measure to Use for Cyber-risk?

As we have seen, risk level may be measured in multiple ways. The same holds for cyber-risk. We have presented the two-factor approach based on consequence and likelihood. The two-factor approach is the one most commonly used in practice, also within cybersecurity. We have also considered one of several alternative approaches employing three factors developed for the security domain. Finally, we have discussed the use of more than three factors.

Which approach you should use and how you should use it depends on the context and your risk assessment situation. What data is available is an important parameter when deciding how to measure risk level. If you have good data on frequency and consequence you will probably go for the two-factor approach, and accordingly for other measures if they are favored by the data available.

Within cybersecurity our impression is that the popularity of approaches using more than two factors is growing. One reason is that measuring likelihood with a reasonable degree of uncertainty in practice may be difficult. Consider, for example, an attack by a malicious threat source on some given target. It may be the case that the likelihood of a successful attack depends almost entirely on the motive and abilities of the attacker, in addition to the vulnerabilities of the target with respect to the attack in question. If these factors are easy to measure within acceptable uncertainty, you may use them directly to calculate the risk level, instead of going indirectly via likelihood.

Most cyber-systems generate logs automatically with respect to a (large) number of indicators. Hence, when assessing risk, the problem normally is not the lack of data, but the lack of the right kind of data with respect to predefined factors. In such situations you may try to define your own risk function from factors matching the indicators logged by the cyber-system in question. To do this, however, requires some experience and great care.

If, as is often the case, you rely on expert or stakeholder opinions to estimate risk level, make sure that the factors are carefully defined and easy to keep apart. Moreover, it is also crucial that you select the right kind of scale for each factor. This will be further detailed in the next chapter.

11.5 Further Reading

Section 11.2 employs NIACAP [57] to exemplify a three-factor risk measure. Three-factor measures are not specific to cybersecurity. Risk of terrorism, or malicious attack in general, is often measured accordingly [85]. In Sect. 11.3 we use the OWASP approach [64] as an example of a many-factor risk measure. The number of factors and how the factors are decomposed vary. While OWASP describes the attacker in terms of skill level, motive, opportunity, and size, the Common Criteria [8] employs the elapsed time (for the attack), expertise, knowledge of target, window of opportunity, and equipment (for the attack).