Chapter 15
Conclusion

We have structured the conclusion into three parts. First we draw conclusions on the general theme of cyber-risk management as described in Parts I and II. Then we do the same for the four issues addressed in further detail in Part III. A technical brief is by its very definition short; hence, much has just been touched on and even more has not been covered at all. We end this chapter by identifying some of these issues.

15.1 What We Have Put Forward in General

Cyber-risk management is not fundamentally different from risk management in general; as we have explicated in the first two parts of this book, we recommend stakeholders to conduct cyber-risk management by following the processes and recommendations of established standards and practices on risk management.

There are however aspects of cyber-systems that make cyber-risk management challenging. The main feature in this respect is the use of cyberspace. Cyber-systems and cyberspace have brought significant improvements for individuals, businesses, and society as a whole within numerous areas, including social life, public services, trade and economy, entertainment, and critical infrastructures. At the same time, the use of and dependence on cyberspace has introduced a number of new threats and vulnerabilities.

In order to understand how to conduct cyber-risk management in an effective and efficient way it is necessary to understand the kinds of systems that we are concerned with, as well as the nature of the risks these systems are exposed to. This is why we have devoted separate chapters to cyber-systems, cybersecurity, and cyber-risk management in the first part of this book.

One important aspect of cyber-risk is the distinction between malicious cyber-risk and non-malicious cyber-risk. The distinction has implications for how we assess and handle cyber-risk, and we have therefore organized much of the contents in the two first parts of the book to account for this. The possibility of malicious threats requires a strong focus on human intent, motives, and capabilities. This has

A. Refsdal et al., *Cyber-Risk Management*, SpringerBriefs
in Computer Science, DOI 10.1007/978-3-319-23570-7_15

led to the publication of dynamically evolving catalogues and repositories documenting potential cyber-threats, exploits, and vulnerabilities to malicious attacks, as well as techniques for the modeling of malicious threats. At the same time, the many possibilities of accidental and unintended incidents require a similar focus on non-malicious threats, including both the technical and the sociotechnical aspects of cyber-systems. Together with the wide extension of cyberspace, and therefore the wide possibilities for threats to arise, the different ways in which to tackle malicious and non-malicious threats represent a challenge for cyber-risk management. This challenge must be handled in a methodical manner, as we have put forward in this book.

Another major challenge regarding cyber-risk management is that cyberspace evolves rapidly and often in a manner that is difficult to predict. Cyber-systems must be able to cope with this evolution. In fact, cyber-systems are forced to evolve in response to the evolution of cyberspace. This requires increased focus on monitoring and risk assessment in real time as part of the overall cyber-risk management.

Although cyber-systems are challenging from a risk management point of view, there are also features of cyber-systems that we can take advantage of and that have a simplifying effect. The fact that cyber-systems are computerized to a large degree is beneficial when it comes to data collection, which is why we have stressed the use of techniques such as monitoring and testing throughout Part I and Part II of this book. Moreover, computerized harvesting of data may reduce uncertainty in risk assessment. In fact, the possibility of data collection in real time provides a foundation for real-time risk assessment.

15.2 What We Have Put Forward in Particular

Risk level may be measured in multiple ways. We have presented the two-factor approach based on consequence and likelihood, which is the one most commonly used in practice. We have also considered an alternative approach employing three factors developed for the security domain, and we have discussed the use of more than three factors. Which approach to use and how to use it depends on the context and your risk assessment situation. Which data are available is an important parameter when deciding how to measure risk level. If you have good data on frequency and consequence, and not on other factors, you will probably go for the two-factor approach, and accordingly for other measures if they are favored by the data available.

Estimating or measuring likelihood tends to be difficult. One reason is that there may be considerable uncertainty as to what the likelihood is. Another reason is that in some cases there is a lack of experience or historical data with respect to the event in question. A third reason is that we may all too easily complicate the task ourselves by selecting quantitative likelihood scales that are badly suited to the task. In general, we do not recommend using probabilities when interacting with human beings in a risk assessment situation. A probability is always defined implicitly with respect to some interval or context, and the existence of this implicit interval or con-

text is easily overlooked or misunderstood leading to bad estimates and confusion. In most cases natural frequencies are better suited to risk analysis purposes.

Make sure not to confuse likelihood with uncertainty. It makes good sense to document uncertainty for each risk factor separately. When working quantitatively, in our experience a practical approach to take uncertainty into consideration is to use intervals. When employing qualitative scales, uncertainty may be characterized separately, for example, as a separate natural language expression for each measurement. In a risk assessment, whether the level of uncertainty is tolerable depends on to what extent the uncertainty impacts the decision procedure. If it does not, the uncertainty is at an acceptable level.

Risk assessment has its limitations. In particular, as we emphasized in Chap. 14, risk assessment will in most cases be of little help in identifying and predicting black swans. On the other hand, we have argued that risk assessment may be well suited to coping with gray swans. To reduce the chance of gray swans not being considered we have argued that it is often fruitful to observe the target of assessment from different viewpoints. This has several implications for how we conduct risk identification. For example, we should involve all relevant stakeholder roles, split the risk identification into a set of independent processes, and embed the use of different kinds of tools in the risk identification process.

15.3 What We Have not Covered

The main focus of this book is on cyber-risk assessment. The more general and continuous risk management activities corresponding to the processes for "communication and consultation" as well as "monitoring and review" are just covered briefly.

Another topic that we have touched upon, but which requires much more careful consideration, is system evolution and its implications for risk assessment. Real-time risk assessment is another important aspect of risk management not covered by this book. We believe risk assessment in real time will become more and more important in order to cope with ever more dynamic cyber-systems.

Within the general fields of cyber-systems and cybersecurity there are numerous sub-fields imposing more specialized challenges to risk management. Privacy is one such sub-field; compliance, cloud computing, and big data are other examples, none of which are covered by this book.