Chapter 5
Cyber-risk Management

In this chapter we specialize risk management to the domain of cyber-systems. We highlight what is special about cyber-systems and cyber-threats from a risk management perspective, focusing in particular on the nature of cyber-risks and the options and means we have for managing them. First we explain what we mean by cyber-risk. Thereafter we specialize the three main processes of risk management to cope with cyber-risk.

5.1 What is Cyber-risk?

Cyberspace has considerable impact on the kind and nature of the threats and the risks that may appear, as well as on the procedures and techniques to conduct risk management and risk assessment. One striking aspect of cyberspace is that it is potentially extremely far-reaching. This means that the possible threat sources can reside anywhere in the world, yet with the potential of causing damage deep inside the cyber-system of our concern. Another crucial aspect is that a substantial share of cyber-threats are malicious; they are caused by adversaries with motives and intentions. On the other hand, there are also non-malicious cyber-threats.

Cyber-risk management is concerned with risks caused by cyber-threats, which motivates the following definition.

Definition 5.1 A *cyber-risk* is a risk that is caused by a cyber-threat.

Although we are concerned with cyber-systems, it is important to understand that cyber-risk is not the same as any risk that a cyber-system can be exposed to; cyber-risks are limited to the risks that are caused by cyber-threats. The risk of a server on which our cyber-system is running being damaged by water flooding, for example, is not a cyber-risk unless a cyber-threat is a contributing factor. Confidentiality breaches due to virus attacks via cyberspace and loss of availability due to DoS attacks, however, are examples of cyber-risks.

A. Refsdal et al., *Cyber-Risk Management*, SpringerBriefs
in Computer Science, DOI 10.1007/978-3-319-23570-7_5

Next, in order to understand the nature of cyber-risks and how to manage them we distinguish between *malicious cyber-risk* and *non-malicious cyber-risk*. We say that a cyber-risk is malicious if it is (at least partly) caused by a malicious threat, and non-malicious otherwise.

Notice, importantly, that by this definition some cyber-risks are both malicious and non-malicious. These are cyber-risks that can be caused by either a malicious threat or a non-malicious threat. Consider, for example, an incident of unauthorized access to some sensitive data. A potential occurrence of this incident as caused by a hacker is a malicious cyber-risk, while a potential occurrence that is caused by accidental posting of the data on an open website is a non-malicious cyber-risk.

There are also incidents that happen only due to the combined occurrence of a malicious and a non-malicious threat. An example of this is an intrusion that occurs while the intrusion detection and prevention system is down due to an accidental failure. We classify these as malicious cyber-risks since they cannot occur without the malicious threat.

The Venn diagram of Fig. 5.1 provides a summary: Cyber-risks are the union of malicious and non-malicious cyber-risks, and cyber-risks are only a subset of the risks that cyber-systems can be exposed to. Moreover, the intersection between malicious and non-malicious cyber-risk represents the cyber-risks that can be caused by either a malicious threat or a non-malicious threat.

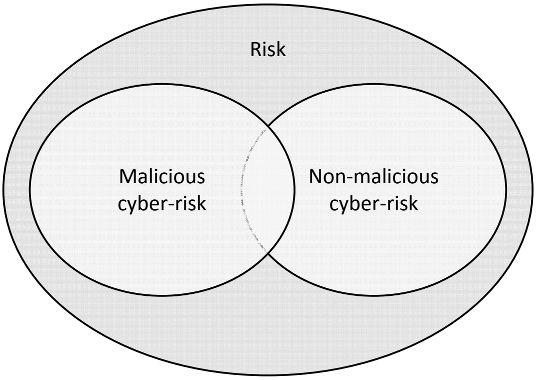

Fig. 5.1 Malicious and non-malicious cyber-risk

5.2 Communication and Consultation of Cyber-risk

The process of communication and consultation described in Sect. 2.3 for risk management in general is equally suited to the more narrow domain of cyber-risk. There are, however, certain issues imposed by cyberspace that require particular attention. First, due to the nature of cyberspace, cyber-systems may potentially have stakeholders everywhere. These stakeholders may be consumers of services or information provided by the cyber-system of our concern, or they may be providers of services to this cyber-system. It is important to consider all stakeholders, both individuals and organizations, when determining relevant sources of information and identifying who may be affected by cyber-risks. We moreover need plans and procedures for how to provide, share, obtain, and make use of the information of relevance.

Second, also due to cyberspace, there may potentially be adversaries everywhere, and any major incident somewhere in the world may have considerable impact on our cyber-system. Coping with these numerous parameters requires increased focus on information collection by monitoring and surveillance.

For the process to be efficient it is necessary to establish a classification and categorization of information. For the purpose of representing and understanding relevant information, organizations may use established standards or repositories, see Sect. 5.5, or they may define their own. The objective is to maintain a repository of up-to-date information regarding, for example, cyber-threats, vulnerabilities and incidents, potential and confirmed adversary profiles, current strategies and mechanisms for cyber-risk mitigation, and so forth. The classification and categorization may also include characterizations of cyber-systems, including, for example, assets and cyber-system profiling.

For many organizations it is essential to establish communication procedures for handling major incidents. Efficient communication, for example via a public relations team, is often an important element of good incident response planning.

5.3 Cyber-risk Assessment

There are two things in particular that distinguish risk assessment in the context of cyber-systems from the general case. First, the potentially far-reaching extent of a cyberspace implies that also the origins of threats are widespread, possibly global. Second, the number of potential threat sources and threats, both malicious and non-malicious, is very large. In combination this means that the search area and the number of sources of potentially relevant information about cyber-risk are extremely large and may seem overwhelming. We therefore need procedures and techniques that provide guidance and direction.

Figure 5.2 shows the specialization of the risk assessment process to cyber-systems. The most obvious difference from the general case is that the risk identification step is divided into two separate steps: Step 2a focusing on malicious cyber-risks and Step 2b focusing on non-malicious cyber-risks. We make this distinction because the nature of threats, threat sources, and vulnerabilities, and how to approach their identification, is highly dependent on whether we are dealing with malicious intent or not.

Human adversaries who deliberately and actively seek to cause harm are hard to predict, and the consequences of the incidents they cause can be difficult to estimate. We basically assess a game. There are two opponents with opposing goals: The

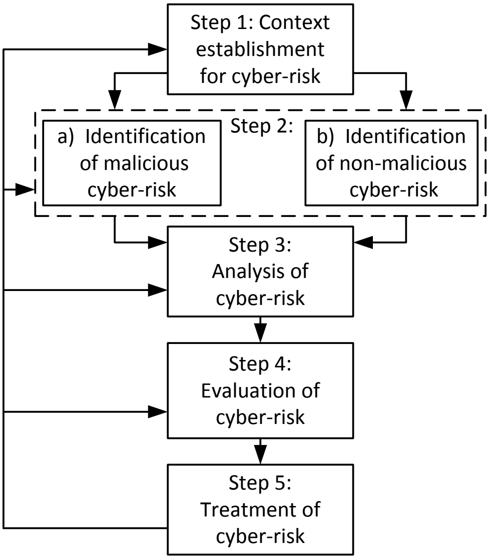
Step 1: Context establishment for cyber-risk
Step 2:
a) Identification of malicious cyber-risk
b) Identification of non-malicious cyber-risk
Step 3: Analysis of cyber-risk
Step 4: Evaluation of cyber-risk
Step 5: Treatment of cyber-risk

Fig. 5.2 Process for cyber-risk assessment

adversary (the malicious threat source) who actively seeks to harm assets, and the defender (the system owner or the party on whose behalf we do the assessment) who tries to prevent this from happening. The aim of Step 2a is to identify risks based on the potential ways in which such a game can play out. The motives, intentions, abilities, skills, resources, and so forth of the adversary are essential in this context. A good starting point in the identification of cyber-risks caused by malicious threats is therefore the identification and characterization of potential threat sources.

Understanding how non-malicious threats arise, such as accidents and failures, on the other hand, is a different kind of challenge. There is normally little need to capture intent or motive for such threats. Moreover, because there are an almost unlimited number of ways unintentional things may happen, it easily becomes overwhelming if we start by identifying threat sources and threats. In conducting Step 2b we recommend instead to start from the assets and the ways in which they may be harmed. In this way we make sure that we focus strictly on what we seek to protect, and that we proceed in a manner that is both effective and efficient. In other words, by first asking what can go wrong and then asking how, we help ourselves to keep the right focus. If, instead, we started by asking how something could happen unintentionally or by accident and what could possibly be the cause, we would soon find ourselves moving in all kinds of directions.

In the rest of this section we describe the specialization of each step of the cyber-risk assessment process in more detail.

5.3.1 Context Establishment for Cyber-risk

What distinguishes the context establishment of a cyber-risk assessment from the general case is that we need to understand and document how the cyber-system in question makes use of and interacts with cyberspace. This gives a basis for understanding how and where cyber-threats arise, as well as which assets are relevant to focus on.

As part of the description of the target of the assessment, we therefore include the interface to and interaction with the cyberspace and other relevant parts of the environment. Understanding and documenting the interface to the cyberspace is important for cyber-risk management in general and for identification of cyber-risks in particular. The cyber-threats arise in or via the cyberspace, and the interface between the cyberspace and the target of assessment overlaps with the attack surface. The *attack surface* is all of the different points where an attacker or other threat source could get into the cyber-system, and where information or data can get out [60].

Typical assets of concern in the setting of cyber-risk assessment are information and information infrastructures, including software, services, and networks. However, in order to understand the wider implications of cyber-threats and incidents, we need to take into account assets that can be harmed as a further consequence. Relevant concerns in this respect are, for example, reputation, image, market share, revenue, and legal compliance. The latter is relevant regarding, for example, data protection and privacy. Moreover, although cyberspace and cyber-systems are typically associated with the virtual and the intangible, it is important not to limit the focus to such aspects alone. Cyber-threats and incidents can also cause physical harm, including harm to life, health, and the environment.

5.3.2 Identification of Malicious Cyber-risk

To identify malicious cyber-risk it is often helpful to think in terms of a game such as chess. As illustrated by the UML class diagram in Fig. 5.3, there are two players, namely an adversary (the opponent or malicious threat source) and a defender on whose behalf we are assessing. The defender is represented by the target and a set of assets. Our role as risk assessors is to observe and assess this game. In particular, we try to foresee what the future moves of the adversary might be and to provide advice on how to counter these moves. What we can expect from the adversary depends on the motives and the abilities of the adversary, as well as on the helpers and the resources available to the adversary.

The attack strategies of the adversary are typically conditional on the strengths and weaknesses of the defender. As illustrated by the lowermost ellipse in Fig. 5.4, we as assessors are supposed to deliver as output a risk model obtained by documenting and assessing how and to what extent the adversaries of relevance may exploit these weaknesses. As captured by the uppermost ellipse in Fig. 5.4, our input is the target description and the selected assets, both obtained from Step 1.

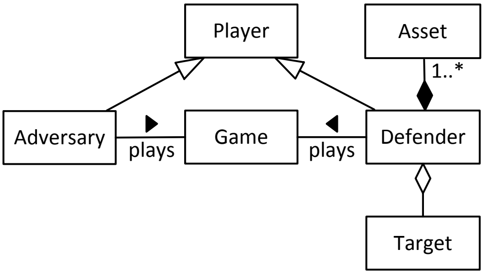

Fig. 5.3 Assessing the game between an adversary and a defender

The nature of the game obviously depends on who the defender is facing. As indicated by Fig. 5.4, we therefore start by identifying and documenting the properties of the potential adversaries, namely the malicious threat sources. When the threat sources have been identified and sufficiently documented, we proceed by investigating for each of them to what extent and in what way they may harm the assets. As illustrated by Fig. 5.4, we proceed via identification of malicious threats and the vulnerabilities these threats may exploit (called malicious vulnerabilities) to the identification of incidents. When we have completed the identification of malicious cyber-risk we document the results in a risk model which forms the output of the malicious risk identification. By *risk model* we mean any representation of risk information, such as threats, vulnerabilities, incidents, risks, and how they are related.

In practice, and as illustrated by the arrows in the figure, there may of course be exceptions from the ordering, as well as iterations back and forth, while identifying new elements. In the following we describe the contents of each step in further detail.

- *Malicious threat source identification:* To identify relevant and possible malicious threat sources we need to understand who may want to initiate attacks, what motivates them, what their capabilities and intentions are, how attacks can be launched, and so forth. We also need to take into account that although the malicious threat sources are often human, they may also be non-human such as a computer virus. There is motive and intent behind even non-human malicious threat sources because such threat sources are introduced deliberately and for a purpose. In principle we could choose to view the initial human actor as the threat source, but this depends on our target and scope and their relation to the threat in question. Typically, if malware has been developed specially to attack our target of assessment, then we view the developer of the malware as the initial threat source; otherwise, we view the malware itself as the threat source.

  Many malicious threat sources reside outside the cyber-system in question, but some are internal. To facilitate the identification it may be useful to consult rel-

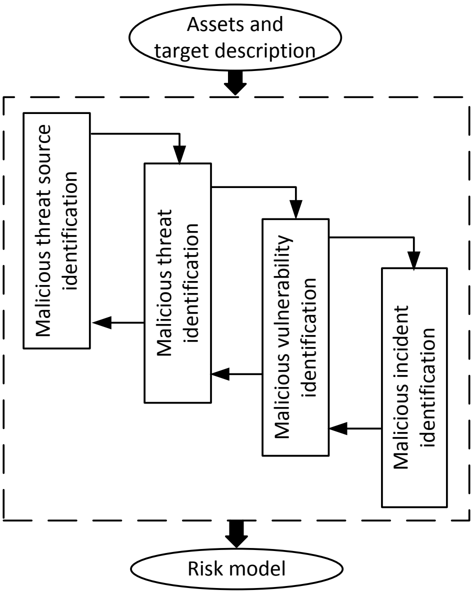
Assets and target description
Malicious threat source identification
Malicious threat identification
Malicious vulnerability identification
Malicious incident identification
Risk model

Fig. 5.4 Identification of malicious cyber-risk

evant sources such as international standards, annual and biannual reports on cybersecurity and cyber-threats, and open repositories.

- *Malicious threat identification:* For each of the malicious threat sources we proceed by identifying the malicious threats it may initiate that in some way or another may harm the identified assets. We pay particular attention to the interface to the cyberspace and the documented attack surface. In conducting this task we may involve people with first-hand knowledge about the target of assessment. Information can be gathered, for example, via questionnaires, interviews, workshops, and brainstorming sessions. We make active use of the description of the target of assessment, investigating where and how attacks can be launched. Examples of helpful catalogues and repositories that concern cybersecurity and cyber-threats in particular are those that are provided by MITRE [51, 52] and OWASP [61].
- *Malicious vulnerability identification:* In order to identify the vulnerabilities that the malicious threats may exploit we still focus on the identified attack surface. Additionally, we investigate existing controls and defense mechanisms to determine their strength and adequacy with respect to the identified threats and assets. As before we may consult system users and other personnel, as well as open information sources. For specific threats or vulnerabilities we may also conduct various kinds of security testing, such as penetration testing and vulnerability scanning. Such testing can serve as a means to check whether or how easily a specific threat source can actually launch an attack. We can do testing also to investigate the severity of known vulnerabilities, search for potential vulnerabilities, and search for possible incidents that the malicious threats may lead to.

- *Malicious incident identification:* We proceed to the incident identification by investigating how the malicious threats can cause harm to the identified assets given the identified vulnerabilities. We may use most of the techniques mentioned above also for this purpose. Furthermore, event logs provide information about previous incidents of relevance, and the various means of testing help the investigation of the kinds of incidents that the threats and vulnerabilities may lead to.

During this process it may well be that we backtrack and identify further threat sources and threats after the vulnerability identification, and it may also be that we already have an overview of some potential incidents that we aim to assess further. In general we gradually fill in and complete the risk model by revisiting the above-mentioned steps.

5.3.3 Identification of Non-malicious Cyber-risk

Normally there is no intent or motive behind non-malicious risks and there are so many possibilities that we can easily get overwhelmed. It is therefore normally not practical to start by identifying and documenting threat sources. Instead, as illustrated by Fig. 5.5, we recommend starting from the valuables to be defended, namely the identified assets, and then working outwards in the direction of the arrows. For each asset, the initial question is in what way it may be directly harmed. Each possibility corresponds to an incident. Next, we proceed by identifying the vulnerabilities and threats that may cause these incidents, focusing only on the parts and aspects of the target that are of relevance to the identified incidents. Finally, we identify the non-malicious threat sources that can cause the threats.

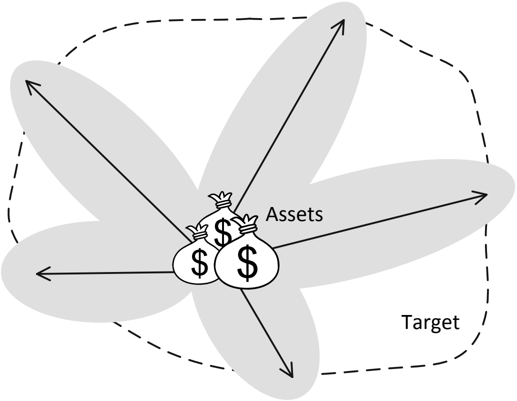

Fig. 5.5 Assessing how assets can be exposed to non-malicious threats

This asset-driven process, as illustrated by Fig. 5.5, allows us to ignore all parts of the target (the area with light shading) that are not relevant to the assets in question.

By starting from and strictly focusing on the assets, we make sure that we address only the relevant parts and aspects of the target (the area with darker shading). In other words, we use the assets to make the identification of non-malicious cyber-risks as efficient as possible.

The process is further illustrated by Fig. 5.6, where the initial step is the incident identification using the assets and the target description from the context establishment as input. For each incident, and as illustrated by the subsequent steps in the figure, we then proceed via vulnerabilities and threats to the identification of threat sources. We document the results during the process to produce the risk model that is the output of the risk identification, as illustrated by the ellipse at the bottom of the figure. Also here we may iterate back and forth, and deviate from the presented order when appropriate. In the following we describe the contents of each step in turn, following the overall order as depicted in Fig. 5.6.

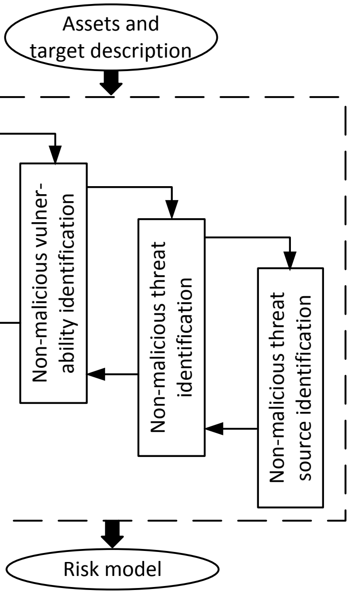
Assets and target description
Non-malicious incident identification
Non-malicious vulner-ability identification
Non-malicious threat identification
Non-malicious threat source identification
Risk model

Fig. 5.6 Identification of non-malicious cyber-risk

- *Non-malicious incident identification:* To identify incidents it is often useful to start by investigating how the assets are represented and how they are related to the target of assessment. For incidents with respect to information assets, for example, we investigate how the information is stored and processed in the system and in cyberspace, which applications and users have access to read or modify the information from where, how the information is transmitted, and so forth. For intangible assets, such as reputation, we need to understand how these are related to which parts or aspects of the target of assessment. Accidents and unintended acts are often recurring and known; we may therefore use logs, monitored data, and other historical data to support the identification.

- *Non-malicious vulnerability identification:* For the identification of vulnerabilities we may investigate technical parts of the target of assessment, as well as the culture, routines, awareness, and so forth of the organization and personnel in question. Relevant system properties that need to be investigated may, for example, be liberal access control, security mechanisms or barriers that are missing or that can be bypassed, and inconvenient application interfaces to the extent they open for accidental or unintended incidents to occur. Relevant issues regarding the organization and personnel include, for example, training, routines and procedures, and time pressure. Open sources, such as the ISO 27005 standard [32], come with lists of typical vulnerabilities.
- *Non-malicious threat identification:* In the identification of non-malicious threats we make use of the target description to systematically go through the uses and processes of the system in question, both technical and non-technical. Which unintended events may lead to the identified incidents due to the identified vulnerabilities, and how? We also need to carefully consider the interface to the cyberspace to identify non-malicious threats that arise outside of the system. Cyber-systems make use of external services and infrastructures, and accidents or other unintended events that harm such services or infrastructures can cause incidents. For example, if a cloud file server goes down, it may be that systems that depend on it also fail. Relevant sources on typical threats include, for example, the ISO 27005 standard and the NIST risk assessment guide [54], which provide representative examples of non-malicious threats.
- *Non-malicious threat source identification:* For each of the identified threats we identify threat sources in a similar manner. Who are the users of the system, and how can they cause the unintended or accidental events? We also need to consider non-human threat sources, such as failure of hardware or other technical components, wear and tear, acts of nature, and so forth. Event logs and historical data aid the identification of non-malicious threat sources, as do open sources such as the abovementioned ISO standard and NIST guide, which both provide categorized lists.

As for the identification of malicious cyber-risks, we conduct the process iteratively and document the results along the way to produce the risk model that is the final output.

5.3.4 Analysis of Cyber-risk

There are two aspects in particular that distinguish the analysis of cyber-risk from risk analysis in general. First, for malicious threats behind which there is human intent and motive, it can be hard to estimate the likelihood of occurrence. Second, due to the nature of cyber-systems we have several options for logging, monitoring, and testing that can facilitate the analysis. In addition to this there are various open resources that we can make use of.

The mentioned MITRE repositories of attacks and vulnerabilities, for example, offer lists of typical kinds of consequences (such as loss of integrity or confidentiality), and estimates of typical severity (such as low or high). Others, such as the OWASP list of the top 10 security risks [63], come with estimates of the severity of the technical impact of the attacks. Still, when using such predefined estimates, we always need to adjust them to the specific target, assets, and party in question. Other means to aid the consequence estimation include, for example, security testing such as penetration testing and software testing. This helps risk assessors to judge the severity of vulnerabilities, and to explore the possible outcomes of attacks.

We can use similar sources and techniques for the estimation of likelihoods. In some cases we may be able to estimate the likelihoods of incidents directly, but we often need to analyze the causes of risks, namely the cyber-threats and vulnerabilities. Another advantage of doing the latter is that we get a better understanding of the most important causes of cyber-risk. Such an understanding is useful in particular during the identification of risk treatments.

For the analysis of malicious threats we may use techniques for threat modeling to describe aspects such as attack prerequisites, attacker skills or knowledge required, resources required, attacker motive, attack opportunity, and so forth [8, 51, 61]. Similar descriptions can be made for vulnerabilities, such as ease of discovery and ease of exploit. In combination, this information can be used to derive likelihoods of threats and incidents, as discussed further in Chap. 11.

In analyzing threats and vulnerabilities we make use of the techniques mentioned before. For both malicious and non-malicious threats, the aim is to estimate the likelihood of cyber-threats to occur and the severity of the vulnerabilities that the threats may exploit. In combination, these estimates serve as a basis for achieving the main goal of the risk assessment, namely to estimate risk levels. Knowledge about who or what the threat sources are, how they cause threats, and which vulnerabilities the threats exploit also facilitates the estimation of the consequences of the incidents.

5.3.5 Evaluation of Cyber-risk

Following the risk evaluation as described in Sect. 2.4.4, there are four tasks involved in this step, namely risk consolidation, risk evaluation, risk aggregation, and risk grouping. In the following we explain the particular concerns for each of these tasks for the domain of cyber-risk.

- *Consolidation of risk analysis results:* The consolidation of cyber-risk is similar to the general case; we focus on the cyber-risks for which the estimates are uncertain and where this uncertainty may affect the risk level or our decision making. What is specific to cyber-risk is the distinction between malicious and non-malicious cyber-risk, and we must take care and check for any risks that are both malicious and non-malicious. When estimating such risks, we need to take into account both the malicious threats and non-malicious threats together. Consider, for example, the incident of unauthorized access to some sensitive data. If this incident may be caused by either a hacker or some accidental information leakage, we must ensure that we add up the respective likelihoods.

- *Evaluation of risk level:* The evaluation of cyber-risk is similar to the general case. However, for our own convenience we may choose to evaluate malicious and non-malicious cyber-risks separately.
- *Risk aggregation:* For the risk aggregation we do as in the general case and look for situations in which there are individual risks that must be evaluated together when this may yield a higher combined risk level.
- *Risk grouping:* The grouping of cyber-risk is similar to the general case, apart from one thing. Due to the distinction between malicious and non-malicious cyber-risk, we have this additional and useful way of grouping the identified risks. Some treatments, such as intrusion detection, apply mostly to malicious risks, while other treatments, such as security training, apply mostly to non-malicious risks.

5.3.6 Treatment of Cyber-risk

There are two features in particular that distinguish the risk treatment of cyber-systems from the general case. First, the highly technical nature of cyber-systems means that to a large extent the options for risk treatment are also technical. In addition we need to consider the sociotechnical aspects and human involvement. Second, the distinction between malicious and non-malicious cyber-risks has implications for how we can most adequately treat the risks. In the following we discuss these aspects in relation to the treatment options of risk reduction, risk retention, risk avoidance, and risk sharing.

For the treatment option of risk reduction we seek means to eliminate threat sources and threats, reduce the severity of vulnerabilities, or by other means reduce the likelihood or consequence of incidents. In general, the kinds of means and controls useful for risk reduction include: correction, elimination, prevention, impact minimization, deterrence, detection, recovery, monitoring, and awareness [32]. In order to determine how to most effectively and efficiently reduce risk, we make use of the obtained risk models since they give information about the most likely threats and the most severe vulnerabilities.

For malicious threats it may be hard, if not impossible, to eliminate the threat sources. In some cases it might be possible to bring charges or take legal action, but often we seek other means. To reduce the likelihood of threats and the severity of vulnerabilities, we consider the various parts and aspects of the cyber-system in question, and how it interacts with the cyberspace. This includes applications, servers, clients and networks. For non-malicious threats it may, for example, be possible to eliminate threat sources by implementing technical barriers, such as stricter access control to reduce the chance of accidental leakage of sensitive data. Treatments of a more sociotechnical nature include increased security awareness and training, improved security policies, and improved processes and routines.

When conducting the treatment identification we take into account the cost of the possible means of risk reduction. This includes the cost of acquisition, implementation, administration, operation, monitoring, and maintenance of the treatments. Other aspects to consider are, for example, performance issues and the end-user perspective. Some security mechanisms come at the cost of performance, and we need to make sure that the system continues to fulfill any performance requirements. Usability is of course also important. For end users some security controls are too cumbersome. For example, if a password regime is complex, end users may be inclined to have the credentials written down in clear text, for instance, on a sticker glued to the technical device in question.

In conducting the treatment identification, we make use of techniques such as interviews, brainstorming and questionnaires, focusing on the cyber-threats, vulnerabilities, and incidents that cause unacceptable risks. We may also make use of open lists and databases, such as the ISO standards on ICT security [33, 34].

The treatment option of risk retention is similar for cyber-systems as for the general case. For the option of risk avoidance it is sometimes relevant to look for alternatives to current solutions in case these are exposed to unacceptable cyber-risks. This can, for example, be to terminate the use of cloud services or web applications and replace them with in-house solutions.

The final kind of treatment option is risk sharing, for example by sub-contracting or insurance. A specific kind of insurance that is emerging within the domain of cyber-systems is that of cyber-insurance [15]. Cyber-insurance is the transfer of financial risk associated with network and computer incidents to a third party [6]. The cyber-insurance products and market are still immature, but insurance companies are increasingly offering such policies, in particular in the USA, but also in Europe. There are several challenges related to cyber-insurance, such as the assessment of cybersecurity and cyber-risk in terms of monetary cost and benefit. For some organizations, cyber-insurance may, however, be a good way to reduce their exposure to cyber-risk or to reduce uncertainty regarding cyber-risk.

5.4 Monitoring and Review of Cyber-risk

The process of monitoring and review as described in Sect. 2.5 makes a clear distinction between

- monitoring and review of risk, and
- monitoring and review of risk management

In the first case we are concerned with the system in question; in the second case we focus on the implementation and operation of the risk management process for the system in question. This distinction is of course also relevant within cyber-risk management.

5.4.1 Monitoring and Review of Cyber-risk

We benefit from the fact that cyber-systems are computerized, at least to a large degree. The options for monitoring and surveying cyber-risks are numerous. We can, for example, keep logs of the number and frequency of detected attacks or viruses, monitor the network traffic to detect irregularities, gather information from firewalls and intrusion detection systems. For the purpose of risk monitoring it is useful to identify and specify a set of cyber-risk indicators to be monitored. Such indicators may be the frequency of detected attacks, the frequency of successful attacks, the accumulated downtime of specific services over a given time period, or the frequency of rejected logins due to invalid credentials. The current values of indicators give implicit information about the current risk picture at any point in time. To make the best use of indicators, organizations may define procedures or functions for combining them and for mapping them to explicit risk information.

In order to maximize the value of the cyber-risk information that we gather by system monitoring, risk assessments and open repositories, we need efficient and useful means for representing the information. One option is to establish a classification and categorization of information as mentioned previously. An additional option is to establish a risk register where the information is available to all relevant stakeholders. The register may include, for example, top incidents, threats, and vulnerabilities that stakeholders need to be aware of. How organizations represent the data should be adapted to the user roles, so that, for example, management staff, security personnel, software developers, and system architects get the right kind of information for their individual needs.

5.4.2 Monitoring and Review of Cyber-risk Management

Since cyberspace is a continuously evolving and fast-changing environment, the process of cyber-risk management is required to be more dynamic than a conventional risk management process. In fact, it must be largely computerized, and in the future in almost real time.

This means, of course, that the monitoring and review of cyber-risk management must to the extent possible also be computerized; otherwise it will not be possible to react in time. Hence, cyber-risk managers should aim for a computer-based infrastructure to monitor the performance of the cyber-risk management process itself. This includes not only how risk assessments are planned and conducted, but also how and to what extent measures and controls are implemented and how information is obtained and communicated.

5.5 Further Reading

For up-to-date information about cyber-threats, vulnerabilities, and incidents there are several open lists and repositories that can be used such as the MITRE attack patterns [51] and vulnerability lists [52], as well as the lists of security risks. Such overviews often come with estimates of attack likelihood, vulnerability severity, and incident consequence. There are also several organizations that regularly publish statistics on cyber-incidents and top cyber-risks, such as [61, 66, 73, 76, 82].

Some standards and guidelines on ICT security offer lists of threat sources, threats, and vulnerabilities that can be used as input to the cyber-risk identification. This includes, for example, ISO 27005 [32], ISO 27032 [28] and NIST SP 800-30 [54]. The same kinds of standards and guidelines often offer advice on options for cyber-risk treatment. There is also literature and guidance on attacker modeling, for example as provided by OWASP [64] or the Common Criteria [8].

We also refer to Part II of this book where we demonstrate the whole process of cyber-risk assessment.