Chapter 10
Risk Treatment

The final step of the cyber-risk assessment starts with identification of treatments for selected risks, as explained in Sect. 2.4.5 and Sect. 5.3.6. We then assess the effect of the treatments and consider whether the residual risk is acceptable. If it is, the documentation is finalized and the process terminates, otherwise we need to go back and do another iteration of the treatment identification.

10.1 Risk Treatment Identification

The techniques we use for treatment identification are to a large degree the same as those described for risk identification in Sect. 7.1, in particular when it comes to obtaining information from standards and repositories, as well as people. In the following we demonstrate treatment identification with respect to malicious and non-malicious risks.

10.1.1 Malicious Risks

Ideally, we would of course like to find treatments for all identified risks. However, since we always have limited time and resources, we need to focus on those that are most important. We therefore start by selecting risks based on the results of the risk evaluation. Here we make sure to include:

- all individual risks that are not *Low* according to the risk evaluation criteria, and
- individual risks that are part of an aggregated risk that is not *Low*.

For the aggregated risks, we prefer to list each individual contributing incident rather than giving a common, more abstract description. This is because the more detailed descriptions of the individual risks can provide information that is useful for coming

A. Refsdal et al., *Cyber-Risk Management*, SpringerBriefs
in Computer Science, DOI 10.1007/978-3-319-23570-7_10

up with treatments. However, when evaluating the proposed treatments during the risk acceptance later, we will consider the effect on the aggregated risk.

Table 10.1 shows the result of the selection of malicious risks for which to identify treatments. The second column from the right shows whether the risk is part of an aggregated risk. If so, the aggregation is indicated by a plus sign between the individual risk numbers, as in Fig. 9.5. The rightmost column shows whether the risk is part of a group and, if so, which risks are members of the group. The members of a group are separated by a comma.

Table 10.1 Malicious risks selected for treatment identification

No.	Risk level	Incident	Aggr.	Group
1	High	Data from metering nodes cannot be received by the central system due to DDoS attack	No	No
2	High	False control data received by all or most choke components	No	No
3	Medium	False meter data for a limited number of electricity customers received by the central system	No	No
4	Low	Malware compromises meter data	4+11	4,5,6
5	Low	Malware disrupts transmission of meter data	5+12	4,5,6
6	Low	Malware disrupts the choke functionality	6+13	4,5,6

The next step is to identify treatments for the selected risks. Here we make sure to exploit all the information about threat sources, threats, vulnerabilities, and so on that we obtained during the risk identification, as each of these elements may potentially be targeted by treatments. For each risk we therefore create a small table summarizing this information. Table 10.2 and Table 10.3 show the results for risk no. 1 and risk no. 4, respectively. The final row of the table is dedicated to documenting the treatments that we identify. For risk no. 1, the treatment consists of updating the DDoS detection and response mechanism. This could, for example, be achieved by combining anomaly-based and signature-based detection and classification techniques, and allowing malicious packets to be redirected to a controlled part of the network for analysis, rather than being dropped. For risk no. 4, the treatments consist of frequent updating of malware protection on the metering nodes and strengthening the integrity checking of meter data on the central system. While the former reduces the likelihood of meter data being compromised, the latter will increase the chance that compromised data are detected, thereby allowing the central system operator to take appropriate measures.

We make similar tables for the remaining risks from Table 10.1. These tables are not shown here.

Table 10.2 Treatment identification table for risk no. 1

Element	Description
Risk no.	1
Incident	Data from metering nodes cannot be received by the central system due to DDoS attack
Asset	Availability of meter data
Threat source	Script kiddie; Cyber-terrorist
Threat	DDoS attack on the central system
Attack point	Internet connection to the central system
Vulnerability	Inadequate attack detection and response on central system
Treatment	Implement state-of-the-art DDoS attack detection and response mechanism on central system

Table 10.3 Treatment identification table for risk no. 4

Element	Description
Risk no.	4
Incident	Malware compromises meter data
Asset	Integrity of meter data
Threat source	Malware
Threat	Metering node infected by malware
Attack point	Internet connection to the metering terminal
Vulnerability	Outdated antivirus protection on metering node
Treatment	Frequent updates of malware protection on metering node; Stronger integrity checking of received meter data on central system

10.1.2 Non-malicious Risks

For non-malicious risks we select risks in the same way as we did for malicious risks. Table 10.4 shows the result. Risk no. 9 and risk no. 10 are included due to their individual risk level, while the rest of the risks are included either because they are part of an aggregated risk or a member of one of the risk groups identified during the risk evaluation. Notice that we have decided to include risks nos. 14 and 15, which were grouped together during the risk evaluation, even though each of these risks are *Low*.

For each selected risk we compile the information obtained during the risk identification in a single table to facilitate treatment identification, in a similar way as we did for malicious risks. Table 10.5 shows the result for risk no. 9. Two potential treatments are identified, both of a purely technical nature. The first is to ensure that all electricity customers have a redundant GPRS communication link that can be used in case the Internet connection goes down. The second is to ensure that the choke component does not shut off all power to the electricity customer in the absence of control data. Instead, the default mode should be to allow at least 50% of normal power consumption.

Table 10.4 Non-malicious risks selected for treatment identification

No.	Risk level	Incident	Aggr.	Group
9	High	Communication between the central system and the metering terminal is lost	No	No
10	Medium	Same as the row above	No	No
11	Low	Software bug on the metering terminal compromises meter data	4+11	11,12,13
12	Low	Software bug on the metering terminal disrupts transmission of meter data	5+12	11,12,13
13	Low	Software bug on the metering terminal disrupts the choke functionality	6+13	11,12,13
14	Low	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component	No	14,15
15	Low	Mistakes during maintenance of the central system prevent reception of data from metering nodes	No	14,15

Table 10.5 Treatment identification table for risk no. 9

Element	Description
Risk no.	9
Incident	Communication between the central system and the metering terminal is lost
Asset	Provisioning of power to electricity customers
Threat source	Internet connection to the metering terminal
Threat	Internet connection to the metering terminal goes down
Entry point	Internet connection to the metering terminal
Vulnerability	Single communication channel between central system and metering terminal
Treatment	Install redundant GPRS communication for all electricity customers; Ensure suitable default mode for choke component when communication is lost

For risks nos. 14 and 15, which were grouped together during the risk evaluation, we create a joint table, as shown in Table 10.6. The treatments identified here are of both a human/organizational and technical nature. One option is to simply hire more staff, as heavy workload is recognized as a vulnerability. Another option is to develop executable scripts for performing routine maintenance tasks, which may reduce the likelihood of mistakes during such tasks. Notice that this treatment option could potentially also introduce new risks which must be taken into consideration, for example due to bugs in the scripts. Finally, the last treatment option is to enforce a policy to ensure that only senior personnel are allowed to perform non-routine maintenance tasks.

We create similar tables for the remaining risks from Table 10.4. These tables are not shown here.

Table 10.6 Treatment identification table for risks nos. 14 and 15

Element	Description
Risk no.	14 and 15
Incident	Mistakes during maintenance of the central system disrupt transmission of control data to the choke component; Mistakes during maintenance of the central system prevent reception of data from metering nodes
Asset	Provisioning of power to electricity customers; Availability of meter data
Threat source	Maintenance personnel
Threat	Mistakes during update/maintenance of the central system
Entry point	Central system
Vulnerability	Poor training and heavy workload
Treatment	Hire more staff; Develop executable scripts for routine maintenance tasks; Establish and enforce a policy stating that only senior personnel perform non-routine maintenance tasks

10.2 Risk Acceptance

Implementing treatments always carries a cost, either directly in terms of money or indirectly in terms of, for example, reduced system usability and efficiency, as discussed in Sect. 5.3.6. For each treatment we therefore need to weigh its effect against its cost. We first estimate the effect of a treatment in terms of reduced risk level for the affected risks, before estimating its cost.

Conducting an exact quantitative cost-benefit analysis is not feasible when dealing with the kind of assets and scales that we have defined, and it would be hard to map the consequences to a monetary value. Quantifying the cost of treatments can also sometimes be hard, for example if they involve reduced user-friendliness of systems or security policies affecting the behavior of employees. We therefore decide on a simple, qualitative approach where we adopt the same scale for costs as for risk levels, that is a scale consisting of the steps *High*, *Medium*, and *Low*. The cost-benefit analysis then amounts to comparing costs over this scale with reduction in risk level.

To illustrate the approach, we demonstrate the cost-benefit analysis for some of the treatments identified above. We start with *Implement state-of-the-art DDoS attack detection and response mechanism on central system*. This was identified for risk no. 1, *Data from metering nodes cannot be received by the central system due to DDoS attack*, which has risk level *High* before treatment. Implementing the treatment will hardly prevent script kiddies or cyber-terrorists from launching DDoS attacks, so we do not expect it to have any effect on the threat *DDoS attack on the central system*. However, being able to quickly detect such an attack and respond accordingly will reduce the likelihood that the attack actually leads to the incident in question. Moreover, even if the attack succeeds for a while, a prompt response implies that fewer electricity customers are affected, and that they are affected for a shorter period. We therefore conclude that implementing the treatment will reduce

the likelihood of *Data from metering nodes cannot be received by the central system due to DDoS attack* from *Likely* to *Possible* and at the same time reduce its consequence from *Moderate* to *Minor*. This brings the risk level from *High* to *Low*. As risk no. 1 is not part of an aggregated risk or a risk group and the treatment does not apply to any of the other risks, this concludes the analysis of its effect.

To implement the treatment, the central system operator needs to make a significant investment in hardware and network infrastructure to establish a safe and controlled environment where offending packets can be directed for analysis. Moreover, arriving at an adequate set of detectors, preferably combining anomaly-based and signature-based approaches, will take time and effort. The cost of the treatment is therefore *High*. Table 10.7 documents the results of the cost-benefit analysis.

Table 10.7 Effect of treatments

Treatment	Risk	Effect	Cost
Implement state-of-the-art DDoS attack detection and response mechanism on central system	1	High to Low	High
Stronger integrity checking of received meter data on central system	4 11 4+11	Low to Low Low to Low Medium to Low	High
Hire more staff	14,15	Low to Low	High
Develop executable scripts for routine maintenance tasks	14,15	Low to Low	Low

We now move on to risk no. 4, *Malware compromises meter data*, which is part of the aggregated risk 4+11. According to Table 10.3, the treatments *Frequent updates of malware protection on metering node* and *Stronger integrity checking of received meter data on central system* were identified for this risk. Here we illustrate the considerations regarding the latter.

The treatment *Stronger integrity checking of received meter data on central system* is expected to reduce the consequence of the incident. The reason is that recognizing false meter data early allows the central system operator to discard these data and implement corrective measures. Power consumption can to a large degree be predicted from historical data to which the central system operator has access. As soon as received meter data are recognized as false, it is therefore possible to obtain a good approximation of the correct data, which can adequately serve the needs of the central system operator until the situation is restored. We therefore estimate that implementing the treatment reduces the consequence of risk no. 4 from *Moderate* to *Insignificant*, while the likelihood is unchanged. This will, of course, not reduce the risk level of risk no. 4, which is already *Low* before any treatments.

However, we also need to consider whether the treatment affects the risk level of the aggregated risk 4+11, which has risk level *Medium* before treatment. Here we notice that *Stronger integrity checking of received meter data on central system* is equally good for detecting meter data compromised by software bugs and for de-

tecting data compromised by malware. We therefore estimate that the consequence of risk no. 11 is also reduced from *Moderate* to *Insignificant*. Consequently, we also set the consequence of the aggregated risk 4+11 to *Insignificant*, which takes its risk level from *Medium* to *Low*.

It remains to estimate the cost of the treatment. On the central system side the cost is fairly low. Unfortunately, for certain types of metering terminals, implementation of the treatment requires upgrading of the hardware. The cost is therefore set to *High*.

In addition to the above, in Table 10.7 we have also included two of the treatments for the group consisting of risk no. 14 and risk no. 15, even if each of these risks has risk level *Low* before treatment.

Notice that different treatments may affect each other, either by reinforcing each other or to some extent canceling each other out. We need to take this into account in the cost-benefit analysis. In such cases we can add separate entries for the potential treatment combinations and estimate each combination as if it was an individual treatment. Moreover, with respect to costs of treatments we make sure to take maintenance into account if this is relevant. We also need to consider whether treatments may introduce new risks, as discussed earlier concerning the introduction of executable scripts to address risks nos. 14 and 15.

After performing the cost-benefit analysis, it remains to decide which treatments to implement and whether the residual risk is acceptable. In the end, these decisions must be made by the decision makers of the organization for which the assessment is performed. We terminate the process by recording the decisions and finalizing the documentation.

10.3 Further Reading

ISO/IEC 27032 [28] comes with a list of cybersecurity controls that can be utilized for treatment identification. The data breach investigation report by Verizon [82] also provides an overview of critical security controls mapped to incident patterns which can support the identification of treatments. The OWASP overview of the ten most critical web application security risks [63] offers advice on prevention.

The CORAS method [47] provides further advice on the kind of cost-benefit analysis adopted in this section. Moreover, there is a CORAS extension [4] offering techniques and guidelines to establish compliance with ISO/IEC 27001.