Wise Security Risk Assessment Instructions

by Linda Cornwall

Principles

Purpose and Importance of Risk Assessment

The purpose of a risk assessment is to work out what the threats are to your assets, and which threats need your attention.

There are many ways of carrying out a Security Risk Assessment. We do not consider this to be an exact science, but present here some guidelines and a template to help you carry out a risk assessment. It is better to carry out an imperfect assessment than none at all. Any assessment should at least show up some areas which need your attention, and allow you to take action to mitigate the risk of some of the higher risk threats being carried out.

Currently an increasing number of computing security attacks are happening, so the importance of carrying out a risk assessment and addressing some of the higher risk threats is ever increasing. In particular the rise of 'exploits-as-a-service' increases the risk of attacks happening.

Threats to Assets

Security Threats are threats to assets. An asset may be obvious, such as a computer system, a network, scientific data or personal data. The asset may be less tangible, such as your reputation. For example, if some data is leaked or corrupted which is stored on your system, it may not have any monetary value to you, but it probably will to someone. If personal data is accessed by a hacker, you could be fined, have a poor reputation, and people not use your system again. You could consider the asset to either be data, or reputation. Data may be leaked or corrupted due to many threats: a mis-configured system, a software vulnerability, a rogue administrator, or simply someone who releases data publicly unwittingly.

Some threats may be threats to several assets: for example a hacker accessing a mis-configured system may be a threat to personal data, scientific data, and availability of your system as well as allowing your system to be used to attack another system, or to carry out other unlawful acts such as distributing copyright or illegal data or information.

How Fine Grained should the Risk Assessment be?

You should consider how fine grained you wish your assessment to be. For example software vulnerabilities may cause problems, which may be seen as 1 threat. It is possible to have a very course grained risk assessment where for example you define ‘Software Vulnerabilities’ as a threat.

Within ‘Software Vulnerabilities’ there are more fine grained problems due to e.g. zero day vulnerabilities, vulnerabilities which are found in software which is not under maintenance, sites not patching. There may be problems handling software vulnerabilities relevant to your system due to lack of sufficient manpower.

A very course grained risk assessment may define ‘Software Vulnerabilities’ as a threat, a more fine grained assessment may consider various threats within a category of ‘Software Vulnerabilities’.

Likelihood and Impact

The risk is usually computed as the ‘Likelihood’ of a threat being carried out, multiplied by the ‘impact’ i.e. the effect of the threat being carried out.

Numerical Values based on judgement

Actuarial computation of risk is based on knowing the exact cost of the consequences and the likelihood is based on statistics, e.g. for life insurance the probability of a healthy person of a certain gender and age of dying can be calculated fairly reliably from statistics, and the cost of the insurance pay-out is known. For most computing security threats the likelihood and impact are not so easy to compute, as we don't have statistics on likelihood and impact and the situation is changing very rapidly. Hence we have to rely on judgment.

Note that for some threats which have a very high impact, measures should be in place to ensure that the threat is never carried out.

Confidentiality

The work must be kept confidential. You do not want others to know what the weaknesses are on your own infrastructure.

Carrying out the assessment

Establishing who carries out the assessment

First you need to establish who is carrying out the assessment. This may be a group of people in your own organisation, or for a distributed infrastructure it may be a number of people with experience of computer security from across your distributed project.

Decide on the Scope

It is important to decide on the scope of the assessment. This includes factors such as which systems are included, and which are not. It also includes e.g. whether or not to include physical security of machine rooms. It is also worth noting the assumptions made during the assessment.

Threat establishment

Assets tend to be what management focusses on. It is possible to start from assets, then list the threats to each of those assets

It is also possible to start from threats, and list the multiple assets which are impacted if a threat is carried out.

It is easier generally to compute the risk value based on threats, as it is based on the likelihood of the threat being carried out multiplied by its impact. It is also the likelihood which is generally reduced by carrying out mitigation.

The spreadsheet should help form a template in writing the list of threats.

It is also worth considering how fine grained your assessment should be.

At this state you should fill in the following:--

- Asset or Service
- Business Value
- Threat

Management approval of risks and threats

If this activity is not carried out by management you may consider asking management to check and approve the "risk scenarios" which describes all relevant characteristics of a threat, including concerned assets, and ensure that all the assets which need to be protected are included. Management at this point may wish to include other threats and other assets which need to be protected.

Current situation, mitigation in place

After listing the threats, the team should establish what mitigation is in place. It may be convenient to allocate a few threats per person to check and note the mitigation currently in place.

At this stage you should fill in the following:--

- Risk Targets
- Existing Controls
- Still Existing Vulnerabilities/weaknesses
- Description of impact
- Risk Manager (this may be filled in after the computation of the risk)

Computing Likelihood and Impact

We recommend that the values for both likelihood and impact are between 1 and 4, giving a risk value between 1 and 16. However, if previous risk assessments have been carried out using different numbers it may be preferred to do the same as before, in order to compare the result. For example, if a previous assessment based the impact and likelihood on values between 1 and 5, it is reasonable to do this again.

Guidelines on likelihood and Impact

It is sensible to discuss guidelines for likelihood and impact.

Likelihood Guidelines

Likelihood is how often something is likely to happen.
Suggested likelihood guidelines are:--

Guideline	Unlikely to happen	Happens less than once per year	Happens every few months/more than once a year	Happens every 2-3 months or more frequently
Likelihood	**1**	**2**	**3**	**4**

The likelihood may also be considered as the likelihood of the target not being met.

Impact Guidelines

The impact is the impact if a threat is carried out.
The impact may be the impact on a system or service availability, on data, or on reputation.
The impact which is most significant if it happens to a particular threat is carried out should be considered.

Impact on system/service availability	Minimal impact	Minor impact, local service disruption less than 1 week	Serious disruption for multiple users, more than a week	Serious disruption to the ability to deliver service
Impact value	**1**	**2**	**3**	**4**

Impact on data	Minor leak or loss of scientific data	Loss or leak of significant data	Leakage of small amount of personal data, significant leakage of scientific data	Serious data loss or leak, leakage of significant personal data
Impact value	**1**	**2**	**3**	**4**

Methods for computing likelihood and Impact

There are many ways of computing the Likelihood and impact. Here we make 2 suggestions:-

Team meets for a few hours and discusses

This may be a practical approach if a small team of people are carrying out a risk assessment at 1 particular institute. They may discuss and come to a consensus on the likelihood and impact of a particular threat.

Each member of the team provides their own values

This is a practical way for when the assessment is being carried out by a distributed team of people, such as for a distributed infrastructure. All members may provide their own value of 'Likelihood' and 'Impact' in a spreadsheet, and then the average may be taken. The team may discuss (e.g. by telecon) some of the threats which have the highest risk, as well as those where opinions deviate substantially.

It should be noted that the likelihood and impact should be computed taking account of the current mitigations in place. The risk assessment is based on the current situation, not a hypothetical one.

At this stage the Likelihood (probability) and Impact should be filled in.

RISK

The Risk is the likelihood multiplied by the impact. If the recommended scale of 1 to 4 for each is used, this gives a value between 1 and 16. If 1 to 5 is used, this gives a value of 1 to 25.

After this, the following columns should have been completed

- Impact
- Likelihood
- Risk

Dealing with the outcome

Risk Owner

By definition, management IS the risk owner. Management cannot wash their hands of any risk. Ultimately, management has to decide what to do about a risk. However, the owner can appoint an individual or group of people to be the

- Risk Manager

Acceptance of Risk

Management may decide to accept a risk, at the current risk value. That is a matter of choice.

At this stage it is appropriate to specify the

- Approved Residual Risk

Insurance

In some cases the appropriate response may be to take out insurance. For example, management may take insurance against a computer centre burning down. The insurer may wish for a certain amount of measures to be put in place to minimize the likelihood of this happening.

It may also be possible to insure against being sued for loss of or exposure of data. It may be necessary to demonstrate that appropriate measures are in place to mitigate the likelihood of this happening.

Mitigation

Management may decide to mitigate some of the threats having a higher risk value. Mitigation is generally to reduce the likelihood of a threat being carried out.

Mitigation may also in some cases reduce the impact of an event occurring. For example, putting measures in place to prevent a security incident spreading across your network, due to good incident detection and handling, may mitigate the impact of a threat being carried out.

Since the risk is based on the mitigation currently in place, management must ensure they do not remove mitigation such as by getting rid of an activity which mitigates the risk.

Delegation of Mitigation

While management cannot delegate the risk ownership, management can delegate to a team the handling of the risks, and putting mitigation in place to reduce the likelihood of a threat being carried out. For example, management may delegate responsibility for carrying out security incident prevention and handling to their security officers, but that does not mean they have delegated the ownership of risks, merely delegated the task of their mitigation. The risk manager will normally carry out tasks, according to an agreed procedure, to mitigate the risks. If not already done so, here you should specify the Risk manager and any actions to be carried out.

- Risk Manager
- Action items

For each of the threats.

www.wise-community.org