Global Information Assurance Certification Paper

Prabhakar Rajasingham
GSEC Practical Assgnment
Version 1.2B

Threat And RISK Assessments: Some issues

Guidelines for creating a Threat and Risk Assessment

Theat and Risk Assessments: SOME Issues

Guidelines for Creating a Threat and Risk Assessment

Introduction

If you are reading this paper chances are you think that Information Technology systems need to be secured; you may even be the lucky person who has to secure either your own or your client's systems. The next logical question is what do you need to do to secure them?

There isn't any shortage of good advice: the SANS Reading Room contains a great deal. Sadly though, security measures have to fit inside a budget, just like everything else these days. So how can advice be sorted into crucial things that have to be done, important things that will be done as soon as possible and the things it would be nice to have? More to the point, how can the choices be defended?

Risk Analysis as a way of prioritising measures.

Micksch[1] suggests that the way through this problem to be via a Risk Analysis: the results of a risk analysis can be used in a transparent way to allocate resources. His paper goes on to describe a possible approach to creating a Risk Analysis.

The results of a risk analysis will show, explicitly, where the greatest risks to an organisation lie. It follows that dealing with these risks must take the highest priority. Then the next most important risk can be dealt with and so on.

The risk management approach.

The process that the Risk Management Standard follows is quite straightforward.

The larger the impact of some event, the higher the risk it should be assigned. The problem then becomes working out what the impacts of different events are.

For the purposes of Threat and Risk Assessments, the events in question are damage to some Information system assets through threats being realised. Since frequent, small amounts of damage can add up and be as costly as a rare event that causes lots of damage, frequency of the threat occurring has to be

taken into account as well.

The Scope of this paper

In my paper, I will expand on Micksh's approach by discussing some of the elements of Risk Assessment used within the Australian Commonwealth Government and relate it to the Australian/New Zealand (AS/NZ) Standards. While the approaches in these documents are broadly the same as Micksh, there are some important differences, in particular, the explicit treatment of Threats and Risks.

This paper will briefly outline some of the issues that will need to be looked at for a Risk Assessment. This will be done by outlining the approach that is taken by the AS/NZ Standards and the Australian Communication Security Instruction (ACSI) 33 published by the Defence Security Directorate (DSD) which is one of the standards used by the Australian Commonwealth Government.

Some steps that may be helpful in getting started on the process will then be outlined.

Dealing with Risk

The SANS KickStart course discussed Risk. Essentially, for an IT system to be at risk, two things need to exist. Firstly, there has to be a threat of some sort. Secondly there has to be a vulnerability that the threat can use. Only when both of them exist is there a Risk.

Of course, different environments mean different risks; a stand alone PC isn't all that likely to get hacked from the Internet, but life could get interesting if the hard-drive crashes.

Managing Risk

The AS/NZ Standard on Risk management[2] says that the main elements of Risk management are:

1) Establishing the context,

2) Identifying the risks,

3) Analysing the risks,

4) Evaluating the risks,

5) Treating the risks,

6) Monitoring and reviewing, and

7) Communicating and consulting.

Typically a Threat and Risk Assessment (TRA) will deal with the first four steps.

While this paper does not deal with Risk management, it should be noted that the point of having a TRA is to deal with the Risk. According to the Standard, risk is dealt with by:

* Asking if the risk is acceptable,

* If it is, the acceptance is documented,

* If it isn't, one of the following has to happen:

    1) Reduce the likelihood of the risk taking place by either taking steps to reduce the threat or reduce the vulnerability,

    2) Reduce the impact if the risk happens,

    3) Transfer the risk, for example by taking out insurance, or

    4) Avoid the risk altogether.

The Standard goes into a great deal more detail with how risk should be managed, and it is highly recommended reading. The rest of this paper will look at TRAs.

Focussing on IT Security

The Risk Management Handbook of ACSI 33[3], published by DSD focuses this general strategy outlined in the Standard by this sequence of steps:

* Asset Identification

* Threat and Threat likelihood estimation

* Harm estimation

* Risk assessment

* Required risk estimation and countermeasures rating

* Selection of appropriate countermeasures

* Identification of residual risk and risk acceptance.

While the DSD approach does a very good job of addressing steps two to five outlined in the Standard, it doesn't say a great deal about establishing the context. That should be the first step.

Establishing Context

Step one sets the stage for all of the remaining work, including what sort of work needs to be done. Some questions that will need to be dealt with are:

* Which methodology will you be using? A qualitative or a quantitative one? If it's quantitative, are you going to be attaching monetary values to risk or will you be using some other scale? An excellent description of this issue can be found in Grocott[4].

* Who is sponsoring the TRA? A client? The company you work for?

* Which IT system or systems will the TRA be conducted on?

* What are the IT assets and in particular information assets that are on the systems that need protecting.

* What are the boundaries of the system(s)? For example, if there are network links in place that are not owned by the sponsor, are they to be included in the TRA? If there are remote users of the system, does the TRA have to consider the security off-site? Are the PCs on the desk-tops in-scope?

* Will the TRA look only at IT issues, or will it look into related issues such as personnel and physical security?

* How much detail should the TRA look into? Is it a scoping study to identify areas that will need to be looked into in greater-depth? Or is it to be detailed, looking into how every firewall and router is configured?

* Are there existing policy guidelines for conducting a TRA? Government systems and large corporations generally have guidelines. Lardner[5] mentions some of the constraints that are binding on USA government systems.

Identifiying Assets

Finding things that are worth protecting

After setting the context, at the very least you will know what needs

protecting and where it lives. ACSI 33 suggests an approach to identifying assets:

* **Confidentiality.** Think about what information is the most sensitive. Could that information be considered a valuable asset? Are there less sensitive assets that could be more valuable? Where does the information live? Protecting a mainframe and protecting a notebook are very different propositions.

* **Integrity.** What information has to be accurate? Client database information is one obvious place. A related issue is, how do you know if the information has been corrupted? If there is no way to discover corrupted information (until the company gets an angry phone call) perhaps this information needs to be added to the list.

* **Availability.** Think about resources and systems that the company will die without. At the same time, think about how long things can go for before the company does die. If you have access to it, the Business Continuity Plan or Disaster Recovery plan would be a good place to start. If your company has done any work in the lead-up to Y2K, have a look at that material. You might be able to update it.

* **Equipment.** There is a whole bunch of stuff here that need to be looked at. Buildings get broken into and equipment gets stolen. But more and more there is a trend, especially in management, for mobile computing. That means notebooks, generally with sensitive company data on them packaged in a convenient carry-case.

* **Staff.** People have a lot of information in their heads and sometimes, if offered the right inducements, will pass it on. Staff are mentioned here for completeness but this is a large topic all of its own and will not be discussed further.

* **Physical.** Again this is an area that is a specialised area and a critical pat of any security strategy. As reams could be written on this topic, it has been included for completeness but will not be discussed further.

Looking through this list it will become very obvious that a careful analysis of every single item that your company has will take far too long. So the question now becomes, which assets are the ones that are going to be looked at in detail? When you identify them, at the same time identify the owners of the assets.

One of the things that you will do to finish this section of the TRA process is to document which assets you are going to consider (generally the most important ones) and why you've decided to focus on them (why are the selected

assets the most important ones?) Documenting all the steps that you've taken to get to this point is going to speed up the process for the next time that you do this and makes your reasoning clear.

Threats and liklihoods

What can happen to the assets?

The next thing to look at is threats to your assets. Some threats are just about universal (for example fire, flood and earthquake) but some aren't (a stand-alone system isn't all that likely to be hacked from the Internet.)

The bad news here is that you still have to decide what sort of threats you're going to look at. Of course the interesting one is always going to be external threats such as hackers but there are more mundane things to be considered. For example:

* How good and pure is your power supply? If your power is dirty, and you don't have filters, how long before a major server dies?

* What is the crime rate like in the area around your office? How often have similar offices to yours in your area been broken into? Crime statistics may make interesting reading.

* How about fire risk? Or flood or earthquake for that matter?

When you look at these sorts of issues, maybe your biggest threat isn't hackers coming in via the Internet.

Typically though, one of the things that you will be looking at is the risk that you are exposed to from the Internet. Beck[6] looks at the sorts of human threats that are likely to affect IT systems and estimates how likely they are.

How often might it happen?

Once you have a list of threats to your systems, you have to look at how likely it is that each threat will affect your system. The problem here is that some threats are harder than others to get numbers for: it is much easier to get an idea of how likely it is to face a flood or an earthquake than it is to estimate how often you're going to be hit by a hacker.

One approach to getting a handle on frequency is to use the framework of seven steps from "Negligible" to "Extreme" that ACSI 33 uses. A similar approach is in Appendix E of the Risk Management Standard talks about a range of five steps from "Rare" to "Almost Certain." One may be more suitable for you than the other

When you have finished this step, you will have a large list of threats from which you have selected some threats to focus on, and assigned a likelihood of the threat being realised. You now need to document your reasoning for both the selection of the threats and the likelihoods.

To summarise it you might set up a table with two columns. For example it could look something like:

Threat	Likelyhood
Attack via the Internet	Very High
Flood	Very low
Illegal modification by staff	Negligible

- *Table: Threats related to consequences*

What happens if it turns to custard?

At this point you can start putting things together.

You have a list of assets and a list of threats against them. Ignoring for the time being how likely the threats are for each asset think about the threats that can affect them and work out how much damage will be done. Clearly there will have to be significant input into this step from the owners of the different assets.

When thinking about this start assigning consequence ratings. ACSI 33 has a set of five steps ranging from "Minor" to "Grave" and the Risk Management Standard has five steps from "Insignificant" to "Catastrophic." Typically people are uncomfortable assigning a label but it is the only way to keep things under control.

Recording this will be a bit tedious because a great deal of reasoning will have to be captured. To summarise it you might set up a table with three columns. For example, using the steps specified in ACSI 33 it could look something like:

Assets	Threat	Consequnces
Customer database	Attack via the Internet	Serious
	Flood	Significant
Personnel database	Illegal modification by staff	Minor

- *Table: Assets related to consequences*

At this point you know what you are protecting (your assets) what you are protecting them from (the risk) and what will happen if the threat is realised (the consequences) Well and good, but how does this help? Where do you start?

The next step is to get the risks into priority order. The way that this happens is discussed in several places (ACSI 33, Beck's paper and the Standard.) Central to this process is the idea that a risk with a high likelihood but not very serious consequences is as worrying as a very unlikely risk that has very serious consequences.

For example, consider two possible threat and risk combinations:

* Suppose the likelihood of a web server being compromised is high (say it happens every couple of days) but the consequences aren't that serious, it just has to get rebuilt afterwards (say half an hour for one of the server staff).

* On the other hand, it's pretty unlikely that someone might break into the office and steal large quantities of the equipment including a bunch of high-end servers. Similar offices in the same area as yours have been broken into about once a year. The consequences here are much more serious.

When you compare the two combinations over a given year, the cost of all of those restores might well turn out to be about as expensive as a single break in. Therefore, the risk of both of those should be treated as about the same.

So much for the theory. Actually working out the risks is a very straightforward process. There are tables in both ACSI 33 and in the Risk Management standard that index threat likelihood against consequence level. You could grow the table that you developed in the last section to look like this, if you used the table in ACSI 33:

Assets	Threat	Likelyhood	Consequnces	Risk
Customer database	Attack via the Internet	Very High	Serious	Extreme
	Flood	Very low	Significant	Low
Personnel database	Illegal modification by staff	Negligible	Minor	Nil

■ *Table: Threat and Risk summary*

On the face of it, it looks as if something will have to be done about protecting the customer database, but the Personnel database isn't really worth worrying about.

What you have now is quite an impressive document. It lists the threats that your most important assets face and how at risk they are. The next logical question is: how much needs to be done to protect them? That, alas, is the first step out of the Threat and Risk Assessment process into the Risk Management process so we won't be taking it.

If you have persisted this far, you are the proud owner of a Threat and Risk assessment! Congratulations!

* **Establishing the context.**
    - Which methodology will you be using?
    - Who is sponsoring the TRA?
    - Which IT system or systems will the TRA be conducted on?
    - What are the IT assets that are on the system that need protecting?
    - What are the boundaries of the system?
    - Will the TRA look only at IT issues, or will it look into related issues such as personnel and physical security?
    - How much detail should the TRA look into?
    - Are there existing policy guidelines for conducting a TRA?
* **Finding the assets.** Things to think about:
    - Confidentiality
    - Availability
    - Integrity
    - Equipment
    - Staff
    - Physical
* **Identifying the threats.** Some possibilities are:
    - Forces of nature
    - Insiders
    - External attackers
* **Think about likelihood**

- How often will each threat manifest?
- Pick an approach to summarising the likelihood

* **Estimate consequences for each threat.**
    - For each asset, what will happen if the threat actually happens?
    - Summarise the consequences.

* **Finish the Risk Assessment**
    - Using the table in either the ACSI or the Risk Management Standard, look up the Risk for each Threat and Consequence.

* **Relax!**

aPPENDIX

Threat Likelihood and Impact definitions, and consequence levels

ACSI 33[7]

These definitions for threat likelihood, definition of impacts and consequence level are taken from ACSI 33. It is strongly recommended that you read the publication before using the tables.

Likelihood	Definttons
Negligible	Unlikely to occur
Very Low	Likely to occur two/three times every five years
Low	Likely to occur every year or less
Medium	Likely to occur once every six month or less
High	Likely to occur once per month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times per day

▪ *Table: Threat Likelihoods*

Impact	Definition
Minor	Will have almost no impact if threat is realised
Significant	Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals or agencies. Will require some expenditure of resources to repair (eg "political embarrassment")
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. Will require expenditure of significant resources to repair
Serious	May cause extended system outage, and/or loss of connected customers or business confidence. May result in compromise of large amounts of Government information or services

Grave	May cause system to be permanently closed, and/or be subsumed by another (secure) environment. May result in complete compromise of Government Agencies

- *Table: Impact descriptions*

		Consequence					
		Insignificant	Minor	Significant	Damaging	Serious	Grave
THREAT	Negligible	Nil	Nil	Nil	Nil	Nil	Nil
	Very Low	Nil	Low	Low	Low	Medium	Medium
	Low	Nil	Low	Medium	Medium	High	High
	Medium	Nil	Low	Medium	High	High	Critical
	High	Nil	Medium	High	High	Critical	Extreme
	Very High	Nil	Medium	High	Critical	Extreme	Extreme
	Extreme	Nil	Medium	High	Critical	Extreme	Extreme

- *Table: Risk*

AS/NZ4360:1999[8]

These definitions for threat likelihood, definition of impacts and consequence level are taken from the Standard. As the Standard talks about risk generally, the definition are not as precise as the ACSI, but you should be able to get a feel for what is meant.

The publication talks about a great deal more, so it is strongly recommended that you read it.

Impact	Definition
Almost Certain	Is expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Might occur at some time
Unlikely	Could occur at some time
Rare	May occur only in exceptional circumstances

- *Table: Threat Likelihoods*

Descriptor	Example detail description
Insignificant	No injuries, low financial loss
Minor	First aid treatment, on-site release immediately contained, medium financial loss
Moderate	Medical treatment required, on-site release contained with outside assistance, high financial loss
Major	Extensive injuries, loss of production capability, off-site release with no detrimental effects, major financial loss.
High	Likely to occur once per month or less
Very High	Likely to occur multiple times per month or less
Catastrophic	Death, toxic release off-site with detrimental effect, huge financial loss

- *Table: Impact*

		Consecuences				
		Insignificant	Minor	Moderate	Major	Catastrophic
THREAT	Almost Certain	High	High	Extreme	Extreme	Extreme
	Likely	Moderate	High	High	Extreme	Extreme
	Possible	Low	Moderate	High	Extreme	Extreme
	Unlikely	Low	Low	Moderate	High	Extreme
	Rare	Low	Low	Moderate	High	High

- *Table: Threat and Risk summary*

Extreme risk: Immediate action required

High risk: Senior management attention needed

Moderate risk: Management responsibilities must be specified

Low risk: Mange by routine procedures.

---

[1] Micksch, Allan. "Information Systems Risk Analysis, Assessment and Management" September 13, 2000 URL: http://www.sans.org/infosecFAQ/policy/risk.htm (April 4, 2001)

[2] Standards Australia, Risk Management AS/NZ 4360:1995. Sydney :Standards Australia,1995, p7

[3] Defence Signals Directorate. "Australian Communications – Electronic Security Instruction 33: Handbook

3 – Risk Management, Version 1.0"Decmber 20, 2000 URL: http://www.dsd.gov.au/infosec/acsi33/HB3.html (April 4, 2001)

[4] Grocott, Darren. "Security Risk Analysis, selecting the right methodology." GIAC Information Security KickStart Practical Assignment for Certification V2.0 2000

[5] Lardner Jr, Thomas P. "Risk, Vulnerability Assessments, PDD63 and Risk Management – An Overview" November 22, 2000 URL: http://www.sans.org/infosecFAQ/threats/threats_list.htm (April 4, 2001)

[6] Beck, David F. "A Review of Cybersecurity Risk Factors" January 16, 2001 URL: http://www.sans.org/infosecFAQ/securitybasics/risk.htm (April 4, 2001)

[7] Defence Signals Directorate. "Australian Communications – Electronic Security Instruction 33: Handbook 3 – Risk Management, Version 1.0"Decmber 20, 2000 URL: http://www.dsd.gov.au/infosec/acsi33/HB3.html (April 4, 2001)

[8] Standards Australia, Risk Management AS/NZ 4360:1995. Sydney :Standards Australia,1995, p34–35

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS