

RISK ANALYSIS APPROACH FOR THE SECURITY OF HIGH SPEED NETWORK LINKS

By Andrew Younger CISSP

When making the decision to secure your High Speed network, you need to ensure that decision is appropriate for your organisation, and in line with the organisational security policy. The process used to determine what needs to be done is sometimes called the Risk Management Process. In Australia and New Zealand it is defined by the Australian and New Zealand Standard for Risk Management (AS/NZS 4360:2004). In its own words, the Standard can be summarised as:

“The Standard provides a generic guide for managing risk. The Standard provides guidance to enable public, private or community enterprises, groups and individuals to achieve:

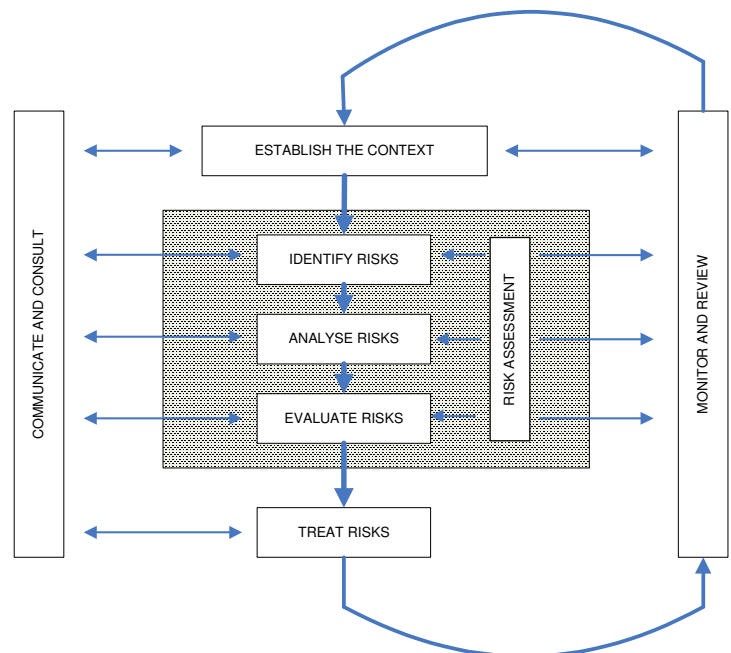
- *a more confident and rigorous basis for decision-making and planning;*
- *better identification of opportunities and threats;*
- *gaining value from uncertainty and variability;*
- *pro-active rather than re-active management;*
- *more effective allocation and use of resources;*
- *improved incident management and reduction in loss and the cost of risk, including commercial insurance premiums;*
- *improved stakeholder confidence and trust;*
- *improved compliance with relevant legislation; and*
- *better corporate governance.”*

We will follow through the various sections of the Standard, and show how this can be applied to the security of high speed networking links.

Risk Management Approach

Senetas follows the processes outlined in the above Standard (AS/NZS 4360:2004). When dealing with matters relating to Information Security, Senetas bases all recommendations on the Standard, in order to provide consistent, reliable information and advice to our customers.

The Risk Management approach involves identifying risks, analysing and evaluating these risks, and then treatment of the risk. Not all risks can be totally removed, and some residual risks remain, therefore it is important to have a monitor and review step, which can be used to restart the process. This ensures organisations do not lose sight of all the relevant risks that may occur, since regulatory, legal, and technological landscapes are prone to change. Constant review of risk mitigation strategies is needed to ensure changing circumstances do not alter priorities.



The Risk Analysis for High Speed Network Links

We will concentrate on the three main steps of the Risk Management Process: Identification, Analysis and Evaluation.

1. Identify the Risk

For any high speed link there are a number of security risks:

- (i) Information travelling across the link is vulnerable to interception;
- (ii) Information travelling across the link is vulnerable to manipulation;
- (iii) Information is injected onto the link;

These three well understood risks typically lead to the implementation of preventative security measures, such as deployment of network firewalls and some form of encryption solution.

This therefore creates a further risk that:

- (iv) The current security solutions being employed are not flexible enough or don't perform well enough; encryption is not being used, it is being used very selectively, or used in a manner that negatively impacts the ability of the network to deliver its business objectives.

2. Analyse the Risk

Risk Analysis is about developing an understanding of the risk. This involves consideration of the sources of risk, their positive and negative consequences and the likelihood that those consequences may occur.

For the purposes of this document and to keep the discussion brief, we will use "Low", "Medium" and "High" to categorise the magnitude, the likelihood and the level of risk for each of the identified risks above. This is by no means a thorough approach, but is useful in that it helps to understand how the process works.

	Magnitude	Likelihood	Level of Risk
(i) Interception	High	Medium	Medium
(ii) Manipulation	Low	Low	Low
(iii) Injection	Medium	Low	Low
(iv) Inadequate protection	High	High	High

It is very common for security and networking professionals to concentrate on the first three risks. However you can see from the table above that the choice of technology used to secure your high speed network is important – It has the potential of being a very risky proposition if the wrong decision is made.

It is extremely common for network security solutions to be very selective in what they secure and what they don't. When a new application is added to the network, the network encryption needs to be modified, and this is usually on a live network. This is time consuming - resulting in network downtime - and potentially very complex, which can result in simple mistakes being made. A more reasonable approach is to assume that all traffic on the network is as sensitive as the most sensitive application, and therefore the whole link needs to be secured in a way that ensures the network runs at a reasonable level of performance.

3. Evaluate the Risk

The purpose of risk evaluation is to make decisions, based on the outcomes of risk analysis, about which risks need treatment and treatment priorities.

In our example above, choosing an encryption solution that is: (1) simple to setup and configure, (2) performs as fast as the network operates and (3) creates no additional latency and complexity, should be a high priority once you have identified the need to protect against interception of data on the network. The Senetas CypherNet encryption hardware is specifically designed for this purpose.

The Senetas CypherNet Encryption Security Platform, developed in Melbourne, Australia and used around the world, comprises standards-based, purpose-built solutions that enable organisations to achieve their business goals through unsurpassed levels of network performance, efficiency and security, without compromise. Senetas Security products are accredited to the highest international levels, including FIPS 140-2 Level 3 and Common Criteria EAL4.

In Conclusion

The Standard for Risk Management (AS/NZS 4360:2004) is an excellent document that outlines a process that is very simple to follow and one that all organisations should adopt. By taking a thorough view of what you need to achieve, and by prioritising the requirements against the risks, organisations can clearly navigate their way through the complexity that is business in the 21st Century. According to the Standard "Organisations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at lower overall cost".

About Senetas

Senetas Corporation Limited (ASX Code: SEN) is an Australian ASX company and is the world's leading developer and supplier of high speed network encryption hardware products. Its products are accredited to the highest international government security standards. Customers include Government departments in the USA, Australia, the Middle East, Asia, and European Countries as well as some of the world's leading financial institutions.

For further information please contact the Senetas Team:

- Horst Marcinsky (horst.marcinsky@senetas.com)
- Don Babbs (don.babbs@senetas.com)
- Andrew Younger (andrew.younger@senetas.com)
- Julian Fay (julian.fay@senetas.com)