

# SecurityElectronics

SOLUTIONS FOR SECURITY MANAGERS AND INSTALLERS

February 2006 Issue 263

## global automation

- Supporting locking systems
- NICE wins De Beers contract
- Secure wireless networking
- Simulating border security
- The future of smart cards
- Risk management strategies
- Lenel's management software

PP 255003/03820

ISSN 1444-2647



9 771444 264006



# PROTECT YOUR INTERESTS

Risk Management is a tried and tested, logical way to lessen the impact of those incidents that might adversely affect an organisation. The Risk Management process must be accurate and logical to be of benefit – but there are many obstacles and standards only take you so far...

By Simon Hensworth\*.



Australian Standards for Risk Management are detailed in AS/NZ 4360:2004 and HB 436:2004. These provide a good source of fundamental concepts and suggested methods for tackling Risk Management. It is not possible for the Standards to demonstrate a Risk Management method to suit every situation. AS/NZ 4360 provides the basis for the process, and organisations need to take this and run with it. This is where some organisations experience difficulties. The AS/NZ 4360 platform often needs to be extended or expanded in order to become a system that an organisation can use, whilst suiting its needs.

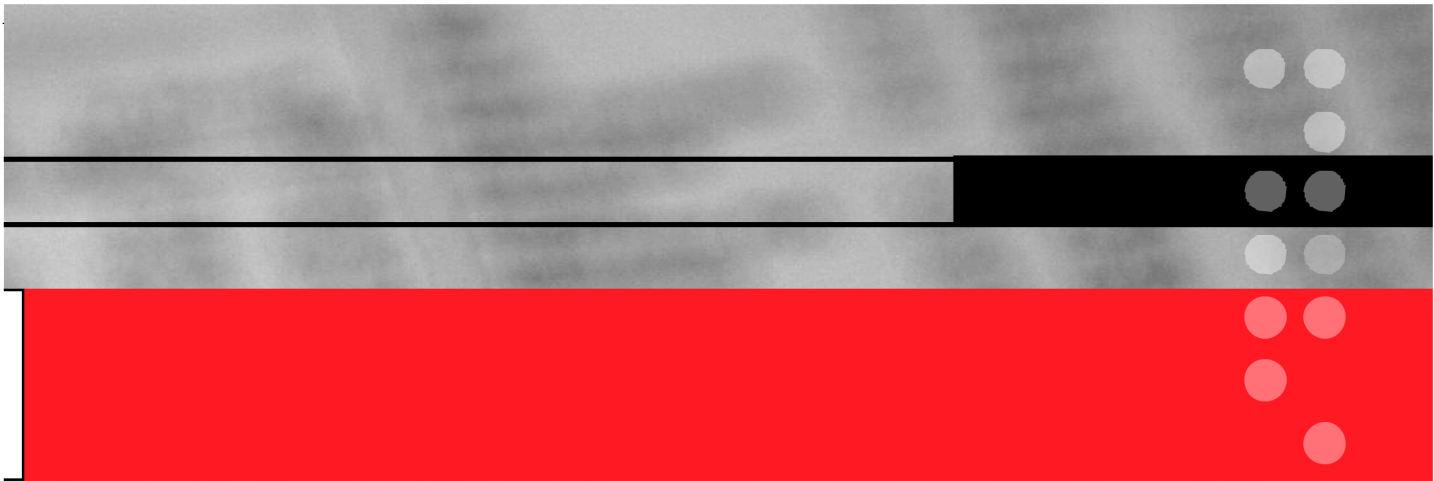
Organisations can experience problems when

expanding on AS/NZ 4360 methods to tailor a system to their own requirements. Common problems include:

- Creating a system that is too complex
  - Setting Likelihood and Consequence parameters that do not reflect reality for their organisation
  - Manipulating a system to get the outcome you want to see (rather than the reality)
- Ignoring (or accepting) risks that are 'too difficult' to manage

#### DEALING WITH COMPLEXITY

If a Risk Management process is made too complex it can be difficult to "see the forest for the trees". Some Risk Management processes evolve into



An organisation needs to decide for itself what is a low-risk, what is a high-consequence, and what is a moderate-likelihood. These scales cannot simply be plucked from a standard. Scales need to reflect the reality for the organisation. Setting Likelihood and Consequence scales requires careful consideration of the strategic, tactical and operational goals of an organisation.

**ONE SCALE**

Generally, an organisation should use one Likelihood and Consequence scale to ensure that risk is managed in a uniform manner. There are some instances where an organisation may have more than one scale, for example, one for strategic-level-risks and one for operation-level-risks. However, these should be relative to each other. For example, higher-risks on the operational-level-scale would probably equate to lower-risks on the strategic-level-scale.

An organisation can run into problems if they manipulate the system to make a situation look better than it is. For example, if a risk is weighed as 'high' on the existing scale (and cannot be reduced further-but is unacceptable as 'high') an organisation might consider introducing a new Likelihood and Consequence scale that gives the same risk a level of 'moderate or low'. This is a dangerous practice. If this risk is realised and there is an investigation into the incident and multiple (conflicting) Likelihood and Consequence scales are identified, an organisation will appear to be 'manipulating the system'. An organisation that 'manipulates the system' in this way is only digging itself a deeper hole.

**DESIGN FOR PROTECTION**

Some organisations can run into problems when they lose sight of the big picture. The Risk Management process can become a game of 'how good can I make it look', when the point of Risk Management is to protect an organisation. Making the situation look better than it really is, is dangerous. This can lead to risks not being treated, or a lack of on-going management of risks.

**INHERENT RISKS**

There are often situations where an organisation will engage in activity that has inherent risk that cannot be reduced, avoided, or shared via a single risk treatment measure. Sometimes the only way to deal with this type of situation is through ongoing

complex mathematical systems but this can tend to 'blind' the situation. Too much emphasis can be put on fine detail, while ignoring the bigger picture. Complex mathematical systems can also make it difficult to identify mistakes or find where the root of a problem lays. When systems become too complex, they can also become too difficult to use as often as they should be used.

**ORGANISATION SPECIFIC**

AS/NZ 4360:2004 and HB 436:2004 provide examples of Likelihood and Consequence scales that are excellent guides for organisations to adopt. However, the standards cannot provide scales that suit your specific organisation.



“There are often situations where an organisation will engage in activity that has inherent risk that cannot be reduced, avoided, or shared via a single risk treatment measure...”

management of the risk. This type of situation is often the case where a risk has higher-scale consequences and lower-scale likelihood.

Higher-scale consequence/ lower-scale likelihood type risks will usually produce a mid to high risk level. When they end up with a higher risk level they can become a dilemma for those charged with the responsibility to manage them.

Inherent risks will sometimes be difficult to reduce or treat, and so become a vexing problem for managers of risk. There is potential for an organisation to ignore (or accept) these type of risks, because of the difficulty in treating or managing them. This can be a dangerous practice, especially if it is a risk that involves consequences of harm to people. If a risk has been identified and appears on Risk Management records but is not actioned, and then the risk is realized and someone is seriously injured or killed; the subsequent investigation can be a catastrophic event for an organisation.

Sometimes the only way to treat inherent risks is on-going management of the surrounding elements connected to the risk. For example, regular inspections, training, awareness campaigns and crisis management plans, and identifying and documenting risks on a regular basis.

**NO WAY TO PREDICT THE FUTURE**

It can be easy to forget that much of Risk Management is about predicting the future.

Consequences can often be quantifiable, but what is the likelihood of a particular incident happening in the future? Obviously, some incidents are easier to predict than others. Commonly occurring incidents are probably quite easy to predict with a certain accuracy. But what about those catastrophic incidents that might only occur once in a blue moon? Some incidents cannot be predicted with accuracy, and should be considered as such. Risk Management should be a logical way to manage risks, remembering that there is no perfect way to predict the future.

**INFO, INFO, INFO**

Accurate information is the best basis for 'predicting the future'. Organisations should be implementing whatever strategies they can to collect and record all the relevant information available that can contribute to the accuracy of the Risk Management process. Records of past incidents can be a good predictor of future incidents. It takes time to develop a good system that will accurately capture all events. Complex systems can be too difficult to use and so some events may get overlooked because they were never recorded.

Records should link into Likelihood scales. Consider the following Likelihood scale:

Descriptor	Description
Almost Certain	Once a year or more frequently
Likely	Once every three years
Possible	Once every ten years

But what if an organisation's records only go back for five years? How would we know if an incident occurred once in the past ten years if it occurred more than five years ago? (beyond the five-year records). Considering the table above, this organisation should maintain incident records for a minimum of ten years. Once records reach beyond ten years, the organisation could review its Likelihood scale to incorporate rarer-than-once-in-ten-year incidents.

However Risk Management is done, it should ensure that it is of benefit to an organisation, is realistic, logical, trackable and will stand up to outside scrutiny. ▽ ▽ ▽

*\*Simon Hensworth is a Senior Security Professional with global engineering consultancy GHD based in GHD's Defence and Security stream - Asset Protection Group located in the GHD Perth Office. Simon has a Bachelor of Science Degree in Security Science from Edith Cowan University and has provided security solutions for many clients with major assets in Western Australia. T 61 8 6222 8640, E simon.hensworth@ghd.com.au*