DSW Consulting Pty Ltd

ABN: 88 131 241 113
NSW SECURITY MASTER LICENCE: 409991858
ACT SECURITY MASTER LICENCE: 17501699
VIC SECURITY REGISTRATION: 716 877 70S
QLD SECURITY ADVISOR LICENCE: 3440620

www.dswconsulting.com.au

Enterprise Security Risk Assessments

"*What are we trying to protect and why?*"

Donald S. Williams CPP

Introduction

Executives and managers understand the need to protect the assets of the organisation and to do this they engage guards and security managers/supervisors at the local level. An enterprise security risk assessments (ESRA) is about looking at security in a different, broader way – supporting organisational capability.

An enterprise security risk assessment is an assurance tool utilised at the highest level possible to assess if the assets and functions of the organisation are protected. It can also be used to consider the security of future activities.

This article outlines the concept and value of the enterprise security risk assessment and is based on enterprise-wide security risk assessments conducted for a range of government and corporate clients.

Enterprise Security Risk Assessment

To gain an oversight of what is encompassed by the concept of ESRA it is of benefit to review each element of "Enterprise - Security - Risk Assessment", in reverse order.

Risk Assessment

As per ISO 31,000 and the earlier AS 4360, a risk is an event that could occur, the results of which may be beneficial or harmful. Risk Assessment is a methodology for defining what could happen, why, when, the effects and to identify mitigation treatments to reduce unwanted risks to the lowest reasonable level. An assessment of the risks leads to the ability to manage the risks.

The usual matrix-based methodology requires identification of the context, identification of assets and threats, the definition of the risks, determination of likelihood and consequence and their alignment on an agreed matrix to determine the risk rating. The resultant rating providing the basis for priority of treatment.

The risk is mitigated by either reducing the likelihood of the event occurring (by fixing some or all of the exposures identified in the Likelihood part of the assessment) or reducing the Consequences should the risk be realised. In all cases the proposed risk mitigation treatments must be related to the observations in the assessment.

Once the mitigation treatments have been identified the "residual risk", should the proposed treatments are implemented, can be calculated based on the reduced likelihood and/or consequences.

An enterprise security risk assessment uses a similar approach but differs primarily in the breadth of the assets and functions considered and of the existing and potential mitigation treatments reviewed. The enterprise security risk assessment seeks to ensure the entire organisation is protected from all reasonable security threat vectors.

Security

The definition of security used here is protection from deliberate, malicious human action or "*Human Initiated Threat (HIT)*". Other management disciplines protect from human error, mechanical failure and alternate sources of damage and loss to the organisation as shown in Figure 1.

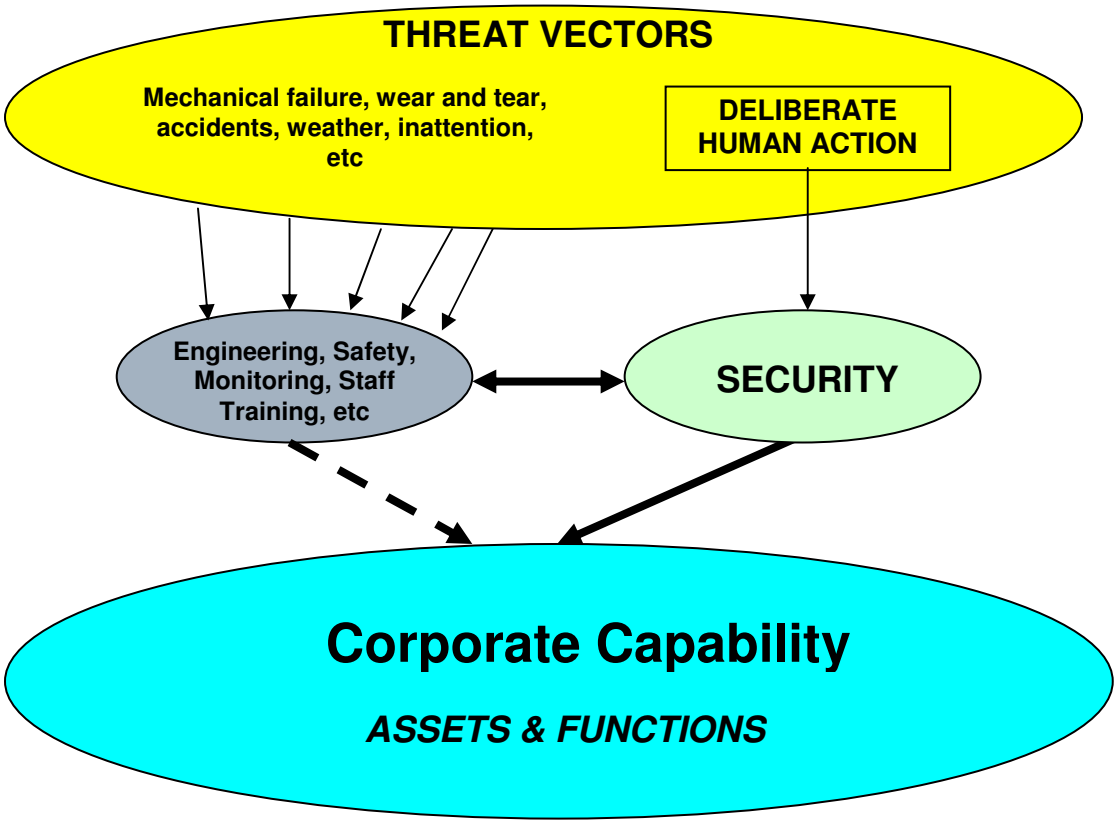

Figure 1 Threat - Asset Relationship

An organisation can use a number of tools to assess its security:

- Risk Assessments
- Compliance checks
- Threat assessments
- Vulnerability assessments
- Loss estimates

These are all elements of an enterprise security risk analysis.

Enterprise

An enterprise-wide assessment requires looking at issues from the organisational perspective: "*what are we trying to protect and why?*". The "what" are the key assets and functions that support the business. The "why" is to align security to the strategic goals of the organisation.

At the tactical (guards) and operational (supervisor/manager) levels security measures relate to the assets and threats in the immediate area of responsibility. Enterprise thinking requires a broader view. It requires consideration of:

- The organisation's aims, goals and image.
- Not only assets but the functions; protecting what we *do* as well as what we *have*.
- An understanding of other skills/disciplines and how they relate to security, for example:
  - Emergency management,
  - Workplace Health and Safety,
  - Human resources such as post-incident counselling,
  - Facility management,
  - Business Continuity/Resilience planning,
  - Media management, and
  - Environmental management.

Once an ESRA has been completed for the entire organisation the same methodology and mind set can be used to assess each main business unit (BU). Asking:

- Does the individual BU, because of its assets, functions and threats, have all of the enterprise risks identified for the organisation, if not which ones do not apply?
- Does the individual BU have additional key risks not identified for the organisation, if so what are they? (Perhaps there is a particular asset that only exists within this BU or overseas staff or particular compliance requirements?)
- Does the BU have particular mitigation measures that alter the organisational risk rating in their particular context? Or, are they limited from applying some of the organisational mitigation measures?

Examples include the differences between a BU that conducts bulk storage and one that has retail activities, or the considerations for a corporate headquarters as opposed to a mining or manufacturing BU.

"Enterprise" can also relate to a new opportunity or endeavour. When the organisation looks to take on new activities or assets it is of benefit to conduct an assessment to determine what security exposures will be generated and what new threats may result. New locations, new business processes, new relationships all deserve a security assessment.

Another case for an enterprise security risk assessment is to pre-plan for an event that might occur where the specifics of the event can not be known but the general nature of the threat can be predicted. An enterprise security risk assessment can provide general guidance as to what protective and response measures may be required. The specific details of the measures can be further determined if the event becomes more likely and the location can be identified. The security considerations for organisational response to a natural disaster might fall into this category.

Definition of ESRA

If enterprise security is "*ensuring the organisation is free to meet its goals protected from deliberate, malicious human action*" then the purpose of an enterprise security risk assessment is assurance.

- Assurance that adequate levels of protection are in place.
- Assurance that appropriate response measures are in place.
- Assurance that future activities and assets will be protected.

What are <u>Enterprise</u> security risks?

Defining the risk is often the most difficult part of the risk assessment process. Often risks are (incorrectly) expressed in terms of the threats e.g. "terrorists" which is actually a source of risk. Or, in terms of consequence e.g. "tools are stolen from the workplace", this is not the risk, rather it is a consequence of a risk such as "failure to protect tools".

Risk should be expressed in relation to the asset or function being protected. Enterprise risks relate to the entire organisation or at least a complete business unit. It is suggested that Enterprise risks may include:

- Failure to protect People.
- Failure to protect Information.
- Failure to protect Equipment.
- Failure to protect Reputation. (Collectively referred to as: PIER)

(Each of the above at the highest grouping that can effectively be assessed).

- Failure to identify a security incident.
- Failure to respond appropriately to a security incident.
- Failure to comply with (specific security-related requirement).

Figure 2 shows a potential breakdown of "People" as an asset at the highest levels possible for a security risk assessment. In this case the environment is a judicial court system where four distinct populations have been identified, each having its own threats, exposures and vulnerabilities. To enable accurate assessment two of the populations are further refined due to their movements, locations and specific security considerations.

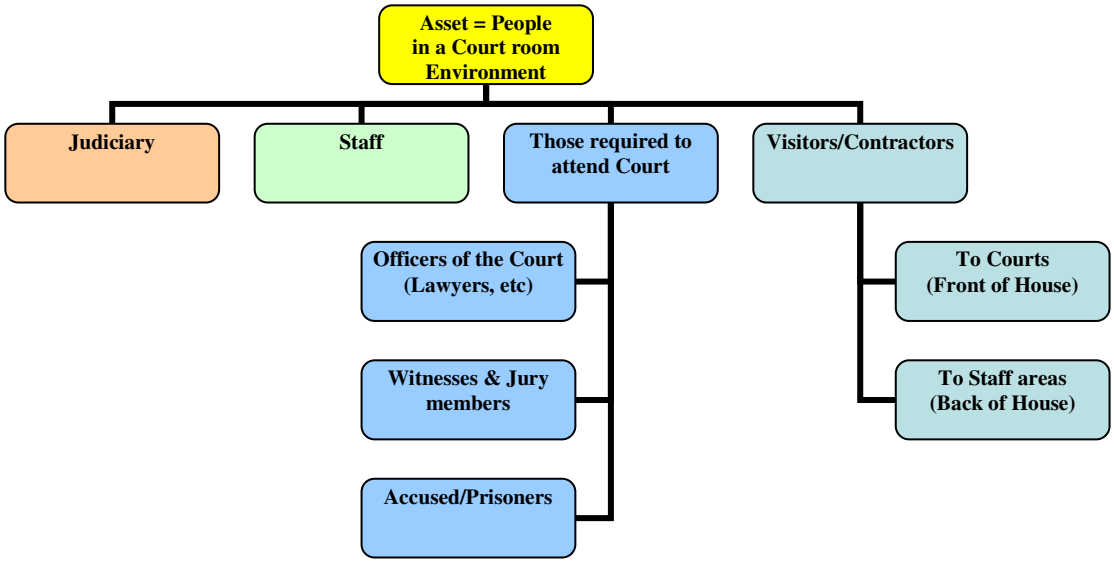

Figure 2 Example of Asset (People) grouped at highest level suitable for assessment

ESRA Process:

The process for an enterprise security risk assessment is:

- Identify organisation's goals and aims.
- Define the scope: inclusions/exclusions.
- Define the physical, temporal and organisational boundaries.
- Agree definitions for: likelihood, consequences, risk ratings.
- Identify the key assets and functions.
- Identify theats.
- Define enterprise risks in terms of key assets and functions.
- For each defined enterprise risk:
  - Assess the effectiveness of existing (or proposed) protective measures on a systems basis
  - Assess the effectiveness of existing (or proposed) consequence mitigation measures on a systems basis
  - Define likelihood of risk occurring and consequences should risk be realised.
  - Rate the risk.
  - Identify and recommend treatments to mitigate likelihood and consequences.
  - Rate the residual risk if treatments are implemented.
- Draft risk management plan to implement recommended treatments.

While the above elements may be considered part of any matrix-based risk assessment, an enterprise security risk assessment specifically includes:

- Emphasis on policies, procedures and processes.
- Assessing treatment measures as systems rather than individual components.
- Identification and recognition of inter- and intra-organisational relationships, responsibilities and protocols.

- Considering the effect of other managerial disciplines on the security of the organisation's assets and functions.
- Considering the implications of treatments on the organisation's goals and image when developing recommendations.

An enterprise review does not assess individual, technical or other measures; it reviews the system that includes the particular technology or process. Rather than checking if cameras are used, the question should be "are the cameras effective?" For example, in relation to CCTV, the following could be assessed:

- Has the intended purpose of the cameras been stated?
- Is the equipment being used suitable for the stated purpose?
- Are the sight lines and lighting correct?
- What is the monitoring capability/ procedures/ training/ qualifications?
- What recording and evidentiary capabilities are provided?
- What are the response measures and how are they verified?
- What maintenance and repair contracts are in place and what are the associated maximum down times?
- What other CCTV systems overlap areas of interest and are arrangements in place to access their recordings?

Many security systems are based on deterrence and detection. A key consideration is "what will happen when we find that for which we are looking?" For each detection capability there needs to be associated response measures to ensure the event is recorded, reported, contained and controlled with the minimum possible disruption to organisation's goals. Goals which may include maintaining its reputation for providing a safe and secure environment.

Likelihood

Given that there are assets or functions that are important there may be those who wish to take or damage them. Threat is related to motive – why would they want to do this? It could be for financial gain, for business advantage, political reasons, personal gratification, or other reasons. The question is whether those who may wish to do us harm (the intent) have the capability and this relates to whether we let them attack us by leaving open exposures resulting in vulnerabilities.

While a local or "tactical" security risk assessment must be aware of the various threats and threat vectors (i.e. how each threat source may attack) an enterprise security risk review can adopt more of an "All Hazards" approach. Rather than trying to identify a protective measure for each potential attack, an All Hazards approach ensures that the asset is protected from all reasonable vectors regardless of motive. If appropriate measures are in place to protect the item from the known and identified threats then they (usually) will deter or detect attacks from other threat sources that are less easy to identify or quantify.

The preventative measures in place, both physical and procedural, should be reviewed to determine if they are effective barriers to the threat vectors. An enterprise review should be an honest and objective assessment of the entire system not just a compliance check.

A security risk assessment will review available data and statistics, noting that security often deals with low likelihood/high consequence events and therefore a statistical basis for likelihood calculations may not exist and the likelihood rating may rely on qualitative rather than quantitative assessments. Exceptions to this generalisation may include events such as retail theft, and graffiti. Statistics will indicate how many events have been recorded, not where the vulnerabilities are or which events were not detected or reported.

Likelihood is usually expressed in terms of how frequently the event may occur within a given period of time. It is essential the temporal boundaries be defined i.e. over what period of time is the risk being rated. At an enterprise-level this is more likely to be over a longer period, for example the expected life of a facility or activity. An enterprise review can also be used to validate detailed, integrated planning for a specific short-term event such as a Shareholder meeting.

Consequence

The consequences should the risk be realised must be identified, based on what will be lost, usually expressed in terms of: people, financial value, time, and reputation. This can be altered depending on the business under review.

Response to a security event may rely on management areas outside security personnel and processes. An understanding of the related skills/disciplines and how they relate to security is an essential element of an enterprise security risk assessment including: emergency management, Workplace Health and Safety, Facility management. Each of these as well as being able to assist security may also present security vulnerabilities that need analysis. For example, how is the site secured once it has been evacuated? Also, in relation to the Courts environment (as shown in Figure 2) it is essential that the Judiciary, witnesses, juries and prisoners all be considered in the evacuation plan to ensure they are separated and controlled. If not, the security of prisoners may be reduced, witnesses and juries may come in contact with each other, and they may be exposed to those who would seek to influence them. In all cases the trial/hearing will most likely be compromised because of a lack of security input to an emergency management plan.

For all organisations, how they manage the after-event media will be critical as an expected consequence will be a drop in business activity as clients migrate to competitors. Even for organisations where there is less competition, such as government departments and international airports, there may still be a reduced confidence in the capability to protect assets and functions and increased disruption due to investigations and inquiries.

Risk Rating

By comparing the likelihood and the consequence, the Risk Rating can be determined. The risk rating indicates the importance of the risk, the priority with which it must be reduced, who will be responsible for reducing the risk, and who will monitor the risk reduction. For an enterprise review the level of responsibility is likely to be higher than for a tactical security risk assessment.

Enterprise Risk Mitigation

In an enterprise assessment the mitigation treatment measures may be directed to management areas other than security. Potential enterprise security mitigation recommendations might include:

- HR revising its ability to provide post-incident counselling;
- contract management considerations for lighting, cleaning, chemical storage;
- inclusions or exclusions in staff induction training;
- alterations to Business Continuity/Resilience plans;
- facility management and environmental considerations that affect how long staff and visitors can be held on site during an external event; or
- revision of emergency plans to provide security during and after an evacuation.

Treatments have to be cost effective (i.e. cost less than the assets they are protecting) and fit within the image and operating environment of the organisation.

The following are generic observations on risk mitigation treatments but are particularly pertinent to an enterprise review.

- Each risk will usually require a number of treatments.
- One treatment may address a number of risks (e.g. appropriate access control procedures/polices/practices/training/hardware may treat the likelihood element of a number of risks).
- It is usually easier to reduce the Likelihood i.e. to prevent access to the asset than to mitigate the Consequence once the event has occurred.
- At the tactical level it may not be possible to reduce the consequences: “if the event occurs this will happen”. But, at the enterprise level reducing the consequences may be possible through the application of other resources such as media management, legal support, HR/counselling support, and BCP.

Observations on the methodology:

The traditional matrix-based methodology, while effective in assessing assets, is not particularly useful when assessing risks related to processes i.e. what happens if we do more or less of an activity, what if we put in too much or too little or the wrong element into the flow, what if we slow, stop or speed up the process? Risks related to processes may be better assessed using different methodologies.

The matrix methodology also has difficulty expressing extremely low likelihood/very high consequence risks such as those (usually) posed by terrorism. Based purely on statistics it would hardly seem cost effective to employ some of the current preventative measures. But, it is understood that if existing protective measures are reduced the likelihood of such attacks will increase and the consequences of even one successful attack will be horrendous. Therefore, risks of extremely low likelihood can be assessed by considering the threat (the intent and capability of the perpetrator) and the exposures to the assets – usually related to weaknesses in the physical and procedural security measures.

Summary

ESRA is an assurance tool to provide those responsible for governance with a snapshot of whether the key assets and functions of the organisation are or will be protected from deliberate human action.

ESRA can be used to assess the security implications of future activities.

ESRA is not a check of locks and doors rather it is a corporate assurance tool that not only protects but also supports the organisation's goals and image.

Don Williams CPP *holds qualifications in Security Management and Security Risk Management as well as Project and Resource Management and is a Certified Protection Professional. Don has provided professional managerial advice on security and strategic security analysis for over 25 years. Don has lead enterprise-wide security risk assessments for a wide variety of private and public sector clients and can assist organisations by either conducting ESRA or by assisting organisations to plan and conduct their own internal ESRA. He is the secretary of the Australasian Council of Security Professionals. Don can be contacted at* donwilliams@dswconsulting.com.au .