Risk Mitigation & Protective Security by Al Prescott

Working in the security industry at whatever level you are operating at, in my mind is split in to two elements. Risk Mitigation and Protective Security; and as we all know in simple terms is protecting people and property.

Risk Mitigation is about minimising and reducing risk:

- Can we **REMOVE** the Risk?
- What we can't Remove can we **AVOID?**
- What we can't Avoid can we **REDUCE?**
- What we can't reduce do we **ACCEPT?**

This is something a security operator does as part of their daily routine whether working as part of a specific risk management plan or a dynamic risk assessment.

Protective Security; for me the main principles are:

- **Deter** (stop or displace)
- **Detect** (identify that something has happened so a response can be initiated)
- **Delay** (prevent the intruder or attacker from reaching the assets)
- **Respond** (prevent the intruder or attacker from reaching the asset)

These principles should be the basis of any Operation Requirement (*something I will cover later on)* . If you cannot **respond** to protect the asset then the **Deter**, **Detect**, **Delay** levels that you have in place are not at the correct level.

Holistically think of building protection as **beyond the perimeter**, the **perimeter**, the **site**, buildings on the site and the **assets** within the building.
How would you implement deter, detect, delay to allow the security measures to respond at the various stages of building protection?

Method / System	Deter	Detect	Delay
Security Officer (Static & Patrols)	Yes / No	Yes / No	Yes / No
CCTV (Fixed and PTZ)	Yes / No	Yes / No	Yes / No
Fence	Yes / No	Yes / No	Yes / No
Access Control Manned or System)	Yes / No	Yes / No	Yes / No
(Search & Screening	Yes / No	Yes / No	Yes / No

Lights (Purpose & Scheme)	Yes / No	Yes / No	Yes / No
Perimeter Intrusion Detection Systems (PIDS)	Yes / No	Yes / No	Yes / No
Intrusion Detection Systems (IDS)	Yes / No	Yes / No	Yes / No

Look at your own work place or environment and how much of the above is in place, more importantly do you know what the success criteria is for each method of protection.

What do I mean by success criteria, if we look at the table above and we look at each of the methods or systems, how useful are they going to be? Example would a fence stop someone? Or would it slow someone down? If it going to slow someone down; by how much will it slow them down. If it going to slow them down can we respond in time?

If we have a perimeter intrusion detection system (PID) in place what percentage would I want it to detect an intruder? Probably 100%. I would also want a PTZ connected to the PID so the intruder could be tracked. This again links in to the response requirement. Don't always assume that every method or system is going to be 100% as long as the success criteria is met. That may be as simple as 100% protection of the asset but there is a percentage of success for each method or system depending if it fits in to the deter, detect, delay category.

Looking at the **Remove, Avoid, Reduce, Accept (R.A.R.A)** concept for risk mitigation, it is important to understand about Risk.

To the identify Risk, break it down to two parts: **Threat and Vulnerability.**
For a threat to exist there must be an **intent** and the **capability** to carry out the intent.

The **intent** can be many things. kill, maim, destroy, disrupt, embarrass, steal, intimidate. If the attacker does not have the capability, then how credible is the **Threat**? If however, there is capability, then the target is **vulnerable**. A Vulnerability assessment has to be carried out. This would normally be done by identifying how predictable is the target and what security measures are in place. At this point I would look at a **Threat TRIAD** (basically a triangle)

Intent

Method **Location**

If you can remove one of the 3, then the threat is mitigated. It is difficult to remove the intent. If however, you know what the intent is, you can use the deter, detect, delay, respond, process with the tools that you have to hand, to remove, avoid, reduce accept. This

should be reflected in the Operational Requirement (OR) document by identifying and mapping protective security measures to the main areas of vulnerability and then listing recommendations to reduce the risk and them implementing those security measures.

So, what is the success criteria you are working to? Is this reflected in your assignment instructions? and have you been briefed on what is expected? Do you know what the operational requirement is? Do your supervisors know? What happens when you ask the question? Unfortunately, often the answer when you ask is ”it’s a need to know basis and you don’t need to know” This is probably because the supervisor does not know, or poor leadership.

How to deal with it?
Have a plan and mentally rehearse the plan. If time permits, physically rehearse the plan.

The situation you will end up in will be one of the three listed below.

- **You know what you know**. When this is the case you have the assignment instructions for guidance. (fire panel alarms etc.)
- **You know what you don’t know** (you know there is a possibility of something happening, working the doors is a good example, but you don’t know where, when or how the breach or incident will happen). If this happens then you have to use a dynamic assessment to get to a position where you **know what you know.**
- **You don’t know what you don’t know.** This is something that is normally outside the risk and threat assessment or may be a generic threat and not specific to your site or location. (London Bridge attacks) If this case it’s about doing something till you get to a known point.

Do you have a plan based on the facts, and can the protective security measures be part of the effective response options?

Al Prescott: MD & owner of HZL

After 36 years in the Ministry of Defence, Al founded HZL in 2000. Now a successful international training organisation and consultancy specialising in Teaching Education & Training, Assessing & Internal Quality Assurance, Consultancy Services, Confined Space Training, Medical and First Aid, Security Risk Management, Close Protection & Conflict Management Courses and CBRN Training.

Al has been instrumental in the development of various courses and projects including the training of military personnel, ex-military and civilians, in preparation for projects in the UK and abroad.

al@hzlgroup.com **www.hzlgroup.com**

Facebook: HZL Training Solutions **Twitter:** @info_hzl