THREAT & RISK ASSESSMENT

edexcel
advancing learning, changing lives

THREAT AND RISK ASSESSMENT

Aim:

- ✓ **To understand the importance of threat assessment and risk management.**
- ✓ **To produce a risk assessment**

Intended Learning Outcomes: By the end of this session trainees will be able to:

1. Explain what Threat Assessment and Risk Management mean and understand the relationship
2. Explain the main threats to a Principal within a Close Protection context
3. Explain why it is necessary to conduct Threat Assessment and Risk Assessment on people and venues
4. Describe Threat and Risk Assessment techniques concerning people and venues
5. Understand the process for carrying out Threat Assessment and Risk Management when a Principal is arriving and leaving a destination
6. Explain the need for on-going assessment, response and contingency plans
7. Describe how Close Protection operatives gather operational intelligence within the UK
8. Understand the factors to be taken into account in assessing risks
9. Describe the various threat levels
10. Carry out and produce a Risk Assessment / Audit.

THREAT AND RISK ASSESSMENT

National Occupational Standards:

PCP 1 - Assess level of threats and risks to Principals

PCP 2 – Plan and prepare to minimise threat and risk to Principals

PCP 3 – Liaise and communicate with Principals and others

PCP 4 – Establish and maintain secure environments

PCP 5 (SLP 2) – Communicate effectively in the workplace

PCP 6 – Maintain the safety and security of Principals whilst on foot

PCP 7 – Maintain the safety and security of Principals whilst in transit

PCP 8 – Maintain protection whilst driving

PCP 9 – Use control and restraint to support Close Protection

PCP 10 – Respond to potential conflict whilst providing Close Protection

Employment NTO

UNIT 5 – Give a positive image of yourself.

PERSONAL SECURITY:

<u>What is Personal Security?</u> –

"The Application of Principles and Procedures in Daily Life That Will Reduce the Risk of Exposure to Harm, Kidnap, and Assassination"

Personal Security covers every aspect of our daily lives and the life of the Principal. There are three Principals that cover the subject, and they affect every aspect of our work. These are:

THE INDIVIDUAL IS RESPONSIBLE FOR HIS OR HER OWN SECURITY

SECURITY MEASURES MUST BE COMMENSURATE WITH THE THREAT

CONSTANT AWARENESS IS THE CORNERSTONE OF GOOD PERSONAL SECURITY.

The Individual Is Responsible For His Or Her Own Security:

We and equally our Clients are responsible to us for our own security. In the Close Protection industry all security is a compromise! The compromise is between the requirements of security and the demands of living as near normal a life as possible by the Client. To give security the best chance of working, most people will try to modify their behaviour. It is purely a personal choice, and it is the individual's responsibility to decide whether they will compromise security for convenience

Security Measures Must Be Commensurate With The Threat:

The Client's wishes are always a major compromise imposed on us consistently by the VIP. You are constantly torn between the potential threats made toward your Client and their ability or willingness to pay for what we might professionally believe to be the right protection. You will need to make the decision as to what profile will be the best deterrent for your Client's safety.

High or Low? To lower your profile will not necessarily lower your protection. New CPO's can be over-enthusiastic and treat every job as a High risk; it is all too easy to get carried away. This can be as much a problem on a job as someone who is 'switched off' most of the time.

Constant Awareness Is the Cornerstone of All Good Personal Security:

Whether they are a CPO or a Client, everyone will eventually "switch off" when going about their daily chores, repeating the same old tasks every day. It is difficult even for trained people to stay alert. It's not easy and you cannot expect to stay switched on 24hrs a day; every day. Staying alert is a trained skill that you will not learn overnight. It takes a lot of self-discipline and practice to stay alert, even after making a conscious decision to remain so. So we need to have a system that is simple and that will work when you are under pressure

Awareness / Response Levels Colour-Code System:

It is very easy to become so familiar with the things and routines in our daily lives that you become complacent. You become lost in your own world. And if danger were to strike you would be caught off guard. Instead, try to become aware of what's going all around you. Begin to hear the sounds; see further than just what is directly in front of you; even try to smell the air around you. Begin to take it all in and process it.

A useful guide to awareness / response levels is a colour-code system developed by a Master Defensive Instructor many years ago and still valid today.

WHITE	Oblivious to what is happening around you
YELLOW	**Relaxed awareness of what‘s happen around you**
ORANGE	**Aware of potential danger. Able to quickly form a plan**
RED	**Putting your plan into action**

Where are you on this colour-coded system right now???

Most people live their lives in Condition White. If you said Condition **Yellow** you would be in the right place. Knowing what‘s going on around you will help to make sure you don‘t have to go to Condition Orange or, worse yet, Condition Red.

Our main objectives are:

- ✓ Avoid routine
- ✓ Be suspicious
- ✓ Be methodical
- ✓ Be aware
- ✓ Use initiative
- ✓ Use common sense
- ✓ Always have good communications.

Staff vetting

- ✓ It is your responsibility to vet all the personal staff of your Client. Do this whether or not the Client approves; don't forget you are at risk

- ✓ Your personal safety and that of the Client are the main priorities
- ✓ Check the files of your Client, they usually vet their own staff and this can make your job easier
- ✓ Pay particular attention to staff that are, or were employed in your Client's firm in the last six months
- ✓ If you can, use external contacts to get the right information
- ✓ Your Threat Assessment will dictate how much time and research is put into the vetting of staff
- ✓ If the job has too many conditions and you are not satisfied, don't take the job!.

Other precautions

- ✓ Do not take valuables into the field
- ✓ Lock personal effects in a discreet and secure case/safe
- ✓ Lock living accommodations
- ✓ Let colleagues know where you are going and your estimated time of return.
- ✓ Never travel alone
- ✓ Wear sensible clothing and footwear suitable for the weather and terrain. i.e. Flack-Jacket
- ✓ Always take mobile communications
- ✓ Always be aware of your surroundings and the mood of the population
- ✓ Be methodical in planning
- ✓ Avoid routine
- ✓ Do not carry confidential documents outside areas
- ✓ Secure office (s)
- ✓ Always have grab bags packed and on hand
- ✓ **DO NOT** abuse alcohol and drugs.

Vehicles:

These basic rules should be applied whether undertaking long or short journeys:

- ✓ Always check communication equipment and vehicle worthiness before departure
- ✓ Book in time of departure – destination – estimated time of return on booking out board
- ✓ Keep doors locked while driving
- ✓ Vehicle fuel tanks should be full at the start of the day
- ✓ All vehicles should have appropriate emergency equipment (including fire extinguishers)
- ✓ Where possible, travel in vehicle pairs for mutual support. 7.Windows should only be opened to a maximum of 2 inches, particularly when moving through towns and populated areas.

INTRODUCTION TO THE THREAT ASSESSMENT PROCESS

The first stage of a close protection assignment should be the ‘Threat assessment’. The lack of appropriate intelligence to facilitate a thorough, current situation appraisal is not uncommon. It is therefore necessary to establish the likely source and extent of potential threats. Once this assessment has been achieved it can be used to help establish an effective security plan that has the flexibility to provide effective protection

It would be unrealistic and impractical to cover every eventuality, so the more clearly the threat can be defined; the easier it is to determine the recourses needed for the task. Because of possible manpower and financial constraints a compromise in some aspects is often necessary. It now becomes apparent that a thorough assessment will help you prioritise tasking, maximise cover and provide the most efficient protection within any limitations.

REASON FOR THREAT ASSESSMENT

- ✓ Defines the current situation: Identifies specific and non-specific threat possibilities
- ✓ Helps to analyse vulnerabilities of the potential target
- ✓ Basis for all security planning: Helps identify logistical, technical and manpower requirements
- ✓ Helps identify prioritisation of tasking
- ✓ Allows you to maximise protection within constraints
- ✓ Helps you decide whether the situation is acceptable to you as a professional PPO.

FACTORS IN THREAT ASSESSMENT

1. *"A definitive assessment is not possible"*

2. **It is unrealistic and impractical to cover everything**

    a. To control risk is appropriate & feasible
    b. To eliminate risk is impossible
    c. Cost 'Versus' Benefit must be considered

3. **When assessing risk we must ask, does a potential aggressor have**

    1. **THE MOTIVATION**
    2. **THE ABILITY**
    3. **THE OPPORTUNITY**

"If these viability factors exist, then the threat should be taken seriously!".

4. Specific, plausible details are a critical factor in evaluating a threat

Details can include the identity of the victim or victims, the reason for making the threat, the means, weapon and method by which it is to be carried out. The date, time and place where the threatened act will occur and concrete information about plans or preparations that have already been made

Note: *As it is likely you will at sometime be involved with the Threat Assessment process, an understanding of the concept is essential. Apart from the operational necessity it can also serve as an opportunity for you; create a favourable first impression, establish your credibility, and reassure the client*

"THREAT ASSESSMENT - THE KEY TO ALL PERSONAL PROTECTION".

THE DIFFERENCE BETWEEN THREATS AND RISKS

A THREAT is an accelerated risk i.e. where the probability of a risk is considered high because of recognisably clear and present danger

A RISK is an unwanted future event that has a realistic probability of occurring given the prevailing threats, vulnerabilities and security controls already in place

Definition of a Threat;

"Declaration or intention to harm, injure etc. A person or thing regarded as dangerous";.

Also refers to a source of danger to our Principal. The best and most effective way to determine the correct amount and type of security measures is to complete a Threat Assessment. It is almost impossible to try and protect people from everything all of the time. To try to do so is neither effective nor efficient, unless the type and amount of threat has been established

A Threat Assessment is the easiest way to establish what level of protection is required; by identifying the enemy, their most likely form of attack, place of attack and time it will take place.

Focus your efforts on minimising the risk or danger to the Client. The convenience of the Client will always weigh heavily against whatever security is implemented. If possible, avoid risks all together; where this is not possible; you must put all your effort into reducing the consequences of the risk

The purpose of a Threat Assessment is to identify what risks exist and then separate them; into risks that we can avoid and risks that we cannot avoid. Of course we avoid any risks that we can. Unavoidable risks have to be confronted and analysed. From this we will decide what course of action to take and what equipment will be needed to minimise the risks.

DEFINITION OF A THREAT ASSESSMENT FOR A CPO:

“To assess all potential risks and weigh these against the security measures we can employ to negate them.”

-

“PREVENTION IS BETTER THAN CURE”

Our aim is not just to stop an assassination or a kidnapping; we are there to prevent all types of harm befalling the client. This includes every day risks, such as:.

1.Fire,

2.Theft,

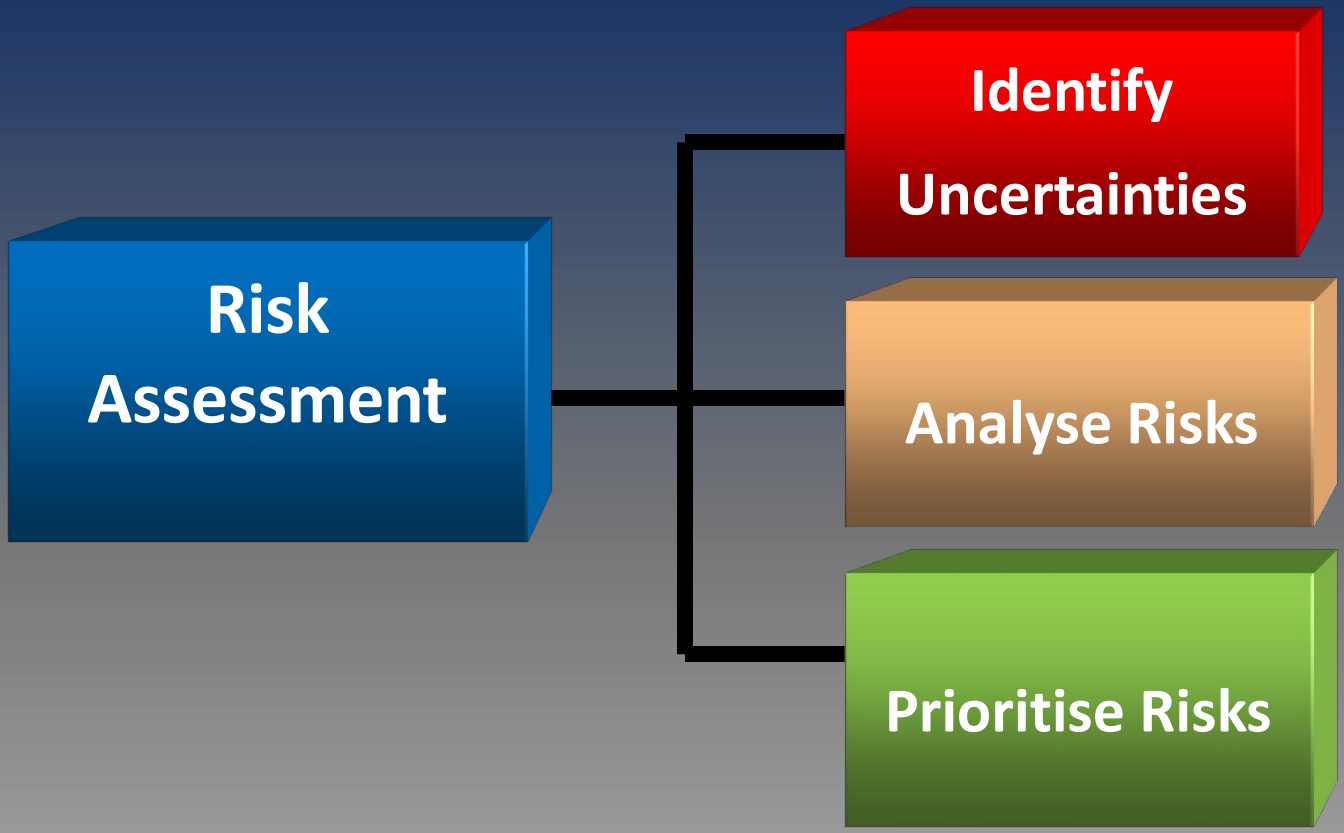
3.Traffic Accidents,

4.Illness,

5.Harassment etc

Unless informed to the contrary, we are looking after their physical well-being, their peace of mind, privacy and reputation. Anything that intrudes into the client's life at all must be considered a threat and will be included in your assessment.

ELEMENTS OF THREAT/RISK ASSESSMENT



Before We Decide On The Type And Amount Of Security Required, We Need To Analyse All Factors:.

ELEMENTS OF THREAT/RISK ASSESSMENT

Before We Decide On The Type And Amount Of Security Required

We Need To Analyse All Factors:

Leaving no question unanswered we start to put the Threat Assessment together. It may be frustrating; the Client may well have dismissed some of your questions. This could be because the security measures that we want to implement cost more than the Client is prepared to pay, it cramps his style or he has just been ruled it out as a potential threat. A good threat assessment is the result of methodical planning, in-depth research and the ability to put it all together into a workable assignment.

ELEMENTS OF THREAT/RISK ASSESSMENT

Once you've put it together, **Do it again**. Go over every detail, especially the list of threats. A Threat Assessment is never complete; you are always reassessing, rewriting and updating it due to circumstances beyond your control. When all the information has been attained you can then categorise the threat level and establish the procedures needed to conduct a full Risk Assessment to determine the correct level of protection needed.

RISK ASSESSMENT

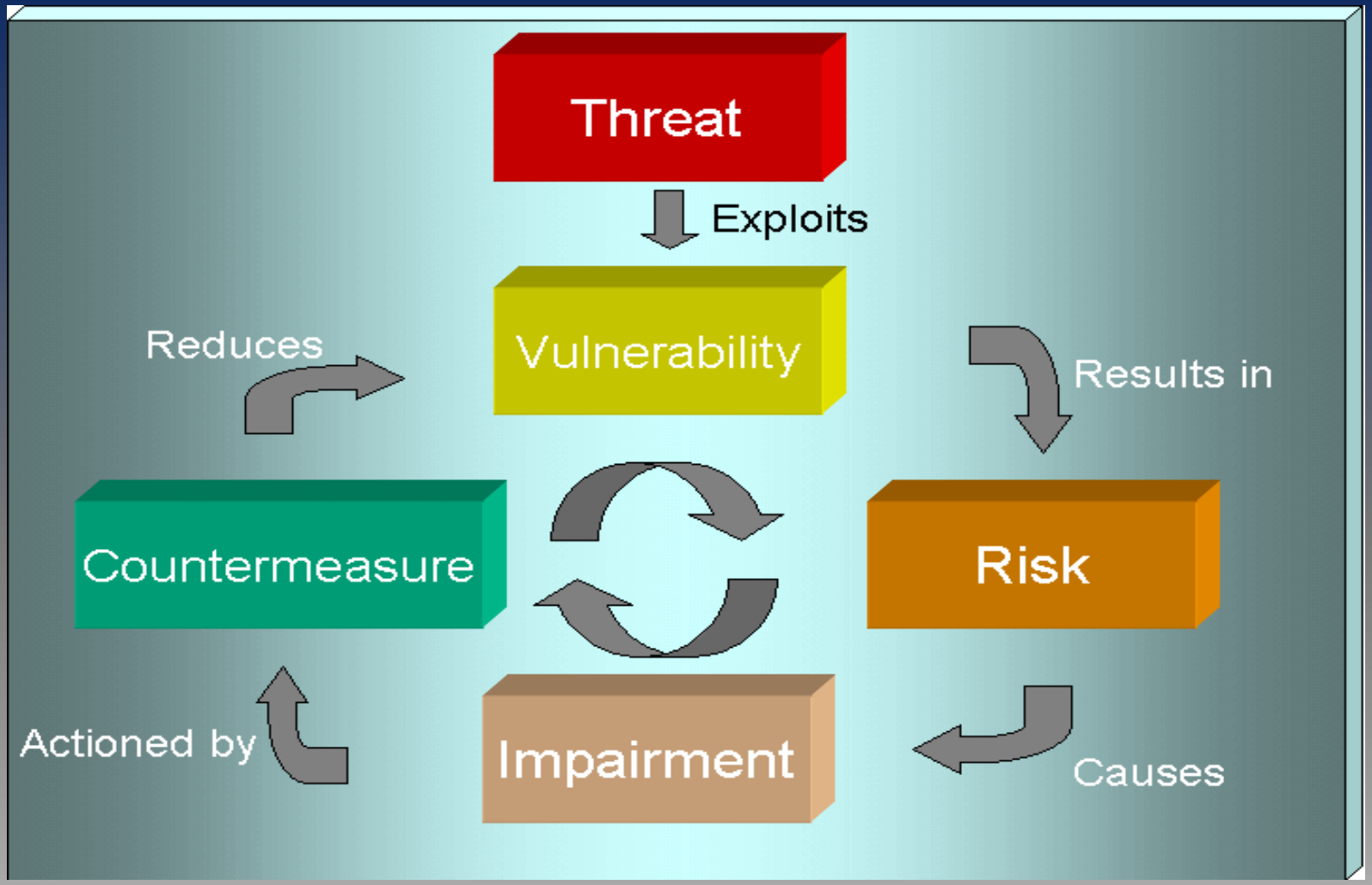
THE DEFINITION OF A RISK ASSESSMENT

RISK - (*in jeopardy, expose to danger, hazard*) the possibility of danger from a threat to our client

From the Threat Assessment and the examination of the threats to your principal from information obtained you should have identified the threats relating to your client and his family

To understand what risks you have ascertained from those threats you will have to carry out the risk assessment.

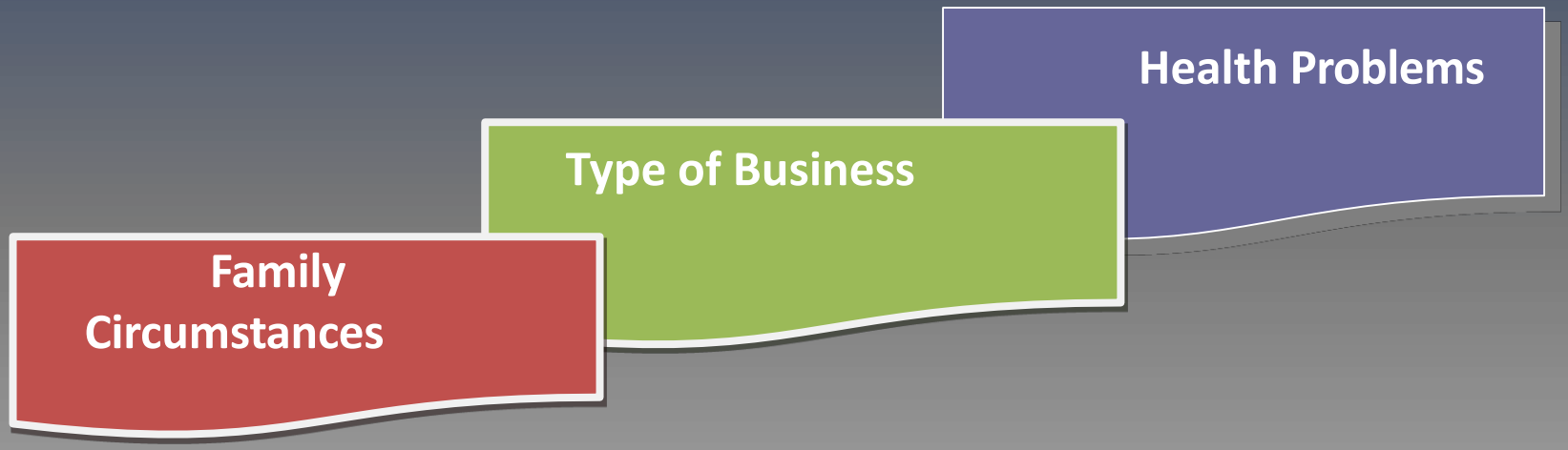
RISK ASSESSMENT



The process of the cycle above allows the CPO to accurately evaluate the risks to the threats.

Information:

1. Interview the principal regarding past incidents 2. Examine threat files, (letters or telephone calls etc) 3. Obtain information from police and specialist task forces. 4. Read newspapers. Open source media internet.5. Study company or personal public relations information that is accessible by all relating to the principle



Collation

- ✓ Gather the open source intelligence and human intelligence on the principal and their routines
- ✓ Go through the itinerary and identify the vulnerable points that make the level of threat and risk increase
- ✓ Formulate the threat files and annotate the particular risks to those files.

Analyse

Analyse the information in relation to the Principal profile to determine the following:

WHO?	Am I protecting?
WHAT?	Am I protecting them from?
WHERE?	Must I protect them
WHY?	Must I protect them

The analysis of the information or intelligence has to be authenticated by cross referencing:

For example:

If a human source informed you that there was a threat from an organisation;

AND they were planning to send your Principal a letter bomb;

AND...you had voice threats from an unknown source on a recorded telephone call suggesting they were going to blow your Principal up;

AND...you had information gathered about the organisation;

AND...what there MO was, which suggested that they had used explosives;

THEN.....by combining these elements together you are given a higher level of authenticity to plan and act on!.

DISSEMINATE:

How you disseminate the information to the Principal or team depends on whether you require oral, written or IT

Also look at what you could achieve by disinformation e.g. if you had a venue and it was publicised that all celebrities were going in a certain route, then allow the potential threat to believe that you were doing this and actually change the route and the way your celebrity goes into the venue.

THREAT LEVELS

It is not easy to categorise the level of threat, as there are many factors and circumstances involved. Some factors you may be aware of and others may not come to light until later

Some may never be revealed. In trying to determine the category of threat, it may help to consider the following definitions:.

THREAT LEVELS

The following convention has been used to categorise the level of threats and risks to principal:

CATEGORY 1- The principal is in significant danger and an attack is **Imminent (when it happens)**

CATEGORY 2- The principal is in some danger and an attack is **Probable (if it happens)**

CATEGORY 3 - The principal could be in danger and an attack is **Possible (everyone else).**

THE PRINCIPAL IS IN SIGNIFICANT DANGER & ATTACK IS IMINENT

Questions you should ask yourself based on the intelligence known:

1. **Is the client in SIGNIFICANT danger? (is there a significant specific direct threat?)**
2. **Is an attack expected**
3. **Not 'IF' but 'WHEN'**

<u>CAT 1 Protection recommendations:</u>

- ✓ **CPO**
- ✓ **Personal Security Team**
- ✓ **Residential Security Team**
- ✓ **Security Advance Party**
- ✓ **Operational Support Team**
- ✓ **Armoured Vehicle**
- ✓ **Full electronic, physical and technical cover.**

CAT 1

THE PRINCIPAL IS IN SOME DANGER AND AN ATTACK IS PROBABLE

Questions you should ask yourself based on the intelligence known:

1. **Is the client in SOME danger?**
2. **An attack is possible**
3. **Not 'WHEN' but 'IF'**

<u>CAT 2 Protection recommendations:</u>

- ✓ **CPO**
- ✓ **PES**
- ✓ **Selected aspects of CAT 1 protection as necessary.**

CAT 2

THE PRINCIPAL COULD BE IN DANGER AND AN ATTACK IS POSSIBLE

Questions you should ask yourself based on the intelligence known:

1. **There 'MAY' be a threat**
2. **Slim chance of attack**
3. **Could be a potential target**

CAT 3 Protection recommendations:

- ✓ **May have a CPO**
- ✓ **Routine searches**
- ✓ **Surveillance awareness**
- ✓ **Security awareness**
- ✓ **PES & RST as necessary.**

CAT 3

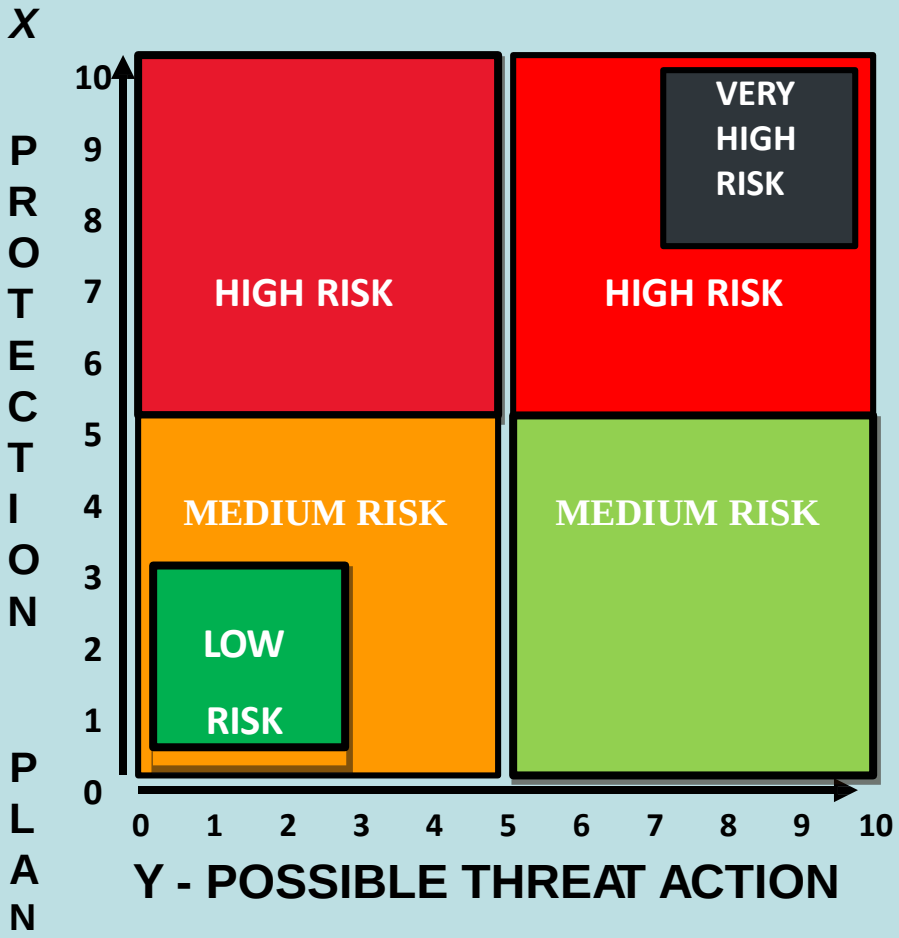
NB: Both CAT 1 and CAT 2 involve 24/7 cover

These categorisations are not an exact science and the edges are often blurred. It is also necessary to recognise that there are problems with both determining the appropriate threat level and implementing procedures accordingly. For instance;

- ✓ Maybe a client needs CAT 1 protection but can only afford CAT 3
- ✓ Maybe a client is unaware even that CAT 1 is required
- ✓ Sometimes CAT 1 protection maybe in place when a lower level would suffice.

Risk Levels Chart

The risks to your Principal are dependent on the proactive protection plans against the possible threat.



Risk Levels Chart

The Risk levels chart is not a precise tool as there are always variables, however, the chart outlines the way you would identify the principals threat levels in relation to his itinerary or natural routines e.g:

If you had a high profile celebrity that was a figurehead and idol in their career they would rank high on the X line between 3 and 10, let's say 8, and they were staying at home the whole week, they would therefore be a medium threat

If they went to a publicised mass event that would rank 8 on the Y line and this would therefore make them a high-risk client CAT 1.

A THREAT ASSESSMENT MUST BE CLEAR:

1. **Comprehensive**
2. **Logical**
3. **Easy to understand**
4. **Accurate**
5. **Relevant & re-visited**

The Main Threats To A Principal Within A Close Protection Context:

Threats come in many forms and will depend on a number of factors including lifestyle, employment, background etc.

The range of threats, which are common to most individuals and clients include:

1. **Embarrassing situation**-Media Control, Public situations, private life
2. **Unintentional injury**- Illness and medical, injury (accidental) fire
3. **Intentional injury or Attack**- Kidnapping, Assassination, Blackmail etc.

THE THREAT LIST

Make an in-depth list of all the threats that may affect your Client. No attempt should be made at this time to try and work out solutions to these threats. Give some thought to each individual threat. They must be sorted into threats that can be avoided and those that can't

Threats may be dismissed or added as information comes to hand or circumstances change

Always remember that the security measures that you implement could interfere with the convenience of the Client. By not visiting a particular place a threat may be avoided. If it is necessary for the Client to go there it would be inconvenient when you tell him or her that they can't. If a Client has to cease what they want to do, to get the protection needed, they probably don’t need you anyway!.

THE PROCESS

This involves establishing as many facts as possible before allocating resources and procedures

WHO?

Identify who is exactly at risk?

1. Principal only?
2. Family?
3. Relatives?
4. Associates?
5. Combination of the above?.

WHAT?

Identify what interests of the client may be at risk?

1. His business interests?
2. Residence?
3. Office?
4. Property / Assets?
5. Reputation / Image?
6. Other?
7. Combination of the above?.

TYPES OF THREAT

Threats fall into two basic categories; ***SPECIFIC AND NON- SPECIFIC***

- **A Specific Threat** is directed against a particular person, group, organisation or asset and can be classed in four categories: ***direct, indirect, veiled or conditional:***

- **A Direct Threat** stipulates a specific act against a specified target and is made in a straightforward, clear and explicit manner: "I *am going to shoot you"*

- **An Indirect Threat** is often vague, unclear and ambiguous. The plan, the intended victim, the motivation and other aspects of the plan are masked and lack conviction. "*If I wanted to, I could kill you and your family".* Although violence is implied it is suggested that violence ***'could'*** occur, not that it ***'will'*** occur.

TYPES OF THREAT

- **A Veiled Threat** is when violence is implied but not explicitly threatened. *"This world would be better off if you were removed".* Clearly hints at possible violent act, but leaves it to the potential victim to interpret the message and define the exact meaning of the threat

- **A Conditional Threat** is the type most seen in extortion cases. It warns that a violent act or specific action will occur unless specified demands or terms are met or agreed to: *"If £20,000 in cash is not handed over by next month I will go to the press".*

TYPES OF THREAT

- **A NON-SPECIFIC THREAT**: This is the type of threat or risk we will all face in our daily lives from a variety of sources such as:

1.Street robbery

2.Gratuitous violence

3.Burglary/Random criminality

4.Fraud

5.Rape

6. Car theft

7. Vandalism etc, the list goes on…..

Other types of threat that need to be considered are:

1.Imagined (Paranoia or fear)
2.Perceived
3.Circumstantial

NATURE OF THREAT

Physical – Death, injury, kidnap
Embarrassment – Media intrusion, eavesdropping, surveillance
Disruptive / Nuisance
Destructive – Sabotage Eavesdropping – Snooping, commercial intelligence, IT security
Other – Intimidation, IT security breaches
Combination.

Commercial Intelligence

Never underestimate the likelihood of this type of threat. Business rivals at all levels including state/government sponsored will pay a lot of money for information that will give a commercial advantage

Threat:

1.Open market sources
2.Criminal
3.Government sponsored commercial intelligence gathering

Primary targets

1.Research & Development
2.Tender information
3.Business world 4.Financial world.

Sources of information

1. Documents and papers
2. Meetings / eavesdropping
3. Laptops
4. Telephone conversations / IT hacking
5. Employees.

EXTENT OF THREAT

1.How long has this been going on?
2.How many incidents?
3.Exactly what happened?
4.Were the incidents related?
5.Who was involved / affected?
6.Is there a pattern?
7.What action was taken?
8.Were security measures breached?
9.Was there a build up?
10. Has there been an escalation?
11. Have others in similar positions been affected?.

MOTIVATION

The motivation for threats normally fall into one of the following categories:

1. Political
2. Criminal – Theft, violence, K&R
3. Environmental – activists (Greenpeace etc)
4. Religious – Al Qaeda, Islam for UK, PIRA etc
5. Racial – KKK / Black Panthers
6. Cultural
8. Radical pressure groups – ALF
9. Revenge
10. Obsession
11. Grievance
12. Vendetta
13. Rivalry
14. Other
15. Combination.

Other questions:

1.What might the client represent in the mind of the attacker?

2.Is the client a potential threat to anyone?

3.Have others been targeted?

Once the source has been identified, their Modus Operandi (MO) and capabilities must be assessed.

By studying reports of incidents, awareness of the client vulnerabilities and we can plan to minimise the opportunity for attack.

VULNERABILITY FACTORS

1.Nationality / Race
2.Religion
3.Politics
4.Associations
5.Personal wealth
6.Social activates
7.Family routine
8.Residence location
9. Routes used, Vehicles used, places visited
10.Nature of business
11.Poor existing security
12.Sports / Pastimes / Interests
13.Attitude to security.

Mistaken identity:

- ✓ Lookalike
- ✓ Same name
- ✓ Address/previous resident
- ✓ Vehicular similarities
- ✓ Telephone number
- ✓ Medical history
- ✓ Family medical history
- ✓ Chronic condition.

Other vulnerability factors worth considering:

Other vulnerability factors worth considering:

1. Debts
2. Legal proceedings (past, present, pending)
3. Indiscretions
4. Infidelities
5. Previous history

Client Health

1. Age
2. Fitness
3. Allergies.

LIMITATIONS

It is very difficult to formulate a definitive process on how to effectively assess the level of threat. Neither is it easy to determine exactly how vulnerable a client is to the dangers or risks posed by the threat. We know also that it would be unrealistic and impractical to try and cover everything and that you can never provide 100% protection. All we can really do is strive to ***CONTROL RISK*** within whatever parameters exist

POSSIBILITIES

We can look logically at a series of factors and possibilities and try to work out how it might affect a particular individual, company or organisation

We can assess the client's vulnerability to threat, establish what we are up against and put in place a security plan.

Decide what security is needed

You must go through your list of threats and decide which security measures are needed to minimise or overcome them. Many factors now come into question

Example of a particular threat:

1. A terrorist organization
2. How is this threat going to become apparent?
3. You must look further into your assessment to understand this
4. We must ask what the particular aims of the terrorist group are
5. What is their Modus Operandi? (MO)
6. Do they shoot, bomb, kidnap, blackmail or are they capable of all these
7. If they shoot; is it short or long range?
8. Do they have a history of killing, or kidnapping their hostages?.

Operational intelligence

There are a number of ways we can gather intelligence on terrorist organisations in the UK such as the Internet, newspapers, local police or local intelligence in our area of operations

“Before We Decide On The Type And Amount Of Security Required, We Need To Analyse All Factors”.

CLIENT PROFILING & QUESTIONING

You cannot complete a Threat Assessment without having the necessary knowledge about the person that you are protecting. This follows on from your initial meeting with the Principal you can.
You will have to gather as much information as ***Information at this stage is the name of the game***

- The Client profiling and questioning should indicate the level and nature of the threat to your Client

- What is the Client like? What do they do? A jeweller who has been robbed before? A businessperson travelling to a high-risk country? Or a child whose parents has been kidnapped?.

CLIENT PROFILING & QUESTIONING

There are hundreds of possible combinations, all with different risk categories. Before you can draw up a contingency plan, there are some obvious questions that must be taken into consideration. Has an actual threat been made? If so; when and by whom? You must then assess whether the threat is to be taken seriously. Question your employer as to why he wants protection. Assess his reasons. Are they genuine or imagined? Have the police or any security agencies been informed? If so, what action has been taken?.

CLIENT PROFILING & QUESTIONING

We need to know everything about our Client. In reality we are often only told what the Client himself thinks we need to know. The more we know about our Client, the easier a Threat Assessment becomes. Every bit of information that we can gather, however insignificant, will be of use when compiling our assessment

You should be able to identify the following:

Why the criminal has selected your Client?

- **Threat is directed at the Client for who he is?**
- **Threat is directed at Client for who he represents?**
- **Threat is directed at Client for what he represents?.**

CLIENT PROFILING & QUESTIONING

Motivation for attack:

1. Political
2. Criminal
3. Religious
4. Vendetta/Grievance
5. Financial
6. Mentally disturbed
7. Publicity.

Attackers MO:

1. Bomb
2. Shooting
3. Knife
4. Poisoning

Method of attack:

1. Assassination
2. Kidnap
3. Injury
4. Psychotically

USE THE "7 Ps OF CLIENT PROFILING

✓Places

Where people are born and grow up, go to school, where they work, holiday, live, eat/drink, and play, are all important to the Threat Assessment. Places that can be safe for some people can take on a dangerous aspect for others according to their relationships.

USE THE "7 Ps OF CLIENT PROFILING

It is a vital part of Threat Assessment that you know who you are dealing with. Consider the 7 'P's of client profiling:

1. **People**
2. **Places**
3. **Personality**
4. **Personal History**
5. **Private Lifestyle**
6. **Prejudices**
7. **Political & Religious**

People

We must know (or get to know) the people that our Principal comes into contact with every day. Clients are related to many people in lots of different ways; by blood, marriage, friendship, business, leisure, casually or intimately

Any relationship can be the cause of problems; an unscrupulous business associate, a jealous wife, a girlfriend or boyfriend, problem children, social contacts, enemies/rivals - the list can be huge.

USE THE “7 Ps OF CLIENT PROFILING

- ✓ **Personality**

Many professional businessmen have combative personalities and make friends or enemies very quickly. This is the kind of personality that is abrasive and tends to draw trouble. If your Client has this type of personality you will probably be acutely aware of it! Equipped with the right knowledge, a Close Protection Officer **will stay on his guard!!.**

USE THE "7 Ps OF CLIENT PROFILING"

Consider the following:

Arrogant
Brash
Dismissive
Provocative
Boastful
Vain
Violent
Ambitious
Devious
Unscrupulous
Fastidious
Methodical.

Personal History

This part of your profile should note things such as: past known names, marital status, family ties, date and place of birth, nationality and languages, places of residence, military service or other public service honours and distinctions; any medical history, medications, blood group, allergies, etc. A lot of personal information can be obtained at the library, i.e. in "Who's Who". You should look at:.

1. Full name & title
2. Place of birth
3. Where educated
4. Marital status
5. Outstanding achievements
6. Nationalities (Previous and current)
7. Previous residences
8. Languages
9. Military service
10. Awards
11. Qualifications
12. Positions held
13. Previous spouse
14. Children
15. Medical history
16. Political history
17. Convictions.

Private Lifestyle

The more we know the better our protective efforts can be.
Does he:

1. Work long hours and if so, is it at home or at the office?
2. See other Women / men; commit adultery, buggery?
3. Go to nightclubs often, or entertain at home/hotels?
4. Mountain climb, horse ride, swims in a pool or the ocean?
5. Paraglide, race speedboats or cars?
6. Drive his or her own vehicles or have a chauffeur?
7. Travel extensively or internationally?
8. High profile?.

Private Lifestyle

9. Awards
10. Qualifications
11. Positions held
12. Previous spouse
13. Children
14. Medical history
15. Political history
16. Convictions
17. Are they drug users?
18. Are they a workaholic, alcoholic, kleptomaniac?

Ask plenty!.

Prejudices

Prejudices are particularly dangerous attitudes as they are often ingrained in the person from an early age. Carefully watch and be aware of your Client's attitudes so that you can pre-empt or eliminate the specific hazards that they might generate. Be aware and ready to react. Does he have:

1. Religious
2. Race
3. Cultural
4. Controversial issues?.

Political and Religious

We need to know the Client's political standing; is he or she an active member of any political party? A Client's political beliefs and religious beliefs can cause big problems to any Close Protection Officer. CPO's will be aware and will anticipate when these beliefs or ideals may cause problems. Consider the following political possibilities:

1. Influence
2. Open support
3. Published opinions and comments
4. Associations
5. Donations
6. Memberships
7. Political ambitions

Once this has been produced a report must be completed detailing the threat level and the risk factors to our Principal.

Other possible threats to a Client

The Client must also be protected from other possible threats and accidents such as the unintentional injury or attack and embarrassing situations

"The First Step In Recognising If An Attack Is Possible Is To Realise Whether Or Not The Clients Movements Or Locations Are Predictable"!.

We are now in a position to consider elements of security planning and accept that all security is a combination of:

1.Procedures
2.Technical
3.Physical

Planning considerations should include the following:

1.Surveillance vulnerability assessment
2.Counter surveillance
3.Routine procedures
4.Emergency procedures
5.Standing Operating Procedures (SOP).

6. Problem handling routines
7. Problems that may be beyond human reaction time
9. Security team composition
10. Vehicles, administration and logistical needs
11. Communication requirements
12. Technical equipment requirements
13. Physical security upgrade if necessary
14. Security profile/Briefings/Awareness training
15. Recces/familiarisation
16. Liaison as necessary – Key Leader Engagements (KLE).

Sources of Information

1.Previous security
2.Media
3.Archival/library
4.Internet

All information, from whatever source must be:

1.Collated
2.Evaluated
3.Recorded
5.Filed
6.Staff (past & present)
7.Police, crime prevention
8.Pinkerton's & other intelligence agencies
9.Foreign & Commonwealth Office (FCO)
10.Protected
11.Revised & Updated.
12.Disseminated as necessary

Keeping abreast of current world affairs

CPO's must ensure that they know a little about what is going on in the world. This business can quickly take you from an environment that you know well and are comfortable with to another continent with a hundred and one problems that you should be aware of if you are to do your job properly!

Just reading a ***QUALITY*** newspaper daily or browsing the news websites is a start. The Daily Sport although entertaining and keeping you informed of the latest place that Elvis has been spotted, is not exactly going to keep you up to speed with current affairs

The FCO website is also an excellent source of up to date information on every country in the world today. You can subscribe free of charge by following this link:.

http://www.fco.gov.uk/en/secure/subscribe?action=subscribe

Knowing the Enemy?

Crime and Terrorism affects everyone. You do not have to be a VIP or work in the Security Sector to be exposed to the dangers of either! A few different types of Terrorists and Criminals are outlined below:

1. **Anarchists** - (Anti-Government)
2. **Anti-Abortionists**
3. **Anti-Globalisation** - (Oppose Global Capitalism)
4. **Communist / Socialist** - (Want to spread the wealth; eg: Tu'pac Amaru Revolutionary Movement in Peru).

5. **Environmental / ALF** – Use Terror to attack Governments and Companies using Animals for research
6. **Nationalist / Separatist** – ETA & Tamil Tigers
7. **Racists –** KKK / Nation of Islam / Black Panther Party
8. **Religious** – Al Qaeda / Lord's Resistance Army of Uganda / Armed Islamic Groups / PIRA
9. **Stalkers** – Celebrity stalkers such as Mark Chapman (John Lennon).

Stalkers are a very common and **REAL** threat to high profile celebrities / sportsman, such as Brad Pitt, Steven Spielberg and Monica Seles being some of the more famous to have suffered

You should never ignore a stalker hoping they will go away. Most of the time they get progressively worse as time goes on until action is taken and they are locked up. In many cases, even this does not prevent them from carrying on their harassment and they carry on stalking campaign from within their prison cell. If your client is a victim of stalking you must take care to gather as much evidence as possible showing the wilful, malicious and repeated harassment of your client in order to present to the Police so they can take positive action and arrest the offender.

Lots of different actions have been tried in the past to put a stop to stalking. Stalking the stalker is one option, and it may work, but giving the stalker a taste of his own medicine is against the law. So is ‘making him an offer he can’t refuse’!

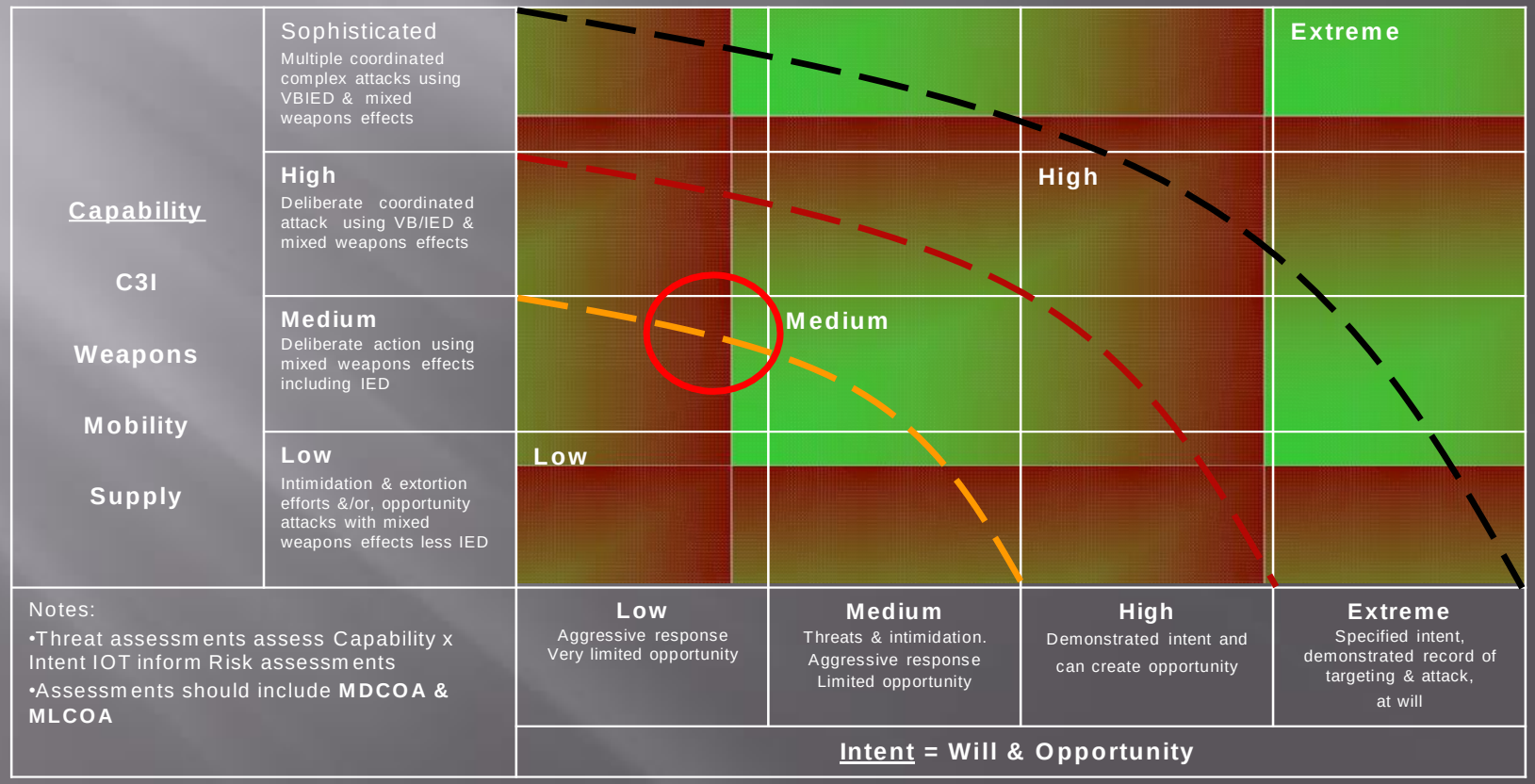
The best way forward is to involve the Police as soon as possible, gather as much evidence as you can along the way as you concentrate on your priority of **‘PROTECTING THE CLIENT’.**

On the following slides are examples of a Threat Assessment Matrix by an Intelligence Analyst that was produced for a mission planned and executed by me in Iraq:

After studying the Threat Assessment, the decision to commence with the mission was made by me as the Team Leader. I arrived at that decision as I believed the 'Medium' threat to the team was acceptable based off of the mission request which was classed as an 'Essential' mission and the mitigating factors including; route selection, timings, tactics, liaison with Military support and weapons, I had already planned in to the mission itself to prevent the enemy, AQIZAM, from having the opportunity to attack.

MLCOA	Most Likely Course of Action (By the enemy) Most
MDCOA	Dangerous Course of Action (By the enemy) Small
SAF IED	Arms Fire i.e. AK47 / Pistol etc
VBIED	Improvised Explosive Device
SVBIED	Vehicle Bourne IED (Car bomb)
SVIED	Suicide VBIED
RPG ISF	Suicide Vest IED
CP	Rocket Propelled Grenade
TCP	Iraqi Security Forces
TTP	Checkpoint
AQIZAM	Temporary Check Point Tactics,
PSC	Techniques & Practices Al Qaeda
	in Iraq
	Private Security Contractor.

Threat Assessment Matrix



Example Threat Assessment

THREAT GROUP	AQIZAM	
ASSESSMENT OF CAPABILITY	ASSESSMENT OF INTENT	THREAT ASSESSMENT
MEDIUM	**LOW / MEDIUM**	**MEDIUM**
AQIZAM are capable of conducting SAF, IED, and RPG attacks. The group has also used VBIEDs, largely against the local populace and the ISF. The attacks are often effective simply due to the softer targets chosen, such as civilian gatherings and dismounted ISF or poorly- protected ISF patrols. However, the attacks appear to lack coordination and complexity, implying that they are hasty ambushes. AQIZAM's operational capability in eastern Baghdad has been greatly reduced over the past 12 months.	AQIZAM in Karadah and Rusafa have shown a demonstrated consistent intent to target the ISF and cause mass civilian casualties. The Sunni insurgents exhibit the highest freedom of movement in the Karadah peninsula,, where the preferred attack TTP is the mass casualty-causing (S)VBIED or suicide vest as part of their campaign to discredit and demoralise the ISF and intimidate the local populace. The first week in May has witnessed two VBIED attacks in the area, targeting the ISF. Attacks against PSCs by AQIZAM in this area are very rare, and it is unlikely that a valuable VBIED or SVEST would be used against a passing PSC convoy.	**ENEMY ACTION IS LIKELY** **MOST LIKELY COA:** SAF or IED whilst transiting through the main routes. **MOST DANGEROUS COA:** VBIED/SVBIED attack in Rusafa as well as the Karadah area, most likely while static at, or passing through, an ISF TCP. **S/VBIED THREAT:** LOW / MEDIUM (HIGH at civilian gathering points and ISF CPs).

As previously mentioned; in order to be able to launch a successful attack against a target, you must ask yourself if the criminal possesses **ALL** three of the following:

- **THE MOTIVATION**
- **THE CAPABILITY**
- **THE OPPORTUNITY**

If the answer is **YES,** then there is a real danger of attack and your job then becomes much more difficult. There is nothing you can feasibly do to prevent the criminal's motivation or indeed his capability to launch an attack.
However; you can and MUST prevent him from having the opportunity and you do that by means of mitigating the risk factors.

CONCLUSION

The main purpose of a threat assessment is to determine what it is you are up against so as to be able to plan effective measures against it. This is probably one of the most difficult aspects of CP work. The results of an assessment set the scene for implementing a security plan

If the assessment is flawed then the consequences could be serious. Remember it is vitally important to examine every aspect of a clients lifestyle to help you develop and maintain a secure environment within which they can operate.
'Perception is a basis for action, but beware "THE ILLUSION OF PREDICTION"

REMEMBER – "YOU CAN NEVER ELIMINATE RISK.....
BUT YOU CAN CONTROL IT".

QUESTIONS?