Introduction to Threat Management

Focusing on the Criminal Development Pathway to guide, counter or neutralise the criminal or terrorist's intentions and attack planning cycle.

by David Harding

Welcome to:

Introduction to Threat Management:

Focusing on the Criminal Development Pathway to guide, counter or neutralise the criminal or terrorist's intentions and attack planning cycle

By David J.R. Harding

Published by David J.R. Harding at Criminal Threat Management

Welcome to Threat Management.

I would personally like to welcome you to a concept that I have been working on for more than thirty years within the protective security environment. This concept, which I call Threat Management, focuses on the criminal and/or terrorist development pathway from initial intent, up to the point just prior to them actioning an attack.

The model that you will find within this Introduction to Threat Management article has been developed from my combined operational and academic experience and knowledge. This experience comes from service within the Australian Special Air Service and the Australian Federal Police's Air Security Officer program. This is combined with over 20 years of conducting security investigations and intelligence operations within the private security space. This experience has been complemented with academic research developed during a Masters Degree and additional follow up research.

I developed the concept of Threat Management because I found that the current focus on Security Risk Management was too limiting. That is, traditional security and risk management focuses on the host organisation. From a defensive viewpoint Security Risk Management is very effective. However, due to its lack of focus on the threat actor that is deliberately trying to attack the organisation, Security Risk Management has limitations.

As Sun Tzu, the ancient Chinese military philosopher stated,

'If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.'

Threat Management seeks to understand what Sun Tzu calls the enemy.

I hope you find this Introduction to Threat Management article interesting and useful in your own personal and professional development. I look forward to offering other learning tools

that will delve into ‘Why to use Threat Management’, ‘How to use Threat Management’, as well as how, when and where to apply Threat Management concepts.

Kind regards

David Harding

INTRODUCTION TO

THREAT MANAGEMENT:

Focusing on the Criminal Development Pathway to guide, counter or neutralise the criminal or terrorist's intentions and attack planning cycle.

On the second of June 2014, two armed attackers threatened staff and robbed the Mortdale Hotel in Mortdale Sydney. On the fifth of June 2014, at the Wentworth Park Hotel in the Sydney suburb of Homebush, armed attackers stormed the hotel carrying machetes and pistols and conducted a robbery. During the Wentworth Park Hotel robbery several staff and patrons were threatened, some were injured. On September 11 2001, in coordinated and simultaneous attacks on various aircraft a terrorist group was able gain control of and use those aircraft as missiles attacking four buildings in New York and Washington, in the United States of America.

The above examples highlight the fact that although each site had appropriate and applicable security and risk management procedures in place that were specifically designed to mitigate such attacks, the criminals or terrorists were still successful. The case of the aircraft hijackings illustrates the difficulty within risk assessments of predicting the low probability but high harm incidents. The case of the hotel attacks illustrates that professional criminals can circumvent security and risk mitigation procedures through good planning, preparation and intelligence gathering. In addition, and as referenced below, academic research conducted by the Australian Institute of Criminology has identified that professional criminals are not deterred by risk and security mitigation strategies.

Given the cost in both human and financial terms of the above examples, it might be prudent to utilise additional concepts and methods to prevent such attacks. One way to achieve this is to supplement current risk and security management strategies with additional strategies that focus on the person, or persons, that could make the attack. This is called Threat Management, and to understand this concept it is first necessary to appreciate how Threat Management differs from Risk Management.

Dictionaries generally define the word 'threat' to be 'the intention to cause harm'. This implies that a threat is made by those with the ability to make rational and conscious choices. This means that threat arises from a person's, or group's conscious decision to cause harm. Threats are measured by assessing a person's or group's capabilities, their past performance and history as actors, and other indicators such as media statements, public rhetoric and levels of community support.

Conversely, the generally accepted Risk Management standard (AS/NZS ISO 31000:2009 Risk management-principles and guidelines) defines Risk to be the 'effect of occurrences on objectives'. Risk focuses on occurrences or events. Risk is event driven and measures the likelihood of a particular event and the harm that that event could cause.

If the two concepts are to be compared, Threat focuses on the intention to harm, Risk on the specific events or occurrences. Threat is assessed by measuring a person's or group's intentions and their capabilities. Risk is assessed by determining the likelihood of a particular event or conceived scenario, and the harm that that event could cause. The two concepts are distinct, as are the methods needed to assess and manage them.

Threat management is defined as 'the coordinated use of resources to guide, counter, or neutralize the behavioural process taken from the development of criminal intent up to the point of actuating a crime or other harmful action'. Threat Management focuses on human-

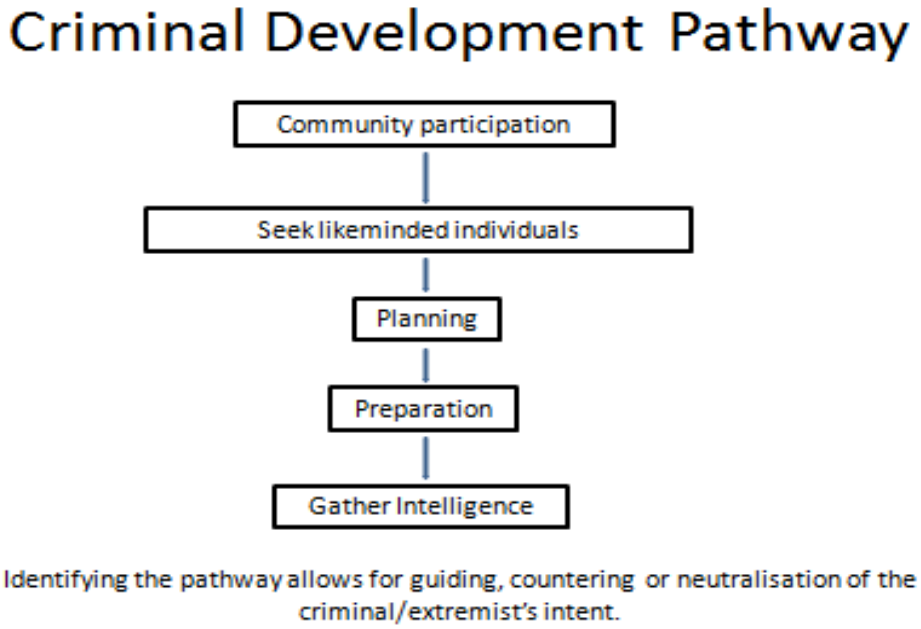
centric threat actors. This means that one of the first priorities is to identify the threat actor, their intentions and stage they have reached in the attack planning cycle. The threat actor's attack planning cycle consists of planning, preparation and intelligence gathering. Once identified, resources can be assigned that can guide, counter or neutralise the threat actor's intentions and capabilities.

Traditional risk and security management concepts would suggest the questions, "Why focus on the person who is going to commit the crime?" and "Shouldn't Security Risk Management strategies mitigate the criminal intentions?" Unfortunately, Security Risk Management Strategies do not. No matter how thorough the security and risk mitigation strategies are, they will be static in both time and location for a particular period. This gives the professional criminal the opportunity to develop their own strategies to overcome or circumvent the security and risk strategies that have been put in place. As Smith and Louis of the Australian Institute of Criminology identified in a report 'Armed robbery in Australia: 2007 National Armed Robbery Monitoring Program' professional criminals are not deterred by security and risk mitigation measures put in place by an organisation. Professional criminals will simply plan a method to overcome the security measures. For the organisation that must develop strategies to counter the professional criminal, investing resources to identify and disrupt the actual criminal are called for. This is especially so in the current security environment that is becoming more ambiguous for all, including for law enforcement and national security authorities. Potential targets need to take much more responsibility for their own security from threat actors.

THE CRIMINAL DEVELOPMENT PATHWAY MODEL

For managers with responsibility for the protection of assets and persons from deliberate attack by criminals, terrorists, or other hostile threat actors, an understanding of the processes and pathways exploited by criminals is vital. Understanding the development of criminal intent to cause harm, the types of groups that the criminal could gravitate towards, and the

planning, preparation and intelligence gathering that is undertaken prior to an attack, can suggest interventions that can prevent criminal, terrorist or other attacks.



Community Participation

Threat actors, such as criminals and terrorists often follow an identifiable and predictable pathway of development. As can be seen from the above diagram, development commences from the community that the individual originates from, where there is an acceptance of a particular illegal activity. However, such acceptance does not necessarily mean the intention

to commit the crime, rather that the community accepts a particular belief or behaviour. An example may be as sublime as “It is all right to take something from someone that can afford it”.

Seek Likeminded Individuals

Potential threat actors will then seek out other like-minded individuals. Here, the potential criminal will further reinforce the belief system that the conduct of a particular activity is acceptable behaviour. Individuals at this stage will gravitate towards gangs, groups, chat rooms or in the case of radicalisation, religious sub-groups.

Planning

The next stage will see intentions turn to actions. Here the potential criminal commences physical actions to plan prepare and gather intelligence on an appropriate target. Planning may consist of the development of an appropriate method of attack, the identification of resources required and perhaps undertaking some form of general intelligence gathering into types of and applicability of targets.

Preparation

Preparation may include the gathering of resources necessary to carry out the crime. For example, a terrorist group intent on placing an improvised explosive device at a particular

location will need to gather and prepare the explosive materials, and also place it at the chosen location. The example being a burglar would be required to gather the tools necessary to gain entry to the target household.

Intelligence Gathering

Intelligence gathering by the threat actor may occur at two points during the criminal development process. Initially the threat actor may need to identify a target that is appropriate to the threat actor's aims and competence. This form of intelligence gathering could often be achieved through the routine activities that criminals engage in. For many criminals the target locations are those that they have had some form of exposure to. In criminology this is called Routine Activity Theory.

The criminal or terrorist will also need to gather specific intelligence that is relative to the intended target. Ultimately, the criminal will need to have knowledge of the security arrangements around the target, its vulnerabilities and how best to exploit them to attack the target. This level of detailed intelligence can only come from specific surveillance and reconnaissance of the target. In some cases this information can be gained through legitimate cover engagement with the target and its personnel. In addition, and of particular importance, the threat actor may conduct reconnaissance and intelligence activities in person, so as to gain a first hand, and eye, knowledge of the potential target.

The Criminal Development Pathway provides a model that can be used to determine at what stage a particular threat actor is in their criminal development. By determining the stage of development it is then possible to develop and implement intervention strategies. Depending on the specific stage of development these intervention strategies can guide, counter or neutralise the specific threat actor's intended pathway and attack plan.

Conclusion

This article has sought to introduce the concept of Threat Management, by identifying the Criminal Development Pathway that criminals and terrorist's follow in their development of harmful intentions up to the point of actual physical attack. Understanding of this pathway could provide opportunities for the organisation to identify the level of intent and timing of potential attacks of the threat actor.

Thank you for your reading this Introduction to Threat Management article. I hope you found it beneficial to your interests and work environment. Please feel free to share this Introduction with anyone that you feel may benefit from it. You could also send them to my blog site Criminal Threat Management or http://www.criminalthreatmanagement.com/

Kind regards

David Harding

Links:

Harding, D. (2014). *Threat Management: the coordinated focus on the threat actor, their intentions and attack cycle*. Journal of Applied Security Research: http://www.tandfonline.com/doi/abs/10.1080/19361610.2014.942825#preview .

Threat. (n.d.). In *Merriam-Webster's online dictionary* (2014.) Retrieved from http://www.merriam-webster.com/dictionary/threat

Smith, L. & Louis, E. (2010b, July). *Cash in transit armed robbery in Australia.* (Trends and Issues in Crime and Criminal Justice Issue No. 397), Australian Institute of Criminology. Retrieved from http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi397.pdf

Smith, L. & Louis, E. (2010a). *Armed robbery in Australia: 2007 National Armed Robbery Monitoring Program* (annual report). Retrieved from Australian Institute of Criminology website: http://www.aic.gov.au/publications/current%20series/mr/1-20/11.html

Standards Australia/Standards New Zealand. (2009). *AS/NZS ISO 31000:2009, Risk Management-Principles and Guidelines.* Sydney, Australia: Standards Australia Limited/ Standards New Zealand: https://www.iso.org/obp/ui/%23iso:std:iso:31000:ed-1:v1:en