ADVENT IM

Protective Security:

The Importance of Determining Threat in a Risk-based Approach to Security

Mark Jones - Senior Security Consultant, Advent IM

Introduction

Terrorism seeks publicity to feed and inspire its followers by focussing attacks against high-profile targets, in the UK and abroad. Major public events, such as the recent Winter Olympics, present new opportunities for terrorists. The UK's police and intelligence services continue their efforts to counter the ongoing threat from international terrorism, but as the former Director General of the Security Service, Dame Eliza Manningham-Buller said , "we will continue to stop most [terrorist attacks], but we will not stop all of them." Clearly law-enforcement agencies have to be lucky every time - whereas a terrorist simply needs to be lucky just once!

Terrorism however, is not the only security threat that we face, therefore a clear understanding of the real, rather than perceived threats is essential, not only for Government but also for all businesses. Threat is a vital component of Risk Assessment that does not always receive the level of focus it deserves and needs. This may be because threat assessments require expert knowledge and an understanding of a Threat Actor's *Modus Operandi* (MO) to inform the process. Historically, these assessments have been carried out using experienced analysts who often specialise in a very small area of the threat spectrum, possibly a geographical region, threat source or industry sector; therefore, the expertise is not widely available at business or organisational level.

In this short paper, we discuss why Threat Assessment is fundamental to a risk-based approach to security.

Is the Threat real?

The perception of threat and the actual likelihood of an attack i.e. the risk of that threat being manifested can vary enormously. For example, the likelihood of an individual or business being involved in a terrorist incident can be calculated using statistical analysis and is, in most cases very low. However, the *perception* of the threat from terrorist action can be very high among the public and businesses due in no small part to the spectacular nature of some of the attacks; 9/11 being clearly the most symbolic example.

In both the public and private sectors, Risk Assessments are recognised as an increasingly important tool that is used to inform organisations before actions are taken, often at a strategic level where significant investment is involved. Risk Assessments can be used to provide a balanced judgement by exploring potential threats and vulnerabilities in the context that the impact of threat realisation may have upon the organisation. The result from an assessment therefore, may have significant influence on decision-makers when considering future courses of action.

In the UK, we have endured decades of terrorist activity, which in the past has emanated from Irish extremists, and more recently Islamic extremists. Acts of terrorism vary in scale and

purpose; some aim merely to inflict superficial damage or cause public distress to draw attention to a particular cause. However, others can be more violent and indiscriminate with far-reaching consequences. The UK Government published in 2010, the National Security Strategy which set out a 3-tier set of priority risks and threats to the UK, with the top most Tier One risks being as follows:

- International Terrorism;
- Cyber Attacks;
- Major Accident or Natural Hazards; and
- International Military Crisis between states.

As stated above, the most significant current threat comes from international terrorism with its ambitions to mount high-impact attacks combining mass casualties with substantial disruption to vital services such as energy, transport and communications. Although International terrorism is a serious and ongoing threat, there is also growing discontent again among dissident Republicans in Northern Ireland. The 2018 FIFA World Cup to be held in Russia will provide significant opportunities for terrorists, extremists and single-issue pressure groups to gain world-wide publicity for their cause.

In security terms, the principle components of Threat are Capability and Motivation. While the former can be reasonably easy to measure, the latter is often more difficult to quantify and therefore needs an understanding of the Threat actor's MO to make an informed judgement. Thus, the involvement of qualified analysts is required. There are other components that can inform the Threat Assessment process, but in this short paper, we will focus on the fundamental elements.

The West's open democracies within which businesses must operate provide the freedom of information where investigative journalists often seek sensitive information or indeed scandal. There have been many instances when journalists posing as official visitors or accredited sources have been permitted access to sensitive areas, or been given some information "off the record". The recent and ongoing investigation into phone-hacking clearly demonstrates the lengths that investigative journalists will go to get a story. One of the main dangers of this type of threat is the leak of sensitive information. Debt collection and investigation agencies are known to attempt to obtain personal information held in confidence by government. Investigative journalists have also exploited personal tax information. The information age has therefore enabled this type of threat source and increased its capability.

The criminal threat (this category also includes gangsters and warlords) is primarily assessed as one that seeks financial gain through the acquisition of information and this is now mainly carried out by cyber-based attacks and the use of ransomware. Identity theft in support of illegal immigration, money laundering and using corporate systems to conduct criminal

activity are examples. Since much terrorist action is funded through criminal activity it is possible that, information on the movements of law-enforcement agencies may have significant value to criminals involved in the movement of illicit drugs, money, weapons or human-trafficking. Furthermore, there are massive sums of money involved within these transactions; for example, the UN estimates that every year up to four million women and children are trafficked in a world-wide business said to be worth in excess of $7 billion. International organised crime groups may become increasingly dependent on information to successfully ply their trade. Therefore, law enforcement information systems and those working with them will become targets for those whose intent is to avoid the attention of those agencies.

In the information world, the objective of cyber hackers is often to demonstrate their skill to their peers and thus increase their status. Alternatively, their aim is to access systems to take advantage of the additional resources that the entry provides. The technical ability of the hacker is often the driver for action rather than a perceived benefit that the attacker will derive from the target. Hackers may be used by other groups such as serious and organised crime (cyber criminals) to act on their behalf due to their particular level of skill and their status may influence their potential value for work of this nature. Such is the seriousness of cyber-based threats to the UK, the National Cyber Security Centre (NCSC) now provides a Weekly Threat Report. The Report contains details of how cyber threats can emanate from various threat sources such as malicious insiders who can damage company computer networks and cloud service providers who have not addressed vulnerabilities in the cloud architectures leaving them open to a range of international cyber criminals.

The threat from Commercial Groups will mainly be one of industrial Espionage to obtain some economic advantage. There is also the possibility that the group will use other means such as the subversion of an insider in an attempt to influence a Nation State for commercial benefit.

Pressure groups for such causes as anti-globalisation, animal rights, nuclear disarmament or environment issues often carry out demonstrations against government policy and activities. Although usually confined to peaceful demonstrations, anarchists or extremist elements often encourage violent attacks against individuals or property which can pose a threat as significant as terrorism.

The threat from insiders is likely to remain one of the most serious. In information assurance terms, recent analysis indicates that the theft of Intellectual Property is seen to be the most significant target. In a wider context, disillusioned or disaffected staff, particularly in the current economic climate may seek recompense for redundancy or even revenge for perceived injustice.

Clearly, there are many threats to both government as well as business assets.

Why do we need a Threat Assessment?

Threat is part of the Risk Assessment process, but often does not attract the level of attention that it deserves. In reality, the Threat Assessment provides the foundation on which the Risk Assessment process should be based and by extension, used to determine the security counter-measures that are appropriate and proportionate for the organisation, set in the context of asset value and the threat environment. In reality, it is my belief that no security planning should be undertaken without the benefit of first conducting a site-specific Threat Assessment. How can protective measures be installed without first knowing what the defences are there to protect against?

It is widely recognised within the security industry that "defence in depth" or a layered approach to security provides the most effective protection for organisational assets. It is also known that technical security components such as CCTV, access control or alarm systems etc require a substantial financial investment that is often driven by the supplier or installer rather than the assessed need of the business.

In the latest HMG Security Policy Framework, one of the overarching security principles makes it clear that:

> 'Risk management is key and should be driven from Board level. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to people, information and infrastructure to an acceptable level.'

Although this document is aimed at Government and public services, it offers best practice for any organisation.

There have been many examples in both the public and private sectors of security controls being applied to an organisation that clearly do not warrant the level of security controls and its associated financial investment, based on the assets held within the site and the threat environment. This is a disservice to both the organisation and the security profession. It is the responsibility of security professionals to ensure that recommendations made for improvements to an organisation's security infrastructure are appropriate and proportionate, rather than for the commercial benefit of a security equipment installer or supplier.

Summary

There will potentially be a rise in the Terrorist Threat level in the run-up to and possibly during next year's FIFA World Cup in Russia. There should be no rush to install additional security controls without the benefit of a Threat Assessment to ensure that security controls are appropriate and proportionate.

Terrorism or violent extremism are not the only threats facing the UK; businesses as well as government agencies should understand their own threat environment and the emergence of

ever growing cyber-based threats such as ransomware and malicious insiders compromising company networks.

Undertaking security planning without the benefit of first conducting a site-specific Threat Assessment may waste scarce financial resources. In this tough economic climate, this does not make sense.

I believe this underlines the importance of a current, site-specific Threat Assessment upon which security controls can be based and strategic decision-making made. The senior management team should insist that no significant expenditure on security controls should occur without the benefit of a Threat Assessment.

Mark Jones - Senior Security Consultant, Advent IM

0121 559 6699
www.advent-im.co.uk
www.adventim.wordpress.com
bestpractice@advent-im.co.uk