The Enemy Within? The Connection between Insider Threat and Terrorism

D. BaMaung, D. McIlhatton, M. MacDonald and R. Beattie

Original citation & hyperlink:
BaMaung, David, et al. "The enemy within? The connection between insider threat and terrorism." *Studies in Conflict & Terrorism* 41.2 (2018): 133-150
http://dx.doi.org/10.1080/1057610X.2016.1249776

ISSN - 1057-610X

Publisher: Taylor and Francis

The Enemy Within? The connection between Insider Threat and Terrorism

Abstract

While the threat from terrorism has gained widespread acknowledgement over the last decade, the infiltration of organisations by 'terrorist' insiders has not, and the potential dangers these individuals present has not been fully explored. There is a need to understand the wider aspects of insider threats, including motivations and attack methodologies, and to be able to demonstrate the potential devastation that could be caused. Organisations can attempt to mitigate the potential for insider infiltration by both terrorist and other hostile actors, and if such individuals were within an organisation, there are procedures and strategies which can be employed to prevent exploitation of existing organisational vulnerabilities and detection of insiders. This paper provides an informed and new approach to the connection between insider threat and terrorism.

Keywords

Insider Threat, Security, Integrated Security, HRM, Terrorism

Section 1 – Introduction

> *(We) should infiltrate the police forces, the armies, the different political parties, the newspapers, the Islamic groups, the petroleum companies (as an employee or as an engineer), private security companies, sensitive civil institutions, etc. That actually began several decades ago, but we need to increase it in light of recent developments. Likewise, we may need to infiltrate a single place with more than one member—one member will not know another (member) and vice versa—for different roles or the same role if it requires more than one member.*
>
> *(*sourced from Naji, 2006*)*

High-profile terrorist attacks and the resultant increase in global terrorist threat levels in recent years have demonstrated that securing society is a highly complex and dynamic process and as a consequence, governments face unprecedented local, national and global challenges in achieving this. The intended and unintended consequences of terrorist actions have impacted significantly on the capacity and capability of society to function in a manner that attracts investment, promotes socio-economic well-being, develops social relations and cohesion and delivers prosperity. Instead, terrorism has

resulted in the instilment of fear, loss of life and destruction of property globally. The complex and ever changing nature of terrorism has been furthered by the rapid evolution of ideology, behaviour and action, coupled with the emergence of new forms of terrorist tactics and technology. It is therefore of little surprise that research in areas related to terrorism has both evolved and increased substantially in recent decades with a cultural shift away from Northern Ireland Related Terrorism towards emerging threats such as lone actors (Gill et al., 2014; Gill & Corner, 2013), radicalization (Silke, 2008; Horgan, 2008; King & Taylor, 2011) and cyber-terrorism (Lewis, 2002; Matusitz, 2011). One area of focus that has not gained significant attention in the terrorism discourse, but poses a substantial risk, is that of insider threat. Whilst insider threat is inter-connected and aligned with terrorism, the focus of insider threat related scholarly attention has been mostly concerned with the development of capabilities for countering insider threat in organisations through the development of IT-based security mechanisms.

The rationale for the research presented in this article is derived from the distinct lack of literature connecting terrorism and insider threat. Most research in the current literature base has focused on cyber insider, insider crime/fraud and the actions of disgruntled employees with little reference to the potentiality for adoption as a terrorist tactic. Indeed, the necessity for research in this area is furthered by an evident lack of critical analysis where the connection between terrorism and insider threat is made. In these cases, the research predominantly identifies that terrorism is a motivating factor for insiders, but does not categorically focus on terrorism and insider threat. Discussion on the terrorist insider threat typology is also not well advanced despite the significant threat that it poses.

This research therefore develops this rationale and is structured as follows: Section 2 explores the insider threat phenomena and discusses the complexity of interpreting what an 'insider' is, as well as their motivations and key behaviours. Section 3 illustrates examples of terrorist insider attacks globally; Section 4 presents a narrative on mitigating terrorist insider threats, and Section 5 draws conclusions.

Section 2 – The Insider Threat

The defining of insider threat is well established in the current literature base, with significant scholarly attention paid to the concept of what constitutes an '*Insider'* and the threat that they pose although variation exists across security critical disciplines and by academic-practitioner communities. Despite this, no commonly agreed definition exists. In general terms, a research study by Einwechter (2002), defines an insider as 'someone who is entrusted with authorized access, who instead of fulfilling assigned

responsibilities, manipulates access to a system to exploit it'. In a similar vein, Shalini Punithavathani et al. (2015) agree that insider threat develops from someone who has access to privileged resources and exploits those privileges, but is furthered by those members of an organization who also have knowledge of internal information systems, may be involved in decision making and who are in positions of authority over critical operations. Indeed, knowledge of internal systems is also critical in Probst et al's (2007) definition which argues that an insider posing a threat to an organization has developed a strong knowledge about internal procedures, potential high-value critical targets and points of vulnerability. Similarly, Loffi and Wallace (2014) in their research on insider threat within the aviation industry illustrate that insider knowledge allows the perpetrators to exploit vulnerabilities in the nation's aviation systems with the intent of causing harm. Greitzer et al (2012) goes further by stating that insider threat relates to 'harmful acts that trusted individuals might carry out' and that 'the insider threat is manifested when human behaviours depart from established policies, regardless of whether it results from malice or disregard for security policies'. Brackney & Anderson (2004) refer to an insider threat as consisting of malevolent actions carried out by an employee who is already trusted by the organisation, and who has access to sensitive information and information systems.

From a government perspective, there are also no agreed definitions of insider threat and as a consequence, numerous examples exist and are usually much advanced on the definitions found within the academic literature base. The National Insider Threat Task Force (2011) in the United States describe insider threat as 'a threat posed to U.S national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any U.S government resource'. The National Counterintelligence and Security Center (2014) builds upon this definition by asserting that those with access to U.S Government resources, including personnel, facilities, information, equipment, networks, and systems, exploit that access to harm the security of the United States and that such malicious activity can result in incalculable damage. At the UK level, the Centre for the Protection of National Infrastructure (2015) highlight that attacks, including criminal, terrorism and from those seeking commercial advantage, may depend on the co-operation of an insider. Indeed, this insider could potentially be an employee or any contract or agency staff who has access to the organisations premises, who may already work for that organization, or who may have recently joined specifically to exploit the access to that organization.

Whilst there are no agreed definitions relating to insider threat, there is a strong emergence of key themes emanating from the literature of what defines an insider (Figure 1.). First, there is general consensus that *trust* is a core element exploited by those who are engaged or may engage in insider activity (Einwechter, 2002; Bishop, 2005; RAND, 2004; Probst et al. (2007); Greitzer et al. 2012). Second, is the notion of

accessibility. Most of the definitions that exist, reference access to premises, security critical areas or systems within their narrative (CPNI, 2015; Noonan and Archuleta; 2008; National Counterintelligence and Security Center, 2014; National Insider Threat Taskforce, 2011; Greitzer et al. 2012; DHS, 2012; Loffi and Wallace, 2014; RAND, 2004; Probst et al. 2007; Theoharidou et al., 2005; Einwechter, 2002; Shalini Punithavathani et al. 2014). Third, is the element of *knowledge*. In many definitions, the threat is posed when an insider uses their knowledge of the organization and its systems and/or security procedures to cause harm (Mitnick and Simon, 2002; Schneier, 2000; Shalini Punithavathani et al. 2014; Loffi and Wallace, 2014). The next theme that is evident in the definitional discourse is that of the *exploitation* of vulnerabilities (DHS, 2012; Loffi and Wallace, 2014). The fifth theme is that of *intent*. In many instances, there is a requirement that the insider must be exploiting vulnerabilities and security protocols for commercial, criminal and/or terrorist gain and/ or to cause harm (Einwechter, 2002; DHS, 2012; Loffi and Wallace, 2014; Probst et al. 2007; Mitnick and Simon, 2002).

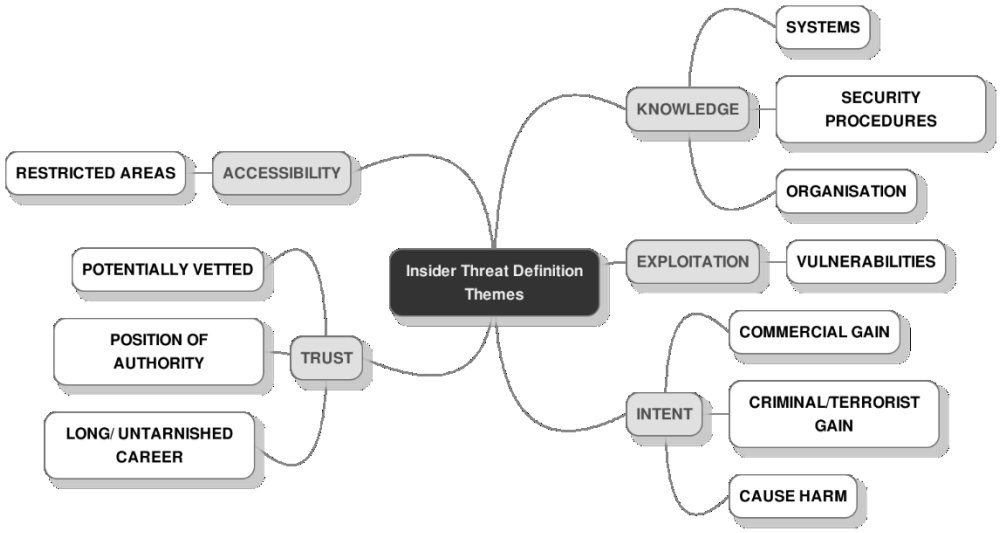

Figure 1. Key themes emerging from Insider Threat definitions in literature base

Key Motivating Factors of Insider Threat

Understanding the key motivations underpinning insider attacks can in many cases be difficult to ascertain. Indeed, there may not be one single motivation attributable to such incidents and in many cases, the motivating drivers may be both multiple and highly dynamic, as well as intentional or un-intentional. In turn, this adds considerably to the complexity of countering the threat, risk and harm associated with actual attacks. Whilst this complexity exists, the current academic and professional discourse identifies a series of thematic motivational factors that manifest themselves in the majority of insider attacks, albeit with varying levels of attention. The most common motivations include

espionage (historically analogue and more contemporaneously, cyber), disgruntlement (of employees) and criminal intent (individual and organized criminal gain).

In recent years, there has been a steady rise in instances of insider activity which have be predominantly driven by espionage (Laska et al. 2014). Indeed, most of this increase has emerged from cyber-espionage which has seen nation states or affiliated organisations utilizing cyber-attack methodologies to obtain military and in most cases, proprietary commercial intellectual property, in order to counter military capabilities and enhance competitiveness and wealth of hostile countries. Whilst cyber has been a key strategy, the 'turning' of an existing employee into 'a spy', whether through financial incentive or under duress, has provided numerous benefits for indirect attackers. First, the external entity does not have to penetrate security critical sites, which in turn, potentially reduces the risk of detection. Instead, they are able to recruit, voluntarily or involuntarily, insiders who can compromise and bypass security measures as trusted members of staff (Laska et al. 2014). Second, the external entity does not have to have a comprehensive knowledge and understanding of the physical or information system location of secret information, instead, they can utilize the insider for this purpose. In a similar vein, the external attackers can utilize the insider to interpret the content of the information that they may obtain and therefore do not need to understand the procedures, protocols or encryption of that secret information. In the context of a new employee, the 'insider' may have joined the organization with the express purpose of obtaining access to information, or compromising that organizations electronic systems.

A second fundamental motivation of an insider attack is often aligned with an individual's disgruntlement with their organization of work and is, in many instances, a result of that organizations failure to recognize an individual's job related achievements (Keeney et al., 2005; Kowaliski et al., 2008). Despite this, the NIAC (2008) found that there was no direct correlation between disgruntlement and insider threat, with their research concluding that the vast majority of disgruntled staff do not engage in actual attacks. Nevertheless, research conducted by Shaw and Fischer (2005) found that 9 out of 10 cases of insider attack studied illustrated significant issues within their employment and that in nearly all cases, those employees' demonstrated signs of disgruntlement and personal problems 1 - 48 months prior to an attack. These findings are furthered by Greitzer et al. (2012) whose research highlights through a survey of professionals that disgruntlement can be identified through understanding the behavior of employees in their workplace. Indeed, the research identified that individuals demonstrating anger towards management and other co-workers, confrontation and general negativity were all identifiable traits of potential threats. In other research, Charney (2010) identified from several in-depth studies of insider spies that a key factor in turning an employee into a traitor has been an intolerable sense of personal failure that they feel in relation to themselves. He opined that 'how this intolerable sense of

personal failure gets managed' will decide whether a person becomes an insider threat. Indeed, the same author also acknowledges that injury to male pride and ego are the cause of many cases of insider threat and espionage.

Attacks which are inherently concerned with financial gain and sabotage are undoubtedly the most commonly researched areas in academic and practitioner discourses with many studies not isolating single motivating factors, but instead illustrating the linkages between motivating factors. Randazzo et al. (2004), through joint research between the US Secret Service National Threat Assessment Centre and the CERT® Coordination Centre, examined known insider incidents within the banking and financial sectors (2003-2004) and established that financial gain was the primary motivation of most attackers. In 2006, research conducted by Lynch (2006) highlighted numerous examples of criminal intent by insider attackers. In one example, data broker Acxiom Corporation, were victims to significant data theft that resulted in losses of $5.8 million. The perpetrator was identified as a contract employee who was subsequently sentenced to 45 months in prison. Indeed, Claycomb et al. (2012) illustrate that an employee of a telecommunication company, when advised to tender resignation, intentionally sabotaged the IT systems of the organization, which in turn, disabled their telecommunications and blocked emergency 911 services in 4 major cities. In another case of sabotage, a disgruntled former employee who was overlooked for a full time position, remotely accessed IT control systems for a sewage treatment plant and facilitated over 200,000 gallons of raw sewage being pumped in to nearby waterways and businesses (Claycomb et al., 2012).

Section 3 - Terrorist Insider Activity

A less well researched area of insider threat is that which is driven by terrorism. This is despite the fact that the conclusion of such terrorist insider events, in many cases, can lead to devastating consequences. Examples of terrorist insider activity support this, such as the 2009 mass shooting which killed 13 people and wounded or injured another 43 at a U.S. Army Soldier Readiness Processing Center (for troops being deployed in theatre overseas) in Fort Hood, Texas. The perpetrator was a serving Army Major, Nidal Malik Hasan, who jumped on a desk and shouted "Allahu Akbar!" - Arabic for "God is great!" before firing from the two pistols in his possession (Webster et al., 2012). Hasan was born in Arlington, Virginia to Palestinian immigrant parents and joined the Army against their wishes, however, rose through the ranks pursuing a career in psychiatry. He began to doubt his military commitment due to harassment in the Army for his Muslim faith (Ross et al., 2009) and had consulted a lawyer whilst he sought discharge as a conscientious objector, a process which intensified after he was told that he was to deploy to Afghanistan himself (Carter and Carter, 2011, Post et al., 2014). During the lead in time to his attack, he was described by colleagues as a ticking time bomb due to his radical views on Islam and wrote papers defending Osama Bin Laden. Despite the outrage of his colleagues, such behaviour was interpreted by line managers

as having a keen interest in Islamic culture and Hasan was subsequently promoted (McCaul, 2012).

Looking more closely at the background of Hasan, evidence suggests that he was relatively introverted and isolated in his personal life (Blomfield, 2009). This intensified with the deaths of his parents in 1998 and 2001 and he began a stricter practice of Islam (Schneider, 2009). In 2001, he attended the Dar al-Hijrah mosque in Falls Church, Virginia where Anwar al-Awlaki was Imam and two of the 9/11 hijackers also attended (Post et al., 2014). Whilst the extent of the relationship at that time, if any, between the two is unclear, al-Awlaki was not then viewed publicly as the inspiration to many young English-speaking Salafi-Jihadi supporters in the west (Barclay, 2010), radicalization leader (Webster et al., 2012), indirect enabler of terrorism (Spaaij and Hamm, 2015) or the new and improved version of Osama bin Laden (Brachman and Levine, 2011) that he is now. This was due to al-Awlaki's relocation to Yemen and subsequent leadership of Al-Qa'ida in the Arabian Peninsula (AQAP) and their launch in 2010 of Inspire magazine, an AQAP-branded, English-language publication inciting and providing practical guidance for attacks on the west.

In addition to Hasan's clearly outspoken views, a further example of observable digital traces or weak signals (Brynielsson et al., 2012) in his pre attack behaviour is the email contact which attracted the attention of the Federal Bureau of Investigation (FBI) between Hasan and al-Awlaki from December 1998 to June 1999 (Berger, 2012a, Berger, 2012b, Webster et al., 2012). Hasan emailed al-Awlaki sixteen times which generated two responses from al-Awlaki. Alarmingly in the first email, he asks al-Awlaki if Hasan Akbar would have been a martyr if he had died during his attack (Gartenstein-Ross and Morgan, 2012). Hasan Akbar was a U.S. Army Sergeant who killed two U.S. Army officers and wounded 14 others in a shooting and grenade attack at Camp Pennsylvania in Kuwait, 25 miles from the border with Iraq. The attack was two days prior to the 2003 invasion of Iraq and at his subsequent court martial, Akbar's attorney argued that Akbar was concerned that the invasion of Iraq would result in the deaths of Muslims and that U.S. soldiers would rape Iraqi women (Bjelopera and Randol, 2010). Further emails to al-Awlaki show that Hasan plainly expressed the view that Western forces were at war with Islam and he sought counsel from al-Awlaki on questions such as whether suicide bombings were acceptable and if collateral damage was permissible in the course of a suicide attack (Gartenstein-Ross and Morgan, 2012).

Two years after the Hasan attack on Fort Hood, a serving Private First Class in the U.S. Army named Naser Jason Abdo was arrested and subsequently convicted of planning a bomb and firearms attack on a restaurant frequented by military personnel based at Fort Hood (Brown, 2012). In a similar manner to Hasan, he previously sought conscientious objector status due to his Muslim beliefs prior to deployment to Afghanistan although at the time of his arrest, he had been reported Absent Without Leave (AWOL) and was awaiting a military trial on charges of possession of child pornography (Johnson, 2011). Interestingly, at one of his court appearances Abdo shouted, "Nidal Hasan, Fort Hood, 2009" (Sivek, 2013) which could be interpreted as a form of inspirational contagion

(Nacos, 2009). Whilst Abdo was linked to al-Awlaki only through possession of the ''Make a Bomb in the Kitchen of Your Mom'' article from Inspire edition 1 (Lemieux et al., 2014), the reach of al-Awlaki expands into wider examples of insider attacks for terrorist purposes.

In 2010, a British Airways (BA) employee named Rajib Karim was arrested after it was discovered that he had been in contact with al-Awlaki and was actively using his position within the organisation to carry out a terrorist attack on behalf of AQAP (Loffi and Wallace, 2014). Karim was an IT employee with BA and found guilty in 2011 of plotting to blow up an aircraft, sharing information of use to al-Awlaki and offering to help financial or disruptive attacks on BA. In a somewhat opportunist element to his attack methodology, Karim volunteered to join BA cabin crew during a period in time when regular cabin crew were on strike but failed because of a technicality (Dodd, 2011). Within the aviation sector, vulnerabilities to terrorist forms of insider attack can extend beyond employees of individual airlines to the wider group of airport staff who have privileged airside access. This can be indirectly, as was the 2006 instance where the AQ linked individual Sohail Anjum Qureshi was in contact with a female who was employed as a retail assistant working airside at London's Heathrow Airport. Whilst the two appear to have been in email contact only, Qureshi was able to obtain information about the security searching regime from her (Casciani, 2008). In a more direct manner, this can be seen in the case of Terry Loewen, a 58-year old Wichita, Kansas airport avionics technician who claimed that Osama bin Laden and Anwar al-Awlaki were his inspiration for engaging in violent jihad (McLaughlin, 2013). He was arrested during an FBI led operation where he believed that he was driving a vehicle laden with explosives into the secure area of the airport to detonate the vehicle between the airport's two terminals at the early morning peak passenger time (Loffi and Wallace, 2014).

The emergence of the self-declared Islamic State (IS) has brought the issue of insider terrorist attacks in the aviation industry to a worldwide audience with the suspected bombing of Metrojet Flight 9268 shortly after departing Sharm el-Sheikh International Airport in Egypt on the 31st October 2015. It has been reported that the aircraft was destroyed by a homemade explosive device equivalent in power to up to 1kg of TNT although initial claims that 2 Egyptian baggage handlers had been arrested in connection to the incident have since been refuted (Hille et al., 2015), it has been described in testimony to the U.S. Senate Committee on Homeland Security and Governmental Affairs that the bomb was almost certainly smuggled aboard the Metrojet flight by an insider at Sharm el-Sheikh airport (Bergen, 2015). Whilst this is still very much a live investigation at time of writing and further facts will emerge in due course, it serves to highlight the risk of terrorist insiders to the aviation industry. This can also be seen in an earlier 2015 U.S. audit that compared the Transport Security Agency's (TSA) aviation worker data against information on individuals who were known to the Intelligence Community. Specifically, the National Counterterrorism Center (NCTC) performed a data match of over 900,000 airport workers with access to secure areas

against the NCTC's Terrorist Identities Datamart Environment (TIDE) and 73 individuals with terrorism-related category codes were identified (Roth, 2015). Whilst the nature of these traces is not in the public domain, this figure is of concern in an operating environment where Miami and Orlando are the only airports in the U.S. that subject workers with airside access to the same security screening regime as that of passengers (Costello and Winter, 2015), despite such screening being in place in the UK since the early 1990's and within the European Union since 2004 (Parkinson, 2015). Following on from the January 2015 terrorist attacks in Paris, similar concerns were raised in relation to 57 workers with airside access who were on an intelligence watchlist as potential Islamist extremists (Campbell and Pancevski, 2015) which resulted in 10 airside electronic pass-key fobs for Charles de Gaulle airport having been removed from employees and 50 employees refused access to the key (Haddad and Lister, 2015).

The anti-western rhetoric of IS with multi-level calls for attacks in the West (Hegghammer and Nesser, 2015) can be seen in an insider context out with the aviation industry when we again look to the military. John T. Booker, JR. (also known as Mohammed Abdullah Hassan) was arrested in 2015 in an FBI led case similar to that of Terry Loewen in that he was driving a van that he believed contained a large quantity of explosives with the intention of attacking a U.S. military base (Shankar, 2015). In 2014, he was denied entry to the U.S. Army less than a month before he was scheduled to report for basic training due to an FBI investigation into publically available content of concern on his Facebook account around him preparing to be killed in jihad. During interview, he admitted that he enlisted in the army with the intent to commit an insider attack against American soldiers like Major Nidal Hassan had done at Fort Hood and stated that if he went overseas and was told to kill a fellow Muslim, he would rather turn around and shoot the person giving orders (Criminal Complaint, 2015). Shannon Maureen Conley was arrested in 2014 whilst attempting to travel to Turkey on a one way ticket with the intention of marrying a Tunisian Islamic State fighter in Syria. In a move away from using her position as an insider for direct targeting purposes such as Hasan, Abdo and Booker, Conley had become a U.S. Army explorer to learn American combat tactics that she could then teach to Islamic State fighters in Syria (Vidino and Hughes, 2015). This exploitation of sensitive techniques and tactics can also be seen with the desertion of a Sergeant in the Netherlands Royal Air Force who is believed to have joined IS (Loveluck, 2015) who had access to information on the computer systems of the Apache attack helicopters, causing the Ministry of Defence to immediately encrypt the information on the helicopter systems to prevent him from accessing the data anymore (Sennels, 2015).

However, the union of insider threat and terrorism is not limited to the post 9/11 Islamic extremism examples above. This wider involvement of insider threat and terrorism ranges from the assassination of Indira Gandhi in 1984 by two of her Sikh bodyguards in apparent retaliation for the Indian military storming of the Golden Temple in Amritsar (Bryjak, 1985) to the 2004 Northern Bank robbery in Belfast in December 2004 in which

suspicions were raised by the media and the security forces about the possibility of Provisional Irish Republican Army (PIRA) involvement (Ashe, 2006). The insider aspect to this last example was actually due to the tiger kidnap style hostage taking of two families to coerce two senior executives to bypass the security systems of the bank and facilitate the robbery (Noor-Mohamed, 2014). Such examples are by no means exhaustive and serve to highlight the diverse range of insider threat aspects which can appear as terrorist attack methodologies.

Section 4 - Mitigating Terrorist Insider Threat

In order to mitigate insider activity of this nature, it is important to understand, develop and employ policies and procedures within organisations. Given the complexity involved in terrorist insider threat and the disparate motivations and consequences that are experienced, it is essential that any mitigation measures transcend high level organisational policy and are delivered operationally in a holistic manner. As previously discussed, the motivation or 'drivers' of insider attacks can be many and varied. Irrespective of what they are, there is an urgency and fundamental need to understand, counter and mitigate such activities. This research proffers that the most effective way to achieve this is through a holistic approach to security within the organisation, which is centred on the concept of integrated security management connecting personnel (people) security, physical security, and cyber security. The rationale behind a holistic approach is due to the interdependencies that exist between these three security strands. Essentially, if one of these fails, the others may become compromised. The connection point between each of these is the development of procedures which can be applied across all three of these security strands. Failure to comply with security procedures may compromise an organisation despite strong security processes in other areas. Research has found that many organisations do not have a cohesive link between these three areas, and the resultant disjointed approach presents the identification of organisational weaknesses that may lead to opportunities for exploitation (Beattie and BaMaung, 2015).Indeed, much of these opportunities relate to issues connected with human resource management and organisational culture.

From a personnel (people) security perspective, there are a number of countermeasures to insider attack which can be employed. An insider threat can come from a number of stages in an employees working life cycle and it therefore fundamental that such stages are routinely managed. Identifying signs of disgruntlement or changed behaviour patterns amongst the workforce could be important indicators of potential threats by individual employees and should be acted on at an early stage. This process should commence as early as the first day of employment and continue to an employee's dismissal, resignation or retirement (Hanley et al, 2009). There are certain predisposed traits exhibited by potential insiders which can be impacted on by situational stressors within an organisation, and the general organisational environment. By screening potential employees for these traits and rejecting those who show strong indications of them, it may be possible to reduce the overall risk from insider attack (Shaw et al., 1998). There are several personality tests and assessments available,

which can be used from the initial recruitment stage, through to the final stages of employment, to flag potential or actual issues of concern with employees (Furnham & Taylor, 2011; Vernon, 1953; Anastasi, 1968; Cohen et al, 2002). If an organisation was being deliberately targeted by a terrorist group, the threat group may attempt to infiltrate an 'insider' into the targeted organisation. Such an attack form carries many risks for the terrorists. The 'insider' must undergo some form of recruitment process, where candidates will be screened in an attempt to mitigate some of the infiltration techniques which can be used during recruitment. These include the provision of exaggerated experience/skillsets, false qualifications/certification being presented, or the provision of false references.

The deterrence process to prevent recruitment of an employee that may pose a potential insider threat, particularly for security critical jobs, can start at the job advertisement stage. By introducing awareness that full security screening would be required for successful applicants, it can serve as a filter for 'problem individuals' (Mortell, 2006). It may therefore be possible to screen out some individuals who would see the risk of undergoing the full recruitment and vetting process as too great. There should also be some form of background check carried out, and for organisations which work within a high security sector, these checks may be comprehensive and intrusive. Properly conducted background checks may reveal inconsistencies in the job applicant's story and provide a warning to the recruiters. Nevertheless, some groups may spend considerable time and effort attempting to subvert the recruitment process and therefore checks must go beyond an individual's background and focus on aspects such as an individual's character. Whilst it may seem rudimentary, threat mitigation measures must involve the rigorous checking of a job applicant's referees and previous employers. In practice, however, many organisations do not carry out proper confirmatory checks in relation to this and as a consequence may leave themselves open to vulnerability. These checks should be well structured and capture the information that the potential employer seeks to understand in a manner that ensures factuality is achieved.

Document verification is another area where significant accuracy must achieved. Training in the identification of fraudulent documentation must be delivered to all staff responsible for document verification. Despite this, research has shown that many organisations do not train front line staff sufficiently to identify discrepancies in key documents (BaMaung and Beattie, 2014; Beattie & BaMaung 2015). Research carried out by BaMaung and Beattie (2014) found that in many cases the responsibility for checking documentation of job applicants (e.g. birth certificates, qualifications, driving licenses, passports, etc.) was usually delegated to a junior member of staff. These members of staff were rarely trained in document verification and identifying fraudulent documents, and a job applicant could potentially join an organisation using fraudulent means. Even if this individual had no initial wish to compromise the organisation, they could be left vulnerable by this fraudulent activity and open to blackmail or compromise in the future, should someone find out. Until an encrypted message standard is

achieved across sectors whereby methods such as steganography are adopted by those issuing documentation, the creation and utilisation of fraudulent documents will continue to enhance vulnerability, particularly in cases where it is difficult to efficiently and effectively check.

Measures discussed so far may be of assistance to respond to a threat from terrorist or other hostile individuals if they attempted to join an organisation. However if the threat is already present within existing staff, there must be a means for suspicions by colleagues to be voiced. There are many examples evident in the literature base that illustrate the issues that genuine whistleblowers have faced in the past when speaking out against their organisations practices or activities by work colleagues. Indeed, the punishment for this has often been significant. Examples such as that of Jeffrey Wigand, who exposed highly questionable practices within the tobacco industry, demonstrate clearly that there is a distinct need to safeguard those who express genuine concerns about individuals and occurrences within organisations. His actions cost him his job, his family, and left him in relative poverty (Lyman, 1999). Whilst this example is not terrorist focused, the need to protect individuals concerned about behaviours which may have a terrorist motive and impact is fundamental. In order to provide an opportunity for legitimate worker concerns to be expressed, many organisations have introduced anonymous staff reporting systems and this is considered a necessary mechanism in the views of this research. Whilst it is important to have such a system, there must also be controls in place to ensure that misuse is negligible.

Indeed, it is also important to train staff on the ability to understand behaviours of concerned in order to protect themselves and work towards safeguarding those who may be potential insiders. There are certain predisposed traits exhibited by potential insiders which can be impacted on by situational stressors within an organisation, and the general organisational environment. By screening potential employees for these traits and rejecting and/or better managing those who show strong indications of them, it may be possible to reduce the overall risk from insider attack (Shaw et al., 1998). There are several personality tests and assessments available which can be used from the initial recruitment stage, through to the final stages of employment in order to flag potential or actual issues of concern with employees (Furnham & Taylor, 2011; Vernon, 1953; Anastasi, 1968; Cohen et al, 2002).

Moving beyond recruitment and human resource management related mitigation methods, a key factor in ‘target hardening’ the working environment against terrorist or hostile attack relates to the culture within that organisation. If the organisation has a weak security culture, poor security practices may be accepted as being normal. This could allow a hostile individual, be they terrorist, criminal or disaffected employee, to better avoid detection of potential aberrant behaviour. Research has been carried out into organisational culture (Jackson, 2012; Lacey, 2009; Smith & Kleiner, 1987) but the

ability to change poor or weak security culture and wider organisational cultures is extremely difficult and may only be achieved over years or decades rather than weeks or months. The simple matter of raising awareness at an executive level of the danger from insider attack or infiltration is not being achieved in many organisations. Relating the potential for insider threat to affect an organisations 'bottom line' is a message that is not getting across to many senior managers with research conducted by Lacey (2009) suggesting that business objectives and security cultures need to be aligned as in many cases, they are actually incompatible. Indeed, an insider attack could potentially impact on intellectual or physical property within an organisation, however, the motivations of the insider may influence the type of organisation selected and the manner of attack.

Insider attack for financial gain may be more aligned to a criminal venture by an employee, organised crime group or a disgruntled employee. However, a terrorist related motivation involving some form of financial crime cannot be totally ruled out, as pre-attack planning and preparation by terrorist groups requires funding. This funding can either be provided by those sympathetic to the terrorist cause, or through the commission of crime (including theft and fraud). Should an employee be identified by a colleague or other person as presenting 'behaviours of concern' it is critical that an integrated approach be taken to review the matter and that all relevant stakeholders are involved in this e.g. line managers, HR, Information Security, legal and IT. An integrated approach to security would then ensure that an insider threat was mitigated against by ensuring appropriate physical security measures, such as access control, are in place to hinder or disrupt behaviour by the insider. This can be augmented by a cyber security response involving the analysis of information accessed by the individual, prevention of data lifting/destruction, back up data procedures and monitoring of an individual's use of systems.

The importance of procedures within an organisation is critical to any integrated approach. This would include issues such as enforcement of a clear desk policy, prevention of tailgating through particular areas, password control and management as well as operating a need-to-know approach for the most sensitive documents and systems. In 2015, the Centre for the Protection of National Infrastructure (CPNI) published a document on their findings in relation to poor workplace practices and behaviours (CPNI, 2015). This document identified seven key security culture issues in the workplace that enhance vulnerability to insider attack.

- Staff not wearing their pass while in the office or forgetting to take it off when they leave work
- Computers left unlocked when staff are away from their desks
- Staff continuing sensitive discussions outside the meeting room
- Sensitive documents being left out for anyone passing by to see

- Sensitive materials being destroyed inappropriately, such as not using a shredder
- Staff ignoring company security policies and measures
- Letting visitors walk around the office unescorted or without a pass

At a more strategic level a clear link was identified between an insider act taking place and exploitable weaknesses in an employer's protective security and management processes. The organisational-level factors identified relate to:

- Poor management practices
- Poor use of auditing functions
- Lack of protective security controls
- Poor security culture
- Lack of adequate, role-based, personnel security risk assessment
- Poor pre-employment screening
- Poor communication between business areas
- Lack of awareness of people risk at a senior level
- Inadequate corporate governance

(CPNI, 2013 pp5)

If these simple security procedures were complied with by everyone within the organisation, the opportunities available to the 'insider' would be greatly reduced.

An important strand to a mitigation strategy should be the acknowledgement of the potential impact of insider threat and inclusion of this threat within the organisations risk register. Only by acknowledging the risk, assigning a strategic risk owner, and developing a risk mitigation strategy, will the issue begin to be addressed in a cohesive manner. When calculating the level of risk and mitigation measures required, it may be necessary to consider the different types of insider threats and calculate both the likelihood of such an attack happening, and the impact of such an attack. Another consideration to be factored in, is the potential reputational damage if an terrorist insider attack occurs.

Finally, the need to have clear procedures regarding departing employees cannot be overemphasised. It is essential that access to sensitive information is withdrawn, along with password access and dial-in numbers (Mitnick and Simon 2002). Approaches in organisations vary considerably. Some refuse, with immediate effect, to allow access to employees who have been suspended or fired. Others allow employees to continue accessing systems once they have been advised of the termination of their employment. While this paper does not provide a definitive list of all actions which

could/should be taken by an organisation if they find themselves in the unfortunate position of having an insider present, it should provide a wider understanding of the dangers presented by potential terrorist insiders. Once this danger is recognized and acknowledged, it is then possible to develop an appropriate mitigation strategy.

Section 5 – Conclusions

While the causes and impacts of terrorism are widely researched, there has been very little research conducted in the area of insider threats to organisations motivated by terrorist individuals and ideologies. The impact a terrorist insider could have, if located within a critical infrastructure or key organisations, could be immense and there is a need to explore this topic further. Examples are already available of individuals who have been within organisations and have been motivated by terrorist ideologies, to attack their organisation and colleagues, and there is information available which can be used to mitigate the opportunities for this type of threat to develop to attack stage in the future. In order to successfully combat insider threat, there is a need for strategic engagement and support within organisations in the development of insider threat mitigation strategies, and this must involve a holistic security approach to the threat, with engagement of the whole workforce. Without this strategic drive and widespread engagement with staff, any attempts to mitigate the threat from insider attack will be limited.

Anastasi, A. (1968) Psychological Testing. (3rd Ed) *Macmillan, Oxford, England.*

Ashe, F. (2006) The McCartney Sisters' Search for Justice: Gender and Political Protest in Northern Ireland. *Politics,* 26**,** 161-167.

Barclay, J. (2010) Challenging the Influence of Anwar Al-Awlaki. *In: Rubin, H. & Bew, J. (eds.) Developments in Radicalisation and Political Violence.* London: ICSR.

Bergen, P. (2015) The Impact of ISIS on the Homeland and Refugee Resettlement. *Testimony presented to the U.S. Senate Committee on Homeland Security and Governmental Affairs.* Washington, D.C.

Berger, J. M. (2012a) *Anwar Awlaki E-Mail Exchange With Fort Hood Shooter Nidal Hasan* [Online]. Intelwire. Available: http://news.intelwire.com/2012/07/the-following-e-mails-between-maj.html.

Berger, J. M. (2012b) *The Content and Context of Anwar Awlaki's E-mails with Fort Hood Shooter Nidal Hasan* [Online]. Intelwire. Available: http://news.intelwire.com/2012/08/the-content-and-context-of-anwar.html.

Bishop, M. (2005) September. Position: Insider is relative. In *Proceedings of the 2005 workshop on New security paradigms* (pp. 77-78). ACM.

Bjelopera, J. P. & Randol, M. A. (2010) American Jihadist Terrorism: Combating a Complex Threat. *Washington, DC: Congressional Research Service.*

Blomfield, A. (2009) Fort Hood shooter is deeply sensitive introvert, say Palestinian relatives. *The Telegraph*, 2009/11/07.

Brachman, J. M. & Levine, A. N. (2011) You too can be Awlaki. *The Fletcher Forum of World Affairs,* 35**,** 25-46.

Brackney, R.C. and Anderson, R.H. (2004) Understanding the Insider Threat. Proceedings of a March 2004 Workshop. *Rand Corp Santa Monica CA.*

Brown, A. (2012) Judge won't toss confession in Fort Hood bomb plot. *TwinCities.com*, 2012/04/20.

Bryjak, G. J. (1985) The Economics of Assassination: The Punjab Crisis and the Death of Indira Gandhi. *Asian Affairs: An American Review,* 12**,** 25-39.

Brynielsson, J. et al. (2012) Analysis of Weak Signals for Detecting Lone Wolf Terrorists. Analysis of Weak Signals for Detecting Lone Wolf Terrorists. *Los Alamitos, CA. IEEE Computer Society, 197-204.*

Campbell, M. & Pancevski, B. (2015) French panic over Islamists with runway clearance. *The Sunday Times*, 2015/11/29.

Carter, J. G. & Carter, D. L. (2011) Law enforcement intelligence: implications for self-radicalized terrorism. *Police Practice and Research,* 13**,** 138-154.

Casciani, D. (2008) The terrorist and the shop girl [Online]. BBC News. Available: http://news.bbc.co.uk/1/hi/uk/7177702.stm.

Claycomb, W. R. et al. (2012) Chronological examination of insider threat sabotage: preliminary observations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *3*(4), pp.4-20.

Cohen, R. J. et al. (2002) Psychological testing and assessment: An introduction to tests and measurement. (5th Ed) *McGraw-Hill, New York, US*

Complaint, C. (2015) United States of America V. John T. Booker JR. a/k/a "Mohammed Abdullah Hassan" *In:* KANSAS, U. S. D.C.F.T.D.O.(ed.).

Costello, T. & Winter, T. (2015) 'The Insider Threat Is Real': Gaps in Airport Security Highlighted in New Video [Online]. *NBC News. Available: http://www.nbcnews.com/news/us-news/insider-threat-real-gaps-airport-security-highlighted-new-video-n469701.*

Department of Homeland Security Office of Inspector General (2012) *Transportation Security Administration has taken steps to address the insider threat but challenges remain.* (DHS OIG Report No. OIG-12-120). Retrieved from http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-120_Sep12.pdf

Dodd, V. (2011) British Airways worker Rajib Karim convicted of terrorist plot. *The Guardian*, 2011/02/28.

Einwechter, N. (2002) Preventing and detecting insider attacks using ids.*SecurityFocus, March*.

Gartenstein-Ross, D. & Morgan, L. (2012) Nidal Hasan's "Fairly Benign" Correspondence with Anwar al Awlaki [Online]. Available: http://www.daveedgr.com/news/nidal-hasans-fairly-benign-correspondence-with-anwar-al-awlaki/.

Gill, P. & **Corner, E.** (2013). Disaggregating terrorist offenders: Implications for research and practice. Criminology & Public Policy, 12, 93-101. doi: http://dx.doi.org/10.1111/1745-9133.12015

Gill, P., Horgan, J. and Deckert, P. (2014), Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists. *J Forensic Sci, 59: 425–435*

Greitzer, F.L., et al. (2012) January. Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2392-2401). IEEE.

Haddad, M. & Lister, T. (2015). France has been investigating radicalized public transit workers, source says [Online]. CNN. Available: http://edition.cnn.com/2015/11/24/europe/airport-public-transit-employees-paris-investigation/index.html.

Harney, D.L. (2005) True Psychology of the Insider Spy. *Journal of U.S. Intelligence Studies. Fall/Winter 2010*

Hegghammer, T. & Nesser, P. (2015) Assessing the Islamic State's Commitment to Attacking the West. *Perspectives on Terrorism,* 9**,** 14-30.

Hille, K., Dombey, D. & Solomon, E. (2015) Russia says terrorist bomb brought down Metrojet aircraft. *Financial Times*, 2015/11/17.

Horgan, J. (2008) From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. *The Annals of the American Academy of Political and Social Science*, *618*(1), pp.80-94.

Johnson, K. (2011) AWOL soldier charged in bombing plan on Texas post. *USA Today*, 2011/07/29.

Keeney, M. et al. (2005) Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. *Pittsburgh, PA Carnegie Mellon University Software Engineering Institute/ United States Secret Service.*
www.cert.org/archive/pdf/insidercross051105.pdf

King, M. and Taylor, D. M. (2011) The radicalization of homegrown jihadists: A review of theoretical models and social psychological evidence. *Terrorism and Political Violence*, *23*(4), pp.602-622.

Kowalski, E. T. et al. (2008) Insider Threat Study: Illicit Cyber Activity in the Government Sector. *U.S. Secret Service and CERT/SEI.*

Lacey, D. (2009) Managing the Human factor in Information Security *pp 181. John Wiley and Sons Ltd, Chichester*

Lemieux, A. F., Brachman, J. M., Levitt, J. & Wood, J. (2014) Inspire Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model. *Terrorism and Political Violence,* 26**,** 354-371.

Lewis, J. A. (2002) Assessing the risks of cyber terrorism, cyber war and other cyber threats. *Washington, DC: Center for Strategic & International Studies.*

Loffi, J. M. & Wallace, R. J. (2014) The unmitigated insider threat to aviation (Part 1): a qualitative analysis of risks. *Journal of Transportation Security,* 7**,** 289-305.

Loveluck, L. (2015) Dutch air force sergeant joins Islamic State in first such desertion. *The Telegraph*, 2015/09/03.

Lyman, R. (1999) A Tobacco Whistle-Blower's Life Is Transformed. *New York Times, 15 October 1999*

Lynch, D. M. (2006). Securing Against Insider Attacks. *Information Security and Risk Management, 15(5), 39-47*

Matusitz, J. (2011) Social network theory: A comparative analysis of the Jewish revolt in antiquity and the cyber terrorism incident over Kosovo. *Information Security Journal: A Global Perspective*, *20*(1), pp.34-44.

McCaul, M. T. (2012) Lessons from Fort Hood: Improving our ability to connect the dots. *Hearing Before the Subcommittee on Oversight, Investigations, and Management of the Committee on Homeland Security House of Representatives.* Washington, DC.

McLaughlin, E. C. (2013) Local man planned suicide attack at Wichita, Kansas, airport, feds say. *CNN*, 2013/12/14.

Mitnick, K. and Simon, W. (2002) The art of deception. *Hoboken.*

Nacos, B. L. (2009) Revisiting the Contagion Hypothesis: Terrorism, News Coverage, and Copycat Attacks. *Perspectives on Terrorism,* 3**,** 3-13.

Naji, A. B. (2006) Management of Savagery: The Most Critical Stage Through Which The Umma Will Pass. Section Nine: Mastering the security dimension: Surveillance and infiltrating adversaries and opponents of every kind. *Section 9 (52) (Translation by William McCants – 23 May 2006 – funded by the John M. Olin Institute for Strategic Studies, Harvard University)*

National Infrastructure Advisory Council (US), (Noonan, T. and Archuleta, E.) (2008) *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*. DHS/NIAC.

Noor-Mohamed, M. K. (2014) The Definitional Ambiguities of Kidnapping and Abduction, and its Categorisation: The Case for a More Inclusive Typology. *The Howard Journal of Criminal Justice,* 53**,** 83-100.

Parkinson, J. (2015) *Russian plane crash: How has airport security changed?* [Online]. *BBC News Magazine. Available*: http://www.bbc.co.uk/news/magazine-34731146.

Post, J. M., McGinnis, C. & Moody, K. (2014) The Changing Face of Terrorism in the 21st Century: The Communications Revolution and the Virtual Community of Hatred. *Behavioral Sciences & the Law,* 32**,** 306-334.

Probst, C.W., Hansen, R.R. and Nielson, F. (2007) Where can an insider attack? In *Formal Aspects in Security and Trust (pp. 127-142). Springer Berlin Heidelberg.*

Punithavathani, D.S., Sujatha, K. and Jain, J.M. (2015) Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence. *Cluster Computing*, 18(1), pp.435-451.

Randazzo, M. R. et al. (2004) Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. *U.S. Secret Service and CERT Coordination Center/ Software Engineering Institute, 25.*

RAND (2004) Understanding the Insider Threat. *RAND Corporation. Santa Monica, California*

Ross, B. et al. (2009) Nidal Malik Hasan, Suspected Fort Hood Shooter, Was Called "Camel Jockey" [Online]. ABC News. Available: http://abcnews.go.com/Blotter/nidal-malik-hasan-wanted-army-family/story?id=9008184.

Roth, J. (2015) Statement of Inspector General of the Department of Homeland Security concerning TSA Security Gaps. *Washington, D.C.*

Schneider, H. (2009) Fort Hood suspect became more devout after mother's death, cousin says. *The Washington Post*, 2009/11/07.

Schneier, B. (2000) Secrets and Lies: Digital Security in a networked world. *New York. John Wiley & Sons Inc. ISBN: 0-471-25311-1*, *4*, pp.100-15.

Sennels, N. (2015) Holland: Dutch soldier who defected to Islamic State is of Turkish descent. *10News.dk*, 2015/10/08.

Shankar, A. (2015) Would-Be Suicide Bomber Targeted Kansas Army Base. *For The Record - The Investigative Project on Terrorism Blog* [Online]. Available from: http://www.investigativeproject.org/4822/would-be-suicide-bomber-targeted-kansas-army-base#.

Shaw, E.D. and Fischer, L.F. (2005) Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations. *(No. PERS-TR-05-13). Defense Personnel Security Research Center Monterey CA.*

Silke, A. (2008). Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalisation. *European Journal of Criminology, 5/1, pp.99-123*

Sivek, S. C. (2013) Packaging Inspiration: Al Qaeda's Digital Magazine Inspire in the Self-Radicalization Process. *International Journal of Communication, 7* 584–606.

Spaaij, R. & Hamm, M. S. (2015) Key Issues and Research Agendas in Lone Wolf Terrorism. *Studies in Conflict & Terrorism,* 38**,** 167-178.

Vernon, P. (1953) Personality Tests and Assessments. *Methuen & Co., Oxford, England.*

Vidino, L. & Hughes, S. (2015) ISIS in America: From Retweets to Raqqa. Washington, D.C.: *Program on Extremism, The George Washington University.*

Webster, W. H. et al. (2012) Final Report of the William H. Webster Commission on The Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009. *In:* FBI (ed.). Washington, DC.