Mitigating malicious insider cyber threat

Jason Anthony Smith

Technical Report


4 March 2015

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom
Final Year Project Report

Mitigating malicious insider cyber threat

Jason Anthony Smith
SRN: 030326125

Supervisor: William Rothwell

Department of Computer Science
Royal Holloway, University of London

Submitted as part of the requirements for the award of the MSc in Information Security of the University of London
Declaration

This report has been prepared on the basis of my own work. Where other published and unpublished source materials have been used, these have been acknowledged.

Word Count: 19,019

Student Name: Jason Anthony Smith

Date of Submission: 31st March 2014

Signature: J.A. Smith

Acknowledgements

With no implication of significance conveyed by ordering, I would like to sincerely thank my wife Karen, my family, friends, line manager, colleagues, company and project supervisor for the help and support they have generously given to me on what has been a long but interesting and rewarding journey.

Abstract

This paper examines malicious insider threat and explains the key differences from other types of insider threat and from external threat actors. A phase based “kill-chain” malicious insider threat model is developed and proposed to help inform selection of mitigation countermeasures which are complementary or incremental to a typically implemented traditional ISO 17799/27002 information security management system (ISMS). An analysis of best practice guidance is used to select appropriate countermeasures and strategic considerations for implementing an effective insider threat mitigation programme.
# Table of Contents

## INTRODUCTION .................................................................................................................. 5

### BACKGROUND AND PURPOSE .................................................................................. 5

### DOCUMENT OUTLINE .................................................................................................. 6

## CHAPTER 1: INSIDER THREAT ....................................................................................... 7

1.1 INSIDERS .................................................................................................................... 7
1.2 NON-MALICIOUS INSIDERS .................................................................................. 9
1.3 MALICIOUS INSIDERS .......................................................................................... 10
1.4 INSIDER ADVANTAGE ............................................................................................ 12
1.5 THREAT ACTOR LANDSCAPE ............................................................................... 14
1.6 INSIDER CRIMES .................................................................................................... 16
1.7 MALICIOUS INSIDER CHARACTERISTICS ......................................................... 18
1.8 THREAT MODEL .................................................................................................... 19
1.9 RISKS AND VULNERABILITIES ........................................................................... 23
1.9.1 Risk bow-tie ..................................................................................................... 23
1.9.2 Vulnerabilities and exploitation methods ..................................................... 24

## CHAPTER 2: MITIGATION .............................................................................................. 29

2.1 INTRODUCTION ....................................................................................................... 29
2.1.1 Scope .................................................................................................................. 29
2.1.2 Approach and analysis ..................................................................................... 30
2.1.3 Using the threat model ..................................................................................... 32
2.2 MITIGATION COUNTERMEASURES ...................................................................... 33
2.2.1 Insider threat awareness and intervention programme (C1,C5,C7) ............... 33
2.2.2 Pre-employment and on-boarding processes (C2) ....................................... 34
2.2.3 Identity and access management (C3) ............................................................. 34
2.2.4 Technical baseline profiling and anomalous behaviour detection (C4) ......... 35
2.2.5 Insider threat incident response (C6) ............................................................. 35
2.2.6 Internal social engineering (C8) ..................................................................... 35
2.2.7 Data loss prevention (C9) ................................................................................. 36
2.2.8 Information rights management (C10) ........................................................... 37
2.3 MITIGATION STRATEGY .......................................................................................... 37
2.3.1 Malicious insider mitigation complements traditional ISMS (S1, S2) .......... 37
2.3.2 Bias towards deterrence (S3) .......................................................................... 38
2.3.3 Risk prioritised (S4) ......................................................................................... 38
2.3.4 Continuous improvement (S5) ....................................................................... 39
2.3.5 Governance (S6, S7) ....................................................................................... 39
2.3.6 Compliance with international laws and regulations (S8) ......................... 39
2.4 INITIATING A PROGRAMME ..................................................................................... 40

## CHAPTER 3: CONCLUSION ............................................................................................. 42

3.1 SUMMARY ................................................................................................................. 42
3.2 FURTHER RESEARCH ............................................................................................... 43

## LIST OF ABBREVIATIONS AND ACRONYMS ............................................................. 44

## TERMS AND DEFINITIONS ............................................................................................ 45

## BIBLIOGRAPHY .............................................................................................................. 46
List of figures and tables

Figure 1  Insider definition chosen for this report .................................................................8
Figure 2  Non-malicious insider definition chosen for this report ........................................10
Figure 3  Malicious insider definition chosen for this report. ...............................................12
Figure 8  Malicious insider threat model ...........................................................................23
Figure 4  High-level risk ‘bow-tie’ for insider crime ..............................................................24
Figure 5  Example methods for achieving the crime of IP theft ...........................................25
Figure 6  Example methods for achieving the crime of Fraud ...............................................27
Figure 7  Example methods for achieving the crime of Sabotage .........................................27
Figure 9  Complementary mitigation programmes for different threats .................................30
Figure 10  Intersection of variables: criticality, means, motive and opportunity ..................38

Table 1  Ranking of threat actors using a simple judgement based (qualitative) threat model ....15
Table 2  Analysis of best practice guidance .........................................................................32
Table 3  Phase based malicious insider threat model – key to labels ..................................33
Introduction

“I believe that organizations who have good insider threat and data protection programs will be around in 10 years, and those that don't -- won't.” [PR13].

Patrick Reidy, FBI CISO, 2013.

Background and purpose

Most large organisations have become increasingly dependent upon their digital systems and information to remain competitive and therefore strongly rely upon their information security protection programmes to maintain the confidentiality, integrity and availability of that information. This is becoming more demanding as IT becomes more pervasive and complex, whilst at the same time the sophistication and volume of cyber-attacks is increasing at an alarming rate year on year [VE13].

FBI Director Robert Mueller has predicted that the cyber threat will equal or even eclipse the terrorist threat [RM13].

Information security programmes have naturally evolved with a focus on protecting the organisation against non-trusted entities whom are external to the organisation, however the UK Cyber Strategy notes that “Computer systems, networks and applications all rely upon people for their development, delivery, operation and protection” and “the likely success of an attack is increased when a so-called ‘insider’ is involved” [UK09].

An insider has a degree of trust invested in them by the organisation and have likely been granted physical and logical access to the organisation’s IT systems and information in order to fulfil the duties of their role. Herein lies the fundamental difference between defending against external attackers and defending against insiders, in that preventing a security incident originating from an external attacker is largely about preventing their access to systems and information, whereas insiders have that access granted to them already.

In one set of investigations, 87 percent of identified intruders into DoD information systems were either employees or others internal to the organization [DD00]. In contrast though, Verizon’s findings [VE13] indicate that by volume only 14 percent of breaches across a broad range of industries and organisations were committed by insiders.

Care needs to be taken when attempting to interpret and compare these DoD and Verizon statistics. For example, perhaps over time the external threat has increased, and/or the internal threat has decreased, and/or DoD systems taken in isolation are more likely breached by insiders than non-insiders, and/or DoD has more success in identifying the perpetrators of breaches when they are insiders than the average organisation, or many more reasons. And note too that these statistics relate to the volume/number of attacks rather than the impact caused be them.

Rather than try and precisely quantify the relative threat from insiders versus others, it is enough to acknowledge that the threat from insiders is real, can significantly impact an organisation including destroying it [BC06, p57], and needs to be appropriately treated.

Effective solutions to the insider problem have however proven to be elusive. Insiders can probably do anything an external attacker can do, and then much more because of the advantage
of being inside the perimeter with already granted access to systems and information. When a roundtable of US government agencies compiled a list of “the hardest and most critical challenges in INFOSEC research that must be addressed for the development and deployment of trustworthy systems for the U.S. Government.” this so-called “Hard Problem List (HPL)” ranked insider threat as the number two hardest problem behind ‘global scale identity management.’ [DM06].

The purpose of this report is to examine malicious insider threat and propose a pragmatic set of countermeasures and a strategy for its mitigation in the context of a large global organisation.

**Document outline**

**Chapter 1: Insider threat**

A thorough examination of insider threat is presented in this chapter. It describes how insiders can deliberately and unintentionally contribute to incidents. The terms “insider”, “non-malicious insider” and “malicious insider” are defined. The motivations of a broad range of threat actor categories are examined. The unique opportunities which insiders have over external attackers is discussed. A high level risk model for malicious insider threat is presented along with example methods of exploiting typical vulnerabilities. Malicious insider characteristics are discussed. A phase based (kill-chain) malicious insider threat model is developed and presented.

**Chapter 2: Mitigation**

Mitigation countermeasures and strategy are presented in this chapter. A rationale is explained for a scope which is incremental and different to a typical traditional information security management system (ISMS) and which is also not addressed by a kill chain methodology designed against external intrusion. A critical analysis of best practice countermeasures and strategic considerations is presented. Countermeasures are explained and set against the phase based malicious insider threat model which was developed in chapter one. Strategic considerations are explained and presented. A proposal for an ordered programme to build incremental capability for mitigating malicious insider threat is presented.

**Chapter 3: Conclusion**

This chapter closes out the report with a summary, final comments and some thoughts related to areas of further research.
Chapter 1: Insider threat

To solve a problem, it is essential that the problem is understood as deeply and completely as possible. Without focussing enough energy of this step then assumption and dogma will underpin the solution which is designed [GP45]. This chapter presents a thorough examination of insider threat so that the emergence of an elegant and efficient solution can be more likely.

1.1 Insiders

An intuitive starting point is that the insiders of an organisation are simply its employees. This organisational relationship only definition is quickly challenged as inadequate when consideration is given to the resourcing strategies of modern organisations with a contingent labour force made up of contractors, managed service personnel, consultants, third party support personnel and others. If these groups are ignored in the definition then on what basis can that be defended when often they are almost indistinguishable from employees in that they have the same access to the same systems and information, are supplied with the same equipment and work out of the same buildings?

It would seem then that as well as organisational relationship, a key attribute of the insider definition is related to access.

A purely access centric definition is proposed by Gabrielson [BG06, p1] whom also says that insiders should be considered in two categories: true-insiders and pseudo-insiders. This definition and the two proposed categories are instructive to examine in detail.

True insiders are defined as “any entity (person, system, or code) authorized by command and control elements to access network, system, or data”. This avoids the organisational relationship attribute discussed above and focuses purely on access, and also introduces the concept that systems and code, which have been given access, should also be considered to be insiders. This non-human definition of insider is a departure from the human-only position of many widely accepted definitions [DD00, DC12]. Use of this proposed definition for insider would invalidate many of the statistics, trends and findings from a great deal of existing analysis and research on insider threat. This would seem to be a huge disadvantage as much insider threat mitigation work is informed, directed and prioritised based on insights from mining the data from past incidents. On that basis, choosing a widely accepted definition of insider should be considered extremely important.

Pseudo-insiders are defined as “someone who, by policy, is not authorized the accesses, roles, and/or permissions they currently have but may have gotten them inadvertently or through malicious activities”. Interestingly, this definition switches back to only people being in scope, but introduces the concept that anyone could be considered an insider whom has access whether it was granted to them legitimately or not. This implies that remote external hackers, with no current or former relationship to the organisation, whom maliciously gain access to a system should then be considered to be insiders. This would seem problematic as a definition of insider because it doesn’t seem to exclude anyone apart from those that don’t attack the organisation. Again, this proposed definition contrasts with the widely accepted position that a key attribute of the insider definition is that access has been legitimately granted to them.

Consider a scenario where an employee works for a company and has privileged access and intimate knowledge of its networks and systems in order to operate and support them.
Subsequently that person no longer works for the company but uses knowledge of the company’s systems together with unchanged system credentials to perpetrate a crime. Has this crime been committed by an insider or not?

The majority of IT sabotage is committed by former employees [GS12, p49]. This is less surprising when you consider that when someone leaves, knowledge of the systems and their potential weaknesses, knowledge of organisational processes, and other knowledge gained whilst having worked for an organisation will still remain with that person. And in many cases, insufficient joiner/mover/leaver processes may also leave access to systems and data with that person. It would seem that the definition being built needs to be extended so that it doesn’t exclude people that leave and it acknowledges that access may have been granted at any time in the past.

So far, key attributes of the definition being sought include i) humans actors (not code or systems), ii) explicit organisational relationship, iii) the person may have left the organisation, iv) access to systems or data, v) that access was legitimately authorised at some point in time, vi) the definition is widely used/accepted by other researchers.

According to [CW10], an insider is: “a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization’s structure.” This definition does not exclude former access authorisations in addition to current access although it’s not explicitly stated. It does explicitly state ‘person’ but does not attempt to define the organisational relationship, and it uses the term ‘assets’ instead of putting IT assets into scope explicitly. This definition doesn’t meet enough of the attributes discussed so far as being important and so won’t be used.

The CERT definition is widely used and cited by others: “a current or former employee, contractor, or other business partner who has or has had authorised access to an organisation’s network, systems, or data” [DC12]. It benefits in terms of ease of understanding, and therefore value. It meets all of the attributes discussed above and therefore will be used as the reference definition of insider for the purposes of this report.

See Figure 1 below for a summary of this chosen definition along with the key attributes which have been discussed above.

![Figure 1 Insider definition chosen for this report.](image)

There are a great many insiders whom never do any harm to their organisations [TN08], but in consideration of those that do it’s useful to consider both those that ‘intended’ to do harm (malicious insiders), as well as those that ‘did not intend’ to do harm but nevertheless performed,
or neglected to perform, an act which resulted in harm to the organisation (non-malicious insiders).

According to Hayden [MH99], these two categories can be divided further such that malicious insiders are either ‘Traitors’ (motivated by malevolence or profit) or ‘Zealots’ (motivated by strong belief or ideology), and non-malicious insiders are either ‘Browsers’ (motivated by curiosity) or ‘Well-intentioned’ (who may cause accidental incidents). Malicious and non-malicious insiders will be examined in more detail in the sections that follow below.

1.2 Non-malicious insiders

This section discusses non-malicious insiders whom can cause harm to an organisation unintentionally by their actions.

From a broad collection of security incidents in 2013 Verizon [VE13] note that 14% were committed by insiders and whilst most were deliberate and malicious in nature, there is still an appreciable impact from unintentional acts including ‘low-tech’ events, such as sending sensitive documents to the wrong recipients, as well as less-frequent mistakes by system administrators and programmers

Insiders can incidentally put information at risk of compromise unintentionally simply because the accepted business work processes that they operate are risky or they haven’t been provided the right training or tools for the job. For example, it may be common accepted practice in the organisation that people email work to themselves at home using consumer grade web based email systems such as Hotmail or Gmail, or that they share documents with others using personal cloud storage solutions like Dropbox or Evernote. Use of these personal Internet hosted systems takes the information beyond the system of control of the organisation and can put it at risk of compromise.

According to CERT [CT13], non-malicious insiders cause security incidents unintentionally for many reasons including simple human error, fatigue or sleepiness, feelings of stress, poor situational awareness, lack or attention, mood, drugs and other factors such as gender, age and culture. They refer to the threat from non-malicious insiders as the “Unintentional Insider Threat (UIT)” and define it as “a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems”. Note this definition is a natural extension of the insider definition chosen for use in this report that was presented earlier in this report.

Examples of accidental, and therefore unintentional, security incidents which insiders can cause include granting excessive rights to the wrong people, making configuration errors, disabling security controls, introducing vulnerabilities during software development or simply leaving an unencrypted portable storage device unattended in a public place so that it is at risk of being stolen.

Consider malicious but non-targeted attacks by external parties such as viruses and worms, which are created with no specific target in mind, but simply propagate as far as possible through compromising vulnerabilities which they are designed to exploit. Insiders can unintentionally contribute to the effectiveness of these non-targeted malware attacks in many ways including by unwitting cooperation in social engineering attacks, ingress of malware into systems via infected removable media, visiting hostile web-sites, or opening unsafe attachments to emails.
The above risk is exacerbated when the attack is specifically targeting the individual or organisation (so-called Advanced Persistent Threat (APT)) and has been specially crafted to enhance the likelihood success. For example, the person may receive an email or instant message from an attacker which appears to be from a friend because it contains specific information or is written in a particular conversational style which the friend uses. The person is much more likely to trust the communication and be duped into performing an act which unintentionally leads to a security breach.

See Figure 2 below for a summary of the non-malicious insider definition along with some examples of contributing factors noted.

![Figure 2 Non-malicious insider definition chosen for this report.](image)

For many examples of specific security incidents caused by non-malicious insiders see CERT [CT13].

### 1.3 Malicious insiders

Insider threat lies in the potential that a trusted employee may betray their obligations and allegiances to their employer. [TN08]. This cuts to the very nature of the problem, in that employees are given trusted access to the organisation’s systems and information with the expectation that they will properly act in its best interest at all times.

This section presents some established definitions for malicious insiders and insider threat which have been in use, and in some cases, evolved over many years.

According to CERT [DC12], a malicious insider is “a current or former employee, contractor, or other business partner who has or has had authorised access to an organisation’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation’s information or information systems.” where ‘other business partner’ includes staff at cloud service providers or
Mitigating malicious insider cyber threat

at outsourced or offshore partner companies. Note, as before this definition cleanly extends the previously presented definition of insider.

With the essence of the definition the same but with language more aligned for military use as opposed to commercial use, US DoD [DD00] uses the definition: “anyone who is or has been authorized access to a DoD information system whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector and exceeds or abuses their authorized access to exploit, attack or otherwise misuse DoD information systems.”

There are many more definitions in use [JG08] for insider threat which are fundamentally aligned to the above definitions, including:

- “deliberate misuse by those who are authorized to use computers and networks”,
- “threats originating from people who have been given access rights to an IS and misuse their privileges, thus violating the IS security policy of the organization”, and
- “intentionally disruptive, unethical, or illegal behaviour enacted by individuals who possess substantial internal access to the organization’s information assets”

The CERT definition cited above will be used as the reference definition of a malicious insider for the purposes of this report. It is human actor centric, specifically acknowledges both currently legitimate and formerly legitimate access authorisations, fundamentally aligns with a broad consensus of definitions from the last three decades or so, and is widely used by other researchers – and as noted above in the section defining insiders, it may be this last mentioned attribute of the definition which is of prime importance.

According to this definition, a person doesn’t become a malicious insider until they have actually abused their access and committed a crime. Before this time, they are simply an insider, however it is worth examining the route that a person might take from insider to malicious insider. ‘Self-initiated insiders’ start like most people whom will have joined the organisation without any deliberate intent to abuse their position, but at some later time they decide to do so. ‘Exploited/recruited insiders’ are those people that join the organisation without deliberate intent to do harm but are coerced or recruited to do harm at some later time. And finally, ‘deliberate insiders’ are those people that join the organisation with a deliberate intent to abuse their access and do harm [CP13b].

It is conceivable that one insider will masquerade as another insider for the purposes of perpetrating a crime, perhaps because of the increased access to systems or information or to cover their tracks and implicate someone other than themselves. In this case, the masquerader is considered a malicious insider, as opposed to the situation where a non-insider masquerades as an insider to commit a crime in which case that masquerader would not be considered a malicious insider. A likely term for that person would be hacker, intruder or simply attacker.

See Figure 3 below for a summary of the malicious insider definition along with origins noted.
1.4 Insider advantage

It is difficult to conceive of an attack scenario with an insider involved which would not be more likely to succeed compared to the same attack without an insider involved. Reinforcing this view, Schneier [BS09] writes: “Insiders are especially pernicious attackers because they’re trusted. They have access because they’re supposed to have access. They have opportunity, and an understanding of the system, because they use it—or they designed, built, or installed it. They’re already inside the security system, making them much harder to defend against.”

The significant advantages which insiders have over external threat agents are discussed below:

Authorised access and proximity

By nature of their role, the insider may have direct physical and/or logical access to the assets they are intending to exploit as a legitimate part of their job role. In more than half of cases the insider simply abused their access rights [AC12]. This is the key differentiator between insiders and non-insiders, as explained above, and the factor which gives the insider the most advantage, as well as being the factor which makes defence most difficult.

Being physically close to the people and assets of the organisation is an advantage in some types of insider crime. For example:

- using the technique of shoulder surfing, where information on one person’s screen is overlooked by another, may allow an attacker to learn confidential information which they can exploit for gain.
- deploying a hardware keystroke logging device between the keyboard and docking station of another employee to capture their credentials or other sensitive information.
- Stealing documents or removable and portable storage devices which are left unsecured.
Organisational and technical knowledge

Insiders gain knowledge of the organisation simply from being employed by that organisation. For example, they gain an understanding of the organisation’s culture, processes, technical and people capabilities, and the location and worth of its valuable assets. This knowledge makes planning and executing an attack against the organisation much easier than trying to do so from the outside without this knowledge.

Ironically, staff are considered more valuable to the organisation when they have a better understanding of the business and its processes because that allows those people to be more effective in their roles. Because of this, large complex organisations may mandate awareness programmes to teach people about the business, and/or organise job sharing or job rotation schemes.

Insiders may also have access to technical documentation, vulnerability assessments and other artefacts which enable them to plan an effective attack. Whilst this is true, this doesn’t mean that attacks are necessarily always predicated on technical expertise. Research indicates that as many as 78 percent of insider incidents are perpetrated by people in non-technical roles [IR06].

Inside relationships

Insiders are able to use their relationships with other people within the organisation to increase their chances of success in an attack. Other people in the organisation will naturally trust a colleague more than an external party, even if it’s a colleague they have never met before, simply because that person is working for the same organisation. Even though collusion between insiders has been very rare [AC12], the advantage afforded by being trusted can be leveraged.

For example, social engineering of co-workers is much easier for insiders than for external parties. Many social engineering attempts starts with establishing some form of trust relationship, and the basis for that could be simply persuading the victim that you work for the same organisation.

Insider security programme and architecture maturity

The capability maturity of the information protection programme in an organisation is often less mature in relation to insider threat than for external threat. Organisations have typically focussed on defending the business from outside attackers first and foremost. One of the key reasons for this is that defending the organisation from insiders cannot be achieved with only technology controls, but instead relies upon humanities skills such as sociology, behavioural analytics, psychology and other fields [ES98].

The IT infrastructure of many organisations evolved from supporting standalone computers, to supporting networked computers within the same buildings or campuses, to having to support complex global intranets spanning many countries and with many interfaces to untrusted ‘external’ networks such as the Internet. For many of these organisations, the organic security architecture which emerged was often the so-called “egg model” where the perimeter is protected from external access but traffic originating on the internal network is naturally regarded as more trustworthy. This gives insiders an advantage as the security auditing and monitoring services are often outward facing.

In contrast though, note that insiders do have some disadvantages over external attackers although they may not be significant. For example, non-insiders have the advantage of being
unknown to the organisation they are attacking, and unlike insiders, they probably don’t have HR records, vetting reports, and a home address on record. Also, insiders are likely to be physically remote from the organisation, potentially in a different part of the world. This anonymity could allow external attackers to be bolder and be less concerned about a compromise being discovered, as being personally held to account for the crime may be less likely.

1.5 Threat actor landscape

This section presents a broader view of the threat actors which organisations face as context for understanding how malicious insiders relate to this overall landscape.

As discussed earlier in this report, without common agreed definitions it is difficult to share information unambiguously and it can lead to inaccurate and inconsistent threat profiles to systems and organisations. The umbrella term ‘hacker’ is in common use for someone that compromises an IT system, but it is useful to have a more granular set of definitions. The OCTAVE framework [CA99] describes a taxonomy of threat actors including: non-malicious employees, disgruntled employees, attackers, spies, terrorists, competitors, criminals and vandals. This was developed in 1999 and testament to the pace at which the threat landscape has evolved over the last decade, hacktivists and nation/state sponsored threat actors are notable by their absence in the list.

Typically accepted characteristics for common threat actor categorisations are listed below:

- **Terrorists** want to generate media attention for a particular cause or political aim and are likely to do so using fear and destruction without regard for property or people’s well-being.
- **Hacktivists** are civil or radical activists whom are also driven by similar socio-political agendas to terrorists but may be less inclined to cause physical harm to people than terrorists are.
- **Criminals** are driven by financial objectives.
- **Competitors** are characterised as wanting to steal Intellectual Property to gain competitive advantage, but it may be reasonable to assume that they also might perform other acts which reduce the competitive advantage of the victim organisation. For example, various types of denial of service attack could be effective.
- **Nation-state** sponsored groups are characterised by similar objectives as competitors but are likely to have vastly more resources and capability at their disposal.
- **(Malicious insiders and non-malicious insiders** have been discussed at length already)

It is especially important to realise that the categories are not mutually exclusive. In particular, malicious insiders could be members of one or more of the other malicious threat actor categorisations. i.e. it’s possible to be, for example, a “criminal insider”, or a “terrorist insider”. In addition, beliefs, ideologies and other drivers for a person’s behaviour can and do change at any time, and therefore their association with a particular threat actor group could change at any time too.

Intel has developed and published a Threat Agent Library (TAL) [TC07] which provides comprehensive coverage of human threat agents. It also explicitly considers a number of threat agents in combination with that person being a malicious insider. For example, as well as the standard ‘disgruntled insider’, the TAL also contains government spy, internal spy, thief and vendor (described as a business partner who seeks inside information for financial advantage over competitors). Understandably, but unfortunately, Intel considers the strength of threat rating for each of the threat actors to be proprietary information and do not share it publicly.
In order to estimate the relative ranking of the threat from these threat actors, a simple model will be developed below using a rudimentary scoring system based on the attributes of means, motive and opportunity and using a qualitative judgement based method to pick individual scores. These attributes were selected because with many legal systems, the establishment of motive, means and opportunity, together with evidence proving beyond reasonable doubt that the opportunity was seized, will suffice to warrant a guilty verdict for a crime.

The linear equation \( \text{Threat} = \text{Means} \times \text{Motive} \times \text{Opportunity} \) will be used.

‘Means’ refers to a combination of the technical or other ‘Skill’ of the threat actor together with the ‘Resources’ that they might have at their disposal. Therefore: \( \text{Threat} = (\text{Skill} + \text{Resources}) \times \text{Motive} \times \text{Opportunity} \)

‘Motive’ refers to the strength of a threat actors conviction to act/succeed including their regard or disregard towards being caught and held to account for the act.

‘Opportunity’ refers to the ease by which a malicious act may be performed by a threat actor because of such factors as circumstances and timing. For example, as described previously, it is reasonable to assume that insiders have a great deal more opportunity to commit a malicious act against their organisation than an external party because they are trusted by their organisation and have had legitimate access to various assets already granted to them.

According to [MM12], a good cyber threat model highlights the details of interest regarding a threat and will generally address both a threat’s capabilities and its intent. The model proposed here is consistent with this guidance with ‘motive’ corresponding to ‘intent’ and both ‘means’ and ‘opportunity’ corresponding to ‘capabilities’.

The following scoring scheme will be used:

- Skills: unskilled=0.5, proficient=1, significant=1.5 and formidable=2.
- Resources: acting alone=1, organised group=1.5, government=2.
- Motive: casual=1, enthusiastic=2, determined=3, fanatical=4.
- Opportunity: no access=1, minimal access, internal=3, privileged internal=4.

<table>
<thead>
<tr>
<th>Threat actor</th>
<th>Skills</th>
<th>Resources</th>
<th>Motive</th>
<th>Opportunity</th>
<th>Threat score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacktivist</td>
<td>1</td>
<td>1.5</td>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Competitor</td>
<td>1.5</td>
<td>1.5</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Criminal</td>
<td>1.5</td>
<td>1.5</td>
<td>3</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>Terrorist</td>
<td>1</td>
<td>1.5</td>
<td>4</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Nation State</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>16</td>
</tr>
</tbody>
</table>

Table 1  Ranking of threat actors using a simple judgement based (qualitative) threat model
Table 1 shows the results of using the scheme described above to produce a relative threat ranking for threat actors.

Bearing in mind the statement earlier that the categories should not be considered mutually exclusive to each other, it would seem reasonable to assert, that on the basis that any external threat actor could possibly become an insider — including those external threat actors considered to be the greatest threat to a particular organisation - then taken as a group, insiders must be the greatest threat overall. The only challenge to this assertion is that some external threat actor groups could never become insiders in a particular organisation as they definitely would never be trusted by that organisation and have access granted to them. This, though, assumes perfectly functioning vetting processes being operated at all times, not just in the organisation but across all the organisation’s business partners as well. This surely could not be 100% guaranteed, in which case the original assertion holds.

1.6 Insider crimes

This section discusses different types of crimes which malicious insiders can and do commit.

Over the last several decades, company valuations being made up of primarily tangible assets has shifted towards largely being of intangible assets in the form of intellectual capital. This has brought with it many more opportunities for digital crime. The potential impact from insider crime can range from minor nuisance to catastrophic in proportion and could conceivably result in loss of life, bankruptcy, regulatory censure, environmental disaster, weapons systems countered, reputation damage, stock market collapse, or even a declaration of war between nations.

As far back as 2004, theft of IP from just U.S. companies due to espionage alone was estimated to be costing $250 billion/year, although it’s not clear to what degree insider action contributes to this or what the true figure might really be because many companies do not realise they have been compromised and more than half of those that are aware then decide not to report the breach for fear or reducing shareholder value. [ON04].

There are five main categories of insider crime [CP13a]:

1. Facilitation of 3rd party access to sites/information
2. Unauthorised disclosure of information (either to a third party or the media)
3. Financial & process corruption (defined as illegitimately altering an internal process or system to achieve a specific, non-authorised objective)
4. Sabotage (electronic or physical)
5. Theft of materials or information

MERIT (Management and Education of the Risk of Insider Threat) is a database of insider incidents maintained by CERT which has over 800 entries collected from public sources since 2001 [RT11]. The entries are organised in three main categories which encapsulate the five categories noted above:

1. IT sabotage: insider incidents in which the insider uses IT to direct specific harm at an organisation or individual.
2. Theft of Intellectual Property (IP): an insider’s use of IT to steal proprietary information from the organisation.
3. Fraud – an insider’s use of IT for the unauthorised modification, addition, or deletion of an organisation’s data for personal gain, or the theft of information that leads to an identity crime.
A key insight from the CERT research [DC12] is that it’s advantageous to regard these three crimes independently and distinctly as the nature of them, the roles and personality traits of people perpetrating them, and therefore the detection and prevention of them, can be different. For example, IT sabotage (24% of cases) is typically committed by technical insiders and more often than not executed following termination from the organisation, whereas insider theft of IP (16%) is usually committed by the people that have worked with that IP as part of their job, and fraud (44%) is usually committed by lower level employees such as customer services personnel and help desk workers.

Some typical insider incident examples from the MERIT database [RT11] include:

- A group of insiders at a wireless telecommunications firm created clones of more than 16,000 customer cell phones. For at least six months, the insiders made approximately $15 million worth of unauthorized calls
- A branch manager for a banking institution, after running into gambling issues, family health issues, and unforeseen expenses, stole over $225,000 from business accounts.
- Over a 5-year period, a secretary who worked at a youth organization for over 20 years used a point-of-sale system to issue at least 500 fraudulent refunds totalling over $300,000 to the insider’s own bank account.
- An electrical supervisor developed applications for a SCADA system used by the water industry. After termination, he installed a malicious programme on one of the organization’s critical systems, damaging the SCADA system.

Probably the most well-known and notorious insider crime was committed by US Army Soldier Bradley Manning whom, in his role of intelligence analyst, abused legitimately granted access to classified databases and, through WikiLeaks organisation, released the largest set of classified documents ever leaked to the public. This included 250,000 U.S. diplomatic cables and 500,000 other reports relating to the Iraq and Afghan wars. In 2013 he was convicted under the espionage act and sentenced to 35 years confinement [BM14].

In addition to the impacts caused to the organisation itself, the personal impact of insider crimes is important to consider as well. Many years ago, I lead the investigation of an insider incident involving the use of a hardware keystroke logger that was found plugged into a laptop docking station on an employee’s desk between the external keyboard and the docking station. The device was a small innocuous looking connector with s USB plug on one side and a USB socket the other. When the victim came in to work with their laptop and plugged it into the docking station so that they could use a full sized monitor, mouse and keyboard, the keystroke logger was able to capture each button press of the keyboard. This included the user’s username and password which was subsequently retrieved from the device and used to access the victim’s HR records. The investigation was a time consuming process which took several weeks of evidence collection to conclude. Because the keystroke logger was encrypted and the default password had been changed, the only course of action to uncover the contents of the logging device was to brute force the password by trying every possible combination. The key-space was relatively modest as the keyboard combination to unlock the device consisted of holding any three chosen keys down simultaneously. The motive of the crime was ultimately determined to be curiosity as to the compensation of the victim relative to the attacker. Whilst the crime had no real impact to the organisation I worked for, other than the time taken to investigate, I was struck by how much personal impact there was on the victim whom suffered a great deal of anguish both during and after the investigation. During the investigation, she was aware that the unknown perpetrator had targeted her and looked at her HR records which contained her home address, and this naturally created concern about motive and whether she was physically safe at home. Following the conclusion of the investigation, when the victim became aware of whom the perpetrator was and realised it was a close colleague and someone previously regarded as a friend, she naturally
felt let down but also experienced a loss of trust in her own ability to judge the character and integrity of others.

1.7 Malicious insider characteristics

According to [TN08], “there is no correlation between disgruntled workers and insider threats, with the majority of disgruntled workers never betraying their employer.” This however doesn’t mean that some or all malicious insiders might not be disgruntled.

A study conducted in the context of sabotage to computer systems found that most insiders held a work-related grievance prior to the incident and the most frequently reported motive was revenge [SS05]. However one or more motives may be in play at any time and, according to DoD Defense personnel Security Research Center [SW92], in their study of 117 cases of espionage from world war II through to 1992, they found that money was the primary motivation in 52% of cases, ideology in 18%, revenge in 15%, ingratiating in 9% coercion in 4% and thrill seeking in 3%.

A great deal of research has been conducted [SW92, DC12, ES98, SS05, FG08] to analyse personality, demeanour and actions of people whom have committed insider crime so that where statistical correlations exist they can be used to inform the development of countermeasures based on observing and reacting to these as leading indicators.

For example, according to [ES98], emotional distress, disappointment, frustration, disgruntlement, introversion, perceived entitlement, lack of empathy and other traits have been discovered to correlate with an increase in the risk of an insider performing illegal acts or being vulnerable to recruitment or manipulation by others.

According to [FG08], strong indicators are disgruntlement, difficulty accepting feedback, anger management, disregard for authority, low performance, stress and confrontational, whilst weaker indicators of insider threat risk are personal issues, self-centredness, dependability and absenteeism.

Personality is defined as a dynamic and organised set of characteristics possessed by a person that uniquely influences his or her cognitions, motivations, and behaviours in various situations [RR04]. According to [SH07], it is this intrinsic personality, combined with extrinsic temporal and dynamic factors such as motivation and other external stimuli that form the basis for indicators that may correlate with a higher risk of insider threat.

A personal or work related event could be the trigger (an external stimuli) which causes an insider to decide to commit a crime against the organisation that trusts them. This could include being fired, financial pressure, family or marital issues, coercion or recruitment by a third party, or many other events or changes in circumstance. For example, people become affiliated with various organisations of like-minded individuals with similar beliefs, ideologies or causes. These could include religious sects, gangs, clubs, political parties, radical and extremist groups etc. Peer pressure from other members of these groups to commit a crime could cause the trigger point to be reached for a particular individual with a particular personality at a particular time in their life when they were vulnerable.

In addition, when an insider crime is being prepared for or is in progress, it’s reasonable to assume there may be observable actions that could give rise to suspicion. For example, the US Defense Security Service [DS10] regard many behaviours as reportable including:

- Keeping classified materials in an unauthorised location
- Removing classification markings from documents
- Attempting to conceal foreign travel
- Sudden repayment of large debts
- Repeated or un-required work outside of normal duty hours

A major study, called project Slammer, was conducted by mental health care professionals to try to discover common characteristics of those people that had been convicted of espionage. It involved interviewing not just the criminal, but also colleagues, friends and family whom were able to describe the person's character traits, habits, moods, behaviours and other factors from before the crime and during it. The conclusion was that a complex interaction of many factors led to the malicious act with none of the factors being a decisive predictor in its own right. Rather, each extra indicator that was observed added weight to the possibility that an intervention should be made to better understand the threat posed by the insider. [PS90]

According to [SH07], people exhibit polymorphous behaviour in that they tend to hide their true emotions from their peers and their behaviour tends to be self-modifying in response to changes in the environment. For example, an insider would wait for an opportune moment to access a system and steal intellectual property and would be sophisticated enough to continually monitor and evaluate the risk of being caught versus the reward of accomplishing the theft.

This is reminiscent of polymorphic computer viruses which first appeared in the early 1990s and used mutation engines to encrypt and obfuscate the malicious code so that the common technique of pattern matching that was used by virus detection algorithms was rendered useless and a new generation of heuristic based malware detection was required [SM96]. This polymorphic virus behaviour though relied on a random number generator to create the next iteration of the code, so perhaps with even greater similarity to the polymorphic human behaviour mentioned above, is the case of malware detecting the presence of a virtual environment, concluding that it may be being studied by anti-malware analysts in a safe sandbox environment, and modifying its behaviour to thwart the analysis. Even this example stops short though of being a perfect match for human behaviour, as the malware has been pre-programmed for a specific response in a specific expected situation, whereas human actors are able to continuously adapt their behaviour to even unexpected situations.

The sophistication of human beings makes tackling insider threats a difficult problem which requires much more than technology alone. A combination of techniques from the sociological and the socio-technical domains will be required too [CW10].

1.8 Threat model

In this section a threat model for malicious insider threat will be developed which will be used to understand options for the implementation of flexible mitigating countermeasures.

Threat models can be built for many purposes. For example, [SB06] have developed separate descriptive threat models for insider espionage and sabotage, together with an abstracted common model, which capture the complex relationships amongst variables in the problem space. These models use a system dynamics method which captures underlying feedback loops that tend to either reinforce or weaken a contributory relationship between elements of the graph. The models are valuable to understand and communicate contributing factors and implications for insider threat and will be used to inform the threat model being built in this section.
An attack can be considered as a sequence of phases, each of which may or may not necessarily be present and which may also overlap with each other during some attacks. For each moment along the time sequence of the attack there is an opportunity to design countermeasures to prevent or detect, and hence mitigate the threat [TS08].

Using a phase based model of defence and countermeasure strategy in the context of defending against Advanced Persistent Threat (APT) was described in a paper entitled “Intelligence driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains” by Lockheed Martin in 2010 [EH10]. In contrast to traditional network defence strategies which focus upon the vulnerability element of risk, the approach described is focused on the threat element of risk. This is attractive because of the huge number of methods which could potentially be used by an insider to commit a crime, and also because a basic scope assumption of this paper is that the organisation has a mature traditional security risk management programme.

As described earlier, malicious insiders’ actions are polymorphic in nature in that they will adjust their actions based upon the environment they encounter and the success or failure of the actions they are taking. APT actors share this characteristic too, in that the tools they use are often specially crafted for the organisations and people being attacked and can be tailored on an ongoing basis throughout the attack campaign - which may last for many years. This necessitates that the defence against APT actors must be dynamic and able to leverage lessons learned in a continuous improvement cycle. Because of the similarities between malicious insiders and APT actors, it is worth exploring the intelligence driven intrusion kill chain developed in [EH10] further for insight into features that a malicious insider threat model might benefit from.

A kill chain is defined as a systematic process to target and engage an adversary to create desired effects. This corresponds to the concept of a sequence of phases, which was noted above. A desirable property of the ‘chain’ is that once it is broken, the attack comes to an end. In the context of intrusion, the kill chain described by Lockheed Martin consists of the following phases:

i) **Reconnaissance.** Research, identification and selection of targets.

ii) **Weaponisation.** Coupling a remote access tool with an exploit into a deliverable payload.

iii) **Delivery.** Transmission of the weapon to the targeted environment.

iv) **Exploitation.** Exploitation of an application or operating system vulnerability – or a person.

v) **Installation.** Installation of the remote access tool or backdoor onto the victim’s system.

vi) **Command & control (C2).** The remote APT actor takes over the system in the target environment.

vii) **Intrusion and takeover complete.** At this point, the APT actor can focus on the operational objectives of the mission. If this is exfiltration of information then further steps in the kill chain may involve lateral movement within the organisation, elevation of privileges, data acquisition, encryption and packaging, exfiltration and clean-up.

Each of these phases provides an opportunity for intelligence gathering and or intervention to stop the threat from being realised. Another key feature of the Lockheed Martin approach is to implement a “courses of action matrix” with controls and contingencies annotated against the intrusion kill chain phases. According to [WL08], “Cyberspace favors offensive operations. These operations will deny, degrade, disrupt, destroy, or deceive an adversary”. It is no surprise that these are the dimensions used in the courses of action matrix together with the passive course of action ‘detect’.
An observation that the kill chain developed for intrusion is not appropriate for insider threat is made by [PR13], whom go on to propose an insider threat kill chain consisting the following four stages:

i) Recruitment/tipping point. Recruitment or cohesion (sic, presumably ‘coercion’?).
ii) Search/reconnaissance. Find the data / target.
iii) Acquisition/collection. Grab the data.
iv) Exfiltration/action. Game over! (sic)

Whilst this proposed kill chain captures the phases starting at the tipping point and ending at the crime, the presentation does also note the continuum of insider threat from non-insider to malicious insider with opportunities for predictive and diagnostic analytics.

A model ignores, masks or abstracts unimportant or unnecessary details, thereby highlighting the details of interest. [MM12]. To help with building the phase based model, the understanding gained by the author so far and presented in this report will be leveraged, the details of interest extracted, and a narrative set down which is made up of statements and observations arranged in a natural progressive order.

1. Non-Insider phase
   - People start off as non-insiders to the organisation, progress to becoming an insider by being granted access, and then commit a crime which causes them to be labelled as a malicious insider.
   - People may have joined an organisation deliberately intending to the commit the insider crime, or may decide to do so after joining. This choice may have been because of recruitment or coercion by others or it may be self-initiated.
   - People have intrinsic characteristics and traits which make up their personality. They also have different social and cultural backgrounds, religious and political beliefs.
   - People may have criminal records and other historic records of past unwanted behaviour in their background.
   - People have families and friends and also may have associations with many other groups of likeminded individuals or individuals desiring similar actions or outcomes. These associations and these people can influence them.

2. Normal insider phase
   - A key transition state from non-insider to insider happens when the person is granted access by the organisation as an employee, contractor or business partner.
   - The mental states of people, whilst not directly observable, are able to be inferred to some degree of accuracy by people interacting with or observing the individuals behaviour and demeanour.
   - In the course of performing their role, the insider will perform physical actions and technical actions which are observable and will be the basis for the establishment of ‘normality’
   - There may be a very short or no normal insider phase, particularly if the insider joined the organisation with the deliberate intent of committing a crime. It may be possible to infer normal technical actions for a role from what peers in the same role do.

3. Tipping point phase
   - At some point in time there is a tipping point, before which the person is not intending to commit a crime and after which that person has the intention to commit the crime.
The tipping point may have been caused by one or more precipitating events, or triggers, in the person's professional or personal life.

Events happen in people's personal and professional life continuously which may influence them and change their motivations and outlook. Some of these events will be obvious to the organisation, such as giving the person notice of redundancy, and others will be less visible.

Leading up to the tipping point there may have been a progressive deterioration of trustworthiness of the individual towards the tipping point which resulted in observable behaviour changes.

4. Crime preparation phase

Following the tipping point, in order to accomplish the mission of achieving the crime, the person may need to plan and execute one or more preparatory actions.

Actions and behaviours after the tipping point may be different to those actions and behaviours which were considered normal for the individual before the tipping point. For example, the individual may start hoarding information or working strange hours.

5. Crime execution phase

The actual criminal act may happen after the person has, or should have had, their access rights removed. E.g. after they are dismissed from the organisation.

There may be opportunities to deter or prevent the person from committing a crime right up until the crime is actually committed. i.e. both before and after the tipping point.

The crime may not be an instantaneous or one-time event. Instead it may execute over a long period of time or be repeated numerous times by the same actor.

Deterrence, detection and prevention may be achieved using technology, process or people controls.

6. Organisation recovery phase

As well as response and recovery from the crime, this phase should give opportunities to perform root cause analysis and feed lessons learned back into the defence system.

Depending on the nature of the crime, the organisation may not ever fully recover.

Revisiting USAF cyber doctrine [WL08] and the Lockheed Martin “courses of action matrix”, at each phase there is an opportunity to ‘detect’ unwanted physical and technical actions, ‘deter’ insiders from attempting a particular course of action, ‘deny’ attempts to execute a particular course of action, ‘disrupt’ a particular course of action after it has begun, ‘degrade’ a particular course of action to be less effective or efficient, ‘deceive’ the insider so that they are disadvantaged, or ‘defeat’ the insider such that all future possible courses of action by the insider are of no consequence to the organisation.

At each phase there is also an opportunity to monitor and analyse observable data, which may be generated by technical actions taken on systems and electronically captured, or as a result of behaviours and physical actions associated with the insider which may be observed by other people. One or more observable data points might be considered to be an indicator that the threat level of a particular insider is increasing which could lead to a particular intervention or course of action being pursued. The data could be used not just to indicate that an attack is in progress or has succeeded (through diagnostic analytics) but also to warn that the probability of an attack is rising (predictive analytics).

See Figure 4 for a graphical representation of the threat model.
1.9 Risks and vulnerabilities

1.9.1 Risk bow-tie

Operators in hazardous environments, such as oil and gas exploration, mining, aviation, health and defence industries commonly use a diagrammatic representation of hazardous events, their causes and the consequences, using a method known as the bow-tie method. It has this name because of the shape. The centre of the diagram is the unwanted hazardous event. On the far left of the diagram the threats and causes are listed with potential preventive controls positioned between the threats and the hazardous event. On the far right of the diagram the impacts are listed with potential contingencies positioned between the hazardous event and the impact. One of the greatest benefits of the risk bow-tie method is conceptualising the entire risk at a high level in a single picture [GB07].
Figure 5 High-level risk ‘bow-tie’ for insider crime

See Figure 5 where a risk bow-tie for insider crime is presented. The hazardous event is the ‘insider crime’ and is shown in the centre. Threat actors whom could be insiders are positioned on the far left side to represent the threat. IT systems and information representative of the threat surface for insider threat are also positioned on the left. The labels ‘intelligence’ and ‘controls’ represent the concept of using preventive controls to reduce the likelihood of the insider crime event occurring including the use of predictive and diagnostic analytics applied to gathered intelligence data. Potential business and IT impacts are positioned on the right of the diagram with the labels ‘contingencies’ and ‘business continuity’ representing the concept of using contingencies to reduce the impact of the hazardous event along with business continuity processes in a response and recovery capacity.

1.9.2 Vulnerabilities and exploitation methods

Insider crimes can have tremendous variety and seem only to be limited by human ingenuity. The following sections examine some methods through which an insider may exploit a control vulnerability and commit a crime.

1.9.2.1 IP Theft

“An insider’s use of IT to steal proprietary information from the organisation” [DC12].

A preliminary problem which must be overcome by the insider intending to steal IP is that of acquiring the IP. This is achieved in most cases of simply by abusing the legitimate access to the IP already granted by the organisation [AC12], but it may also be achieved by acquisition of unauthorised access rights either through exploitation of system weaknesses, or the exploitation of process and people through social engineering and other methods.
Figure 6 Example methods for achieving the crime of IP theft

Figure 6 above shows a number of methods by which exfiltration of information from an organisation may be achieved. A natural categorisation emerges of physical removal of the IP from the organisation or transmission via electronic means.

Removable media. There are a wide range of removable media in many form factors which can be used to take information out of an organisation. These include USB connected thumb drives, compact flash cards, writable CDs and DVDs, hard disk drives, floppy disks and tapes.

Laptop. Copying information onto a laptop and taking it out of the organisation is simple and therefore likely to be extremely common.

Smartphone or tablet. Smartphones and tablet computers have non-volatile storage which can be used to store information and exfiltrate it from the organisation. They also typically
have a camera and microphone which makes it convenient to collect certain types of information. For example, even when digital rights management (DRM) protection is used to create a control perimeter at the document level so that the insider can’t copy, print or transmit the document, it’s possible for the insider to take pictures of the information directly when it’s displayed on the monitor or other display device.

**Printed material.** Printing documents and removing them from an organisation is likely to be straightforward in many organisations provided there is a low volume of information.

**Memorising information.** Where the volume of information is low enough, it’s possible for IP to be stolen from an organisation simply by the insider knowing the information and then exploiting that knowledge in a way that is not in the interests of the organisation.

**Remote access.** An insider could use remote access software such as the corporate supplied VPN software to access information from an external location and exfiltrate it.

**Personal / corporate email.** Insiders can use email to send information to other people or themselves.

**External file repository.** There are many options in this space which an insider could consider including cloud based file sharing sites, (s)FTP servers, peer to peer networks nodes etc.

**Web site posting.** Insiders could post information onto social media sites, or within comments on many sites which allow comments to be uploaded. Exfiltration of information via public forums might mean the insider needs to obfuscate or encrypt the data to stop others from seeing it. Steganography, a technique where information is introduced into pictures or videos in such a way that although the fidelity of the picture is reduced, the introduction of the extra data is not easily discernable and the information itself cannot be readily accessed without the corresponding algorithms and decryption keys.

**Voice or fax.** Mobile GPRS phone networks, PSTN devices, VOIP, satellite phones and standard or computer based fax machines are all communication channels over which IP could be exfiltrated from an organisation.

**Covert channel.** This category is meant to convey the difficulty in preventing the exfiltration of information from an organisation because of the vast number of communication channels which potentially exist, particularly when the volume of information is very low. For example, the time taken between requests for a particular object on an external web site which the insider controls could be used as a covert channel to exfiltrate information. According to Horenbeeck [MH06] though, as long as there are so many other open channels to exfiltrate information from organisations, the risk of covert channel use may not be a priority for remediation.

### 1.9.2.2 Fraud

“An insider’s use of IT for the unauthorised modification, addition, or deletion of an organisation’s data for personal gain, or the theft of information that leads to an identity crime” [DC12].
Figure 7 Example methods for achieving the crime of Fraud

Figure 7 above shows a number of examples of methods that could be used to commit the crime of fraud.

**Modify records.** As noted previously, the majority of fraud cases are perpetrated by low level staff using their granted legitimate rights to systems and data. For example, it may be possible for an insider working in an HR department to modify records in such a way that a colluding colleague receives an unauthorised bonus. Furthermore, it may be possible that those same records were accessible by a systems administrator whom could perpetrate the same crime misusing their granted super-user privileges.

**Misuse a system.** This method is very similar to the above example of modifying records but directed at the system function level as opposed to at the record or data level. For example, an insider with granted access to a financial payment system could misuse their access to the system to transfer funds to a bank account which they have control over.

**Steal identity.** Stealing a person’s identity facilitates many possible subsequent crimes of fraud by the insider impersonating the victim in transactions to buy goods, take loans, or to gain any number of other benefits in the name of the victim.

**Exploit financial information.** An insider can directly exploit financial information for their own benefit. For example, they may be aware of quarterly accounts information before it becomes public information and could commit the crime of fraud by using that information for insider trading on the global equities markets.

1.9.2.3 IT Sabotage

“Insider incidents in which the insider uses IT to direct specific harm at an organisation or individual” [DC12].

Figure 8 Example methods for achieving the crime of Sabotage

Figure 8 above shows a number of examples of methods that could be used to commit the crime of sabotage.
Modify code or introduce malware. An insider, particularly a developer, may have the opportunity to use their access to source code to modify it in such a way that it can be triggered to do harm to the organisation. For example, the insider could introduce code into a system so that if they are not present to disable that code at a certain future date, then that would indicate their access had been removed from the system, perhaps by termination of their employment, and execution of the code would cause valuable databases to be destroyed.

Tamper with data. An insider could tamper with data by making unauthorised changes or deletions so that the information is unusable or lost by the organisation. An insidious data tampering technique involves slowly poisoning data sets over a long period of time so that, by the time the organisation notices how many data discrepancies there are and decides to recover back to a known point of integrity by restoring backups, the backups are also poisoned which forces the organisation to go even further back in time.

Misuse process control interface. Operators who have access to system control and data acquisition (SCADA) interfaces which allow them to directly control industrial systems are in a position to cause significant damage by misusing the access they have been given. For example, an insider working in a chemical plant could be able to redirect dangerous chemicals into public water supplies by directing certain valves to be opened.
Chapter 2: Mitigation

‘Countermeasures’ are what can be done to mitigate the threat, that is, the countermeasures are the building blocks which the strategy guides the implementation of. A ‘strategy’ is a “set of guiding principles that, when communicated and adopted in the organisation, generates a desired pattern of decision making” [MW07]. This corresponds to how things should be done to accomplish the mission – in this case, to mitigate malicious insider threat.

This chapter builds upon the understanding gained of the insider threat problem by examining countermeasures and strategic considerations.

2.1 Introduction

2.1.1 Scope

Information security management systems (ISMS), such as the widely adopted ISO17799 [IS00], have traditionally been focused on testing policy compliance, removing vulnerabilities from systems, and defence of the digital perimeter. The standard products and services deployed have included firewalls, anti-virus software, web content filters, secure remote access software, intrusion detection and vulnerability/penetration testing amongst many others.

ISO 17799/27002 does contain a personnel security section which contains controls related to insider threat including establishing security responsibilities and a confidentiality agreement in terms and conditions of employment; performing personnel screening; and mandating security education and awareness programmes. But according to [MT05], the theoretical background of ISO 17799/27002 may go towards explaining its relative ineffectiveness against insider threats, because although it has a high relation with General Deterrence Theory, and a medium relation with Situational Crime Prevention Theory, there is a low relation between ISO 17799/27002 and other criminology theories such as Social Bond Theory, Social Learning Theory and the Theory of Planned Behaviour. The authors argue that a multi-methodology approach needs to be adopted for effective mitigation of the insider threat, particularly drawing upon studies of human behaviour such as in sociology and criminology.

The traditional approach is ineffective against today’s threats which include sophisticated attackers perpetrating highly targeted dynamic attacks such as advanced persistent threat (APT) which uses social engineering and other adaptive techniques. Defending against APT requires security safeguards such as dedicated protection/detection solutions, and predictive and diagnostic analytics of security intelligence data which has typically been gathered from specialist companies, government agencies, public sources and through private sharing agreements with trusted partners [PW13].

Unfortunately the intelligence led phase based intrusion kill-chain methodology described earlier is also ineffective for malicious insider threat as it was specifically developed for intrusion from remote external attackers [EH10].

The kill chain developed earlier in this report for mitigating malicious insider threat will be used to inform the selection of appropriate controls, but note that this kill chain approach does not apply to non-malicious insiders. Non-malicious insiders by definition do not
Mitigating malicious insider cyber threat

intend to do harm, they are not recruited or coerced by others, probably don’t descend towards a tipping point after which they prepare to commit the act, and may be less likely to attempt to cover up the act than a malicious insider. The key mitigation measures for the most common underlying factors: user error and negligence, are related to creating a positive security culture, relieving time and workload pressure, awareness training, and providing usable security tools and processes. Traditional information security programmes, as described above, which implement security best practices throughout the organisation are well placed to reduce the threat from non-malicious insiders [CT13].

See Figure 9 for a graphical representation of the complementary programmes which are required to mitigate the three distinct threat areas discussed above, showing example components of the programmes as well as key focus areas and characteristics.

![Figure 9 Complementary mitigation programmes for different threats](image)

This report assumes a mature traditional programme is in place and makes no assumption whether an advanced persistent threat mitigation programme is also being operated. The focus is on additional countermeasures and strategy considerations beyond the traditional ISMS which are required to mitigate the threat from malicious insiders, as well as highlighting some areas covered by the traditional ISMS which may require attention to strengthen them in the context of mitigating against insider threat.

2.1.2 Approach and analysis

An analysis was conducted of a broad range of oft-cited papers and sources of best practice related to mitigating malicious insider.
Where the best practice guidance or control is commonly covered in a traditional ISMS control set, such as ISO 17799/27002, then that item has been omitted from the table.

Across the papers examined, authors variously refer to the same best practice guidance as a ‘strategy’, a ‘countermeasure’, or a ‘control’ etc. interchangeably. Judgement has been used to sort the items according to closest fit for a countermeasure (the ‘what’), or a strategy consideration (the ‘how’).

A summary of the analysis results is presented in Table 2 below. The countermeasures and strategy considerations are discussed in more detail in the sections which follow the table.

<table>
<thead>
<tr>
<th>#</th>
<th>Countermeasures</th>
<th>Sources</th>
<th>Threat model phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Implement training and awareness specific to insider threat.</td>
<td>[DC12a], [IN13], [GS12], [DD00]</td>
<td>A1-F8</td>
</tr>
<tr>
<td>C2</td>
<td>Perform pre-employment background checks and vetting.</td>
<td>[DC12a], [ES98], [GS12], [MH99], [TN08], [DD00]</td>
<td>A1, A2, A6, A7</td>
</tr>
<tr>
<td>C3</td>
<td>Ensure joiner, mover and leaver processes and identity and access management processes are working efficiently.</td>
<td>[DC12a], [IN13], [GS12], [MH99], [CP12], [DD00]</td>
<td>2</td>
</tr>
<tr>
<td>C4</td>
<td>Use technical and psycho-social (behavioural) techniques and controls in a complementary way including technical and behaviour monitoring and analytics.</td>
<td>[PR13], [IN13], [DC12a], [MT05], [FG08], [ES98], [KK13], [SB06], [CW10], [CW10], [CP12], [DD00]</td>
<td>2,3,4,6,7</td>
</tr>
<tr>
<td>C5</td>
<td>Document and enforce policies and controls to properly set rules and expectations in relation to accessing systems and handling information.</td>
<td>[DC12a], [GS12], [MH99], [CP12], [IN13], [NC12]</td>
<td>B1-F8</td>
</tr>
<tr>
<td>C6</td>
<td>Establish an incident response plan specific to Insider threat.</td>
<td>[IN13], [CP12], [DD00]</td>
<td>D8, E8, F8</td>
</tr>
<tr>
<td>C7</td>
<td>Consider back-up positions with overlapping responsibility for critical roles</td>
<td>[IN13], [NC12]</td>
<td>B1-E4, B6-E6</td>
</tr>
<tr>
<td>C8</td>
<td>Perform internal social engineering (e.g. honey-pots</td>
<td>tokens</td>
<td>nets)</td>
</tr>
</tbody>
</table>
2.1.3 Using the threat model

Table 3 shows the malicious insider threat model developed earlier as a grid with labels at the intersection of each kill chain phase and each action stage. The table above has been annotated with these labels to indicate which courses of action and/or phase the countermeasure or strategy is effective in. For example, B1 would indicate that the countermeasure or strategy reduces the risk of insiders reaching the tipping point, and ‘3, 6’ would indicate both detect and disrupt in all phases of the threat model. ‘2-4’ would indicate disrupt, degrade and deceive phases, etc.
### 2.2 Mitigation countermeasures

This section examines and discusses the countermeasures derived from the best practice analysis above.

#### 2.2.1 Insider threat awareness and intervention programme (C1,C5,C7)

Training and awareness can be used effectively to help mitigate malicious insider threat. There are several aspects which need consideration.

As part of a traditional ISMS, all insiders should be aware of accountabilities and acceptable use policies and expectations related to appropriate use of IT systems and of handling information and reinforce this learning regularly [DD00]. In addition, all insiders should be trained to use IT systems in a way that maintains the security of information when they perform their job role and how to report incidents.

Whilst these general training and awareness programmes won’t directly significantly affect malicious insider actions, they provide a solid basis for all insiders to be able to recognise actions by others which are not conformant with appropriate use policy, which could potentially indicate malicious action. A specific insider threat awareness programme will equip the workforce with the capability to recognise suspicious behaviours and appropriately intervene and/or escalate [DD00].

An organisation must harness a fully engaged employee population and workflow design so that there is constant scrutiny, supervision and evaluation rather than rely upon technology and technical specialists for a solution. Using a flight crew co-pilot metaphor, organisations should plan to have a co-pilot in every cabin so that there are no single person dependencies or lack of co-worker oversight. By promoting interest in not just the job but the team as well, teams can become self-policing [NC12].

For example, according to [DS10], if any of the indicators listed below are observed then it should be reported and followed up upon because most of the persons whom have committed espionage were later found to have exhibited one or more of these:

- Failure to report overseas travel or contact with foreign nationals
- Seeking to gain higher clearance or expand access outside the job scope
- Engaging in classified conversations without a need to know
- Working hours inconsistent with job assignment or insistence on working in private
- Repeated security violations
- Attempting to enter areas not granted access to

People need to feel safe enough to report suspicions without fear of retaliation and this may require significant work. For example, to create processes and systems which allow
people to report anonymously or to create a culture where it is accepted as the norm that suspicions will routinely be reported.

2.2.2 Pre-employment and on-boarding processes (C2)

Prior to granting access to systems or information and therefore changing the status of a person to ‘insider’, there are a number of options available to organisations to reduce the threat.

The first line of defence for reducing insider threat is to prevent potentially non-trustworthy individuals from ever becoming insiders in the organisation at all. Background investigations can reveal criminal convictions, confirm credentials including previous job roles and identify financial concerns or credit issues, all of which can contribute to an overall view of trustworthiness. Not only should prospective direct employees and contractors be investigated, but provisions need to be made in contracts with business partners so that contractors and other third parties receive a similar degree of scrutiny. Similarly, processes to investigate acquired staff following mergers and acquisitions should also be in place [GS12].

A greater degree of rigour should be required in background checks where greater trust is required in the person performing the role [NI09]. For example, roles which require a greater degree of trust include super-users, administrators, or people with significant access to critical systems or sensitive information.

Some DoD components have authority to polygraph personnel [DD00], but even where it is legal to do so, this is unlikely to be acceptable in many commercial environments.

A nondisclosure agreement (NDA) is required to be in place with all employees, contractors, and trusted business partners [GS12], so that the expectations around unauthorised disclosure of intellectual capital are clearly communicated to all people before being granted access to it, and so that if a breach takes place then there is supporting evidence to support breach of contract litigation.

2.2.3 Identity and access management (C3)

By definition, insiders were legitimately granted access to systems or information at some point in time. It is therefore important that only the right people are granted only the minimum access (known as least-privilege) to the right systems and information that they require to perform their roles and that that access is promptly and efficiently updated or removed when they change roles or leave the organisation.

Whilst IAM processes are already likely to be operated as part of a traditional ISMS, in relation to the insider threat, it is particularly important to ensure both privileged access controls and segregation of duties controls are operating effectively. Users with privileged access may include administrators/super-users at any layer of the technology stack from infrastructure, operating system, database, middleware, or application layers, as well as ordinary users with access to sensitive information or critical application functionality. These are the people whom are most likely to have the skills, resources and knowledge (i.e. means) to do most damage.

Segregation of duties prevents users from being granted potentially toxic combinations of access rights, for example users should not be granted rights to both create purchase orders and approve them.
2.2.4 Technical baseline profiling and anomalous behaviour detection (C4)

In addition to co-workers taking a responsibility for reporting suspicious behaviours, it is possible to use technology to collect and analyse data.

The preliminary assumption is that users will probably perform the same tasks and access the same systems and information on a routine basis in order to perform their role functions, and if there is a significant variation from this routine pattern then this may indicate suspicious behaviour which should be investigated. Building this baseline profile can require 6 to 12 months of access and activity logs to be captured, probably in an existing SIEM logging solution. Baseline information should include information such as users volume, velocity and frequency in hourly, weekly and monthly normal patterns [PR13]. It is important that training data does not include any attacks.

Once the baseline profile is available then so-called ‘behavioral analytics’ can be used to detect anomalous behaviour. For example, a data exfiltration volumetric anomaly from the baseline for a particular person during a particular time frame would be a possible indicator. Not only can the user’s ongoing activity and access set be analysed against their own historic baseline, but it can also be analysed against a peer group of users whom perform the same or similar roles so that outlying behaviour can be detected and flagged for potential investigation [KK13]. Machine learning techniques include statistical, Markov processes, data mining, support vector machines, artificial neural networks or immune systems [CW10].

In addition to baseline profiling which builds a model of behaviour based on the learning from the users normal usage patterns, it is possible to use rule based detection utilizing pre-defined models of threatening behaviour. These models often use finite state machines, Petri-nets or regular expressions. They have the advantage of not requiring a significant amount of time to collect data and form a baseline, however both approaches require potentially costly maintenance and update processes to be put in place for false positives to be kept under control [CW10].

2.2.5 Insider threat incident response (C6)

Traditional incident response processes may not be adequate to deal with incidents caused by malicious insiders. For example, consideration should be given to creating pre-approved statements which could be used by the organisation when briefing the media, as there may be a different reaction by the public to an incident involving an insider compared to one caused by external intrusion.

The fullest extent of disciplinary action beyond dismissal, for example prosecution, should be considered when a malicious insider has been caught as not only does this prevent that person from simply going to another organisation and potentially committing a crime there, but it also demonstrates commitment by the organisation to pursue perpetrators of these crimes, which sends a strong deterrence message to other people in the organisation [IN13].

2.2.6 Internal social engineering (C8)

According to [PR13], “bait works!!”. Honeypots include “honeynets” and “honeytokens”. These can all be described as instrumented targets and can contribute to early malicious insider detection. All types of honeypots share the concept that they are a resource or entity with no production value [LS03]. Honey-tokens can be as simple as a single piece of data such as a credit card number, or a single document. Honey-nets are more sophisticated and typically include a number of systems operating together in a network.
Honeypots should not see any activity that wasn’t anticipated at design time, and therefore any unanticipated activity seen by monitoring the honeypot should indicate unauthorised or malicious activity. Because of their simplicity and utility value, implementing honey-tokens and using monitoring systems to detect attempted access to these targets would seem to be of great value to a malicious insider protection programme. On the negative side, a malicious insider may never be compelled to interact with a honeypot, however attractive it may seem, and still be able to cause a great deal of damage to the organisation by simply exploiting the legitimate access they have been given to perform their role.

In some environments there may be questions about the acceptability of creating honeypots, which exclude their use as a countermeasure. Similar to a scenario where the owner deploys an alarm bell box on their house to deter would-be thieves when no alarm actually exists, it may be possible that the use of honeypots in an organisation could be widely communicated in order to deter attackers, even though honeypots are not actually deployed at all.

2.2.7 Data loss prevention (C9)

DLP technologies may already exist as part of the control set deployed in a traditional ISMS to help prevent the exfiltration of sensitive information from an organisation. DLP can be configured to enforce security policies for information usage at the network or host device. DLP can recognise sensitive data because it contains a particular field or pattern within the main content or within meta-data tagged to the file and then check whether that particular data is permitted to be used in the context which is being attempted. For example, it can be configured to prevent sensitive information from being transmitted or stored on systems or media that has not been approved for that data such as an unencrypted thumb drive or a consumer web based email system [VS13].

In the context of an insider threat mitigation programme, DLP technology can play several roles. First, it can increase the difficulty for insiders to exfiltrate data. Second, it can provide a rich set of data to SIEM logging systems to facilitate building baseline usage patterns or to supply data that could be used for anomalous behaviour detection. For example, many DLP systems can be configured to monitor and provide auditing information related to file and application access by users which can be fed into SIEM logging systems for real-time analysis, or as evidence to support the prosecution of insider crime allegations.

DLP technology can be implemented to monitor data in-transit, at-rest, or in-use. Implementing DLP at the network layer can be effective for monitoring the movement of data which has a consistent and well-structured format. This would include data such as credit-card numbers, driver licence numbers, and national insurance numbers etc., where signature based pattern matching can discern the type of data and cause an appropriate security incident response. If meta-tagging of documents is implemented, or if honey-tokens are in use, then the DLP system can be configured to look for these markers.

Network based DLP technology is much less effective in the case where the data is either unstructured, such that pattern matching is too difficult, or when the data is encrypted (e.g. with any available bulk encryption cipher) or the transport layer is encrypted (e.g. with SSL, IPSEC, etc.) Whilst some of the products are now capable of deep inspection within common compression formats, such as RAR and WinZip formats, it is still trivial to defeat them by encrypting the compressed file or by using other data encryption, obfuscation and/or exfiltration techniques (e.g., steganography.)

Context aware DLP deployed as an agent at the end-point, covering the so-called data-in-use case, has a much greater capability for preventing unauthorised exfiltration of data.
because it has very low level hooks into the operating system and can gain access to operations that the user is actually performing in real-time whilst data is in the clear. For example, endpoint DLP technology is capable of preventing PUT and POST operations in browser based sessions so that users can’t exfiltrate data through social media site postings etc.; it can prevent users from pasting sensitive information into web-mail sessions; or prevent users applying many compression, obfuscation or encryption operations to sensitive data [VS13].

Whilst this technology is promising, it’s worth bearing in mind that no current technology or process can prevent a person from simply remembering information that they have been granted access to and then subsequently disclosing it or using it in some other unauthorised way. Similarly, insiders could copy type information or take photographs of screens that are displaying sensitive information, which to stop would require very rigorous military style processes designed to prevent physical removal of information.

2.2.8 Information rights management (C10)

Information Rights Management (IRM) technology provides document level encryption and security policy enforcement so that document protection does not have to rely on the security provisions afforded by the containers and networks which they are stored on or have to traverse. For example, a security policy can be applied to a document so that only authorised people are allowed to open it, and at a more granular level, functions such as copying and pasting between documents, or printing can also be restricted.

In the context of insider threat mitigation, IRM can be configured to revoke access to protected documents when a user changes role or is dismissed and should no longer have access to the documents. This can work whether the documents are still stored in the organisations systems or whether the documents have been moved to a hostile network not under control of the organisation. IRM accomplishes this revocation of rights because it forces the process opening a protected document to communicate with an organisation controlled policy server to download a set of entitlements which are currently valid for the user in the context of the document use being requested.

As noted above for DLP technology, whilst the technology is promising and increases the difficulty of data exfiltration, IRM cannot prevent the use of human memory, copy-typing or display screen photography etc.

2.3 Mitigation strategy

This section examines and discusses the strategic considerations derived from the best practice analysis that was performed. As noted above, these strategic considerations describe ‘how’ the approach the programme and implement the countermeasures which have been discussed.

2.3.1 Malicious insider mitigation complements traditional ISMS (S1, S2)

As discussed previously, it’s important that the insider threat mitigation programme is considered as complementary to the traditional ISMS implementation and any other specialist mitigation programme, such as an external intrusion kill chain based program. The traditional ISMS should be considered to be the minimum baseline, or bedrock, of an overall security management programme on which to build other specific threat mitigation programmes.
2.3.2 Bias towards deterrence (S3)

According to [RB04], there is no practical way to prevent exfiltration of data by even a moderately determined adversary. Real enforcement and monitoring may not even be necessary, just the perception of monitoring may be enough, as long as the “fear of God” is put into cleared people. For these reasons deterrence of insider crime should be a key priority.

Ways of deterring insider incidents include letting people know that the latest technologies are being used in the organisation for monitoring and preventing insider threat, and clearly setting the expectation that when malicious insiders are caught they will be disciplined or prosecuted to the fullest extent possible. It’s possible though that a greater deterrent effect can be gained by creating a culture whereby people feel a sense of loyalty to the organisation and a sense of shared ownership to the organisational mission. This theme is explained in detail in [NC12].

2.3.3 Risk prioritised (S4)

Risk management is a function of three variables: criticality, vulnerability and threat [DD00]. Where means, motive and opportunity (threat and vulnerability) for insider crime intersect with the critical information and IT systems, whose compromise would impact the organisation the most, then the risk is greatest. Figure 10 shows this diagrammatically.

A risk prioritised programme will maximise potentially scarce and/or costly security resources and focus where there is most risk. Systematically reducing each of the factors/variables and the intersection of the factors will reduce overall risk. Operating a traditional ISMS will typically ensure that processes are in place to identify which information and systems are critical to the organisation and also to systematically reduce the vulnerabilities found in those systems.

In the context of threat from malicious insiders, an obvious intersection of motive, means, opportunity and critical digital assets is in the case of users with privileged access to systems, for example systems and database administrators of those systems.
2.3.4 Continuous improvement (S5)

Whilst continuous improvement could be seen as a generic principle relevant to almost any programme, it is seen as particularly relevant to malicious insider threat because of the relative infancy of operational research about the subject [PR13]. In addition, the threat is particularly dynamic and the behaviour of human beings in polymorphic in nature [SH07]. For these reasons, the insider threat mitigation programme should be designed to capture the effectiveness of the various countermeasures, and to keep abreast of ongoing research results and countermeasure tools and techniques development related to insider threat mitigation, so that adjustments can be made to the programme over time.

In the Lockheed Martin paper [EH10] which describes the intrusion kill chain methodology, a process for performing ‘campaign analysis’ is described where the goal is to extract characteristics of each attack - the so-called tactics, techniques, and procedures (TTP) – such that attacks can be grouped into campaigns and possibly attributed to particular unique groups of threat actors over time as well. This data can then be used to heuristically predict what might happen next in the campaign based on what has happened before and to measure the effectiveness of the kill-chain countermeasures against the TTPs that are being seen. This example of a practical way of building continuous improvement into a kill chain methodology could be investigated further to see whether it could be adapted to be effective in the context of the insider threat kill chain proposed here.

2.3.5 Governance (S6, S7)

Senior buy-in is a pre-requisite for success and a board member should be appointed to be the single accountable owner for people risk because people risks are of a similar magnitude to other corporate risks which typically require board level oversight [CP12]. Senior management must visibly set the tone from the top.

According to [IN13], “An insider threat mitigation program cannot succeed without senior leadership support and involvement”. In addition to senior management, stakeholders in the governance structure should include representatives from HR, legal, compliance, operations, communications, corporate security and digital security teams.

Important decisions are needed to set the tone and shape of the programme. For example, how extensive will the programme be? At what pace will it be implemented? What is the relevant importance of insider crime risk versus dealing with other operational risks? Will the programme be transparent and widely communicated or discrete and need-to-know?

2.3.6 Compliance with international laws and regulations (S8)

In order to implement a programme for malicious insider threat mitigation which includes user monitoring, it is essential to evaluate and understand the local legal and regulatory obligations in each country as privacy and other laws can vary in each jurisdiction. To simplify compliance it would seem natural to test whether an approach which satisfied the requirements of the strictest country could work. But this approach is not possible because of several contradictory requirements between countries. For example, in France it is illegal to ban personal use of work email, whereas in Germany it is common practice because it avoids application of telecommunications law and potentially lengthy processes involving the German works councils and co-determination rights issues [DL13].

Because of the complexity of legal and regulatory requirements internationally it is essential that an evaluation and risk impact assessment of relevant legislation by suitably qualified privacy law specialists is performed.
2.4 Initiating a programme

This section builds upon the analysis of countermeasures and strategic considerations presented above to propose the order in which an insider threat mitigation programme might be initiated in order to build incremental capability.

In the first instance, the threat to the organisation from malicious insiders must be recognised by someone, perhaps the Chief Information Security Officer (CISO), whom is capable of championing its importance to potential senior executives and establishing support to build a mitigation programme. With senior support, it’s easier to enrol important stakeholders from HR, Legal, Communications, Operational Risk, etc. and form an appropriate governance structure to oversee and steer the programme.

A pre-requisite for a mitigation programme focussed on malicious insider threat is a well-functioning traditional ISMS which maintains a baseline security control environment for the organisation. This baseline will likely include processes for risk assessment and treatment; asset management; physical and environmental security; policy and standards maintenance; personnel security; compliance; operational security; business continuity management and disaster recovery, etc. This baseline control environment will serve to protect the organisation from a broad range of threats including compromise by external attackers, and will serve a role in reducing risk from malicious and non-malicious insiders.

Extend existing incident response processes so that they are able to properly handle incidents caused by malicious insiders and are able to respond to escalations by staff whom have suspicions of wrong-doing by others.

Establish, communicate and enforce acceptable use policies which sufficiently set out the expectations and rules around using the organisation’s information and systems. Introduce insider threat awareness and training programmes to begin to educate personnel to recognise the threat and respond to it.

Taking a risk based approach depends upon ensuring that the critical assets of the organisation are discovered and agreed. In particular understand the location and flow of sensitive or valuable information including intellectual property or information where there are contractual, legal or regulatory obligations for protection or handling. The systems processing this data should be considered critical as well as any systems which play a critical role in the execution of mission critical business processes. A well run traditional ISMS should already have established the critical assets of the organisation and this should form the starting point for prioritising increased protection against the threat from malicious insiders.

Ensure that identity and access management processes are operating efficiently. This means that people are granted least privilege entitlement for access to systems; segregation of duties are checked and enforced; and access changes are made quickly following personnel joining, moving roles within, or leaving the organisation. Pay particular attention to those users with elevated privileges, and as with other measures, in the first instance focus on access which is to critical assets.

Introduce vetting processes prior to on-boarding new personnel and negotiate contractual clauses into master services agreements with business partners for a similar level of screening to take place. Focus in the first instance on those people whom will be granted access to critical assets.
Consider DLP and DRM implementations, especially if exfiltration of sensitive data has been identified as a key risk for the organisation. Consider the introduction of honey-tokens and configure DLP to detect and respond to their discovery in unauthorised locations.

Ensure SIEM logging and event analysis and correlation processes are properly functioning and establish a baseline of normal network traffic patterns and system usage.

Extend the scope of monitoring, logging and auditing to harvest richer data relevant to insider threat including behavioural data and personal event data from HR. Implement behavioural analytics capabilities for prediction and diagnosis of insider incidents.
Chapter 3: Conclusion

This chapter summarises the key points from the project report and reflects on future work which could be considered within the insider threat mitigation subject area.

3.1 Summary

The main objective of the project was to propose a strategy for the mitigation of malicious insider threat. I believe this objective has been accomplished.

The starting place of this project involved an in-depth examination of the insider threat problem. In particular, great care was taken to understand and analyse the various definitions which are in use by researchers within the domain of insider threat. Establishing a common vocabulary from the outset allows for more meaningful dialogue with less ambiguity, and choosing widely accepted definitions gives access to the increasingly available rich statistical analysis that is related to insider threat. This was noted as important because of the dependency of past incident analysis data to inform future mitigation measures.

A key insight which emerged was that whilst the impact might be similar for a non-malicious insider inadvertently causing a security incident compared with a malicious insider deliberately committing a crime, the mitigation programme required for malicious insiders was different and incremental to the programme required for non-malicious insiders. In simple terms, preventing accidents and deterring crime are different problems in the main.

Extending this insight further, it was realised that methodologies like the Lockheed Martin phase-based kill chain methodology for mitigating APT [EH10], whilst ineffective against malicious insiders, could be the basis for creating a framework to structure a malicious insider threat mitigation programme. This led to the creation of a proposal for a phase-based kill chain for mitigation of malicious insider threat. Further research into the value of this kill chain is required.

The judgement-based / qualitative threat actor evaluation which was presented led to the assertion being made that malicious insiders were the most dangerous adversaries on the basis that being an insider is not mutually exclusive to being in any of the other threat actor categories. In other words, if nation-state sponsored teams are thought to be the most dangerous adversary, then surely they are even more dangerous if they manage to infiltrate an organisation such that they are somewhat trusted and potentially granted physical and logical access to that organisation’s systems and information?

A high level risk bow tie was presented which could be used in the context of enrolling executives and operational risk professionals into understanding and appreciating the severity of the insider threat. Vulnerabilities and methods of exploiting weaknesses in the organisational control environment were presented in the three main categories of insider threat: fraud, IT sabotage and theft of IP. This clearly demonstrated the enormity of the insider threat problem by the huge variation of methods and vulnerabilities which could result in an incident. Further research is required to decompose these methods and vulnerabilities within these three categories to a more granular level, so that the choice of granular mitigation measures can be better informed.

Analysis of existing research and other sources of best practice for controls and countermeasures effective for mitigating insider threat was presented in tabular format. Once the countermeasures and strategic considerations which are very common in traditional ISMS
implementations were eliminated, I was surprised at how much consensus there was for which additional controls are required to mitigate insider threat. Perhaps unsurprisingly there was little disagreement that technical controls would not be effective on their own without supplementing the programme with people focused controls. In particular, pre-employment background checks/vetting and then ongoing integration of technical and non-technical behavior monitoring data into SIEM logging systems for predictive and diagnostic analytics processing was seen by most as being essential for an effective mitigation programme. A risk driven approach which focuses on the critical systems and information assets in the first instance - and in particular where those assets intersect with the means, motive, and opportunity to exploit them, such as can be the case for privileged users like administrators – also came through very strongly from the research analysis.

In the final section the countermeasures and strategic considerations are brought together into a proposal for an holistic programme, where the individual elements of the programme are considered relative to each other and ordered such that dependencies are taken into account, and incremental capability to mitigate insider threat is built. Of particular note is that behavioural monitoring and analysis is acknowledged in most best practice guidance as being essential for an effective programme, and yet it naturally fits after most other elements are in place because it’s not only one of the most demanding elements to implement but also has many dependencies.

During my research and work for this project, one of the ideas which provoked a great deal of reflection in me was from the work of [SH07] where it was noted that people exhibit polymorphous behaviour in that they tend to hide their true emotions from their peers and their behaviour tends to be self-modifying in response to changes in the environment. I chose to reiterate this concept at the end of my report because it serves to remind anyone tasked with mitigating malicious insider threat of the enormity and complexity of the problem faced.

### 3.2 Further research

Insider threat mitigation is a complex problem and research is in its infancy and therefore there is a rich opportunity for further research in this area. Whilst researching this topic and writing this project report I recorded some areas of interest which I would like to follow up on:

- In the context of honey-pots|tokens|nets, is it more effective to communicate their existence widely to act as a deterrent to potentially malicious insiders, or is it more effective to conceal their existence so that they are more likely to trap unsuspecting malicious insiders?
- Are the public and the shareholders of an organisation more or less sympathetic to organisations whom have security breaches caused by malicious insiders or to those organisations whom are breached by externals?
- As noted above, further research into the value of the insider threat kill chain as a model for framing mitigation of malicious insider threat.
- Also noted above, further work to develop granular attack trees for the rich variety of insider threats which are possible in organisations.
## List of abbreviations and acronyms

This section contains some abbreviations and acronyms which have been used in this report.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>AV</td>
<td>Anti-Virus</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>DRM</td>
<td>Digital Rights Management</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>IDS</td>
<td>Intruder Detection System</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>IRM</td>
<td>Information Rights Management</td>
</tr>
<tr>
<td>ISMS</td>
<td>Information Security Management System</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Incident and Event Management</td>
</tr>
<tr>
<td>TTP</td>
<td>Tactics, Techniques and Procedures</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
## Terms and definitions

This section contains some terms and definitions which have been used in this report.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Persistent Threat</strong></td>
<td>Threat from well-resourced and trained adversaries whom may conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information.</td>
</tr>
<tr>
<td><strong>Background</strong></td>
<td>Social and cultural backgrounds, religious and political beliefs. Criminal records and other historic records of past actions and behaviours.</td>
</tr>
<tr>
<td><strong>Behaviour</strong></td>
<td>How a person conducts themselves, especially their manner towards others and including the outward expression of how a person may feel which can be judged by others. For example looking stressed or tired.</td>
</tr>
<tr>
<td><strong>Indicators</strong></td>
<td>One or more observable data points might be considered to be an indicator that the threat level of a particular insider is increasing which could lead to a particular intervention or course of action being pursued.</td>
</tr>
<tr>
<td><strong>Observables</strong></td>
<td>Data points which are generated by technical actions taken on systems and electronically captured, or as a result of behaviours and physical actions associated with the insider which may be observed by other people.</td>
</tr>
<tr>
<td><strong>Personality</strong></td>
<td>Dynamic and organised set of characteristics possessed by a person that uniquely influences his or her cognitions, motivations, and behaviours in various situations.</td>
</tr>
<tr>
<td><strong>Physical actions</strong></td>
<td>The things that people do which can be observed. For example photographing documents.</td>
</tr>
<tr>
<td><strong>Strategy</strong></td>
<td>A set of guiding principles that, when communicated and adopted in the organisation, generates a desired pattern of decision making.</td>
</tr>
<tr>
<td><strong>Technical actions</strong></td>
<td>The things which people do whilst interacting with applications, systems and data. For example browsing a web site.</td>
</tr>
</tbody>
</table>
Bibliography

This section contains the references which have been cited within this report. They are listed alphabetically. Where known, URLs are provided and these were all checked as available as of the 25th March 2014.


Mitigating malicious insider cyber threat

http://www.sei.cmu.edu/reports/13tn022.pdf


Best Practice in Construction, Risktec Solutions Ltd, Dubai, UAE, 2007


Mitigating malicious insider cyber threat


[PS90] Project SLAMMER Interim Report (Unclassified). *A CIA sponsored study of Americans convicted of espionage against the United States*, Director of Central Intelligence/Intelligence Community Staff Memorandum ICS 0858, 1990 


http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAN
Mitigating malicious insider cyber threat


http://www.sei.cmu.edu/publications/documents/06.reports/06tr026.html


www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA276043


https://www.verdasys.com/resources/#White Papers