CPNI
Centre for the Protection
of National Infrastructure

CPNI INSIDER DATA COLLECTION STUDY

REPORT OF MAIN FINDINGS

APRIL 2013

Disclaimer

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Contents

Introduction

In 2009 CPNI published the findings of its Insider Data Collection Study, which looked at past cases of known insider activity and identified common themes among the individuals and organisations involved. Since publishing the 2009 report, CPNI has continued to develop its research, analysis and associated guidance in this area. This document provides an updated analysis of both the original and new insider case studies.

As with the original study, this second phase was not intended to quantify the extent of the insider threat in the UK, or the frequency of these events, but rather to provide further insight into the personality types, behaviours and organisational settings associated with insider activity.

This study forms part of an on-going programme of CPNI research into insider threat and underpins a range of guidance and advice provided by CPNI on personnel security. An overview of some of the related products is provided below.

- **Personnel security risk assessment:** this guidance aims to help Security and Human Resource Managers conduct personnel security risk assessments in a way that balances pragmatism with rigour, prioritises the insider risks to an organisation, identifies appropriate countermeasures and allocates resources in a way that is cost effective and commensurate with the level of risk.
  This guidance can be found at: www.cpni.gov.uk/advice/Personnel-Security1/risk-assessment

- **On-going Personnel Security:** this guidance aims to provide advice relating to the management of personnel security issues within an existing workforce. www.cpni.gov.uk/advice/Personnel-security1/Ongoing-measures/

- **Security culture:** Developing a security culture within an organisation is about encouraging staff to respect common values and standards for security, whether they are inside or outside the workplace. More information about developing a strong Security Culture can be found at: www.cpni.gov.uk/advice/Personnel-security1/Security-culture

- **Holistic Management of Employee Risk (HoMER):** this guidance sets out the principles, policies and procedures necessary for managing the risk that employees' behaviour will damage their organisation. The guidance can be found at: www.cpni.gov.uk/advice/Personnel-security1/homer/

- **Online social networking:** Online social networking (OSN) and micro-blogging sites are hugely popular and offer significant business benefits to organisations. However, their use poses risks to both the data on the IT system used to access the sites and to the users of the sites and the organisations they work for. More information and guidance can be found at: www.cpni.gov.uk/advice/Personnel-security1/Online-social-networking

This report summarises the themes emerging from the Insider Data Collection Study research and discusses key implications for personnel security.

Executive summary

This report details the findings from CPNI's Insider Data Collection Study, which forms part of an on-going programme of CPNI research into insider threat. The study used data on insider cases, collected and analysed between 2007 and 2012. For the purposes of this study, an insider is defined as **a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.**

The study analysed over 120 UK-based insider cases from both the public and private sectors. While cases from a range of industry sectors and organisations were included, the research was not designed to provide an insight into all insider activity. We cannot therefore suggest that the findings from this study are indicative of all insider acts.

CPNI identifies five main types of insider activity: unauthorised disclosure of sensitive information; process corruption; facilitation of third party access to an organisation's assets; physical sabotage; and electronic or IT sabotage. The most frequent types of insider activity identified in this study were unauthorised disclosure of sensitive information (47%) and process corruption (42%).

Detailed demographic information was available for the insider cases. Some noteworthy findings included:

- Significantly more males engaged in insider activity (82%) than females (18%).
- 49% of insider cases occurred within the 31-45 years age category. Instances of insider cases increased with age until they peaked within this category and then decreased beyond 45 years of age.
- The majority of insider acts were carried out by permanent staff (88%); only 7% of cases involved contractors and only 5% involved agency or temporary staff.
- The duration of the insider activity ranged from less than six months (41%) to more than 5 years (11%). More than half of the cases were identified within the first year.
- 60% of cases were individuals who had worked for their organisation for less than 5 years.

The majority of insider cases in the study were self-initiated (76%) rather than as a result of deliberate infiltration (6%); i.e. the individual saw an opportunity to exploit their access once they were employed rather than seeking employment with the intention of committing an insider act.

The research demonstrated that the reasons why people undertake insider activity are complex. It is relatively common for insiders to have more than one motivation for their activity, with a third of the cases in the study being identified with more than one motivating factor.

Although financial gain was the single most common primary motivation (47%), ideology (20%), a desire for recognition (14%) and loyalty (14%) were also quite common motivations.

The research also identified a clear pattern in the relationship between primary motivation and type of insider incident. Ideology and desire for recognition were closely linked to unauthorised disclosure of sensitive information and financial gain was most closely linked to process corruption or giving access to assets.

The findings include both individual- and organisational-level factors associated with insider activity.

Three main individual-level factors were considered as part of the study: personality traits, lifestyle/circumstantial vulnerabilities and workplace behaviours. The report includes factors from each of these areas which were considered to be of particular interest (and predictive of insider activity) when significant signs were shown that had a clear and negative impact. It is important that these findings are not taken out of context, and not used as a means to profile or discriminate against individuals who may match some of the characteristics and traits identified.

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

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

This report outlines the key implications for personnel security in order to help organisations reduce their vulnerability to the insider threat. These include having a strong, on-going personnel security regime, establishing effective management practices and recognising that the insider threat can come from anyone with access to an organisation's assets.

Overview of study parameters

The Insider Data Collection Study has analysed information on past cases of known insider activity, where an employee has been identified as committing an insider act and has been the subject of an investigation, either internally by their employer or externally by the Police or other regulatory body.

For the purposes of this study, an insider is defined as **a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.**

Scope

The research included insider cases where the damage was significant to the organisation (e.g. in terms of financial loss, operational or reputational damage, or loss of market position), and included those associated with terrorism, espionage and leaks to third parties (including the media), corruption and fraud for personal gain. Cases of petty or minor employee acts of abuse were excluded, as were unintentional insider acts.

Cases were obtained from both the public and private sectors and occurred across a range of national infrastructure sectors, including Government, Transport, Telecoms, Finance, Energy, Health, and Emergency Services.

The data collection and analysis took place between 2007 and 2012. The insider acts included mainly took place during the last 10 years within UK-based organisations, although the insider activity may have taken place overseas.

Points to note

Context

While cases from a range of industry sectors and organisations were included in the study, the research was not designed to provide an insight into all insider activity. We cannot therefore suggest that the findings from this study are indicative of all insider acts. There will, of course, be many instances of insider activity which remain undetected, or were known about but were either not disclosed by organisations or excluded from our enquiries.

It is important that these findings are not taken out of context, and not used as a means to profile or discriminate against individuals who match some of the characteristics and traits identified.

Approach

Information on insider cases was collected by reviewing case files and paperwork, and through formal interviews with key personnel who had knowledge of the individual, e.g. an investigator, manager or co-worker. A structured interview protocol was used to ensure, where possible, the same type of information was captured for each case. However, due to the retrospective nature of this research, the data gathered are dependent on the quality and quantity of the information either recorded at the time of the incident, or recalled at a later date.

The report includes percentages to represent some of the main findings. Where possible these are based on the total sample size, however some findings are based on slightly less than the total sample due to a small amount of missing data.

Main findings and themes

Type of insider incident

CPNI categorises insider incidents[1] into five main groupings:

- **Unauthorised disclosure of sensitive information** (either to a third party or the media)
- **Process corruption** (defined as illegitimately altering an internal process or system to achieve a specific, non-authorised objective)
- **Facilitation of third party access** to an organisation's assets (including premises, information and people)
- **Physical sabotage**
- **Electronic or IT sabotage**

The most frequent type of insider activity identified in this study was unauthorised disclosure of sensitive information to an external party (47%), followed by those engaging in process corruption (42%). Only 5% of the cases involved physical or electronic/IT sabotage. The five main types of incident are illustrated below:

- **Unauthorised disclosure of sensitive information**

A short-term contractor leaked privileged information from his employer to the media and onto the internet. The employee downloaded customer information from the organisation's computers onto a USB stick, passed it to journalists and then published it on the internet. The leak resulted in significant cost to the organisation in terms of time taken to investigate the matter, dealing with legal issues and ensuring that policies and procedures were in place to prevent it from happening again. There was also significant reputational damage to the employer.

- **Process corruption**

A senior finance manager with over 10 years' employment committed an insider act of process corruption by enabling payments totalling over £250,000 to be made to a personal bank account. The manager manipulated the system to ensure that he was the single point of authorisation for all salary payments made via a third party managing the organisation's payroll. When asked by the Directors to provide a set of accounts showing the salary payments, the manager gave excuses for the unavailability of certified accounts and provided his own spreadsheets showing salary payments across the business. These spreadsheets were doctored to show the insider's salary recorded correctly, and the additional payments spread across all other employees. The manager, with an over-inflated sense of his own value and contribution to the organisation, increased his own salary and claimed overtime payments without oversight or authorisation from another employee. At the same time he established systems to ensure that all questions relating to the payroll were directed to him to avoid anyone within the organisation uncovering his actions. The manager had an extravagant lifestyle based on the inflated income, and his actions were only discovered after he resigned from the organisation.

[1] This study has not specifically looked at cyber insider activity, which CPNI defines as **a person who abuses their legitimate access to an organisation's IT network to further their own agenda or damage their employer**. However, we estimate that over 80% of cases in the study could be described as containing a cyber-element to their activity.

The financial damage inflicted on his employer and colleagues was severe and resulted in a need to reduce staff and services in order to avoid bankruptcy.

- **Facilitation of third party access to an organisation's assets**

An agency employee facilitated access to an ex-employee with links to organised criminals for the purpose of committing major fraud. The employee gave the criminal gang potential access to £2 million of his employer's funds. The individual was motivated by financial gain and by the desire to maintain credibility with criminal friends. The insider activity was spotted by audit management, but only after the loss of £140,000.

- **Physical sabotage**

A temporary employee working as a security guard purposefully tampered with equipment vital to the operation of the organisation. The insider activity was spotted during routine maintenance checks, but the total cost of the damage to equipment was £146,000. The insider's motivation was based on a vendetta against another employee.

- **IT/electronic sabotage**

An employee sabotaged the automatic access system at his workplace causing the access points to lock and requiring a manual pass system to be introduced. The sabotage resulted in the whole site having to close for 3 days while the access system was reset at significant loss of productivity to the employer.

Personal & corporate demographics

Detailed demographic information was available for the insider cases. Although there was some missing data, it was possible to identify patterns of significant interest. The most interesting of these were:

- Significantly more males engaged in insider activity (82%) than females (18%).
- 49% of insider cases occurred within the 31-45 years age category. Instances of insider cases increased with age until they peaked within this category and then decreased beyond 45 years.
- The majority of insider acts were carried out by permanent staff (88%) and the vast majority of them were full-time (93% of the permanent staff). Only 7% of the cases involved contractors and only 5% involved agency or temporary staff.
- Certain job types were more at risk of an insider act being committed than would be expected given their distribution in the workforce. Specifically, the proportions of customer service (20%), financial (11%) and security (11%) staff engaging in insider activity were significantly higher than would be expected from Census data relating to job type published by the National Office of Statistics in 2001.
- Insider acts were relatively evenly split between managers (45%) and staff in non-managerial, administrative or support roles (49%). There were few cases involving either senior management (2%) or front-line manual or operational staff (4%). Census data published by the National Office of Statistics in 2001 suggest that the number of middle and junior managers and administrative and support staff engaging in insider activities is proportional to their numbers in the UK workforce.
- The duration of the insider activity ranged from less than six months (41%) to more than five years

(11%). More than half of the cases were identified within the first year.

- 60% of cases were individuals who had worked for their organisation for less than five years.

- Graduate level employees were more likely to be involved in insider activity then non-graduates. The proportion of graduate level insider cases (58%) was significantly higher than the proportion of graduates in the general population.

What motivated insider activity?

Nature of intent

CPNI defines three main types of insider behaviour:

- **Deliberate insider**: those who obtain employment with the deliberate intent of abusing their access

- **Volunteer/self-initiated insider**: those who obtain employment without deliberate intent to abuse their access but at some point personally decide to do so.

- **Exploited/recruited insider:** those who obtain employment without deliberate intent to abuse their access but at some point are exploited or recruited by a third party to do so.

The last two types of insider behaviour described above are defined as ‘opportunistic’ due to the lack of deliberate targeting of employment, i.e. an insider exploits an opportunity to conduct an insider act after they gain employment. The findings from this study suggest that the vast majority (76%) of insider cases assessed were self-initiated. 15% of cases were exploited or recruited by a third party and only 6% were as a result of deliberate infiltration.

Primary motivation

The research demonstrated that the reasons why people undertake insider activity are complex and multi-faceted. It is relatively common for insiders to have more than one motivation for their activity, with a third of the cases in the study being identified with more than one motivating factor. The range of primary motivations was identified as:

- Financial gain (47% of cases)
- Ideology (20% of cases)
- Desire for recognition (14% of cases)
- Loyalty to friends/family/country (14% of cases)
- Revenge (6% of cases)

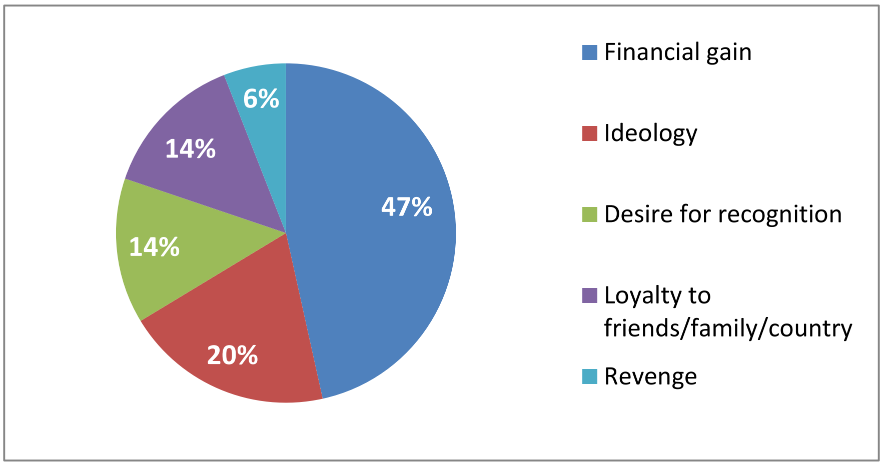

Figure 1: Primary motivation for insider activity

This demonstrates that although financial gain was the single most common primary motivation, ideology, a desire for recognition and loyalty (to friends/family/country) were also quite common motivations.

Although revenge against the employer was noted as a primary motivator in only 6% of cases, general disaffection with the employing organisation continued to be a contributory factor in many of the cases assessed. The research showed that in many insider cases there was an element of disaffection displayed by the employee. This ranged from being the main reason for the employee deciding to commit an insider act, to simply being disengaged from their employer and therefore not feeling committed to their organisation.

The research identified a clear pattern in the relationship between primary motivation and type of insider incident.

- Ideology and desire for recognition were closely linked to unauthorised disclosure of sensitive information. Ideology was the primary motivation for 40% of unauthorised disclosures and desire for recognition accounted for 22%.
- Financial gain was most closely linked to process corruption or giving access to assets. Financial gain was the primary motivation for 83% of process corruption cases and for 63% of facilitation of access to assets.
- Cases involving loyalty were fairly evenly split between unauthorised disclosure and process corruption.
- For those motivated by revenge, the cases were split between unauthorised disclosure and sabotage.

Individual-level factors associated with insider activity

Three main individual-level factors associated with insider activity were considered as part of the study. These were personality traits, lifestyle/circumstantial vulnerabilities, and workplace behaviours.

It is extremely important that these findings are not taken out of context or used as a means to profile or discriminate against individuals who may match some of the characteristics and traits identified.

Personality traits

The study examined the importance of a range of personality factors among the cases that were reviewed in depth. For the purposes of this study, personality was defined as *the characteristics of the individual relating to how they respond to situations and interact with others*.

The personality factors listed below were considered to be of particular interest (and predictive of case type) when *significant signs* were shown that had a *clear and negative impact on work and/or colleagues*:

- **Immature** (e.g. lacks life experience, is naïve and requires excessive guidance, has difficulty making life decisions);
- **Low self-esteem** (e.g. lacks confidence, is extremely dependent on recognition and praise, struggles to cope well with adversity, setbacks and difficult tasks);
- **Amoral and unethical** (e.g. lacks moral values or personal integrity, acts in an unscrupulous manner and shows no remorse, engages in unethical behaviour);
- **Superficial** (e.g. lacks a sense of identity and is hard to get to know, provokes a range of different opinions among people in the workplace);
- **Prone to fantasising** (e.g. believes they are engaged in activities that have no basis in reality, likes to create the impression that they are engaged in something special);
- **Restless and impulsive** (e.g. requires constant stimulation and cannot tolerate boredom, needs or seeks instant gratification and does whatever feels good in the moment, shifts from one thing to another);
- **Lacks conscientiousness** (e.g. does not comply with rules, neglects responsibilities and is unconcerned with duties and obligations, shows poor attention to detail and demonstrates poor judgement, shows a lack of focus);
- **Manipulative** (e.g. uses charm to get their own way and is very persuasive, nurtures relationships and manipulates others to serve their own self-interest, tends to adopt whatever position or attitude will result in getting their own way);
- **Emotionally unstable** (e.g. is prone to exaggerated mood swings, overreacts to problems, complains about unimportant or trivial things);
- **Evidence of psychological or personality disorders.**

Lifestyle and circumstantial vulnerabilities

Information on the individuals' lifestyle and personal circumstances was also sought to establish the extent to which these factors were important among the cases that were reviewed in depth. For the purposes of this study, lifestyle changes were defined as changes in personal circumstances which might increase stress or strain and lead to disaffection. Circumstantial vulnerabilities were defined as work, profile or personal issues which could make an individual vulnerable.

The lifestyle changes and circumstantial vulnerabilities listed below were considered to be of particular interest (and predictive of case type) when *frequent and/or clear signs* were shown which had a *significant negative impact:*

- **Demonstrates a poor work attitude** (e.g. does not follow established procedures, does not read or follow announcements and instructions issued by the organisation);

- **Shows signs of being stressed** (e.g. loses their temper, is apathetic, shows an increase in nervous habits, has memory problems, difficulty making decisions, an inability to concentrate and/or confusion);

- **Exploitable/vulnerable lifestyle** (e.g. has an exploitable weakness such as a serious financial, alcohol, gambling or drug problem, may have turned down offers of organisational support or ignored recommendations for treatment, has a strong desire for financial gain);

- **Exploitable or vulnerable work profile** (e.g. has access to sensitive assets which are highly sought after, has an ability to facilitate criminal activity through unauthorised access);

- **Recent negative life events** (e.g. problems at work resulting in a loss of status, significant personal injury, death of a family member or close friend, relationship break-up, financial difficulty).

Workplace behaviours

The study also examined information on the workplace behaviours identified among the cases that were reviewed in depth. For the purposes of this study, workplace behaviours were categorised as either suspicious (unexpected or difficult to explain workplace behaviours that cause concern) or unauthorised (workplace behaviours that may be part of the normal work role but are unauthorised).

The workplace behaviours listed below were considered to be of particular interest (and predictive of case type) when *frequent signs* were shown and the employee was *unlikely to have an adequate explanation*:

- **Engages in unusual copying activity** (e.g. makes extensive use of computer equipment to reproduce sensitive materials which may exceed job requirements, covers or removes protective markings on documents when copying them, copies protected information in other offices, despite a copier being available in their own area);

- **Engages in unusual IT activity** (e.g. conducts key-word searches in a sensitive database which the individual has no need to know, shows an unusual pattern of computer usage shortly prior to foreign travel);

- **Unauthorised handling of sensitive material** (e.g. stores and carries sensitive material inappropriately and without approval, provides sensitive information outside approved channels to any person without authorisation or need to know, asks others to obtain access to material on their behalf which they are not authorised to see);

- **Commits security violations** (e.g. betrays positions of trust, commits security violations).

The role of organisational factors in insider activity

The study has demonstrated that where an insider act takes place there is often an exploitable weakness with the employer's own protective security or management practices which enables the insider to act. The following organisational practices were identified as key enablers to an insider act:

- **Poor management practices**

A general lack of management supervision or oversight of employees meant that many of the behaviours, problems and activities of the insider were noticed but went unaddressed.

Management failure to address individual issues within the workplace (such as poor relationships with colleagues, absenteeism or anti-social behaviours) often appears to have resulted in the behaviours becoming more frequent or extreme.

Management failure to manage and resolve workplace issues (such as boredom or lack of work, overwork, lack of resources or specific grievances) appears to have contributed to the level of employee disaffection.

- **Poor usage of auditing functions**

Some organisations had not made regular and systematic use of their own IT or financial auditing functions to be in a position to quickly spot irregularities or unusual behaviours. This enabled insiders to act in the first place – and for some to continue acting without detection for longer than necessary.

- **Lack of protective security controls**

Some organisations had not implemented simple systems for controlling how employees could introduce or remove organisational data electronically, and manipulate organisational information remotely even after their employment had been terminated.

Basic 'need to know' principles were not rigorously applied, allowing some insiders to acquire knowledge they did not actually need for their job and then use it to commit an insider act.

Lack of segregation of duties was particularly in evidence in process corruption cases, where one individual would be in a position to manipulate systems or data without needing approval or endorsement from a second employee.

- **Poor security culture**

The case studies often revealed that a poor security culture existed in areas where insider acts took place, with a general lack of adherence to security policies and practices by employees, and with management being either unaware of these malpractices or failing to deal with them effectively.

Examples of the most common occurrences were the sharing of security passwords amongst employees, not locking computer terminals and allowing others to use logged-on terminals, sensitive materials being left on desks, security containers being left unlocked and pass access to secure areas not being enforced.

- **Lack of adequate role-based personnel security risk assessment prior to employment**

In some insider cases organisations had placed individuals in positions without considering their suitability for the role and potential complications that might arise. For example, there were cases where employees had been placed in roles likely to make them more vulnerable to compromise due to their nationality, family connections or ideological sympathies.

There were also cases where the insider simply did not have the skills, experience or aptitude for the role, and without careful management, the employee was easily manipulated by a malicious third party or simply unwittingly committed an insider act.

- **Poor pre-employment screening**

In a small number of process corruption cases it was evident that the appropriate level of pre-employment screening had not been undertaken; most notably failures to identify that the individual had a history of fraudulent behaviour (such as credit card or benefit fraud) prior to recruitment.

- **Poor communication between business areas**

The study has shown that if an organisation does not communicate and share information about threats and risks, but keeps the information in organisational silos, then its ability to mitigate and manage insider activity is severely reduced.

The study found cases where counter-productive workplace behaviour was known in one part of the organisation but had not been shared with others, resulting in delays to the organisation taking mitigating action to reduce the risk.

To fully understand the level of risk an employee poses, an organisation should be able to access information held by Human Resources concerning performance and welfare issues, information held by IT about access to electronic data, and Security for physical breaches of security policies. If information is retained by just one area of the business the organisation may misjudge the risk that it is carrying.

- **Lack of awareness of people risk at a senior level and inadequate governance**

A lack of awareness of people risk at a senior level can lead to organisations missing the attention and resources necessary to address the insider threat. There needs to be a single, senior, accountable owner of people risk to whom all managers with a responsibility for people risk report.

Inadequate corporate governance and unclear policies in managing people risk and strengthening compliance can also make it more difficult to prevent and detect insider activity.

Key implications for personnel security

The findings from the study highlight some key implications for personnel security in terms of helping to reduce vulnerability to the insider threat. These can be summarised as follows:

- Have a strong, on-going personnel security regime. This includes completing a personnel security risk assessment, having robust pre-employment screening checks, adopting on-going personnel security policies in line with the risks identified, and creating a secure culture that will support these policies.

- Whilst pre-employment screening is essential it will not, however comprehensive, identify all individuals who present a potential security risk. The combination of factors which the study has identified as notable to an insider act (including personality factors, lifestyle changes, circumstantial vulnerabilities and workplace behaviours) are not always present or observable at recruitment. Using robust and on-going protective security measures and establishing effective management practices are key to reducing vulnerability.

- Good management practices encourage a loyal and committed workforce where the environmental factors for employees developing feelings of disgruntlement are minimised and employees understand that counter-productive workplace behaviour will be quickly recognised and effectively addressed.

- Recognise that the insider threat can originate from anyone with legitimate access to your organisation. This includes permanent employees, contractors, temporary staff and even business partners. Ensure that the protective security policies and procedures are applied to all employees, regardless of their length of employment and seniority within the organisation.

- Following the principles described in CPNI's *Holistic Management of Employee Risk* (HoMER) guidance will provide a framework for mitigating insider activity in a proportionate and legal way. HoMER underlines the need to ensure that all areas of your organisation work to a single owner of the insider threat and that consistent messages are applied across the whole organisation with regard to security culture, auditing and good management practices.