

ONGOING PERSONNEL SECURITY: A GOOD PRACTICE GUIDE

EDITION TWO: JULY 2010

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

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	2
Ongoing personnel security: an overview	4
Security culture	6
Line management	11
Countering manipulation	17
Screening for the insider threat	22
Reporting hotlines	25
Secure contracting	29
Controlling employee access	35
Controlling employee IT access	39
Monitoring employee access	42
Investigation	47
Exit procedures	53
Glossary	59
Appendix 1: Full list of resources	60
Appendix 2: Generic security appraisal form	62
Appendix 3: An overview of legal requirements	67

Introduction

Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides advice on protecting the country's essential services, facilities and networks from terrorism and other threats.

The National Infrastructure

Nine different sectors form what is known as the national infrastructure. These provide the services which support everyday life:

- Communications
- Finance
- Health
- Emergency Services
- Food
- Transport
- Energy
- Government
- Water

CPNI provides security guidance, training and research from a physical, information and personnel security perspective. It aims specifically to reduce the vulnerabilities within these sectors, with particular emphasis on the most critical elements. Loss or disruption to any of these could cause severe economic or social consequences or even loss of life.

In addition to the nine sectors above, CPNI also provides similar advice to organisations engaged in planning and running the London 2012 Olympics.

The aims of this guidance



This guidance has been written for government departments and organisations that own or operate assets, services and systems which form part of the UK's national infrastructure. More specifically, it is intended to support the people in those organisations who work in human resources and security departments and those with line management responsibilities, all of whom have a role in creating and maintaining a culture of effective ongoing personnel security.

The guidance provides information about good practice in ongoing personnel security, bringing together advice from government departments and private organisations in a single document focusing on the key elements of an effective security culture. This document also draws on research commissioned by CPNI and completed by Adrian Furnham and John Taylor in the area of counter-productive work behaviours.

It is not intended to replace an organisation's established ongoing personnel security procedures, or those specialist security manuals in use in certain sectors of the national infrastructure such as the Security Policy Framework. Nor, given the large numbers and the varied sizes and activities of organisations in the national infrastructure, is it possible to create a document detailed enough to become a handbook for ongoing personnel security in every organisation. Our aim is to provide a useful supplement to existing security procedures and to provide a starting point for security and human resource professionals who are beginning to consider the role of the insider as part of their security regimes.

CPNI recommends that organisations seek professional advice, especially in the area of employment law, when implementing or amending their ongoing personnel security measures.



This document should be read in conjunction with other guidance published by CPNI, in particular:

- [Risk assessment for personnel security: a guide](#)
- [A good practice guide on pre-employment screening](#)

The following areas of personnel security each have associated CPNI guidance documents and some independently commissioned research articles. They are all publically available at www.cpni.gov.uk

- [Pre-Employment Screening & Document Verification](#)
- [Overseas Criminal Record Checks](#)
- [Managing the Disclosure of Employee Related Information](#)
- [Personnel Security in Offshore Locations](#)

Electronic copies of these documents can be found on the CPNI website www.cpni.gov.uk.

A full list of the additional resources which are cited at the end of each chapter throughout this document can be found at [Appendix 1](#).

Ongoing personnel security: an overview

Personnel security is a system of policies and procedures that manages the risk of staff or contractors exploiting legitimate access to an organisation's assets or premises for unauthorised purposes. It is important to distinguish between this and personal security, which seeks to reduce the risks to the safety or well-being of individual employees.

An effective personnel security regime seeks to:

- Reduce the risk of employing personnel who are likely to present a security concern (see CPNI guidance [A good practice guide on pre-employment screening](#) and [A good practice guide to pre-employment screening: document verification](#)).
- Minimise the likelihood of employees becoming a security concern.
- Implement security measures in a way that is proportionate to the risk (see CPNI guidance [Risk assessment for personnel security: a guide](#)).
- Reduce the risk of insider activity, protect the organisation's assets and, where necessary, carry out investigations to resolve suspicions or provide evidence for disciplinary procedures.

Why ongoing personnel security is important



An insider is someone (a permanent, temporary or contract worker) who exploits, or has the intention to exploit, their legitimate access to assets for unauthorised purposes. There are many different individuals and groups who may wish to act as or utilise an insider, including disaffected employees, single issue groups (such as animal rights activists), journalists, commercial competitors, terrorists, and hostile intelligence service agents (see [Screening for the insider threat](#)).

Many organisations already have experience of dealing with insider acts such as fraud, theft and corporate espionage, and some may also have experience of an employee suspected of or being in contact with a terrorist organisation. However, some of the more common insider acts include unauthorised disclosure of information and process corruption (where an employee has illegitimately altered an internal process for their own ends).

Insider motivations vary greatly and are often a combination of factors which can be hard to determine. Examples include political or religious ideology, revenge, notoriety and financial gain or even (where external pressure is exerted on an employee) fear or coercion.

As organisations implement increasingly sophisticated physical and IT security measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.

Pre-employment screening plays an important part in the personnel security process *but it is not a complete solution*. People and attitudes change, either gradually or in response to particular events, and insider acts are often carried out by employees who had no malicious intent when joining the organisation but whose loyalties changed after recruitment. CPNI research into past insider cases from a range of private and public sector organisations has shown that in many instances the employee undertaking the insider act had been in their organisation for some years prior to conducting the activity and opportunistically exploited their access. If organisations are to minimise their vulnerability to the insider threat, the commitment to personnel security must be continuous.

Unfortunately insiders are diverse and unpredictable, and no single set of countermeasures can guarantee protection. For example, additional layers of authentication on IT systems cannot help an organisation to safeguard its intellectual property unless ‘need to know’ and clear desk policies are also in place. A selection of personnel security countermeasures is required, complementing the organisation’s physical and IT security countermeasures, in order to mitigate the threat.



Additional levels of security may result in additional cost so the primary considerations when reviewing ongoing personnel security – other than legal or regulatory frameworks – must be proportionality and priority. Countermeasures should be implemented in proportion to the risk and in line with an agreed schedule of priorities. Practicality is also important, with a survey¹ by security specialists RSA showing that 35% of respondents have felt the need to work around their organisation’s established security policies and procedures just to get their job done. CPNI’s personnel risk assessment guidance offers a straightforward framework for evaluating personnel security risk, enabling practical decisions to be made about the proportionate and prioritised implementation of countermeasures. ([Risk assessment for personnel security: a guide](#)).

Throughout this document, certain words or phrases have specific definitions in the context of ongoing personnel security. For example, ‘employees’ refers to everybody working in an organisation, including permanent and temporary staff, consultants and contractors, from the newest recruit to the Chief Executive Officer. For more definitions, please see the [Glossary](#).

¹ “The Untold Insider Threat” Dec 10 2007

Security culture

Though all work environments possess internal cultures that influence how employees behave and interact, the existing culture may not be supportive of appropriate security behaviours. In such instances, organisations should look to develop a culture where the everyday actions and attitudes of staff effortlessly contribute towards a more secure working environment.

In some of the insider cases analysed as part of the CPNI research programme into insider activity, a poor security culture was often found to exist in the section or department in which the insider worked. This tended to be characterised by a general lack of adherence to basic security policies or good practice by employees, often coupled with managers failing to notice or address poor security behaviours (see [Line management](#)). Examples of some of the poor security behaviours identified included security cupboards not being closed or locked, security passwords being shared, employees not logging out of terminals, employees allowing others to use logged on terminals and sensitive materials being left unsupervised on desks.

Principles of culture management

An organisation must have a clear idea of the security culture it wants, and this will vary according to the nature of the business and the work environment. The term culture in this context refers to the styles, approaches and values that an organisation wishes to adopt towards security. For example, to what extent are individuals expected to make their own decisions about security practice? How will the organisation offer consistent guidance to employees so they take the 'right' kind of initiative? What level of risk is considered acceptable in the drive to achieve business results? To what extent should uniformity of approach be enforced? The organisation then needs to determine the size of the gap between the current and desired culture and what it has to do to achieve the behaviour and performance required².

A number of mechanisms are available, which broadly fall into two main groups:

- Those concerned with embedding the desired culture in the thinking and attitudes of staff. This involves management support and resources for security initiatives or offering incentives to encourage staff towards adopting the desired behaviours and routines (see also the [CIPD factsheet](#) listed at the end of this chapter). The second concerns those that enable staff to follow through their attitudes and thoughts to behave in ways that are consistent with the desired culture. Some of these address the pressures and constraints which may conflict with the desired culture, such as work deadlines or peer pressure. Others are concerned with gauging the efficiency of security systems, such as the quality of internal communications, training and security procedures to reinforce the desired behaviour.

² This model is based upon the Culture Management Model developed by Competence Assurance Solutions (C.E. Johnson, 2008). Organisational Culture and Effect Sizes. Proceedings of the 9th International Conference on Probabilistic Safety Assessment and Management. IAPSAM, Hong Kong.

It is important to remember that different mechanisms are appropriate to different cultures. A mechanism that works well in one organisation is not likely to be suitable for another with a very different culture, style, and approach to managing security. Therefore, it is crucial to clarify the desired culture at the outset, so that the right mechanisms for your organisation, that will support this culture, are adopted. It is the same for any significant change in a company and the following simple principles are applicable to everything:

- Clear explanations (briefings) to all involved
- Modelling of the desirable behaviours, particularly by senior managers
- Consistent implementation of the system
- Consultation with representatives of employee groups involved

Good communication

The success of any organisation's security measures and procedures depends on how effectively they are communicated to employees. Individuals are much more likely to engage if they have an understanding of why the security measures are in place and what their own responsibilities are in relation to these. In this way, each individual can make a positive contribution to the security culture and has the potential to detect or prevent a damaging insider act.

Periodically gauging staff opinion about security standards within the organisation is a useful method of determining current attitudes and to monitor any changing trends over time. Publicising positive results within the organisation will further support an effective security culture. However, it is very important to ensure that negative feedback is (where possible) publically addressed and resolved in order to maintain confidence in management.

The '**Employee attitudes and the recession survey**' found that 48% of employees thought that senior management did not consult them enough about planned changes to the organisation. Additionally, 26% of employees also said that managers did not provide them with feedback on their performance.

CIPD, February 2009,

Management support

Buy-in from senior management is vital in order to demonstrate that the personnel security measures are both worthwhile and necessary. Indeed their support or sponsorship may be crucial to securing the necessary resources to improve or maintain security within the organisation.

Top-down implementation is likely to promote adherence and consistency of behaviour across all employee groups, while a lack of commitment from senior managers could undermine the same process. For example, if the Chief Executive does not wear a pass then why should other employees?

Line managers also play a key role in the security culture of an organisation. Given that they are directly responsible for their employees, they are often best placed to both commend individuals and pick up on behaviours of concern (see [Line management](#) and [Screening for the insider threat](#)). However, the organisation also needs objective monitoring mechanisms to support managers and provide performance feedback, as well as safeguarding employees against any manager holding a grudge.

Clear policy and procedures

In order to maximise the implementation of and adherence to an organisation's security measures, they must be clearly explained within accessible policy documentation. This should include an outline of penalties and procedures to follow in the event of any security breach.



Clearly defining such procedures enables an organisation to clamp down on persistent offenders without being partisan or unfair. For example, an organisation requiring employees to display a security pass could set out the following policy for addressing non-compliance:

- Any employee not displaying a pass should be challenged verbally by any colleague. If they do not respond positively, this should be reported to their line manager, or where this is not known, to security.
- The employee's manager (or security) should provide a verbal warning that continued non-compliance will result in a formal breach.
- If the employee continues to ignore this regulation, they should be issued with a written warning from HR or Security.
- Finally, disciplinary action should be taken in line with the organisation's misconduct procedures.

All policies and procedures need to be followed openly and consistently, as a failure to do this may undermine an organisation's security. For example, if employees know that, in reality, they will never be checked for unauthorised electronic devices (and if staff who are known to have contravened this regulation faced no repercussion), then there is very little incentive for them to adhere to this policy. Furthermore, when procedures are not followed consistently, employees may consider that they are being unfairly singled out when action is taken.

Posters or some other method of raising awareness may help to communicate key policy messages to staff (see section on [Security training and awareness](#), later in this chapter).

Individual responsibility

An effective security culture requires the commitment of *every* member of staff, whether they are permanent, temporary or a contractor. This is important as any employee may misunderstand or ignore any given security measure, forming a weak link in the security culture. It is helpful to ensure that employees who do take responsibility for their own adherence to the organisation's security policies are also supported when they challenge or report those who do not.

It may be useful to ask employees to sign a statement of personal commitment to the security policies and values of the organisation at the outset of their employment. This will need to be supported by regular security briefings and information updates.

Clear desk policy

A clear desk policy requires documents and other items, including keys and removable objects of value, to be locked away when the office is unattended. This reduces the risk of theft and enables an office to be cleaned securely out of normal office hours.

It is important to clarify what is meant by a 'clear' desk so there is no confusion. The policy may refer to only sensitive items and documents; it may include personal items/papers; or it could refer to every removable item on the desk. The latter may be useful if desks are shared, although storage for these items will be needed. Nevertheless, if only sensitive items must be removed from otherwise cluttered desk areas, there is a danger that sensitive material may be overlooked.



All aspects of the office environment should be considered, to ensure there is no weak link. For example, printer buffers should be cleared, no sensitive items should be left in unlocked containers or drawers and all sensitive waste should be shredded to a satisfactory standard before being disposed of or recycled. Moreover, employees should routinely check the security of the office environment before they leave. A final checklist can be used by the last employee present to ensure the whole office is secure before they leave.

Organisations may wish to prevent staff from taking sensitive material out of the office unless it is absolutely necessary. An organisation could ask employees to log the removal and return of sensitive documents, which could be identified with a number or bar-code. They may also wish staff to hold sensitive papers within locked containers while they are out of the office.

Where an organisation is concerned about the loss of sensitive material, it could also restrict access to photocopiers, fax machines and other such devices, perhaps even disabling these out of hours. Other controls could include requiring a PIN before use and using a copier which keeps a secure record of items copied.

Security training and awareness

It is important to ensure that employees are equipped with the necessary skills in order to perform their responsibilities within the security framework of the organisation. Training and awareness can be accomplished through workshops, scenario based role-plays, briefings, road shows, intranet or magazine articles, posters, meetings, focus groups or quizzes.

The induction programme presents an excellent opportunity to emphasise the importance of security. However, there is a difficult balance to achieve in explaining the procedures which must be followed, encouraging staff to accept personal responsibility for security and equipping them to make judgment calls that procedures cannot always predict. Trainers and security personnel should think carefully about their objectives and how to achieve them.

Good training points:

- Encourage staff to see those in security as friendly and approachable Provide a contact number or email address for reporting security concerns
- Demonstrate unconditional support for the security policy (particularly from management)
- Explain the organisation's security policies openly. If there are some areas that are more sensitive than others and where access is restricted this should be clearly stated
- Give employees a realistic picture of the threats to the organisation
- Encourage cultures which resolve and correct rather than focus on establishing blame.

Bad training practice:

- Undermining the status of security. For example, any action or behaviour which implies that the speaker and/or subject is dull or unimportant
- Exaggerating the risks and threats faced by the organisation to gain more credibility
- Making untrue claims about security to try and frighten staff into compliance

Regular refresher training will help to maintain standards and ensure that new security procedures are incorporated into current practice and that employees understand why they are important to follow. It may also be appropriate to include an element of assessment within some training packages to ensure a sufficient standard is achieved.

Balancing risk and response

Finally, it should be remembered that any security measure, and particularly those newly implemented, must be proportionate to the risks faced by the organisation. These can best be identified through a personnel security risk assessment (for further information see CPNI guidance [Risk assessment for personnel security: a guide](#)). Not only will excessive measures waste organisational resources, but they could also undermine the implied duty of trust and confidence that employees have. Breaking this psychological contract could alienate staff and reduce goodwill and confidence in the organisation. CIPD has produced a useful factsheet which discusses these issues (see **Resources** below).

Consulting a wide range of occupational groups during the risk assessment will ensure that all aspects of the business are considered and increase the sense of ownership for those involved. Stakeholders should include human resources, management, personnel, IT and physical security representatives, for example. The presence of these experts should also increase the perceived authority of the process to employees not directly involved.

Resources

- Chartered Institute of Personnel and Development (CIPD) factsheet on performance management: <http://www.cipd.co.uk/subjects/perfmangmt/general/perfman.htm>
- Chartered Institute of Personnel and Development (CIPD) psychological contract factsheet: <http://www.cipd.co.uk/subjects/empreltns/psycntrct/psycontr.htm>

Line management

Line managers play a key role in influencing staff behaviours and are usually best positioned to detect behaviours of concern. Their responsibilities often include HR matters and these can be usefully extended to issues around personnel security.

The ability of managers to identify and resolve unhelpful, suspicious or unusual behaviour in their staff will vary and will be particularly difficult for those based in different geographical locations (although measures such as maintaining daily contact via telephone or video link and holding regular face-to-face meetings will assist).

However, such responsibility should form an integral part of any manager's job description so that it is clear any that failure to attend to these responsibilities will be dealt with as a poor performance issue. In some circumstances, such failure may also justify disciplinary action of some kind in line with an organisation's HR policy. In particular, there are three skills that managers should cultivate, which should help to create an atmosphere of loyalty and commitment as well as reducing the threat of insider activity:

Awareness

Managers need to know about people, not just about the employees who work for them but also the basics of personality, what motivates people, why employees might become disillusioned and how managers and leaders contribute to the problem of the insider threat.

Listening

If something is beginning to go wrong managers need to identify it early on, preferably before it becomes a problem. People need to feel they can talk to their manager, tell them sensitive information, and receive a sympathetic response. Listening is at the core of interpersonal skills.

Front line managers play a pivotal role in terms of implementing and enacting HR policies and practices. Where employees feel positive about their relationship with the front line managers they are more likely to have higher levels of job satisfaction, commitment and loyalty, which are associated with higher levels of performance.

Bath Research – CIPD paper, 2009

Influencing

Having good insight into what an insider might do, understanding their motivation and spotting potential difficulties early on is not helpful in isolation. Managers also need the skill and initiative to tackle any issues quickly and effectively. It may be sufficient just to highlight the issue with an individual, but people usually need to be persuaded. Particularly at times of organisational change, proactive communication, for example open meetings or discussion forums, should help detect, monitor and address any situation or feelings of disaffection.

Unfortunately, negative behaviour of managers at all levels can be a significant influence for those committing insider acts against their employer. Bad management can cause serious long term problems for all stakeholders in an organisation.

CPNI research into a number of past insider cases, from a range of public and private sector organisations, has highlighted that in many cases poor line management practices prevented early discovery of insider activity, or in some cases had contributed to a failure to notice and address growing disaffection within the organisation. Such cases were often characterised by a general lack of management oversight or poor levels of line management supervision of individual employees.

Ineffective communication, particularly at times of organisational change, can also result in high levels of uncertainty and anxiety among the workforce, and such stressors are known to have catalysed insider acts. Therefore, it is important that managers communicate difficult messages to their staff in a timely and appropriate fashion.

Many cultures train young people to say thank you and show gratitude for things done or given and failing to show gratitude can offend against the norms of society. The unrecognised person in the workplace can soon become dispirited, which is unfortunate as it costs nothing to say thank you. Recognition and praise is cheap and done effectively and judiciously can be particularly motivating.

Furnham research, 2010

Employees will treat their customers in the same way that their boss treats them. This could work for or against an organisation depending on the quality of its management. The characteristics of bad managers include:

Arrogance	They are right and everybody else is wrong
Melodrama	They want to be the centre of attention
Volatility	Their mood swings create business swings
Excessive caution	They cannot make important decisions
Habitual distrust	They focus on the negatives all the time
Aloofness	They disengage and disconnect with staff
Eccentricity	They think it is fun to be different just for the sake of it
Passive resistance	Their silence is misinterpreted as agreement
Perfectionism	They get the little things right even if the big things go wrong
Eagerness to please	Their being popular matters most

Employee welfare

An organisation with a strong welfare culture enables employees to share and address issues before they become too great to resolve; perhaps even providing them with access to professional support or advice. This is helpful as there are a number of life circumstances (for example, marital breakdown or personal financial difficulty) which may impair an individual's judgement or increase their vulnerability to third party influence. Without appropriate support such individuals may be susceptible to manipulation or may attempt to abuse their access within an organisation (see [Screening for the insider threat](#)).

It is important that there are clear organisational guidelines regarding what will and will not be supported or tolerated by the organisation. If a manager needs to address any given employee behaviour it is important that this is done sensitively, according to these guidelines. [Appendix 3](#) provides an overview of relevant legislation. However, it is recommended that advice should be sought from HR or an employment lawyer. Managers should be provided with training and support in this area when required.

Valuing employees

Treating each employee as a valued and unique individual, considering their requirements and providing them with opportunities for career and life development, is likely to go a long way to enhancing their commitment to the organisation and reduce the likelihood that they will undertake any insider activity. Every employee should be provided with the right tools to complete their role effectively and regularly discuss and review SMART job and development targets with their management.

Specific
Measurable
Agreed
Realistic
Time-framed

Stress can occur if there is too much pressure and when managers set unobtainable targets or when employees are not given any opportunities to develop new skills. The role of the manager is critical and additional advice and guidance on goal setting is available from CIPD (see [Resources](#) below).

Addressing behaviours of concern

As stated at the outset of this chapter, managers play a key role in maximising the output of their employees and addressing any negative behaviour. However, 'managing poor performance' is a competency that is frequently found wanting, and although failing to act should not be an option at all, it can often be the default position. This can cause employees to become dissatisfied because they have to carry an individual who is not pulling their weight. Alternatively they may conclude that such conduct or poor performance is acceptable and follow their example.

A manager does not have the right to ask an employee personal questions when seeking an explanation for negative behaviour, unless their work performance is suffering or there is a clear breach of organisational policy. Furthermore, in some circumstances, for example where an individual is under formal investigation, it may be counter-productive to alert the individual to the organisation's suspicion. However, this does mean that a manager cannot make general enquiries concerning about an employee's well-being or behaviour.

Case study: 'A problematic employee'

Ms Thompson is a secretary holding considerable access within her department. Until very recently she was regarded as totally reliable and very efficient. However, she has become moody and careless with her work. Her timekeeping has deteriorated badly and she is spending a lot of time visiting the ladies facilities. If anyone tries to speak to her about any of the above she responds very negatively.

A junior member of staff has recently made a formal complaint that she feels intimidated by Ms Thompson (who owes her money but is refusing to pay it back). There have also been a number of reports about petty theft around the office and some are beginning to point the finger of suspicion at Ms Thompson.

- What might be causing Ms Thompson's behaviour and how should her manager respond?

Training material, Cabinet Office

Where an employee presents cause for concern, but the situation is not so serious to merit a formal investigation, an informal interview may be the best way to clarify and/or address things before a more serious problem arises. Although it may be uncomfortable to raise issues with an individual, it could save the manager and organisation much time and effort in the long run.

Open questions are a good way to begin and may provide a platform for moving onto more pertinent issues. For instance, 'how are you getting on at the moment?' or 'how have you been finding your job recently?'

The case study 'A problematic employee' illustrates that, although a manager's first suspicion may be adverse, it is important to remember that there could be an innocent explanation. For example, circumstances which may impact an individual's behaviour (which are explored in more detail in [Screening for the insider threat](#)) could include:

- Personal issues, for example divorce, bereavement or illness.
- Work difficulties which may be causing tension. For example friction between colleagues, disillusionment, boredom or dissent.
- Possible conflicts of interest which may affect the employee's engagement with their work, such as an ethical concern.

Case study 'solution'

Some of the behaviour Ms Thompson is exhibiting could indicate that she has a drug problem. However, there are other explanations and no hard evidence, so this cannot be assumed. Due to the fact that her work has deteriorated and someone has made a formal complaint, Ms Thompson's manager has the right to ask her about the reasons for the change in her behaviour and, if she is not compliant, HR should be informed and the organisation's disciplinary procedures could be enacted.

If further evidence of wrongdoing emerges, or the manager suspects there is more to the issues than Ms Thompson is prepared to admit, those responsible for personnel security should also be informed, as they may wish to conduct their own investigation.

Training material, Cabinet Office

Employee voice

Employees will naturally find avenues for voicing discontent, particularly in the absence of their management, perhaps in the staff canteen or in a social environment after work. However, organisations should actively encourage openness and good communication among all employees (see section on [Good communication](#) in [Security culture](#) chapter).

It is also important to provide employees with mechanisms to raise issues and concerns outside their management chain. Options for this kind of communication include reporting hotlines and elected staff representatives, for example (see [Reporting hotlines](#)). This kind of proactive communication, for example open meetings or discussion forums, should help detect, monitor and address any situation or feelings of disaffection.

CIPD have produced a useful factsheet which outlines the history of employee involvement in decisions at work and describes a number of 'voice mechanisms' in greater detail (see [Resources](#) at the end of this chapter).

Appraisals

Incorporating personnel security checks into performance appraisals is a useful way of ensuring that regular personnel security checks are conducted on all staff. It may also prove an effective use of time and resource but must be done sensitively to avoid staff alienation, especially if it is being introduced as a new measure.



Organisations could consider asking employees in sensitive positions to complete an annual security appraisal form. The example given in [Appendix 2](#) can be adapted as necessary to ensure that the level of detail requested is appropriate. This provides a formalised way of determining any changes to an employee's personal and financial circumstances which may pose a risk to the organisation's security. If an organisation is a likely target for overseas interests a list of business and personal contacts made with foreign nationals during the appraisal period could also be requested.

If such questionnaires are too formal for an organisation or are not appropriate for all employees, then a simple checklist of items can be used to ensure that managers and employees are sharing the right kind of information. Such a checklist also provides a safeguard to employees by directing them to the kind of appropriate questions that a manager may ask.

This checklist could include the following areas:

- Significant changes in financial position (positive or negative).
- Changes of address.
- Significant changes in personal circumstances (bereavement, marriage, or separation, for example).
- Any suspicious approach from third parties regarding the employee's work (see [Countering manipulation](#)).
- Raising awareness of the dangers of sharing too much personal information on the internet.

It should be emphasised, where possible, that employees should not wait until formally asked to report significant changes. Appraisals and security forms should supplement and enhance the communication flow, but are not designed to replace other mechanisms.

Resources

- The role of frontline managers in HR - Chartered Institute of Personnel and Development (CIPD) factsheet (2009):
<http://www.cipd.co.uk/subjects/maneco/general/rolefrntlinemngers.htm?IsSrchRes=1>
- Line management behaviour and stress at work: Updated guidance for line managers
http://www.cipd.co.uk/NR/rdonlyres/898B09D3-6F8A-49AF-BD11-66EC76B086D4/0/stress_at_work_updated_guidance_for_line_managers.pdf
- Employee voice - CIPD factsheet (2010):
<http://www.cipd.co.uk/subjects/empreltns/comconslt/empvoice.htm?IsSrchRes=1>
- Employee communication - CIPD factsheet (2010):
<http://www.cipd.co.uk/subjects/empreltns/comconslt/empcomm.htm?IsSrchRes=1>
- Development planning for individual employees – CIPD factsheet (2008)
<http://www.cipd.co.uk/subjects/lrnanddev/general/devplng.htm>
- DirectGov – Problems at Work
<http://www.direct.gov.uk/en/Employment/ResolvingWorkplaceDisputes/index.htm>
- Advisory, Conciliation and Arbitration Service (ACAS) <http://www.acas.org.uk/>

See [Appendix 3](#) for an overview of relevant legislation.

Countering manipulation

As organisations improve their physical and electronic defences external individuals/groups wishing to obtain confidential or sensitive information may attempt to exploit those within the organisation who already have legitimate access. The process is also known as ‘social engineering’ and employees should be made aware of how it may arise in their private and professional lives and trained to guard against it.

Typically, the social engineer will begin by finding out as much as possible about the target organisation or individual before mounting a ‘dispersed’ or ‘directed’ attack. Although much social engineering is likely to involve rival companies, organisations should be aware that foreign intelligence services, seeking political and/or economic advantage, still pose a threat to UK interests.

Dispersed attacks

A dispersed attack – also known as a ‘mosaic’ attack – is one in which one or more people pose as a co-worker, new employee, delivery person or workman, for example, and attempt to collect information from different sources over an extended period of time. They may ask employees in the target organisation for small favours or apparently insignificant pieces of information, or gather information through seemingly innocent conversation. Although each piece of information may not be useful in isolation, it can still be highly valuable to the social engineer when pieced together.

Sources of information more often used in dispersed than directed attacks include:

Dumpster diving

Gathering information from an organisation’s or employee’s rubbish can help an individual to acquire background knowledge of a company that will help in mounting a social engineering attack.

Phishing/Pharming

Attempting to acquire sensitive information such as an employee’s usernames or passwords by masquerading as a trustworthy third party. Phishing is typically carried out by email or instant messaging; pharming attempts to acquire similar information by redirecting internet users to bogus websites.

Thief charms £15m in diamonds from bank

A conman armed only with chocolates and charm got into a bank vault and made off with diamonds worth over £15 million.

A £1.37 million reward has been offered for information on the smooth-talking, grey-haired thief, who posed as Carlos Hector Flomenbaum, an Argentinian businessman. Philip Claes, spokesman for the Diamond High Council in Antwerp, said despite the city’s ABN Amro bank having one of the most sophisticated security systems in the world, the conman found the weak spot: "He used no violence. He used one weapon - his charm - to gain confidence. He bought chocolates for the personnel, he was a nice guy, he charmed them, got the original of keys to make copies and got information on where the diamonds were."

The 120,000-carat haul included both cut and uncut diamonds. Police believe the raid was planned for over a year and could be the largest robbery committed by one person.

"In the diamond sector, we trust the people we are working with. Sometimes we pay the price for that," said Mr Claes.

DAILY TELEGRAPH, MAY 2007

Trojan horses/Gimmies

Email attachments that take advantage of the victim's curiosity or greed to effect the introduction of malicious software (also known as malware) to an organisation's IT systems. The consequences might range from simply causing occasional annoyance to users, to allowing computers to be remotely controlled by a third party.



Road apple

A CD ROM or USB flash drive, for example, which contains malware and left in a location where it is sure to be found, such as on a desk or in a lift. It will appear quite genuine (organisational logos are readily available from legitimate websites) and have a title intended to pique the curiosity of the finder. Once inserted into a USB port or CD ROM drive, it infects the computer, with results similar to that of the Trojan horse.

Social networking websites

A social networking website is a forum that allows people who share interests and activities, or who are interested in exploring the interests and activities of others, to interact online. Social networking sites enable members to communicate in a number of ways, including email and instant messaging, and to share personal details, information and opinions about their work and their employing organisation, as well as photographs of themselves and others. Research shows that even individuals who are aware of the risk of identity theft and concerned about privacy will engage enthusiastically with such sites, which have varying levels of security.

The organisation's websites

Some organisations, in the interests of transparency, publish structure charts, biographies and personnel contact details, 'employee of the month' pictures, policies, company blogs and even office floor plans on their internet sites. Posting unnecessarily detailed information on the organisational website can be invaluable to social engineers, greatly reducing the research effort required in advance of an attack.

The internet in general

Employees' own websites and blogs, special interest fora or third party websites such as recruitment agencies can all contain large amounts biographical detail – particularly in the CVs of employees looking for new jobs – which will assist social engineers in targeting individuals for attack. Internet archives and the caches of internet search engines can ensure that this information remains accessible for long periods (sometimes years) even after it has been removed from a live website.

Business cards and other handouts



Business cards and information packs often contain a great deal of information – job titles, company logos, names of departments and support staff – which can be useful to social engineers. Depending on the nature of the occasion, it may be appropriate to consider limiting the amount of detail contained in business cards and other handouts.

Organisations should consider developing a corporate data strategy, to ensure that information relating to the organisation and its employees is handled and distributed in a considered and consistent manner.

Directed attacks

A directed attack is generally aimed at a specific individual within an organisation who has access to valuable information. The social engineer will pose as a business contact at a conference, for example, and may spend some time building a close relationship with the targeted individual before using the trust established to access information. This is likely to begin with requests for easily obtainable, non-sensitive information, gradually moving on to demands – sometimes accompanied by a degree of coercion – for more confidential data.

While communicating with a target (either as part of a dispersed or a directed attack), social engineers may adopt a number of different techniques in order to increase the likelihood of a successful outcome, including:

- **Authority**
Emphasising seniority or professional credibility in order to capitalise on a tendency to respond to requests from those in power.
- **Conformity**
Legitimising the request by stating that other colleagues have previously provided information or allowed access.
- **Empathy**
Focusing on shared interests in order to establish a friendship, prevailing upon a target's tendency to be more helpful towards a friend.
- **Reciprocity**
Emphasising any help that the social engineer has given to the target during their relationship, thus capitalising on the target's sense of obligation to return a favour.
- **Consistency**
Pointing out that the target has complied with similar requests in the past, playing on an individual's tendency to behave in a way that is consistent with their previous actions.

Both the dispersed and directed forms of social engineering may be employed simultaneously, or the dispersed attack may be used to gather the information required to mount a more directed attack later.

It is also worth remembering that name-dropping, appearing to be in a hurry and also simple flattery (even when the target is aware it is being used) are still powerful tools for encouraging people to give out information.

Countermeasures

As social engineering targets individuals rather than IT systems or buildings, the most effective countermeasure available to any organisation wishing to protect itself from attack is education. Employees should be made aware of how social engineering works and the value of the information they hold.

A programme of social engineering awareness should include an overview of the wide range of possible social engineering attacks that employees might face and offer practical advice for protecting data, including:

- Being selective when posting information about themselves and their employment on social networking sites.
- Not talking about sensitive work issues in social situations.
- Not opening emails from unknown or suspicious senders.
- Treating all email attachments with caution.



Countermeasures that can be incorporated into the organisation's internet access policy (and which technically competent employees might also consider taking in their home computing environments), include:

- Using software controls that ensure only reputable websites can be accessed, reducing the risk of malicious software being installed on the system (see [Controlling employee access](#)).
- Where it exists, turning off the option to automatically download attachments to emails.
- Implementing effective filtering across internet gateways (spam blockers, firewall and antivirus software, for example) and making sure that the latest updates to these and the operating system are promptly installed.

In addition to electronic countermeasures, the procedural steps that an organisation should consider implementing to support its employees in keeping information secure include:

- Developing and communicating an internet access policy that clearly defines acceptable use of the internet.
- A system of protective marking for sensitive documents with associated handling procedures.
- Providing a mechanism by which employees can report suspected social engineering attacks, and a review process to identify any trends or repeated attempts to acquire certain pieces of information, so that other employees can be made aware.
- Ensuring that the information posted on organisation's websites is sufficient to inform the public, conforming to regulatory requirements where necessary, without offering superfluous details that will assist in the preparation of social engineering attacks.

- Implementing a policy of shredding paper before disposal if it contains sensitive information.
- Requiring that employees declare gifts over a certain value, and reviewing the list frequently so that unusual trends or inappropriate gifts can be spotted.
- Maintaining a clear desk policy and a culture where information is handled on a 'need to know' basis.
- Including social engineering training as a standard element in both induction and regular ongoing security programmes; articles in company newsletters and on the organisation's intranet sites can also help to reinforce the message.



For employees who may be particularly vulnerable to social engineering attacks – those in customer facing roles, for example, or those with access to important assets, such as IT administrators or security guards – additional training in countering manipulation should be considered. These groups of employees should be:

- Reminded of the control procedures which apply to their roles, especially those governing how and when an enquirer's credentials should be checked, before responding to any requests for information.
- Taught to be wary of unusual behaviours, such as a caller's refusal to provide contact details, and the use of the common social engineering techniques of authority, conformity, empathy, reciprocity and consistency.
- Trained to be assertive so that they can terminate a line of questioning they consider to be suspicious.

A customer-facing employee who has to terminate a call or refuse to provide information on the grounds of a suspected social engineering attack must be confident that they will have the support of their line management. It is therefore important to ensure that the subject of social engineering is adequately addressed in the procedures governing that role. Furthermore, all suspected cases of social-engineering should be reported, properly investigated and where possible, resolved.

Resources

- www.getsafeonline.org: a site sponsored by government and private organisations, and offering advice on how to stay secure while accessing the internet.

Screening for the insider threat

Although insider attacks are rare, they can cause significant damage when they do occur. Establishing an effective screening regime that understands the behaviours and characteristics of a potential insider is one of the most challenging aspects of personnel security.

It is difficult to determine a set of indicators that, taken out of a wider context, can reliably identify active insiders or suggest susceptibility to future insider behaviour. Research to date shows that the personality, motivation and behaviour of insiders are extremely varied. Also that insider behaviour is shaped by a complex mix of factors including life history and the work environment. It is therefore extremely unlikely that any single indicator will ever reliably identify a potential insider. It is only when particular combinations or clusters of behaviours are observed that there may be cause for concern. Even then, it is still likely that an innocent explanation may exist.

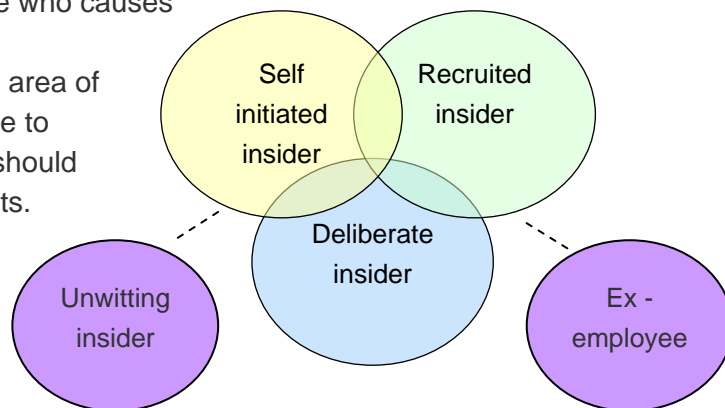
It is important that the level of screening is proportionate to the threat and a personnel security risk assessment will help to identify those roles where the risks are greatest (see CPNI guidance [Risk assessment for personnel security: a guide](#)).

Insider behaviour generally falls into one of three categories:

Self initiated insider	An individual who decides to exploit their access to assets once in post, even though they had no prior intention of doing so, and have not been recruited or exploited by a third party.
Recruited insider	An individual in post who is exploited or recruited by others in order to take advantage of their access.
Deliberate insider	An individual who seeks a specific type of employment, with the intention of abusing their access once in post.

The **unwitting insider**, an employee who causes damage to an organisation through carelessness or ineptitude, is not an area of focus because measures put in place to prevent deliberate insider activities should also guard against the accidental acts.

There is also the **ex-employee**, who is no longer an 'insider', but may still have access unless proper measures have been taken (this area is addressed in [Exit procedures](#)).



Factors influencing likelihood of insider activity

Certain factors may increase an organisation's vulnerability to insider activity:

- Poor management practices and a weak organisational culture, which can help to diminish employee loyalty and commitment.
- Ineffective grievance processes for employees to voice discontent before it escalates into disaffection.
- The lack of a strong security culture, resulting in employees not taking individual responsibility for security and reduced compliance with security procedures.
- Inadequate personnel security measures during pre-employment screening, reducing an organisation's ability to identify deliberate insiders.
- Inadequate personnel security measures after recruitment, limiting the organisation's ability to identify or prevent insider activity among its employees.

In addition, circumstances surrounding an employee's personal life may increase their vulnerability to third party influence, impair their judgement or catalyse their engagement in an insider act. Examples of such circumstances include personal illness, illness or death of a partner, close friend or family member, uncertain employment conditions, personal financial difficulty, or unfair treatment at work (including discrimination and harassment).

Line managers in particular, but all employees generally, should be made aware of the signs of increased vulnerability among their teams. Behaviours that may indicate an underlying personal issue include excessive alcohol consumption or substance abuse, signs of depression (including loss of interest in work) and emotional instability (including overreactions to changes or disappointments).



Purpose of screening

The purpose of screening is threefold:

- To identify any individuals displaying types, levels or clusters of behaviours which have been seen in previous insider cases. These behaviours may require attention in terms of personnel management/welfare (for example to prevent further disaffection) or from a security perspective (for example to reinforce lapsed measures and/or procedures). Identifying *and acting* upon such concerns quickly is an integral part of effective ongoing personnel security management.
- To detect actual insider activity, through the identification of suspicious behaviours in the workplace (such as accessing databases or taking sensitive information offsite without authorisation).
- To assess the risk posed by an individual moving to a more sensitive role, holding greater opportunity for insider activity (see [Controlling employee access](#)).

The screening process

Screening employees to determine their vulnerability to, or active involvement in, insider activity involves identifying those people who give cause for concern by demonstrating suspicious behaviours or possessing individual vulnerabilities. However, this process must then be complemented by the effective resolution or management of these concerns.



The first stage – identifying individuals who may give cause for concern – involves a basic level of screening for all employees, which acts as an initial filter. The tools or techniques used should therefore be suitable for application across sizeable numbers of people and might, for example, take the form of:

- Automated monitoring of employee activities (see [Monitoring employee access](#)) to identify anomalous behaviour.
- Using the appraisal process as an opportunity for line managers to identify signs and behaviours of concern.
- Application of more detailed assessment by trained practitioners when a concern is raised by a line manager or colleague outside of the appraisal process.
- Securing the involvement of all employees in the screening process by raising awareness of personnel security and the insider threat (see [Security culture](#)).
- Providing reporting mechanisms through which they can express their concerns (see [Reporting hotlines](#)).

Once the initial filtering has identified certain individuals about whom an organisation might have a degree of concern, the second stage is to find a way to resolve or manage those concerns. For example, it may be that there is an underlying welfare issue that requires employee assistance. This necessarily involves a more direct approach – generally a face-to-face interaction such as an interview (see [Line management](#)). Any suspicious concerns that persist after this stage should be addressed in more depth, usually by internal investigations.

Interviewing an employee in order to resolve suspicions is clearly labour intensive and requires a highly skilled interviewer. The employee may attempt to portray a false image in order to pass the assessment, and detecting this type of deception is a major issue in ensuring the validity of such interviews.

Organisations should consider running awareness programmes to ensure that line managers and employees do not overlook problematic or negative behaviour (see [Line management](#)). When concerns are raised, it is important not to overreact but to take swift, proportionate action in order to avoid any escalation. It is equally important not to diagnose insider activity where none exists, so organisational procedures should always be followed, to ensure that the correct steps are taken in each instance.

Reporting hotlines

Providing a trusted resource for staff to report security concerns or suspicions, either anonymously or otherwise, is a positive way of helping to nurture a security culture within an organisation. In order to reap the benefits and give staff confidence in the system, it will need to be operated by trained professionals who can listen, probe and react accordingly in each case.

A hotline enables employees to report suspicions or actual incidents of illegal, unethical or improper conduct by their colleagues, such as bullying, failure to adhere to security procedures, fraud or theft. It also provides a means for reporting suspicions about a colleague's behaviour (see [Screening for the insider threat](#)). The hotline may also form part of a staff welfare programme, helping employees to seek advice if they find themselves in financial difficulties, for example.

While 'hotline' is the generic term for an employee reporting facility, it need not be limited to (or even include) a telephone line, and could take the form of an internet contact site or dedicated company email address, among others.



In an organisation with a good security culture, the line manager will usually be the first point of contact for an employee who wishes to report unauthorised activity. Reporting hotlines are not designed to replace this relationship; they are intended to provide additional benefits such as anonymous or out-of-hours reporting, where this is desirable.

Principles

Research indicates that the most successful reporting hotlines have a number of principles in common, including:

- There should be clarity among employees about the types of call that the hotline will accept.
- A hotline provided by a third party organisation is more likely to be perceived by employees as truly confidential and impartial.
- It should be staffed by trained professionals who can listen effectively, ask relevant questions, document the contents of the call, and quickly convey the information to the appropriate point of contact for further action.
- If the hotline is provided internally, it should not be operated by the department responsible for investigating incoming reports.
- If the hotline is provided externally, there should be a clear understanding of how calls concerning criminal activity will be handled (for example, who will be responsible for contacting the Police, if necessary).

- The hotline must be available twenty-four hours a day, as employees are less likely to use it while they are at work with the colleague(s) whose actions they wish to report.
- The hotline provider should be able to deal with reports in a range of languages appropriate to the organisational population to prevent employee groups feeling disenfranchised.
- If the hotline is telephone-based, it should be free or at a low-rate tariff, given that calls are likely to be made from an employees' own telephone.
- The hotline provider must supply meaningful and timely management information concerning the nature of incoming reports, so that trends can be identified and used to influence organisational policy, if appropriate.
- Rewards may be considered for employees whose reports lead to successful action (where 'success' is defined by the organisation), although there is little evidence yet to show that this is an effective incentive.
- A system of support should be in place for employees who make a report in good faith; this can take many forms but is characterised by a general corporate and union goodwill towards the employee who uses the hotline, in order to reassure others who may consider doing the same.
- Conversely, effective sanctions such as disciplinary procedures should be considered in response to malicious reporting.

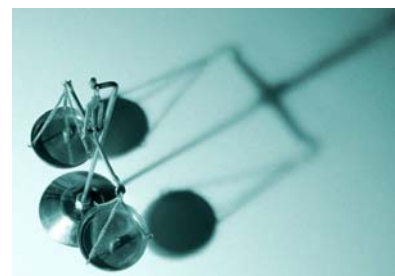
The manner in which incoming incident reports are handled must be clearly documented, and the procedures strictly adhered to if employees are to have confidence in the integrity of the hotline. In order to ensure a consistent response the procedures should not only provide guidance for the handling of incoming reports (including dealing with irrelevant reports), but also for next steps such as assessing the seriousness of the report and ensuring that the details are forwarded to the appropriate party for further action where necessary.

Generally, reports are likely to be forwarded initially to the organisation's investigations team (see [Investigation](#)) but the handling procedures may vary according to the size and structure of the organisation.

Legal considerations

The provision of a reporting hotline raises a number of legal issues that need to be addressed and resolved, and then embedded in the procedures governing the operation of the hotline in the organisation.

It is vital that any organisation wishing to implement an incident reporting hotline seeks legal advice first.



Anonymity

There is some evidence to show that employees prefer not to identify themselves when using a reporting hotline, so a facility that allows employees to remain anonymous might therefore expect to receive a larger number of reports. An anonymous reporting facility brings additional complications, however. Clearly the potential increase in reporting volumes would have to be balanced against the possibility of malicious or spurious reports from employees who know that their identity need not be revealed.

There is also a greater risk that those reporting anonymously might have discriminatory motivations. If such a report is then investigated without steps being taken to clarify the motives of the employee making it – which would be impossible when the report is anonymous – there is a risk that the organisation could become implicated in an act of discrimination.



Similarly, if an anonymous report indicated that an employee needed some sort of assistance, for example, the investigations team may not be able to take the appropriate action and the organisation could subsequently risk being found to be negligent.

It should be a condition of reporting hotlines that the employee making the report gives their name, and that their anonymity will be preserved as far as possible, given the nature of the report and any subsequent investigation. In some cases, it may be possible to carry out the entire investigation without revealing the employee's identity, although this is unlikely to be achievable every time. There may even be a point, depending on the severity of any accusations that have been made, where the employee who made the report is consulted before the investigation proceeds to the point where their involvement is revealed. A separate judgement will have to be made for each case, but anonymity should not be guaranteed for all reports received.

A further complication with anonymity results from a conflict between US and EU legislation. In the US, the Sarbanes-Oxley Act 2002 requires the implementation of an anonymous hotline to facilitate the reporting of accounting, auditing, banking and financial corruption; in the UK, an anonymous hotline would breach the Data Protection Act 1998 (derived from the EU's 1995 Data Protection Directive). European authorities and the US Securities and Exchange Commission are currently attempting to resolve this conflict between legal regimes.

Data protection

In addition to the issue of anonymity, careful consideration needs to be given to the way in which information recorded during reports to the hotline is processed, especially if the hotline provider (whether a department within the organisation or a third party) is based overseas. In the UK, personal data must be handled in accordance with the Data Protection Act 1998, and similar legislation derived from the EU Directive on Data Protection exists across Europe.

However, the regulatory framework will vary according to the territory; for example, some countries do not allow personal data to be transmitted across their borders, while certain government agencies have powers enabling them to access personal data stored on local servers, which means that the confidentiality of hotline reports cannot be guaranteed. Optional schemes, such as the US Department of Commerce's International Safe Harbor Privacy Principles, may offer some degree of reassurance, but these will vary from country to country.

‘Whistleblowing’

The Employment Rights Act 1996, as amended by the Public Interest Disclosure Act 1998, affords protection to employees who make what the legislation defines as a ‘protected disclosure’. Depending on the nature of the incident, this could cover employees who make reports to a hotline. The legislation provides employees with the right to complain to an employment tribunal if they are dismissed or suffer any other form of detriment as a result of making a protected disclosure. It does not, however, provide a general protection in all circumstances.

It has been shown that the overwhelming majority of people support the concept of legal protection for people who report corruption. However, it is helpful if organisations have a clear policy, demonstrating that the issue of malpractice is serious and dealt with firmly, so that employees can raise issues confidentially and without fear of repercussion. Such a policy should include guidelines and time-limits for any consequent investigations and should also specify consequences and penalties for making false and malicious allegations.

Whistle-blowing can be a serious act. The ‘just’ whistle-blower needs to be completely sure of their facts and have sufficient reliable and robust evidence to stand-up in a court of law and they may be advised to seek legal help first. Generally, a disclosure may qualify for protection if, in the reasonable belief of the person making it, it tends to show that one or more of the following has occurred, is occurring, or is likely to occur:

- A criminal offence
- A failure to comply with a legal obligation
- A miscarriage of justice
- The endangering of an individual’s health and safety
- Damage to the environment
- Deliberate concealment of information tending to show any of the above.



However, if the energies of whistle-blowers can be channelled within an organisation they can be enormously valuable. Employees with information about an internal wrong should be able to report on it without fear of reprisal or public exposure. CIPD have produced a useful factsheet on this subject, which examines the legal position and benefits of having a whistleblowing procedure in place (see CIPD factsheet listed in the resources section below).

Resources

- CIPD whistle-blowing factsheet: <http://www.cipd.co.uk/subjects/empreltns/whistleblw/whistle.htm>
- www.bsigroup.com/en/Standards-and-Publications/Industry-Sectors/Risk/PAS-19982008-Whistleblowing: This Publicly Available Specification (PAS) sets out good practice for the introduction, revision, operation and review of effective hotline arrangements.
- http://www.export.gov/safeharbor/SH_Overview.asp Safe Harbor [sic] provides a way for US companies to avoid interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws.
- Anti-bribery legislation: <http://www.justice.gov.uk/publications/bribery-bill.htm>

Secure contracting

The use of contractors is commonplace. However, a contractor's primary loyalty may not be to the employing organisation and their commitment to its security may be diminished. This risk needs to be managed.

Although the majority of the insider cases analysed as part of the CPNI research programme into insider activity involved permanent employees, rather than contractors, this may simply reflect the relative proportion of permanent versus non-permanent staff in most organisations. The main implication of the research was that both contractors and permanent employees should be treated equally in terms of the application of protective security measures and messages as they potentially pose the same level of risk.

Individual contractors

For the purposes of this section, the terms 'contractor' and 'contract worker' are used to refer to an individual worker who is not a permanent employee. This group includes temporary staff and consultants (sometimes referred to as the 'contingent workforce') as well as secondees and attachments.

Contractors may be engaged through an agency or by the organisation directly, and can be based on the organisation's premises, at home or at an external site. Each permutation presents particular personnel security challenges. Other reasons why contractors merit particular attention in ongoing personnel security include:

- Timescales for recruiting contractors are often tight, and if it is anticipated that they will only be employed for a short time there can be pressure to overlook some of the usual pre-employment security measures.
- The income from contract work can be irregular, which can be a driver towards unauthorised activity for financial gain.
- A contractor may work in competitor organisations consecutively or simultaneously.

Fire brigade fraud 'like winning lottery'

The Independent Commission Against Corruption has been told New South Wales taxpayers were defrauded of more than \$2.5 million due to alleged corruption by two fire brigade project managers.

The inquiry will look at whether two of the NSW Fire Brigade's project managers and others were involved in corrupt conduct between mid-2005 and early 2007. The two men were responsible for a total of 18 major projects, including the refurbishment or building of new fire stations in Sydney and regional areas.

Counsel told the inquiry that the evidence will show the men set up an elaborate system of private contractor companies to tender for public works they were meant to be overseeing, and then hired sub-contractors to do the work for less, pocketing the difference.

"There was a substantial loss to the public purse of approximately \$2.5 million," she said.

ABC NEWS, AUG 2008
Reprinted with permission of the Australian Broadcasting Corporation

- Although contractors are not part of the permanent workforce, contracts can be renewed or extended to the point that a contractor may work in one organisation for many years, gaining trust, accumulating responsibility and building an extensive knowledge of the organisation's activities.
- Contractors can be employed in positions of considerable authority, including the recruitment and day-to-day management of other contractors or permanent employees.

Ongoing personnel security therefore plays an important part in managing the insider risks associated with contractors. A personnel security risk assessment (see CPNI guidance [Risk assessment for personnel security: a guide](#)) will inform decisions about ongoing personnel security countermeasures, helping to ensure that they are proportionate to the risk of contractors acting maliciously in post.

When a contractor has been selected by an agency, it is vital to begin by confirming that the person who arrives for work is the person the agency supplied, using document verification (see CPNI guidance [A good practice guide to pre-employment screening: document verification](#)) or an exchange of photographs between the agency and the organisation, for example.



Once on site, contractors are usually given access to the same organisational assets as permanent employees in similar roles. It is advisable, therefore, to subject them to the same ongoing personnel security measures as their permanent counterparts, such as security inductions, control of access according to role, appropriate levels of supervision and a requirement to commit to the organisation's codes of conduct.

Contracts

Contracts should contain clauses relating to personnel security, such as the right of the organisation to audit the contractor's work in progress (bearing in mind that this might not be on the organisation's premises), mandatory disclosure of expulsion from any relevant accrediting body and conforming to the organisation's standards of behaviour. There should also be a clause requiring the contractor to disclose any work being undertaken concurrently for a competitor organisation and providing for immediate termination of the contract if there is thought to be a conflict of interests.

Any standard of behaviour that a permanent employee is expected to observe should be included as a standard part of the contractual agreement. For example, contractors should be expected to commit to policies governing acceptable use of email and the internet, obligations towards data protection and the organisation's gift policy. Some organisations include a premium in the contractor's fee which can be deducted if they fail to comply with these requirements.

Always consult a specialist in employment law when drafting contracts.

Access controls

Contractors often have less predictable working patterns than permanent employees, and may be periodically re-employed by the organisation, which can cause complications when trying to keep track of who is authorised to be on site at any given time. The resulting opportunity for unauthorised activity can be reduced by controlling access to the organisation's assets.



Ideally, local managers from the organisation's permanent workforce should be responsible for contract workers. This may be one-to-one line management or, as is more likely in larger projects or organisations, a line manager may oversee groups of contractors, defining and sponsoring the levels of access required (which should be role-based: see Controlling employee access) and approving renewals when needed.

Contractors should be issued with system passwords and security passes that automatically expire at the end of the contract and, where necessary, with restrictions on the hours during which the passes and passwords will provide access. Alternatively, the employing organisation might retain contractor passes between visits, although this still requires the pass issuing team to know when the pass should be handed in and handed out.

All passes, even those with an automated expiry date, must be retrieved at the end of the period of employment (see Exit procedures). It is also worth considering whether a contractor, if not working regularly on the organisation's premises, should be issued with a pass at all, but provided instead with a visitor's pass when required and escorted while on site.

Other steps that can be taken to restrict access to organisational assets, and therefore the opportunity to commit insider acts, include using passes with a recent photograph of the authorised holder so that the person wearing the pass can be verified as the person it was issued to, and giving contractors passes that are noticeably different in shape or colour from those issued to permanent employees. These measures will work best in organisations where there is a culture of wearing passes at all times and challenging those who do not.

In IT projects it is common practice among organisations within the national infrastructure to allow contractors access only to the development system. Permanent employees are responsible for testing and approving code before it is transferred and allowed to run on the live system.

Systems passwords and security passes should always be terminated – and in the case of passes, reclaimed – as soon as they are no longer needed. Those with responsibility for the organisation's security, as well as those in direct supervisory roles, should be aware of contractors' start and finish dates, and there must be procedures in place for line managers to notify their security contact if a contract worker leaves the organisation before their agreed finish date.

Contingency

The employing organisation and the contracting agency (or the contractor, if no agency is involved) should agree a procedure for providing temporary replacements when the contractor is unavailable. These arrangements should be included in the contractual agreement, and the employing organisation will need to decide what additional personnel security measures to implement – for example, restricted or supervised access – when the replacement contractor is on site.

Re-employment

When a contractor is employed on more than one occasion in the same organisation, it is important not to assume that their circumstances have remained unchanged between periods of employment. This is also the case when a former permanent member of staff is re-employed as a contractor in the organisation they left, where they may automatically assume the status of a trusted employee purely on the basis of their former working relationships.



Personal circumstances and attitudes change over time and can affect an individual's propensity towards unauthorised activity. Steps should therefore be taken, at the beginning of each period of re-employment, to ensure as far as possible that the contractor poses no greater threat to the organisation than previously.

Depending on the time elapsed, the nature of the organisation and the sensitivity of the role, this could range from a short series of questions confirming that contractors' circumstance gives no greater cause for concern than during the initial period of employment, to a repeat of the entire pre-employment screening process.

If the contractor has been employed through a contracting agency, the agency will usually implement these re-checks, but it is the responsibility of the employing organisation to stipulate the extent of the checks to be carried out.

Commitment

On first starting work in an organisation, contractors should ideally attend the same organisational induction (which should include security messages) and regular security reminders/updates as permanent employees. This will help them to understand why security is important and how they are expected to contribute to the organisation's security culture.

If a contractor is employed for only a short time, it may not be worth the loss of productivity that will result from their attendance on lengthy security briefings. In this case a single, shorter briefing should still be considered where practical. However, if the contract is extended or if the contractor is re-employed at a later date, then an induction into the organisation's security culture should be mandatory.

Remote working

Many contractors do not work on the organisation's premises but at home or at an external site such as a building project. They may, as a result, be subject to lower levels of supervision, and feel less involved with the organisation and their colleagues, than might otherwise be the case.



It can be difficult to mitigate the personnel security risk represented by contractors working offsite, and the lengths to which this should be attempted will depend on factors such as the nature of the contractor role and the sensitivity or value of the organisational assets to which they have access. In extreme cases, it may simply not be permissible for the contractor to work offsite at all, but if this is unavoidable then additional restrictions should be considered.

These may take the form of system passwords that limit the quantity or nature of information that can be accessed, for example, or higher levels of supervision, either by permanent members of staff working at the same site or by CCTV (see [Monitoring employee access](#)), depending on the situation. Any employee supervising a contractor will need to understand the contractor's job sufficiently well to be able to identify unauthorised activity if it occurs.

Measures to restrict access to assets should be complemented by face-to-face meetings between contractors and their line manager as often as is practical. This will serve to reinforce the relationship between the contractor and the organisation and, if necessary, provide a channel through which a remote worker can voice any frustrations before they develop into disaffection (see [Reporting hotlines](#)).

In some cases, a contractor may have to be in post without meeting the organisation's usual standards for security clearance. This could be because:

- The urgency for the contractor to begin work means that the necessary pre-employment screening has not yet been completed.
- The results of the pre-employment screening are not entirely satisfactory but the need for the contractor's expertise is such that they are employed anyway.
- It is simply not practical to implement the necessary level of security (for example, where the organisation's IT system does not offer passwords with different levels of authority, and so a contractor has unlimited access to the organisation's files).

In these circumstances the need for ongoing personnel security still exists and should not be overlooked, even temporarily. Some equivalent measure should be considered, such as closer supervision of the contractor by a permanent member of staff, or restrictions on their working hours to ensure they do not stay in the office after the permanent employees have left.

Corporate contractors

In very large or complex projects, organisations may engage a company, rather than an individual, as a contractor, and that company may need to engage others in order to complete the project. When contractors recruit subcontractors, who may in turn recruit further levels of subcontractor, there is potential for the organisation's security standards to become confused or diluted.



To mitigate this risk as far possible, the contract between the organisation and the first contracted company must be absolutely explicit about:

- The security controls (both pre-employment and ongoing) demanded by the organisation, and the need for these to be upheld throughout the entire contracting chain.
- Who is responsible for any lapse in security.
- The right of the organisation to approve any subsequent choice of subcontractor.
- The right of the organisation to audit the implementation of the security standards at any point in the contracting chain.

Controlling employee access

Organisations often focus on external threats without giving similar consideration to the threat from possible ‘insiders’. This section considers a range of measures which can prevent or minimise the risk of individuals with legitimate access engaging in insider activities.

It is important that any employee access controls used by an organisation are proportionate to the scale and nature of the threats faced. The best way to measure this is to conduct a full personnel security risk assessment. This will identify the high priority threat areas and associated high risk employee groups, enable the organisation to determine whether the measures in place are appropriate and provide a clear rationale for the adoption of any new measures. This should assist with ‘buy-in’ from employees but may also prove useful for funding applications or in obtaining board level support (for further details see CPNI guidance [Risk assessment for personnel security: a guide](#)).



Breaches in security can occur when employees share sensitive information unnecessarily with colleagues (see [Countering manipulation](#)). Naturally, employees require some knowledge in order to fulfil their role. However the ‘need to know’ principle enables organisations to reduce the risk posed by each employee by restricting knowledge to only those who require it. This principle also makes it more obvious if someone is inappropriately probing for information.

The physical and electronic equivalent of ‘need to know’ is ‘role-based access’, which limits an employee’s access according to their role. Physical access can be restricted to physical zones, filing systems, cupboards and IT server or storage areas. Computer access can be restricted to different IT systems, file areas and datasets.

If using a role-based access system, it is important to review and amend access rights regularly, particularly if an employee’s role changes or they move to a different department or leave the organisation (see [Exit procedures](#)).

Security passes

Many organisations within the national infrastructure will encourage staff to wear security passes, which also permit entry to their premises. If this is the case there should be no exceptions, even for senior management, security staff or visitors. Furthermore, employees should be encouraged to challenge any individual who is not displaying an appropriate pass (see [Security culture](#)). It may also be useful to test the system periodically, to ensure staff without passes or with inappropriate passes are challenged.

If passes are used to distinguish between different levels of employee clearance or access it may be worth considering how easily these can be identified. One option is to colour code each pass according to the access rights of the holder. Another is to vary the orientation of the pass between landscape and portrait, or to use a distinctive border to distinguish one employee group from another. It is helpful if the pass colour is visible from both sides.



An organisation working across a range of different sites should try to ensure that the pass system is consistent throughout. If there are differences from site to site this may cause confusion and, in a worst case scenario, may lead to a security breach where an employee is given an inappropriate level of access.

A pass also requires indication of its rightful ownership. This will often be a photograph of the employee. However, it may be appropriate to print an employee's name instead of or in addition to a photograph. Nevertheless, it is important to ensure that the information included on the pass would not present a security risk to the individual or organisation should it be lost or stolen. If an organisation chooses to use 'anonymous' passes, a freepost PO Box address can be printed on the reverse for the return of lost passes.

If photographs are used, their quality is important. Using the passport photograph regulations should help to ensure clarity but employees should renew their pass photograph every five years or sooner if their appearance changes markedly. Nevertheless, research has demonstrated that people are not able to accurately identify unfamiliar individuals from a pass photograph alone³. Therefore additional information, such as name, PIN or password, should be requested and verified before access is permitted.

Issuing passes

There should be safeguards in place to prevent any employee from fraudulently obtaining a pass on behalf of a third party. These are easier to manage if pass issue is controlled from a central location. Possible safeguards include:

- Confirm identity with document verification check before issuing pass to new employee.
- Require dual authorisation from HR and Security managers before issuing any pass.
- Restrict the physical production of passes, so that no individual can bypass the authorisation process.

In addition to safeguarding the issue of passes it is important to have a policy that governs the loss or theft of a pass. This should include a reporting mechanism, which an organisation may wish to be available even out of office hours, depending on the risk posed. Once the loss has been reported there should be a system to immediately remove any electronic access that the pass provides. In some circumstances disciplinary action may be appropriate in line with existing organisational policy.

Employees should also be held accountable for inappropriate pass usage. Organisations may require staff to sign for their pass at the outset of their employment and terms and conditions of use may include, for example, not sharing it with any third party and storing it securely when not in use. It is also important to retrieve passes from individuals on their departure from the organisation (see [Exit procedures](#)).

³ Kemp, R., Towell, N. & Pike, G. (1997). When Seeing should not be Believing: Photographs, Credit Cards and Fraud. *Applied Cognitive Psychology*. 11, 3, 187–278. Abstract available at <http://www3.interscience.wiley.com/journal/11942/abstract>

Setting an expiry date for passes, after which time any electronic function ceases to work, provides additional protection. This may be particularly useful for temporary staff and contractors, who would need to re-apply if their contract was extended.

Zoned pass access

Within any organisation there may be a range of sites or areas holding various degrees of sensitive material. While some staff may require access to all of these areas others will not, and it may be helpful to restrict the access of employees to only those areas required by their role.

A zoned access system can use different coloured passes, so that it is easy to spot someone in the 'wrong' zone, but should also employ controls which will physically prevent employees with insufficient access from entering sensitive areas. Systems which will electronically flag any unauthorised attempt to gain entry may also be beneficial.

Entry to an organisation or a particular zoned area can be controlled in a number of different ways. Each system has its own strengths and weaknesses and offers differing levels of protection against unauthorised access. The level of security chosen should be proportionate to the nature of the threat faced by an organisation or risk and damage associated with the loss of assets held therein.

Pass use audits

Using an electronic swipe system can provide useful data regarding employee entry and exit patterns. It may be possible for the system to flag any attempted passback manoeuvre (where an employee swipes in and then hands their pass to a third party to gain entry) or if an employee tries to access the premises outside normal office hours (see [Monitoring employee access](#)). Such a system could also be set up to restrict access outside normal office hours.

From a health and safety viewpoint this kind of system provides valuable information regarding personnel present within the premises at any given time. However, it is important that such a system works properly so that alarms are taken seriously and not just discounted as a system error.

Biometric verification



Biometric data refers to any physiological measurement that can be used to identify an individual, including, for example, iris patterns, finger prints, hand geometry and voice recognition. A common misconception is that this technology is one hundred percent reliable but this is not so and, while biometric verification may provide an additional layer of security, it should not be used in isolation.

An organisation should also consider whether the collection of such personal data is really necessary. Some individuals will object to their personal 'specifications' being held on a security system and this information will also be subject to the data protection act.

Furthermore, it is important to remember that any biometric databank is fundamentally reliant upon genuine initial entries, and safeguards are required to avoid fraudulent applications.

Biometric verification may play an increasingly important role as the technology continues to develop. However, there are alternatives, such as the chip and PIN code, which are less-intrusive and more cost-effective.

Working out of hours

Some organisations may find it useful to restrict employee's access outside normal office hours, particularly to sensitive areas. This will reduce the opportunity of employees, such as the civil servant mentioned in the case study box, to act undetected against organisational interests.

Another option is to use software which forces the shutdown of desktops on any given network at the end of the day, which makes it much easier to detect any PC started up out of hours. Or, alternatively, user accounts can be time limited to prevent logon outside of set hours.

In September 2008, a civil servant was taken to court for fraudulently altering several benefit accounts, creating imaginary twins and triplets to obtain more than £250,000. The employee was reputed to stay late in the office in order to access a computer holding details of tax credit claimants. Investigators found nearly 200 profiles had been altered.

Press reporting, 2008

Visitors

Some organisations may wish to maintain a central record of visitors to any given site (this may also be useful/required from a health and safety perspective). Details provided could include; time and date of visit, the visitor's name, the purpose of their visit and identity of their 'host' employee (who may also be held accountable for the visitor while on site).

Generally, visitor passes should provide only the most basic rights of access to an organisation and their return should be mandatory on exit. Some organisations may wish to issue a limited number of 'executive privilege' passes which allow trusted employees to bring several visitors through an entry system at once. However, these could be easily abused and organisations may wish to restrict their use where possible.

Any prohibited items policy (for example, cameras and mobiles) within an organisation should be emphasised to visitors. It may be appropriate for visitors to leave all such devices at reception, to be held securely until their departure, although this may be hard to enforce without physical screening.

Controlling employee IT access

There is an obvious need to invest in firewalls and anti-virus software to protect IT systems. However such measures may not protect against legitimate employees abusing their IT access, particularly as it is often an individual's computer competence and literacy that dictates access rights, rather than seniority or position. The following provides an overview of managing employee access to IT systems, but is not definitive.

Within most IT systems, it is relatively easy to provide each user with a separate account and password. Setting up the system for individual users has the advantage that electronic access can be individually tailored. Furthermore, some systems are able to record actions which can provide a useful audit trail and can even provide evidence during an investigation (see [Monitoring employee access](#) and [Investigation](#)).

Role-based access

A role-based access policy limits an individual's access rights within an organisation according solely to their functional role (see [Security culture](#)). From an IT perspective, role-based access limits the files or systems which an employee is permitted to view, amend or delete.

Where possible, it is helpful to standardise access rights according to the role right across an organisation, with managers holding responsibility for the authorisation of their employees' access profiles. This assures that access security is consistent throughout the organisation and makes it easier to set up an account for a new employee. Where an employee requires a high level of access (for example, systems administrator) it may be appropriate to adopt other security measures such as increasing their supervision.



Nevertheless, it is equally important to assess and review access rights regularly and particularly when an employee changes jobs or leaves the organisation (see [Exit procedures](#)). An individual's access rights should not be allowed to accumulate unnecessarily over time and, where appropriate, access rights and passwords should be set to expire, for example at the end of a contractor's employment period. Any extension should be applied for in the same fashion as that to obtain initial access.

Network access

There is a danger associated with allowing employees to access other computer networks from their workstations. If these other networks are not protected to the same level, the connection could result in viral infections, data loss or file corruption to either party. Furthermore, whenever two networks connect the potential for insider activity increases.

An organisation should therefore specify which connections can be made and by whom. Any other kind of connection should be blocked by default. Monitoring systems should be set up to capture and report any kind of anomalous behaviour (see [Monitoring employee access](#)).

Consideration should also be given to whether personal devices capable of connecting to a network are permitted within the organisational premises, for example, mobile phones or laptops. However, allowing employees to use such devices at work increases the risk and potential for insider activity. It is important to remember that similar risks also apply to work-issued devices.

Many organisations provide internet access in the workplace, although it may be useful to restrict access to some sites in order to protect the organisation from external attack (and perhaps also in the interest of productivity). Where employees do have a legitimate requirement to view insecure sites 'stand alone' computers (not linked to the organisation's network) could be used. For example, where human resources wish to view details posted on social networking sites as part of the pre-employment screening process.

Controlling the nature and volume of material that employees are able to access or download may help an organisation to avoid contracting computer viruses. Software similar to parental control packages can be used, these create blacklists and white-lists of disallowed or approved sites or use a rule based approach to limit access to certain kinds of sites. Other safeguards include preventing any active or executable programme being run or downloaded, for example Java script. Any persistent attempts to override these constraints should be logged and raised with the system administrator.

Data or equipment removal

Some organisations will wish to control the removal of data from their systems. In extremis this could involve physically disabling the upload/download functions of every computer within an organisation. However, within some organisations, employees have a legitimate requirement to transfer sensitive data from one system to another. One possible solution is to issue such employees with encrypted USB sticks, which require password authentication before they are accepted by the secure system and run virus checks on any content before it can be uploaded. Another option would be to disable all such ports – and instead appoint one key user to be responsible for the import/export of all data to the network.

If an employee requires a laptop, USB stick or other electrical device, this should be uniquely identifiable (for example, with a barcode or serial number) and issued to a specific individual who will remain accountable for it until its return. Such issued items should be audited regularly to ensure they are being used correctly. Each device should be equipped with a sufficient level of encryption for the data held upon it.



If laptops are routinely used within an organisation, it is worth considering the use of anti-theft devices as a deterrent to opportunistic thieves. For example, secure lock attachments are fitted to most computers and can be used to wire laptops or other removable electronic items to a fixed point. However, it should be noted that these devices are only a deterrent and are not robust enough to be used in the absence of any other security measure.

Passwords

The case study below highlights the importance of employees adequately protecting their account passwords, even from colleagues. All employees should adhere to the same level of password security, but the passwords of temporary staff and contractors should expire at the end of their contract period unless an extension has been sought and approved.

Strong passwords or pass phrases should be at least 8 characters long (preferably more) and include a mixture of upper and lower case letters, numbers and characters. Ideally these should be randomised, but could be constituted from a memorable sentence, with characters or numbers substituted for some of the letters.



There are also password practices which should be avoided, such as using an obvious choice like 'password' or an employee's own or partner's name and date of birth. Users should be regularly prompted to change their passwords, but encouraged or prevented from changing back to a previous password or altering only one character. Passwords should not be written down, shared or inputted while a third party is watching.

Screen locks

To avoid unauthorised personnel from hijacking another employee's IT account, all staff should lock their terminals when away from their desks, even for a short time. As an additional safeguard, it may be worth setting up the system to automatically lock any screen which has been inactive for some time. If staff leave the premises completely or are away from their desks for a significant period they should be encouraged to log out of the system.

In 2007 a North American airline fired fifty baggage handlers, having established that these individuals had fraudulently obtained their managers' passwords. These employees had then used these passwords to gain access to a computer system. Once inside this system they had claimed for significant amounts of overtime that they had not actually done.

Press reporting, 2007

To support this further, any terminal which is left locked for a long period should automatically log the user out of the system, preferably saving any work in progress at the same time. However, employees who fail to lock their terminals should be challenged, and organisational policy should set out measures to address persistent neglect in this area.

Resources

- Ferraiolo, D.F. and Kuhn, D.R. (1992). Role Based Access Control. *15th National Computer Security Conference*: 554-563. Article (PDF) available at <http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf>
- International Organisation for Standardization. ISO 27001 sets out industry standards for security. <http://www.iso.org/iso/home.htm>

Monitoring employee access

CPNI research into past insider cases has shown that, in some cases, unauthorised activities could have been identified much earlier had sufficient attention been paid to auditing or protective monitoring systems.

Monitoring can be applied to both physical and electronic activity. A personnel security risk assessment should be used to ensure that it is implemented in proportion to the risk facing the organisation. See CPNI guidance [Risk assessment for personnel security: a guide](#) for more information.

Monitoring across networks

Most IT networks can be configured so that every event that takes place – a user accessing a database file, for example – generates an entry in a log. The entry will typically include the user name or identifier, the date, time and other details relating to the event. Log entries can be generated by many network components such as domain controllers, workstations, web and application servers and boundary protection components such as firewalls. An entry can be recorded in the log even for failed events such as an unsuccessful attempt to open a file.



Although it is more common for electronic information systems to be monitored, consideration should also be given to monitoring the organisation's network of physical access controls such as swipe cards and door PIN codes, so that attempts by employees to enter secure areas do not go unnoticed. Many physical access devices can be programmed to record event data, resulting in event logs similar to those generated by IT system components.

In order to detect breaches of the organisation's access policies, the data recorded in the logs needs to be analysed for signs of unauthorised activity. This might take the form of a single event, such as a rejected swipe card at a secure door, or patterns of events generated by different network components that, taken together, appear similar to patterns that have denoted unauthorised activity in the past. For example, detecting the unauthorised removal of data from an organisation's database might require an examination of the logs from the database, the firewall and the email system. An effective monitoring process may therefore need to combine the logs of different network components.

The analysis may be carried out in real time or offline and, ideally, identify trends over time, producing an alert when it detects a systematic effort to penetrate the organisation's access controls.

Monitoring of single channels

Although the monitoring of events across an organisation's IT network can help to detect complex insider activity, certain channels will also benefit from monitoring in isolation.

- **Internet** use can be monitored to detect attempts by employees to access inappropriate websites and in this context is likely to include sites encouraging radicalisation, for example.
- **Email** facilities could also be monitored and restricted in order to reduce the risk of insider activity. This could take a variety of forms, including:
 - Filtering of outgoing mail and attachments for words denoting sensitive contents, such as 'confidential' or 'secret', and other terms that might indicate a leak of policy or the transmission of commercial data, for example (but be aware that content filtering of emails is not legal in all countries).
 - Blocking the option to open email attachments, in order to reduce the risk of an employee introducing malicious software into the organisation's network.
- **Telephone** details such as the numbers dialled and the duration of calls, but could also extend to the recording of telephone conversations, as is common in call centres. Most organisational telephone networks allow certain telephone numbers (or categories of number) to be barred, a facility often used to contain costs but one that might also help to limit the leak of information, if this is a concern in the organisation.
- **Video telecommunication** equipment is often not monitored at all, which is partly due to the unmanageable volume of data that any such system would accumulate. Without any restriction, such equipment may be misused by staff and it may be useful to control access using a PIN code or locking system.

Monitoring using closed-circuit television (CCTV)



Closed-circuit television is the use of video cameras to transmit a signal to a specific place or a limited set of screens. Depending on the sensitivity of the area under surveillance CCTV may be used in isolation or to support other protective security solutions, such as a secure door that is vulnerable to tailgating.

It is generally thought that the presence of visible CCTV cameras is a deterrent, and obvious targets for CCTV monitoring will be those areas which have already proved to be hotspots for incidents, where particularly sensitive information is stored or where insider activity is suspected but not proven.

The automated interpretation of CCTV images is a developing science and for the time being human observation is still the most reliable method for identifying unauthorised activity in the images captured by CCTV. In an organisation where large numbers of cameras are operating constantly, it would be very resource intensive to monitor CCTV footage constantly, although this may be appropriate if the impact of such an act would be high. Where the risk or impact of insider activity is low, footage may simply be stored, unmonitored, in case it is needed for evidence in the wake of an incident. Most organisations will need to find a practical balance between the two and a personnel security risk assessment will guide this decision.

Monitoring by other means

Not all protective monitoring needs to be carried out electronically. Routine or ad hoc inspection of the workplace by security teams, either during the working day or out of hours, can be useful in identifying factors that might provide opportunities for insider activity, such as:

- Security passes not being worn
- Doors to secure areas left or held open
- Failure to observe a clear desk policy
- Unlocked drawers, key cupboards or safes
- Unattended computers or laptops with users logged in
- The use of removable media such as CD ROMs and USB sticks
- Uncollected papers left on printers

Regular audits of your security systems will help to ensure that adherence is satisfactory and may also facilitate the detection of insider activity. Such checks should not be conducted in isolation, but form part of a wider and ongoing process of assessment and review.

General considerations

Only in rare cases should individuals be monitored covertly (see [Investigation](#)). Even when protective monitoring is overt it can still damage the set of mutual beliefs, perceptions and informal obligations between an employer and employee – the implied duty of trust and confidence sometimes referred to as the ‘psychological contract’ (see CIPD factsheet in the Resources section at the end of this chapter). Employees may feel that restrictions on their use of the internet while at work, or the introduction of CCTV cameras on their site, is evidence that they are not trusted to act responsibly or securely.



Trades unions may also be unhappy to see their members subject to ‘unfair or disproportionate’ monitoring and this could lead to a worsening of industrial relations. These effects can be greatly mitigated by using protective monitoring only where it is clearly justified by the risk and by fostering a culture in which employees and unions understand the rationale for the organisation’s security measures (see [Controlling employee access](#)).

All monitoring systems are likely to produce ‘false positives’ - alerts where no suspicious activity exists. The extent to which the system can be fine-tuned to avoid these will vary from network to network. An employee who regularly mistypes their password might be ignored or might be cause for concern, depending on the nature of the organisation and the sensitivity of its assets. Given that insider activity can take many different forms, alerts should be manually reviewed by somebody who has a good understanding of normal access behaviour.

Conversely, there is also a risk of 'false negatives'. For example, the opening of a restricted file or a secure door by a user name or identifier with the appropriate access privileges will not trigger suspicions as an entry in an event log; yet it is possible that the employee using the unique identifier may not be the person to whom it was issued. Monitoring will only produce useful results in organisations where the likelihood of employees sharing passes, passwords, PINs and other secure access mechanisms is low (see [Security culture](#)).

The frequency of event log analysis is a matter of judgement, depending on the nature of the organisation and the environment in which it operates. Due to the large amounts of data involved, the analysis can be very resource intensive and so is often carried out offline rather than in real time, even though this means that unauthorised activity can only be detected after the event. Generally, the more reliance an organisation places on monitoring, the more frequently the analysis should take place. In an organisation with many other ongoing personnel security measures in place, the dependence upon monitoring can be reduced and the analyses less frequent.

Arrangements must be made for the storage – sometimes over a considerable period – and efficient retrieval of the data generated by monitoring. Depending on the quantity of data involved, a balance may have to be struck between the desired length of audit trail and the cost of storage. This will depend on the nature of the organisation and the types of activity being monitored, but a risk assessment can prioritise the personnel risks facing the organisation and, by extension, identify the key targets for monitoring, such as specific entrances and exits, physical locations, IT applications or transaction types. This will keep the data collected to a minimum.

For monitoring to be an effective tool in minimising the risk of unauthorised activity, each user needs to have a unique identity such as a user-id and password for systems access or a swipe card and PIN for physical access. The event logs must be stored securely so that they cannot be tampered with, so that their validity cannot be questioned in a court of law, and the clocks in all monitoring devices should be synchronised to ensure that data captured can be cross referenced in an investigation.

The introduction of any form of monitoring practices must be accompanied by an explanation to employees that this is taking effect. This may take the form of staff training, information in staff handbooks or an Intranet or perhaps some kind of warning when people log onto their computers. Having these in place makes it difficult for employees who have committed an offence to complain that they did not know that should not have been doing something or have been unfairly victimised.

Legal considerations

The use of protective monitoring raises a number of legal issues that need to be addressed, resolved and then embedded in the procedures governing protective monitoring in the organisation. The most relevant legislation includes:

- **The Data Protection Act 1998 (DPA)**

Almost all forms of monitoring will involve the collection of personal data. The DPA places responsibilities on organisations to ensure that such personal data is collected lawfully and processed in a fair and proper way.



- **Human Rights Act 1998**

Article 8 of the Act provides for the right to respect for private and family life. Individuals' Article 8 rights extend to the workplace.

- **The Regulation of Investigatory Powers Act 2000 (RIPA)**

RIPA regulates the use of intrusive surveillance and investigation techniques, including the interception of communications.

- **The Employment Practices Data Protection Code**

The Code is issued by the Information Commissioner and is intended to help employers comply with the Data Protection Act, and to encourage them to adopt good practice. Part 3 of the Code addresses monitoring in the workplace.

- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

These regulations provide for certain circumstances in which intrusive techniques such as the interception of communications can be used in the business context.

- **CCTV code of practice (revised edition 2008)**

This code is issued by the Information Commissioner and helps organisations to comply with the law when using closed-circuit television to carry out monitoring.

This list is not exhaustive and it is vital that any organisation wishing to implement protective monitoring seeks legal advice first.

Resources

- CIPD psychological contract factsheet:

<http://www.cipd.co.uk/subjects/empreltns/psycntrct/psycontr.htm>

Detailed guidance for protective monitoring (correlations, IP address resolution, limitations of log analysis, attack patterns) and examining audit and accounting logs is available from the CPNI website:

- www.cpni.gov.uk/Docs/re-20030324-00723.pdf: *An Introduction to Audit and Accounting Log Analysis. This document is a little out of date now but the principles remain valid.*

Other material relating to monitoring of employee activity can be found in the [Resources](#) section of the [Investigation](#) chapter.

Investigation

When the actions of a member of staff have been reported as a potential security concern the next step might be to launch a formal investigation. However, there are legal and resource implications to consider, and ensuring that the process is both impartial and proportionate is vital to protect the organisation's integrity and future relations with its staff.

In terms of personnel security, an investigation may take place in response to a report of an unauthorised act such as theft or the leak of sensitive information, or as a result of concerns about an employee's behaviour (see [Screening for the insider threat](#)). In the former, the purpose of the investigation will be to establish who has done what. In the latter, it is whether the individual represents an increased security risk. In both cases the output from the investigation should include a recommended course of action.



The information that prompts an investigation can arrive from various sources, such as:

- Automated warnings from physical or electronic protective monitoring systems.
- Alerts received from within the organisation, possibly via the organisation's reporting hotline or line manager's concerns.
- Evidence emerging that an unauthorised act has taken place.

When an incident or suspicion is reported a decision will need to be made about whether and how to investigate. Some initial filtering will help to keep the investigation on track and avoid unnecessary workloads. Issues to consider at this stage include:

- **Malicious reporting**

Where an employee has used the organisation's hotline to report an incident or suspicions about a colleague – providing the report is not anonymous – is there any history of antagonism between the two parties?

- **Unlawful discrimination**

Where there is an accusation of wrongdoing, the investigation team must ensure that it is neither more nor less disposed to believe the accusation due to the race, religion, gender, sexual orientation, disability or age of either the employee being reported or of the employee making the accusation.

- **What is 'unauthorised'?**

The definition of an 'unauthorised act' may not be standard across the workforce. Contracts signed by the organisation's full-time, permanent employees may differ from those held by employees inherited following organisational take-overs, or by consultants, contractors or agency workers, many of whom may not have signed agreements covering acceptable use of the internet and email, for example, or read the same policies.

- **A proportionate response**

Depending on the nature and scale of the incident, the time and cost required to investigate may be out of proportion to any loss incurred. Where an incident involves purely financial losses, a threshold (below which an investigation will not be carried out) should be set in order to avoid adding unnecessarily to the investigative workload. However, each case should still be assessed, as many 'low value' incidents may have a cumulatively large impact. An investigation may also sometimes be worthwhile to deter similar offences.

- **Might the 'unauthorised act' amount to a disciplinary offence?**

Depending on the nature of the unauthorised act, it may amount to a disciplinary offence under the organisation's disciplinary policy. In these circumstances, any investigation should adhere to the requirements set out in both the organisation's disciplinary policy and the Statutory Dispute Resolution Procedures.

Roles

Once it has been established that an investigation is necessary, a lead investigator should be identified. Their role is to carry out the investigation thoroughly and fairly, on a scale that is in proportion to the incident or suspicion. They should possess a sound working knowledge of the current legislation, regulation, codes of practice and guidelines relating to investigations and, ideally, experience of a broad range of investigative techniques.

Depending on the size and structure of the organisation, the role of lead investigator may be assigned to a senior manager, a senior member of the Human Resources or Security teams, a full-time investigations manager or even somebody from outside the organisation.

Initial discussions between the investigations team and other parties such as Human Resources, senior management and line managers may need to take place before an investigation plan can be agreed. If employees are to be reassured about the integrity of the process, and in order to limit negative impact on morale, the investigation must be carried out promptly and in line with the organisation's published procedures and, where appropriate, with visible consequences for proven wrongdoing.

Key decisions

Running the investigation overtly or covertly

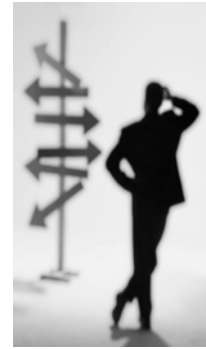
Where an employee is under suspicion, the nature of the incident will dictate whether they should be made aware of the investigation or not. A number of factors will influence whether an investigation needs to be carried out covertly, including (but not limited to):

- Whether a suspicion or incident has been reported, and the varying degrees of additional evidence gathering each of these types of report will normally require.
- Whether the incident concerns some kind of sustained or continuing unauthorised act that needs to be monitored without alerting the perpetrator.
- Whether the investigation concerns a planned unauthorised act that has yet to take place.
- The nature of the incident or suspicion.

Who should be involved?

Depending on the nature of the case, the lead investigator may need to make certain people or business areas aware that an investigation is to take place and engage them in the process as appropriate. These may include:

- Human resources
- Line management and colleagues
- Senior or executive management
- Press office
- Specialist investigators
- Legal advisers
- Police



In order to ensure impartiality, it is important to ensure that anybody involved, or suspected of involvement, in the unauthorised act is not also involved in the investigation. It is possible, for example, that an employee and his or her line manager are suspected of collusion. In which case the next most senior line manager, or other suitable alternative, should be consulted instead.

Should an employee under investigation be suspended?

As with all matters affecting employees, this decision should be made in consultation with Human Resources and an employment lawyer and will depend entirely on the circumstances. If there is a chance that evidence may be removed or tampered with before the investigation team can access it, for example, then suspension may be necessary. On the other hand, it may be more desirable to simply restrict that employee's access to the assets or evidence in question or to move them into another role for the duration of the investigation.

Evidence

There are many ways to gather evidence, any combination of which might be appropriate according to the incident or suspicion being investigated. For example:

- Interviewing witnesses
- Overt or covert surveillance of parties involved (although covert surveillance should only be used in extreme circumstances)
- Forensic examination of office equipment used by the employee
- Forensic examination of equipment in the employee's home
- Examination of audit trails created by the organisation's protective monitoring processes
- Examination of telephone call logs, both mobile and landline
- Reviewing CCTV footage
- Reviewing the employee's use of company credit cards

When gathering evidence, organisations should consider their legal obligations (see [Appendix 3](#) for an overview of these), particularly with regard to the following legislation⁴:

- **The Human Rights Act 1998**

In particular, organisations should bear in mind the importance of respecting employees' Article 8 right to private and family life. Organisations conducting an investigation which may involve the collection of information relating to an employee's private life should ensure that any resultant infringement of the right to privacy can be justified. This means that the amount and extent of evidence collected should be both necessary and proportionate in the context of the type of investigation being carried out and the nature of the incident or suspicion.

- **The Data Protection Act 1998 (DPA)**

The DPA regulates the way in which personal data (including that which is collected in the course of an investigation) can be gathered, retained, stored and destroyed. For example, the DPA allows person data obtained during an investigation to be retained for as long as is necessary for the purposes of that investigation. The organisation would need to be able to justify, by reference to the nature of the incident or suspicion or the likelihood of appeal, for example, why continued retention of the data is necessary. Information collected for the purposes of an investigation should normally be held for the duration of the investigation plus any time allowed afterwards for internal and/ or legal challenges.

- **The Regulation of Investigatory Powers Act 2000 (RIPA)**

RIPA legislates for using certain methods of surveillance and information gathering (for example, the interception of telephone calls or emails, and covert surveillance). It sets out legal requirements which must be followed if these types of methods are to be employed in an investigation.

Organisations should also give thought to storing evidence in a way which guarantees its integrity both for the duration of the investigation and for any additional time allowed for appeals and legal challenges after the investigation has concluded. For example, evidence should be kept securely in order to prevent possible tampering.

Subject to the considerations above, it is good practice to gather as much evidence as possible indirectly through these and other similar methods, encouraging witnesses to come forward where possible, before carrying out a more direct assessment in the form of a face-to-face interview with the employee under suspicion. This should help to ensure that the fairest outcome is reached. However, due to the range of legal considerations, legal advice should always be sought on the proposed methods, and extent, of any evidence gathering.

Monitoring

Monitoring is where an organisation carries out systematic or occasional checks on the behaviour of all, or some, of its employees. During an investigation, many of the methods of evidence gathering available to an organisation, such as opening an employee's emails, checking telephone logs and checking logs of websites visited by an employee, will amount to monitoring.



⁴ Links to this legislation can be found in the Resources section at the end of this chapter.

Although some of this is covered in [Monitoring employee access](#), there are particular issues to bear in mind in the context of an investigation, and the advice of a specialist in employment law is essential.

Whenever any form of monitoring is proposed as part of an investigation, organisations should have regard to section 3 of the Employment Practices Code which is issued by the Information Commissioner. The Code sets out recommendations in order to help organisations comply with the law when carrying out monitoring. For example, unless exceptional circumstances apply, employees should be made aware that they may be monitored.

While the Code states that consent is not a prerequisite in order to carry out such monitoring, employees should, in all but the most extreme circumstances, be told how they may be monitored and how the information obtained from the monitoring may be used. Covert monitoring is only likely to be justified where the organisation has good reasons to suspect a criminal offence or other offence of a similar seriousness. The employment contract may include clauses informing employees about certain types of monitoring (for example, of internet and email use). In addition, employees can be informed of monitoring via an organisation's HR policies or via staff circulars.

As an alternative, an organisation might instigate low-level observation of a suspect individual and those of his or her colleagues with similar levels of access, in order to inform suspicions and justify the use of more intrusive measures at a later stage in the investigation.

The code also states that before commencing any monitoring, an organisation should carry out an impact assessment in order to ascertain whether the benefits which are likely to arise from the monitoring outweigh the level of intrusion into the privacy of the individual. The Code sets out relevant considerations to take into account when carrying out an impact assessment. Ideally, the process of carrying out an impact assessment should be documented.

Possible outcomes

It may be that an apparently malicious act has an entirely innocent explanation, so an employee under suspicion should be given the opportunity to explain their actions. During an interview, the employee should be allowed to have one other person of their choosing – a colleague, a union representative or simply a friend from within the organisation – to accompany them. An impartial observer, usually from Human Resources, should also be present and a detailed record of the proceedings should be kept in all cases.



In reporting the findings from the investigation, the lead investigator should agree a suitable course of action with the investigation's management sponsor. This may be straightforward, ranging from no further action where the employee is found to be innocent of an accusation, through to dismissal, if appropriate (see [Exit procedures](#)). Many other outcomes are also possible, such as:

- Notifying the appropriate authorities (such as the Police or Security Service).
- Developing an individual rehabilitation plan by which the employee can eventually regain the organisation's trust.

- Transferring the individual to a role with different levels of access, or access to different organisational assets to prevent a recurrence).
- Implementing additional levels of either human supervision (such as dual controls) or electronic supervision (such as CCTV) for the individual or department.
- Restricting individual or group access to the workplace outside core hours.
- Routine encryption of sensitive data.
- Introducing additional layers of authentication on key IT systems.
- Amending the organisation's policies and procedures where necessary in order to reduce the risk of the incident recurring.

The investigation sponsor should be aware of any legal implications and other possible consequences of the actions agreed upon and should always take advice from legal and HR specialists. The way in which the recommendations are implemented will depend on who is affected and what needs to be changed, but Human Resources and the organisation's physical, IT and personnel security departments are among those most likely to be involved.

The final step in an investigation should be to update the organisation's central record of investigations to ensure that any learning points are used to enhance the organisation's personnel security measures in the future.

Resources

- http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 The Data Protection Act from the Office of Public Sector Information
- http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1 The Human Rights Act 1998 from the Office of Public Sector Information
- http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1 The Regulation of Investigatory Powers Act 2000 (RIPA)
- http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/about_the_code.html: The Employment Practices Data Protection Code from the Information Commissioner's Office
- http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practice_code_-_supplementary_guidance.pdf: The Employment Practices Data Protection Code supplementary guidance from the Information Commissioner's Office
- <http://www.opsi.gov.uk/si/si2000/20002699.htm>: The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctv_fi_nal_2301.pdf: The CCTV code of practice (Revised edition 2008) from the Information Commissioner's Office
- <http://www.w3.org>: World Wide Web Consortium, promoting standards relating to event logging.

Other material relating to the monitoring of employee activity can be found in the [Resources](#) section of the [Monitoring employee access](#) chapter.

Exit procedures

Employees leaving an organisation take considerable knowledge about operations, assets and security vulnerabilities with them - possibly to a competitor – and the circumstances surrounding a departure are not always amicable. A formal, thorough procedure for all staff departures will ensure the appropriate actions are taken to protect the organisation without unduly disrupting the employer-employee relationship.

The case of Vitek Boden (see box below) demonstrates the damage which can be caused by an ex-employee if an organisation fails to take appropriate steps (be these physical, information or personnel security measures and procedures) to prevent them from abusing their knowledge and access privileges.

The opportunity an employee will have to act maliciously after leaving an organisation will differ according to their role and the exit procedures should take this into account. For example, when a member of the administrative support team leaves, the combination for each secure cabinet should be changed and their IT account terminated, and when an IT systems administrator departs, all of their privileged IT access rights should be removed and any generic passwords remote access codes changed.

In November 2001, Vitek Boden was sentenced to two years in prison for releasing up to one million litres of sewage into a river and the coastal waters of Maroochydore in Queensland, Australia.

Boden had previously worked on the Maroochydore water project as a consultant but had been refused a full-time job by the Maroochy Shire government. He used the internet, a wireless radio, stolen control software and his inside knowledge to carry out the attack.

Press reporting, 2001



An organisation may utilise a comprehensive exit checklist for every departing member of staff. However, it might be more efficient, particularly in large organisations, to establish a variety of role-based exit procedures, with an emphasis on any high-risk staff groups. (These should be known if an organisation has conducted a personnel security risk assessment as described in [Risk assessment for personnel security: a guide](#)).

Protecting the organisation

If someone leaves an organisation feeling badly treated, ignored or unappreciated, they may be less restrained about what they say and may not feel guilty about damaging the organisation or giving away company information. It is perhaps too much to expect former employees to remain loyal to an organisation, but with the right handling and aftercare their propensity to be disloyal can be limited.

As soon as a line manager becomes aware that an employee is leaving an organisation, they should, in consultation with Human Resources if appropriate, assess and where necessary manage the risk that this individual may pose in leaving the organisation. This will be influenced by a number of factors:

- Whether the employee is leaving voluntarily or as the result of a disciplinary process or redundancy
- If they are not leaving voluntarily, the reason for their dismissal
- Whom they are going to work for next (for example, a competitor)
- Their current role and the sensitivity of the organisational assets they have access to

Having assessed the risk, the organisation needs to determine the best next course of action. Broadly, and depending on the employee's contract, the options are likely to include:

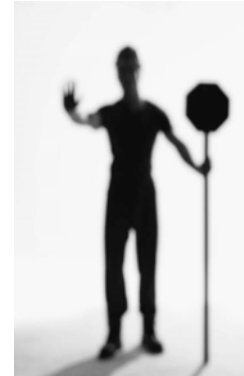
- Allowing the employee to carry on working during their contractual notice period, retaining all their usual access to the organisation's assets.
- Allowing the employee to work their contractual notice period but with reduced access to assets (for example, using additional supervision or by allocating lower-level IT access).
- Asking the employee to leave immediately – possibly under supervision to prevent any unauthorised act while still on the premises – and not to return for the duration of their notice period (this is sometimes referred to as placing the employee on 'gardening leave').

The fact that an employee is leaving voluntarily may not necessarily mean that they can be allowed to continue working unsupervised for their notice period. If they are known to be leaving to work for a competitor, for example, it may be appropriate to remove their access to commercially valuable information. If they are employed in an extremely sensitive position then it may be necessary to ask them to leave immediately, although this is likely to cause ill-feeling and should be used with caution.

Nevertheless, allowing an individual to work their contractual notice period may provide them with an opportunity to abuse their access and damage the organisation. Therefore, in circumstances where there is a risk, but no justification for an immediate exit; the best course of action may be to simply reduce an individual's access and/or introduce additional safeguards for the remainder of their employment.

Once a leaving date has been agreed and regardless of the circumstances of their departure, an employee's opportunity to carry out an unauthorised act will be reduced by their returning all assets, access tools and identifiers which belong to the organisation, such as:

- Uniform(s)
- Security pass(es) and/or identification card(s)
- Mobile/blackberry/pager(s)
- Company credit card(s)
- Any unused personal business card(s)
- Keys to secure/storage areas
- Token(s) for access to electronic system(s)
- Any books, papers or commercially sensitive documentation
- Laptop and any other remote working equipment such as flash drives
- Security containers such as security briefcases



If the employee is leaving immediately, they should be required to return everything within the tightest possible timescales, but if they are expected to continue performing their duties – or a limited subset of them – during their notice period, then the demand will have to be amended accordingly. The main requirement is to recover as many items as possible straight away and not to leave them at the disposal of the employee. For items not recovered at this stage, a date and a method for their return (in person or by post, for example) should be agreed with the employee.

Simultaneously with the recovery of assets, the organisation should consider additional steps to reduce the employee's access to assets, including:

- Selectively or completely blocking the employee's user-ids to prevent systems access
- Changing passwords to common systems
- Making sure that measures are in place to protect the organisation's electronic systems from malware or hacking (see [Monitoring employee access](#))
- Selectively or completely blocking the employee's security pass to prevent physical access
- Changing door codes to common areas
- Changing combinations to storage areas, where the value of the assets merits it
- Cancelling the employees signature authority, credit card and expense accounts and ensuring that all relevant parties are notified
- Where necessary, issuing instructions to security guards regarding the employee's future access to the premises

Some of these measures will have to be delayed if the employee is not leaving immediately, in which case the outstanding items should be diarised and implemented as soon as is practical.

The exit interview

Exit interviews generally focus on Human Resources issues such as the reasons for leaving and attitudes towards the organisation. As a result they are often viewed as having little connection with security but they do offer a useful last opportunity to remind the employee of their security-related obligations and to tie up any loose ends.

When an employee is leaving as a result of a disciplinary outcome the final disciplinary session and the exit interview are likely to be the same meeting. In other cases the employee's line manager and Human Resources manager should be expected to arrange the exit interview, although depending on the circumstances the meeting may be more open and informative if the line manager is not present. A security manager should either attend the meeting or provide advice on how to handle the security issues.

There are different views about the best timing of the interview but this should be largely driven by the personnel security issues; where the risk is high, the interview should be arranged promptly, to make sure that the employee is aware of their security responsibilities at the very start of their notice period.



The exit interview is an opportunity to:

- Remind the employee of their obligations under the Official Secrets Act (where appropriate) and organisational codes of conduct concerning access to assets and intellectual property, for example. Some organisations ask the employee to read and sign a form summarising these points, which may help to focus the mind of the law-abiding employee even if it is unlikely to have an effect on the determined insider.
- Obtain – in order to change if necessary – all passwords or encryption keys for files the employee has been working on.
- Recover as many of the organisational assets, access tools and identifiers as is reasonable at the time.
- Ask the employee if they have any comments/observations about the strength (or weakness) of the security culture, measures and procedures in place within the organisation.

Where an employee is leaving the organisation following the implementation of new or more stringent ongoing personnel security measures which they have failed to meet, it may be appropriate during the exit interview to ask them to sign a compromise agreement, which usually provides the employee with a severance payment in return for agreeing not to pursue any claim to an employment tribunal at a later date. The employee will need to take legal advice (which the organisation may consider paying for) before signing such an agreement, and the employee's legal adviser will have to sign it as well, to show that this has been done. Nevertheless, a compromise agreement could protect the organisation from litigation if the employee later feels that they have been discriminated against as a result of the organisation's ongoing personnel security regime.

Complex situations



Exit procedures are often written with the assumption that the employee is based in a head office or main centre of operations. In more dispersed organisations, the procedures should be carefully drafted to ensure that they can be applied to employees who are not in the same building as their line manager or Human Resources department at the time of leaving. This would include employees:

- Working from home or at other (possibly third party) sites, including overseas
- On paid leave pending an investigation
- On sick leave
- On maternity leave

Where possible, the same procedures should also be implemented when an employee dies in service, as similar risks may exist with the misuse of their former access and/or organisational assets (for example, many of the same items will need to be recovered and access rights revoked). However, in these circumstances it is important that the procedures allow due sensitivity.

Handling resignations

Where an employee decides to resign, and regardless of how important the person is or however critical he or she is to the organisation's work, the principles of handling their departure should be the same:

- An expression of genuine (if appropriate) regret.
- Check conditions of employment and respond to any requests for exceptions with sympathy and where possible flexibility.
- Ask and listen to their reasons for leaving, particularly to any comment on how the organisation might have been responsible for their decision.
- Make time to be with them for their last few hours in the office.
- Make best use of the exit questionnaire and interview.
- Where possible/appropriate, maintain contact after they leave and ensure they feel welcome if they return to visit colleagues.

In some situations, organisations may consider employing someone specifically to help employees who are considering leaving or facing redundancy to find new jobs. The value of this strategy may well outweigh the cost of employing them. The advantages are: employees leaving feel the company is still interested in them; the company can influence where ex-employees go when they leave and therefore deter them from going to the opposition; the outplacement agency/individual can maintain contact with those leaving and organise any further contacts.

Employee references

When an employee has left the organisation as a result of the disciplinary process, it is important to consider how future requests for references will be handled and to advise the department most likely to receive them. Increasingly, as a general policy to reduce the risk of litigation, Human Resources managers are willing to confirm only the most factual details about an individual's former employment – the dates during which they worked for the organisation and their job title is most common.

While references must not be misleading, omission is not illegal so it is not necessary to reveal the circumstances of the employee's departure if it is felt that nobody would benefit from the disclosure. Similarly, stating facts (rather than opinions) when giving references will not expose the organisation to a risk of litigation, so it is acceptable to say that an employee resigned while under investigation or was dismissed following a disciplinary process. If there is any doubt about what should or should not be included in a reference, an employment lawyer should be consulted.

Glossary

Asset

Anything that is of value to the organisation, including people, premises, hardware, customer or commercial data, intellectual property, money and reputation.

Disaffected employee

An individual within an organisation who is disillusioned or disgruntled and takes action that has a security implication.

Employee

Anybody who is granted regular access to the organisation's **assets**, from the CEO to the most junior newcomer. Includes permanent staff, temps, contractors and consultants.

Insider

Any **employee** (see above) who exploits, or may exploit, their legitimate access to an organisation's assets for **unauthorised purposes**.

Insider activity

The exploitation by an **insider** of their legitimate access to the organisation's **assets** for **unauthorised purposes**.

Passback

This describes a procedure where an individual hands their pass to the person behind them, so that both can gain entry to a restricted area.

Psychological contract

The mutual beliefs, perceptions and informal obligations between an employer and **employee**, which set the dynamics for the relationship and define the detailed practicality of the work to be done. It can be formally and consciously acknowledged or informal and implicitly assumed.

Remote assessment

The measurement of human characteristics and behaviours by means other than direct face to face verbal interviewing.

Role-based access

Role-based access is a principle whereby access is solely determined by those systems and assets required in order for an **employee** to complete their work. Role-based access can be applied to technological or physical **assets**.

Tailgating

Gaining unauthorised access to a secure area by following closely behind someone who has authorised access, and entering before the door has closed behind them.

Unauthorised activity or unauthorised purposes

Any activity that is in contravention of the organisation's written procedures or cultural stance.

Appendix 1: Full list of resources

Security culture

- Chartered Institute of Personnel and Development (CIPD) factsheet on performance management: <http://www.cipd.co.uk/subjects/perfmangmt/general/perfman.htm>
- Chartered Institute of Personnel and Development (CIPD) psychological contract factsheet: <http://www.cipd.co.uk/subjects/empreltns/psycntrct/psycontr.htm>

Line management

- The role of frontline managers in HR - Chartered Institute of Personnel and Development (CIPD) factsheet (2009):
<http://www.cipd.co.uk/subjects/maneco/general/rolefrntlinemngers.htm?IsSrchRes=1>
- Line management behaviour and stress at work: Updated guidance for line managers
[http://www.cipd.co.uk/NR/rdonlyres/898B09D3-6F8A-49AF-BD11-66EC76B086D4/0/stress at work updated guidance for line managers.pdf](http://www.cipd.co.uk/NR/rdonlyres/898B09D3-6F8A-49AF-BD11-66EC76B086D4/0/stress%20at%20work%20updated%20guidance%20for%20line%20managers.pdf)
- Employee voice - CIPD factsheet (2010):
<http://www.cipd.co.uk/subjects/empreltns/comconstl/empvoice.htm?IsSrchRes=1>
- Employee communication - CIPD factsheet (2010):
<http://www.cipd.co.uk/subjects/empreltns/comconstl/empcomm.htm?IsSrchRes=1>
- Development planning for individual employees – CIPD factsheet (2008)
<http://www.cipd.co.uk/subjects/lrnanddev/general/devplng.htm>

Reporting hotlines

- CIPD whistle-blowing factsheet: <http://www.cipd.co.uk/subjects/empreltns/whistleblw/whistle.htm>
- www.bsigroup.com/en/Standards-and-Publications/Industry-Sectors/Risk/PAS-19982008-Whistleblowing: This Publicly Available Specification (PAS) sets out good practice for the introduction, revision, operation and review of effective hotline arrangements.
- http://www.export.gov/safeharbor/SH_Overview.asp Safe Harbor [sic] provides a way for US companies to avoid interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws.
- Anti-bribery legislation: <http://www.justice.gov.uk/publications/bribery-bill.htm>

Controlling employee IT access

- Ferraiolo, D.F. and Kuhn, D.R. (1992). Role Based Access Control. *15th National Computer Security Conference*: 554-563. Article (PDF) available at
<http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf>
- International Organisation for Standardization. ISO 27001 sets out industry standards for security. <http://www.iso.org/iso/home.htm>

Monitoring employee access

- CIPD psychological contract factsheet:
<http://www.cipd.co.uk/subjects/empreltns/psycntrct/psycontr.htm>

Detailed guidance for protective monitoring (correlations, IP address resolution, limitations of log analysis, attack patterns) and examining audit and accounting logs is available from the CPNI website:

- www.cpni.gov.uk/Docs/re-20030324-00723.pdf: *An Introduction to Audit and Accounting Log Analysis. This document is a little out of date now but the principles remain valid.*

Investigation

- http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 The Data Protection Act from the Office of Public Sector Information
- http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1 The Human Rights Act 1998 from the Office of Public Sector Information
- http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1 The Regulation of Investigatory Powers Act 2000 (RIPA)
- http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/about_the_code.html: The Employment Practices Data Protection Code from the Information Commissioner's Office
- http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practice_code_-_supplementary_guidance.pdf: The Employment Practices Data Protection Code supplementary guidance from the Information Commissioner's Office
- <http://www.opsi.gov.uk/si/si2000/20002699.htm>: The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctv_final_2301.pdf: The CCTV code of practice (Revised edition 2008) from the Information Commissioner's Office
- <http://www.w3.org>: World Wide Web Consortium, promoting standards relating to event logging.

Appendix 2: Generic security appraisal form

Security appraisal forms are often distributed to employees annually, but this should be altered to suit the circumstances of any given organisation. This example provides an idea of the format and topics which may be included; however, organisations are advised to develop a tailored version according to their own requirements.

Security appraisal forms are often managed by the personnel security team or HR department within an organisation, who keep a confidential record of responses and are best placed to review and address any issues that may arise. Part A is completed by the employee and Part B by the employee's manager(s). An organisation should seek legal advice before introducing this kind of system.

PART A: Employee to complete

Subject Details

- Employee's name and staff number
- Period under review
- Date of issue & return

If it is likely that employees may hold more than one position within a reporting period, then the following may be useful.

Position(s) held	Dates (from – to)	Name of manager(s)

Rationale

It is important to include an explanation regarding the purpose of the form. For example, this may be to keep HR files up to date in case of emergency and to ensure that staff are not unduly vulnerable (to coercion or impaired judgement) as a result of changes in their personal circumstances.

It is helpful to reassure staff that all responses will be stored and dealt with confidentially.

ALL INFORMATION WILL BE HELD AND TREATED CONFIDENTIALLY

Personal Circumstances

The level of intrusion into an individual's personal circumstances will depend on the sensitivity of their employment. The examples below may have a bearing on an individual's security profile.

Q1. Have you experienced any changes in your personal circumstances? For example:

- Changes in marital status
- Details of any new co-residents (if not family members)
- Changes in step-parents or siblings
- Involvement in, or approaches by, any political, religious or protest group
- Details of any criminal or civil legal proceedings
- Any new foreign connections acquired during the appraisal period (for example, close friends, foreign partner or relatives)
- Any approaches by journalists or foreigners, or any other persistent or unusual enquiries about your employment.
- Enrolment for external studies or any part-time work undertaken

Personal Issues

In addition to the examples above, there are a number of personal issues which could affect an individual's resilience. If an employer is given early notice of such issues, there is a greater possibility of working to prevent them from becoming a risk to the organisation.

Q2. Have you experienced any serious personal difficulties or major changes to your lifestyle during the review period? For example;

- Ill health
- Legal troubles
- Domestic or marital difficulties
- Recognised addictions (e.g. gambling or alcohol)

Personal Finance

Financial insecurity has been known to catalyse insider activity. Therefore, in some circumstances, it may be advisable to keep track of your employee's financial status. Unexplained wealth could indicate a nefarious source of income, but there may be an innocuous and verifiable explanation. Example questions are given below:

Q3. Has your debt increased or your ability to manage your debt decreased significantly during the review period?

Q4. Have you received, from any sources, sums of money or assets to the value of £5,000 or more during the review period?

ALL INFORMATION WILL BE HELD AND TREATED CONFIDENTIALLY

Employment Concerns

Depending on the nature of an organisation's business, it may be appropriate to enquire whether employees have any moral concerns about the work or activities in which they or their colleagues are involved. Such concerns, if unaddressed, may lead to disaffection.

Example questions include;

- Q5. Do you have any reservations, moral or otherwise, about your work?
- Q6. Are there any causes of anxiety with regard to your work or concerning a colleague?
- Q7. Do you have any security concerns regarding colleagues or security procedures?
-

Employee declaration

I confirm that I understand my responsibility to report any issues or changes in circumstance in line with the questions above. I have completed this form accurately and to the best of my ability.

- Are there any additional issues that you believe HR should be aware of? (Please expand below)
- Would you like to discuss anything further with a member of the personnel security team?

YES NO

(Please delete as appropriate)

Employee signature

Date

It is important to specify where the information provided will be stored and how it will be managed. It will be useful to explain how matters of concern or interest will be addressed and whether employees need take any action. Quite often no further action will be required until the next review.

ALL INFORMATION WILL BE HELD AND TREATED CONFIDENTIALLY

PART B: Manager to complete

This part of the form should be completed by the manager who has supervised the individual for the greatest part of the period under review. However, there should be an opportunity for another manager to contribute if this is thought to be beneficial. It may be useful to remind managers of their responsibility to complete this form as accurately and fully as possible and within an agreed timeframe.

Subject details

- Name and staff number of employee under review
- Period under review
- Name and staff number of manager(s) completing form
- Date of issue & return

For each of the following sections, sufficient room should be provided for responses to be made (managers can be asked to continue on a separate sheet where necessary).

Personal qualities

- Q1. What is your opinion/estimation of the above named employee's current:
- a) Job/career satisfaction (e.g. level of motivation, ethical concerns, feeling that his/her contribution is valued)
 - b) Personality traits/behaviour (e.g. reliability/stability/discretion, ability to cope with pressure, recklessness)
 - c) Interpersonal skills (e.g. How do they get on with work / management colleagues? Are they a team player? Do they respond positively to constructive criticism?)
 - d) Security awareness (e.g. attitude towards personnel, physical and IT security procedures)

Behaviour

- Q2. Have you noticed any changes (for better or worse) in this individual's behaviour, approach to the job or work performance during the period under review?
- Q3. Is there any indication that this individual has serious financial difficulties, or is inexplicably affluent?
- Q4. Is there anything about this individual that worries you, or that could indicate a matter of potential security concern?
- Q5. Is there any indication that this individual might have an alcohol or drugs problem?

ALL INFORMATION WILL BE HELD AND TREATED CONFIDENTIALLY

Current contact

It is useful to gauge the level of contact a manager has with the employee in question. This may provide an insight as to the validity of any opinions expressed.

Q6. Please indicate your current level of interaction with this employee, by circling the most appropriate responses:

- Work contact, normally: DAILY WEEKLY LESS THAN WEEKLY
- Social contact, normally: REGULAR OCCASIONAL NONE

Declaration – Manager

I confirm that I understand my responsibility as a line manager to report any concern regarding this employee. I have completed this form accordingly, to the best of my knowledge.

- Are there any additional issues that you believe HR should be aware of? (Please expand below)
- Would you like to discuss anything further with a member of the personnel security team?

YES NO
(Please delete as appropriate)

Signature Date

Name Position

Countersigning manager

I confirm that I understand my responsibility as countersigning manager to report any concern regarding this employee. I have completed this form accordingly, to the best of my knowledge.

- Are there any additional issues that you believe HR should be aware of? (Please expand below)
- Would you like to discuss anything further with a member of the personnel security team?

YES NO
(Please delete as appropriate)

Signature Date

Name Position

We will contact you if an interview is required.

ALL INFORMATION WILL BE HELD AND TREATED IN CONFIDENCE

Appendix 3: An overview of legal duties

A wide range of legal issues surround personnel security. Legal advice should always be sought to ensure that all measures are legally compliant. The table provides a general description of some of the relevant legislation.

Issue	Relevant legislation	Implications	Further information
Unlawful discrimination Race	<ul style="list-style-type: none"> • Race Relations Act 1976 (as amended) • Race Relations Act (Amendment) Regulations 2003 • EC Race Directive 2000/43/EC 	Organisations must not discriminate on grounds of race, skin colour, nationality or ethnic or national origins	Equality and Human Rights Commission: www.equalityhumanrights.com/our-job/what-we-do/our-business-plan/race-equality/
Gender	<ul style="list-style-type: none"> • Sex Discrimination Act 1975 (as amended) • The Equal Pay Act (1970 as amended) 	Organisations must not discriminate on grounds of gender	Office of Public Sector Information: www.opsi.gov.uk/si/si2003/20031657.htm
Religion	<ul style="list-style-type: none"> • Employment Equality (Religion or Belief) Regulations 2003 	Organisations must not discriminate on grounds of religion or belief	Equality and Human Rights Commission: www.equalityhumanrights.com/our-job/what-we-do/our-business-plan/religion-belief-equality/
Sexual Orientation	<ul style="list-style-type: none"> • Employment Equality (Sexual Orientation) Regulations 2003 	Organisations must not discriminate on grounds of sexual orientation.	Equality and Human Rights Commission: www.equalityhumanrights.com/our-job/what-we-do/our-business-plan/sexual-orientation-equality/
Age	<ul style="list-style-type: none"> • Employment Equality (Age) Regulations 2006 	Organisations must not discriminate on grounds of age	Advisory, Conciliation and Arbitration Service: www.acas.org.uk/index.aspx?articleid=1841
Disability	<ul style="list-style-type: none"> • Disability Discrimination Act 1995 (as amended) 	Organisations must not discriminate against a disabled person. A disability is defined as a physical or mental impairment which has a substantial and long-term effect on a person's ability to carry out normal day-to-day activities	Office of Public Sector Information: www.opsi.gov.uk/acts/acts1995/ukpga_1995_0050_en_1

Issue	Relevant legislation	Implications	Further information
Unfair dismissal – constructive dismissal	<ul style="list-style-type: none"> • Employment Rights Act 1996 	Organisations must not unfairly dismiss an employee. An employee who considered that the actions of their employee have breached the implied duty of mutual trust and confidence may resign and claim constructive unfair dismissal.	Office of Public Sector Information: www.opsi.gov.uk/acts/acts1996/ukpga_19960018_en_1
Criminal History	<ul style="list-style-type: none"> • Rehabilitation of Offenders Act 1974 • Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975. 	Organisations must not take into account certain criminal convictions after the relevant rehabilitation period has elapsed, except in organisations where the 'Exceptions Order' applies	Criminal Records Bureau: www.crb.homeoffice.gov.uk/ Disclosure Scotland: www.disclosurescotland.co.uk
Immigration	<ul style="list-style-type: none"> • Section 8 of the Asylum and Immigration Act 1996. • The Immigration, Asylum and Nationality Act 2006. 	When employing foreign nationals, organisations must ensure that they have appropriate rights to work	The Immigration and Nationality Directorate: www.ind.homeoffice.gov.uk Office of Public Sector Information: www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1996/cukpga_19960049_en_1 www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/2006/cukpga_20060013_en_1
Handling personal information	<ul style="list-style-type: none"> • Data Protection Act 1998 • EU Council Directive 95/46/EC1998 	Data should be: <ul style="list-style-type: none"> • stored securely • accurate, adequate, relevant and not excessive • used only for the intended purpose • deleted after a reasonable period • accessible to the individual 	Information Commissioner's Office: www.ico.gov.uk Office of Public Sector Information: http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm

Issue	Relevant legislation	Implications	Further information
Protective Monitoring and Investigation	<ul style="list-style-type: none"> Human Rights Act (1998) European Convention on Human Rights (1950) 	<p>An organisation must not infringe an individual's:</p> <ul style="list-style-type: none"> right to liberty (Art 5) right to a private life (Art 8) freedom of thought, conscience and religion (Art 9) freedom of expression (Art 10) <p>Organisations must act in accordance with anti-discrimination legislation</p> <ul style="list-style-type: none"> Article 14 of the Human Rights Act (1998) 	<p>Office of Public Sector Information: http://www.opsi.gov.uk/acts/acts1998/19980042.htm</p> <p>Business Link: http://www.businesslink.gov.uk</p> <p>European Convention on Human Rights: http://www.echr.info/</p> <p>Equal opportunities commission: http://www.eoc.org.uk/Default.aspx?page=15498</p>
	<ul style="list-style-type: none"> Lawful Business Practices Regulations 	<p>It is unlawful to intercept communications except with the individual's consent or where the communication is connected with the operation of the communication system itself. However, there are authorised business purposes contained in the Legal Business Practice Regulations which allow interception over a private network.</p>	<p>Office of Public Sector Information: http://www.opsi.gov.uk/si/si2000/20002699.htm</p>
	<ul style="list-style-type: none"> Data Protection Act 1998 (Part 3: Monitoring at work) 	<p>Monitoring of employee activities (e.g. computer usage) must be done in a way which is consistent with the Act.</p>	<p>Information Commissioner's Office: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi/html/english/employment_practices_code/part_3-monitoring_at_work_1.html</p>
	<ul style="list-style-type: none"> Regulation of Investigatory Powers Act (2000) 	<p>Certain procedures must be followed before interception of communications can take place under those provisions. RIPA applies primarily to those public authorities listed in section 6(2) of the Act.</p>	<p>Office of Public Sector Information: http://www.opsi.gov.uk/ACTS/acts2000/20000023.htm</p>