

ONGOING PERSONNEL SECURITY: A GOOD PRACTICE GUIDE

OCTOBER 2008

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.....	3
Ongoing personnel security: an overview.....	5
Security culture.....	7
Countering manipulation.....	17
Screening for insider threat	23
Reporting hotlines.....	27
Secure contracting.....	31
Controlling employee access.....	37
Monitoring employee access	50
Investigation	55
Exit procedures.....	63
Glossary	68
Appendix A: Generic security appraisal form	70

Introduction

Centre for the Protection of National Infrastructure (CPNI)

The Centre for the Protection of National Infrastructure was formed in February 2007 from the merger of the National Security Advice Centre (NSAC), who provided advice on physical and personnel security and the National Infrastructure Security Co-ordination Centre (NISCC) who advised on computer network defence and other information assurance issues. CPNI provides integrated advice across all three security disciplines, with the aim of reducing the vulnerability of the critical national infrastructure to terrorism and other threats.

The Critical National Infrastructure (CNI)

The national infrastructure is the underlying framework of facilities, systems, networks and sites necessary for the functioning of the UK as well as the supply of essential services such as water, energy and food that the population relies on in every aspect of their daily life. Failure of this infrastructure and loss of the services it delivers could result in severe economic damage, serious social disruption or large scale loss of life.

There are nine sectors that deliver these services:

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

Not every activity within these sectors is critical, but those that are comprise the nation's Critical National Infrastructure.

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 CNI. 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.

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 critical 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 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:

- Personnel Security: Threats, Challenges and Measures
- Personnel Security Risk Assessment: A Guide
- A Good Practice Guide to Pre-employment Screening

[Return to Contents](#)

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 to Pre-employment Screening**).
- Minimise the likelihood of employees becoming a security concern (to be included in future CPNI work on **Good Security Culture**).
- Implement security measures in a way that is proportionate to the risk (see CPNI guidance **Personnel Security Risk Assessment**).
- 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. This is **ongoing personnel security**.

Why ongoing personnel security is important



Those who seek to exploit their legitimate access to an organisation's assets are termed 'insiders'. Insiders can take a variety of forms including disaffected staff, single issue groups (such as animal rights activists), journalists, commercial competitors, terrorists or hostile intelligence service agents. Their motivations are similarly varied and can range from political or religious ideologies to revenge, status, financial gain and coercion.

Many CNi organisations already have experience of dealing with insider acts such as fraud, theft and corporate espionage, and there is a potential threat from employees who may be members of, or have contacts with, terrorist organisations. Some of the more common insider acts include unauthorised disclosure of information and criminal damage.

As organisations implement increasingly sophisticated 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. Despite this, a survey carried out by CPNI has shown that the time and effort invested in personnel security reduces considerably after recruitment. 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; additional layers of authentication on IT systems cannot help an organisation to safeguard its intellectual property without ‘need to know’ and clear desk policies being in place as well. 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 pressures – must be proportionality and priority: countermeasures should be implemented in proportion to the risk and in line with an agreed schedule of priorities. Also important is practicality, with a recent 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 Security 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.

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](#).

[Return to Contents](#)

¹ “The Untold Insider Threat” Dec 10 2007

Security culture

All work environments develop their own internal culture which influences the way staff and clients behave and interact, yet it may not be one that is appropriate for an organisation with security concerns. In such instances, organisations should look to inspire a 'security culture' – one in which the everyday actions and attitudes of staff effortlessly contribute towards maintaining the required standards of security.

Principles of culture management

An organisation must have a clear idea of the security culture it wants, which will vary according to the nature of the business. 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 do you expect individuals to make their own decisions about security practice? What level of risk is considered acceptable? To what extent should uniformity of approach be enforced?

It 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 required. A number of mechanisms are available which broadly fall into two main groups:

- The first are concerned with how the desired culture can be embedded in the thinking of staff. Motivation is key to this and includes the nature of the incentives offered to employees to encourage them to adopt the desired culture and the extent to which management demonstrate their commitment to the cultural goals (by supporting and resourcing security initiatives, for example).
- The second group concerns those mechanisms that enable staff to actually 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.

The key to developing an effective security culture is that the desired culture, current culture and culture change mechanisms should all line up. If any link in the chain is broken, you are unlikely to get the behaviour and performance you want. However, different mechanisms are appropriate to different cultures. Adopting a mechanism because it works for another organisation may not be appropriate if that organisation has a different culture and adopts a different style and approach to managing security. Clarity about the desired culture is crucial if you are going to adopt the right mechanisms for your organisation.

This chapter provides an overview of the policies and procedures required to create and maintain an effective security culture within an organisation. Good communication is crucial, but it is also important that employees understand, accept and play their part. This can only be the case in organisations with a transparent framework of security policies.

Communication

Awareness of roles and responsibilities

In order for ongoing personnel security measures to work it is essential to convey their rationale effectively to employees. Employees are much more likely to engage if they have an understanding of why each security measure is in place and what their responsibilities are. Conversely, employees who have misunderstood or disagreed with security measures may resent, ignore or resist them and could also encourage others to do likewise.



To support this, any security measures and particularly those newly implemented, must be proportionate to the risks as identified through a personnel security risk assessment (for further information please refer to 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. The effect of breaking this psychological contract could be to alienate staff, reducing goodwill and confidence in the organisation.

Steps to consider:

- Review existing personnel security measures to ensure that they are proportionate to the threat.
- Communicate a clear rationale for all protective security measures.
- Raise awareness of security issues and the personal responsibility of every employee through posters, newsletters, staff meetings, focus groups and training courses.

Raising issues

Employees will naturally find avenues for voicing discontent such as when the boss is absent, in the staff canteen or in a social environment after work. However, it is useful if the organisation actively encourages openness and ensures that managers are both accessible and approachable to their staff. It is also important to provide employees with more formal opportunities to raise issues or concerns with individuals outside their management chain. Options for this kind of communication include [Reporting hotlines](#) and elected staff representatives, for example.

Organisational changes that are not communicated effectively could lead to uncertainty among the workforce and raise anxiety levels accordingly. Such stressors are known to have previously catalysed insider acts.

It is also important that managers are open and communicate difficult messages to their staff in a timely and appropriate fashion, particularly at times of organisational change. This kind of proactive communication, for example open meetings or discussion forums, should help detect, monitor and address any situation or feelings of disaffection.

An organisation may require, if not on a daily basis, effective communication systems between and within departments. If it is impossible to find or contact a person this could build frustration and in an emergency situation may pose a security risk. For example, if an employee needs to inform security about a specific threat. It may be useful to maintain an electronic directory or hold inter-departmental events to increase connectivity.

Steps to consider:

- Establish formal communication systems or a 'whistle-blowing' procedure for employees to voice a concern or grievance.
- Elect staff or trade union representatives who can channel concerns appropriately.
- Maintain an electronic directory to enable employees to communicate.

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.

SMART targets are:

S - Specific
M - Measurable
A - Agreed
R - Realistic
T - Time-framed



Where development opportunities are simply not possible within a given role, this should be emphasised during recruitment, so that employees can make an informed decision about taking on the role. If an employee's expectation does not match their experience, with no visible resolution, frustration or disaffection is likely.

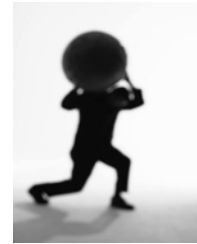
Steps to consider:

- Encourage employees to treat all staff with equal respect, by using first names throughout the organisation, for example.
- Provide development opportunities to all employees where possible.
- Set and review SMART performance and development targets annually.

Ownership

Employee responsibility

An effective security culture requires the commitment of *every* member of staff, whether they are permanent, temporary or a contractor. Employees must take responsibility for their own adherence to the organisation's security policies and be rewarded for challenging or reporting those who do not conform. With top-down support there should be no exemption to this ethos from the newest recruit to the Chief Executive.



It is crucial that employees feel a sense of ownership for the security measures in place, borne out of an understanding of why they are important. 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.

Every employee, irrespective of grade, should ensure that they display their security pass at all times within their organisation (and conceal it when outside, if appropriate). They should also routinely challenge anyone not wearing a pass, reporting this to security where necessary.

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.

Steps to consider:

- Conduct a full personnel security risk assessment to ensure that your security measures are both sufficient and proportionate to the risks.
- Implement proportionate security measures on the basis of risk, not seniority.
- Ask all employees to sign a statement of personal commitment to the security policies and values of the organisation, preferably as part of the induction process.

Senior management responsibility

Buy-in from senior management is vital in order to demonstrate that the personnel security measures are both worthwhile and necessary. In some instances their support may also be required to secure resources to introduce new measures. Top-down implementation is likely to promote adherence, while a lack of commitment from senior managers could undermine the process. For example, if the Chief Executive does not wear a pass it provides a visual indicator that they do not take this policy seriously.



Senior management, particularly in private sector organisations, is likely to be held ultimately responsible for the effect of any financial damage to the organisation caused by employees. Therefore, on a more pragmatic level, they should have a vested interest in the quality of their organisation's security culture.

Steps to consider:

- Ask a senior manager or board member to sponsor personnel security, to assist funding, risk assessment and the implementation of countermeasures.
- Provide senior management with real examples from the press of potential insider damage to the organisation, to encourage their support.

Line management responsibility

Those working in direct management roles are well positioned to identify and address any behaviours of concern in their staff and to encourage engagement with security measures, although it may be advisable to include safeguards to prevent any employee or manager abusing this system (see [Investigation](#)).

A manager's ability to identify and resolve suspicious or unusual behaviour will vary and will be difficult for those who are based in a different location to their staff. Nevertheless, things can be done to improve cohesion where staff work independently, for example, maintaining daily contact between managers and staff via telephone or video link and holding regular face-to-face meetings (see [Secure contracting](#)).

It is important to include these security responsibilities within each line-manager's job description. It may be helpful to assess their skills in this area (through scenario based role-plays, for example) and provide additional training if they do not meet the required standard. If a manager consistently fails to attend to these responsibilities, then the organisation should address this as a disciplinary matter in line with HR policy.

Steps to consider:

- Include security responsibilities within each manager's job description.
- Provide training for employees with line management responsibility to cover these requirements.
- Set out clear procedures for monitoring staff and addressing issues, including safeguards to protect employees from colleagues with a personal grudge.

Transparency

Clear policy and procedures

In order to assist employee understanding and involvement it is important that any security measures are clearly explained within accessible policy documentation. This should include a statement of the penalties for any failure in adherence. There should also be clear procedures to follow in the event of any security breach including, for example, incremental penalties according to the circumstances.



Clearly defining such procedures enables an organisation to clamp down on persistent offenders without being partisan or unfair. An organisation which requires employees to display a security pass could set out the following procedure for non-compliance:

- Staff not displaying pass initially receive a verbal challenge from any colleague.
- If persistent, employee's manager could be asked to provide a verbal warning that continued non-compliance will result in a formal breach.
- This could be followed by a direct/written warning from HR or Security.
- Finally, disciplinary action should be taken in line with the organisation's misconduct procedures.

It is essential to provide staff with access to the relevant policy documents from the outset of their employment, ensuring that they know where to find them and where to direct any queries or concerns.

Steps to consider:

- Hold all policy documents regarding conduct and ethics in a location that is easy to access.
- Notify employees when policy is amended or updated.
- State clear procedures with incremental measures, according to the severity of the breach, or indicating that there is zero-tolerance.

Auditing and enforcement

It is useful to conduct regular audits of your security systems to ensure that adherence is satisfactory. Such checks may also facilitate the detection of insider activity (see [Monitoring employee access](#)). However, establishing a good level of adherence is not the end of the process and it is equally important to maintain these checks to ensure that standards do not decline.

Where it is clear that an individual has violated a security policy it is very important to follow the appropriate disciplinary procedure. This will demonstrate to others that such behaviour is unacceptable and encourage adherence to security regulations. If a criminal act has occurred it may also be appropriate to inform the police (see also [Investigation](#)).

The following example illustrates these points:

- An organisation has a no-mobile phone policy and employees are required to turn off their mobiles and place them in lockers at the entrance. However, staff members know that, in reality, employees are never physically checked for phones and there is no mechanism for detecting an active mobile in the building. Moreover, those known by management to have kept their phones with them have faced no repercussion.

Although the policy described above may be a necessary and proportionate measure, it is totally reliant upon employees' voluntary adherence. Therefore an employee abusing the system, or with ill intent, is unlikely to be detected. Adherence in this instance could be strengthened using some or all of the following measures (see also [Monitoring employee access](#)) which may also address other threats:

- Conducting random checks on staff entering and leaving premises for prohibited items, for example mobile telephones or sensitive documents.
- Placing detectors strategically within the building, to alert the presence of any mobile phone.
- Addressing non-compliance promptly and proportionately, according to the severity of the breach.

Restricting access



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 (see [Controlling employee access](#)).

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 also [Exit procedures](#)).

Steps to consider:

- Ask employees to avoid sharing sensitive information unnecessarily with others, including colleagues or even management.
- Review access annually and when an employee changes job to prevent access from accumulating unnecessarily.
- Set out procedure for penalising employees who break the 'need to know' policy.

Training

It is important to ensure that employees are equipped with the necessary skills to maintain their responsibilities within the security framework of the organisation. This can be achieved using a range of training techniques which might include workshops, scenario based role-plays, briefings, road shows, intranet or staff magazine articles, discussion forums or even quizzes.

Training courses designed to equip managers to resolve suspicions can benefit from using role-play scenarios. These provide a practical way of assessing managers' interpersonal skills and abilities to judge a situation and respond accordingly.

Security training should begin during the induction process, to raise awareness and promote understanding of security measures. This could then be linked to other security training initiatives, for example any poster campaigns or magazine articles. Later, more specific training may be required according to an employee's role.

Regular refresher training may be useful to maintain standards and ensure new procedures are incorporated into current practice. It may be appropriate to incorporate an element of assessment within some training packages to ensure a sufficient standard is achieved. This would be particularly useful, for example, when training managers to resolve concerns regarding suspicious or unusual behaviour in their staff.

Steps to consider:

- Raise awareness among employees with regard to security policies from the outset of their employment.
- Conduct regular refresher training, assessing where necessary, to ensure standards are maintained.
- Provide incentives for employees to engage with these processes such as through personal development recognition.

Employee welfare

An organisation with a strong welfare culture enables employees to share and address issues before they become too great to resolve. 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 insider threat](#) for further details).

If a manager feels that they need to address any given employee behaviour it is extremely important that this is done proportionately and in line with set procedures. If any clarification is required then advice should be sought from HR or an employment lawyer. Any manager who cannot demonstrate their ability to approach and resolve such issues should be provided with further training until a satisfactory proficiency is achieved.

Steps to consider:

- Encourage staff to share personal difficulties with colleagues or management and provide employees with access to professional support or advice when appropriate.
- Set clear guidelines regarding what will and will not be supported or tolerated by the organisation, for example, illegal drug abuse.
- Provide practical and assessed training for managers, to enable them to appropriately address any concern about their staff.

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.

If a manager asks inappropriate questions, which are not relevant to an organisation's security, then they or the organisation may be liable to an employment tribunal. If there is any concern or doubt in this area then the advice of an employment lawyer should be sought.

Employees in sensitive positions could be asked to complete an annual security appraisal form (see [Appendix A](#)). 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 (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.

Steps to consider:

- Ask staff to notify management or HR if there are any significant changes to their personal circumstances. Keep such notifications strictly confidential.
- Include this as a delineated responsibility for new staff joining the organisation.

Staff opinion surveys

Periodically gauging staff opinion regarding personnel security, organisational culture and job satisfaction is a useful method of determining whether your security measures have been well received and understood. This can be done in-house or via a third party, but it is always beneficial to include a measure of anonymity to encourage the fullest and most honest feedback.



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.

Steps to consider:

- Gauge staff opinion using an anonymous survey on a regular basis (for example, every 5 years).
- Host open feedback sessions, where staff can openly discuss the surveys findings and ask management direct questions based upon these anonymous results.

Countering manipulation

As organisations improve their physical and electronic defences, those wishing to obtain confidential or sensitive information may attempt to exploit people within the organisation who already have legitimate access to it. The process of manipulating others to obtain information is also known as 'social engineering'. All employees should be aware of the threat of social engineering in both their private and professional lives, and trained to guard against it in order to protect themselves and the organisation.

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.

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.

Other 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 criminals to acquire background knowledge of a company that will help in mounting a social engineering attack.

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

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 e-mail or instant messaging; pharming attempts to acquire similar information by redirecting internet users to bogus websites.

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 e-mail 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.

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.

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.

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 that 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.



Resources

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

[Return to Contents](#)

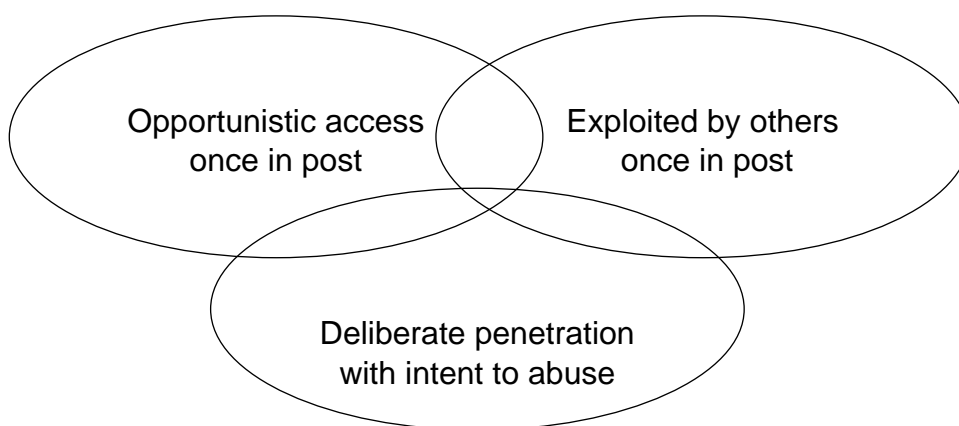
Screening for insider threat

One of the most challenging aspects of personnel security is screening individuals for insider threat. As well as addressing issues such as integrity, honesty and reliability, an effective personnel security regime needs to take into account all the behaviours and psychological characteristics that could be displayed by a potential insider.

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 personalities, motivations and behaviours of insiders are extremely varied, and that insider behaviours are shaped by a complex mix of factors including life history and the work environment, for example. 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 possible that an innocent explanation may exist.

Insider behaviour generally falls into one of three categories:

- **Opportunistic**
An individual exploits their access to assets once in post, even though they had no prior intention of doing so.
- **Recruited**
An individual in post is exploited by others in order to take advantage of their access.
- **Deliberate**
An individual seeks employment with the intention of abusing their access once in post.



The screening of individuals for insider potential therefore needs to be integrated into all aspects of an organisation's personnel security regime, from pre-employment screening –to detect those with deliberate insider intent – to ongoing personnel security measures that capture changes of behaviour in existing employees (see [Security culture](#) and [Monitoring employee access](#)).

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).

Factors influencing likelihood of insider activity

Certain environmental 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 can 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), for example.

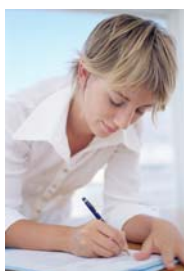
Purpose of screening

Screening can be conducted for a number of reasons, including:

- To identify a predisposition to act as an insider, such as a specific personality trait, personal circumstance or relationship which could either create a vulnerability to pressure or indicate an intent to act as an insider
- To detect actual insider activity, through the identification of suspicious behaviours taking place (such as accessing databases or taking sensitive information offsite without authorisation)
- To detect deception related to acting as an insider, such as spotting untruthful accounts in interviews

Early indications from both CPNI's research and other research into insider activity (including especially experience of espionage and malicious insiders in the US) are that screening for the insider threat should take into account four broad categories of signs or behaviours of concern:

- **Unauthorised behaviours**
Unauthorised or illegal acts, such as downloading sensitive information to which the employee does not have legitimate access, which makes them a serious security risk.
- **Suspicious behaviours**
Activity that is not unauthorised or illegal, but which may be a precursor to an illegal act, such as an unusual interest in the organisation's security measures, unexplained or frequent absences, or unusual levels of questioning colleagues about information or areas to which the individual does not have access.
- **Changes in lifestyle and work behaviours**
Changes in an employee's behaviour at work that might indicate that their loyalty to the organisation is under pressure or at risk (often associated with the process of disaffection) as well as changes in their personal circumstances. These might include changes in religious or political affiliations which have an adverse impact on an individual's work or attitude to security, displays of wealth incompatible with the individual's known income, changes in working patterns (particularly working alone or at unusual hours) or repeated failure to follow the organisation's security procedures.
- **Individual vulnerabilities**
Characteristics that might make an employee more vulnerable to becoming an insider such as adversarial attitudes, familial ties to a country of concern or a personal history of negative life events.



Screening during recruitment and screening as part of ongoing personnel security present different challenges and opportunities. For example, an individual's past history is more readily accessible at the recruitment stage when application forms and CVs are available for examination, while screening during employment will benefit from the fact that the employee's patterns of behaviour have been established and observed and so changes will therefore be more noticeable.

Screening during employment may be prompted by a need to resolve a particular concern about an employee, or by an employee moving to a role that affords greater opportunity for insider activity (see [Controlling employee access](#)).

The screening process

Screening for vulnerability to, or active involvement in, insider activity is a two-stage process: identifying employees who give cause for concern by demonstrating suspicious behaviours or possessing individual vulnerabilities, and then resolving these concerns in some way.



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:

- Psychometric tests or personality questionnaires that can be given to groups of employees at the same time.
- 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.
- Securing the involvement of all employees in the screening process by raising awareness of personnel security and the insider threat (see [Security culture](#)), and 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 those concerns. This necessarily involves a more direct approach – generally a face-to-face interaction such as an interview. Any 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 behaviour. 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 (see [Investigation](#)).

Reporting hotlines

Providing staff with a trusted resource for reporting 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 insider threat](#)). The hotline may even extend to providing a Samaritan function, 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 employees' home telephones.
- 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 (see information about 'protected disclosures', below).
- 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 complexity 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.

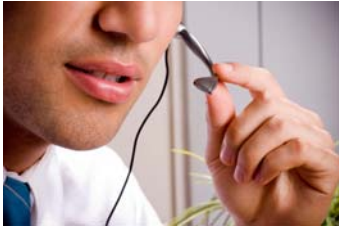
It is vital that any organisation wishing to implement an incident reporting hotline seeks legal advice first.



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 a report made anonymously might have discriminatory motivations. If that 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 the 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.



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.

Resources

- 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 Find out more about the Safe Harbor, 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.

Secure contracting

The use of contractors is commonplace in many sectors of the national infrastructure, as they can provide expertise that an organisation might struggle to develop internally for the same cost or within appropriate timescales. However, it can also result in an increased personnel security risk, as a contractor's primary loyalty may not be to the employing organisation and their commitment to the organisation's security culture may be diminished as a consequence. This risk needs to be managed.

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 in 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 rational, 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. Beyond this, consideration should be given to:

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 standards of behaviour that permanent staff are 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.



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 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 CNI organisations 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 the contractor's circumstances give 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.

In Government, where a contractor is subject to National Security Vetting, their clearance officially expires at the end of one period of employment and the vetting process must be repeated in its entirety before they can begin another.

Commitment

On first starting work in an organisation, contractors should ideally attend the same organisational induction (which should include security messages) and repeated security briefings 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 will be held responsible for any lapse in security standards
- 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.

[Return to Contents](#)

Controlling employee access

Organisations are often suitably protected against external threats, but may not have equally considered the threat from those already on their premises. There is a range of measures that can be implemented by an organisation to prevent legitimate employees and visitors from engaging in nefarious activity or at least limiting the amount of damage they can inflict.

It is important for the employee access controls used by an organisation to be proportionate to the scale and nature of the threats it faces from its employees. The best way to measure this is to conduct a full personnel security risk assessment. This will identify the high priority threat areas and provide a clear rationale for any given measure, which may also be useful for funding purposes and for educating reluctant employees (for full details see CPNI guidance **Risk Assessment for Personnel Security: A Guide**).

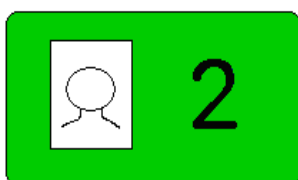
Physical access

Pass display policy

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 or security staff. Furthermore, employees should be encouraged to challenge any individual who is not displaying an appropriate pass (see [Security culture](#)).

Providing versatile pass holders which can be worn round the neck or clipped to clothing may improve adherence levels, while retractable cords are useful if staff need to touch or swipe their passes. However, health and safety must be considered so that any pass does not endanger the wearer (for example plastic pass holders should be provided for electricians and all should be fitted with a choke release mechanism).

Clear differences



If passes are used to distinguish between different levels of clearance or access it may be worth considering how these can be easily identified. One way is to colour code each pass according to the access rights of the holder. It is helpful to ensure the pass colour can be seen from both sides, either through a clear or similarly coloured pass holder.

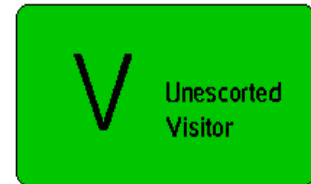


Another option is to vary the orientation of the pass between landscape and portrait, or to use a distinctive border around certain passes to distinguish one group from another, such as contracted staff from permanent employees.

If a more detailed pass coding system is required, additional letters or numbers can be used to specify an employee's occupational group or particular access rights. This system can also be used to assist colour-blind individuals. Nevertheless, it is helpful to keep the whole system as simple as possible, so that employees can be confident about what constitutes a correct pass when a challenge is required.

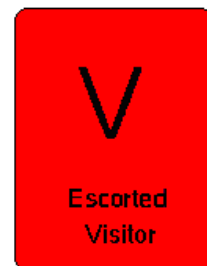
A traffic light system could be used to indicate clearance.
For example;

- Red pass = low or no privileged access
- Orange pass = medium or restricted access
- Green pass = high or unrestricted access



To distinguish between an unescorted and escorted visitor, security could provide the latter with a red portrait orientated pass.

An organisation working across a range of different sites should try to ensure that the pass system is consistent throughout, ideally via a centralised department. 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.



Steps to consider:

- Send out test personnel with no pass to see whether they are challenged. Poor results can be publicised to help promote change in this area.
- Use posters to inform or remind staff of the pass colour coding system and encourage staff to challenge individuals who do not appear to be compliant.
- Provide versatile pass holders which can be worn according to preference. Use retractable cords if passes are required to be touched or swiped at access points.

Identification

Passes used to indicate access rights or clearance levels will also require some form of identification on the pass to determine its ownership. This is particularly important for pass holders with sensitive access rights, as wrongful use may be more damaging. The best form of identification on a pass is a photograph of the employee.

However, it may be appropriate in some circumstances to include a name so that the pass can be used as a form of identification, linking the individual with the organisation in an official capacity. This may be useful if an employee travels regularly on business. However, employee names and organisational labels should ONLY be included if this information does not pose a security risk, should the pass be lost or stolen.

The advantage of using a photograph alone on a distinctive but anonymous pass is that a thief trying to use it will not automatically know 'their name' or where 'they work'. However, research has demonstrated that people are not able to accurately identify unfamiliar individuals from a pass photograph alone. Therefore, where verification is required, entry should only be granted following the provision of a name, PIN or password, which can be confirmed electronically, through data hidden on the pass chip or magnetic strip.

Steps to consider:

- Follow passport style regulations and take your own staff photographs to ensure the best clarity. Hold electronic copies to use for additional verification.
- Ask staff to renew their pass photograph every five years or if their appearance changes markedly.
- Print an anonymous PO Box on the reverse so that lost passes can be returned without further compromising security.

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 that is not the case and, while it may be a useful additional layer of security, biometric verification 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 system is fundamentally reliant upon genuine enrolments to the databank and safeguards will be required to avoid fraudulent applications.

In summary, biometric verification may play an increasingly important role as the technology continues to develop. However, there are still other less intrusive and more cost effective alternatives available.

Issuing passes

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

- Conducting an identity check and document verification for new employees.
- Signing each request off by HR or Security before the pass is issued.
- Restricting the physical production of passes, so that no individual can bypass the authorisation process.

To reduce the risk from new joiners it may be useful to restrict initial access to basic entry and exit only, with management sponsoring any additional privileges as they are required. Sponsors could be expected to maintain responsibility for removing access rights when they are no longer required, thus preventing an individual from accumulating unnecessary access over time.

It is worth noting the importance of retrieving ALL passes from individuals who are no longer employed by the organisation (see also [Exit procedures](#)). Security should be promptly informed when an employee leaves and any electronic access should be deleted on the date of their departure. It may be useful to keep a record of the destruction of returned passes. If there are too many unreturned passes in circulation, then it may become necessary to replace old passes with a distinctive new version.

Steps to consider:

- Centrally control pass issue and provide entry only passes as the default position.
- Notify security immediately when an employee leaves the organisation.
- Delete electronic access from the date of an employee's departure.

Protecting your passes

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 24-7, 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.

Adding extra functionalities to passes may encourage employees to look after them better but also increases the possibilities for abuse, should the pass be lost or stolen. For example, they could be used as a cashless system for in-house vending machines or restaurants, provide car park access or an electronic signature for remote working or for using printers. However, it is important to emphasise that employees should NOT lend passes to colleagues.

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 apply anew if their contract was extended.



Steps to consider:

- Require staff to sign for pass at the outset of their employment. Include terms and conditions of ownership, for example, not sharing pass.
- Encourage employees to take care of their passes by increasing their value through additional features and penalising loss or misuse.
- Conduct an annual audit of passes issued to ensure that those in circulation are still legitimately required.

Zoned pass access

Within any organisation there may be a range of sites or areas holding various degrees of sensitivity. While some staff may require access to all of these areas it may be helpful to restrict the access of employees to only those areas required by their role. This complements the electronic role-based access approach described below.

A zoned access system can be based on different colour passes, so that it is easy to spot someone in the wrong zone, but should also be maintained using door controls which will physically prevent staff without sufficient rights from accessing certain areas and electronically flag up any attempt to gain unauthorised entry. Restricted areas may include server rooms, HR, or any other areas where sensitive information is held.

Steps to consider:

- Colour code zones of differing sensitivity in line with the access (or colour pass) required within them.
- Prevent staff from accessing any unauthorised area and flag any such attempt to security.

Door control

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.

System	Disadvantages
<ul style="list-style-type: none">• Single-code alphanumeric keypad: provides access to only legitimate users who know the code.	<ul style="list-style-type: none">• Former employees maintain access until the code is changed. Anyone can watch it being keyed in and then use it themselves.
<ul style="list-style-type: none">• Centrally protected keys: these are patent controlled, only available from authorised security centres and cannot be copied.	<ul style="list-style-type: none">• If a key is lost the locks may need to be changed. Keys can be lost, stolen or 'borrowed' by unauthorised colleagues.
<ul style="list-style-type: none">• Swipe card or pass: magnetic strip or barcode allows holder to enter.	<ul style="list-style-type: none">• As above.
<ul style="list-style-type: none">• Swipe card, or pass, plus individual PIN, password or biometric feature: provides additional security.	<ul style="list-style-type: none">• Any single door system enables unauthorised individuals to enter behind a legitimate employee or with a large group.
<ul style="list-style-type: none">• Full-body turnstiles or individual entry pods: only allow one individual, with pass and PIN, to enter at a time.	<ul style="list-style-type: none">• If the system allows a pass to be swiped twice in a row 'pass-back' could provide entry to unauthorised individuals.

Steps to consider:

- Select entry systems most appropriate to counter the threats facing the organisation. This may vary within different physical zones of the same organisation.
- Ensure that every entry point within a controlled zone is secure, for example windows and fire escapes, so that individuals cannot by-pass the controlled entrance.
- Provide staff with covert signal that they can use on entry to the organisation to alert security that they are under duress, for example by typing '112' before their PIN.

Visitors

Another useful security measure is to keep a central record of visitors to any given site (this can also be 'sold' to employees and management from a health and safety perspective). Details provided should include; time and date of visit, the visitor's name, the purpose of their visit and identity of their 'host' employee. It is better to specify a single host rather than a generic group, particularly if the visitor requires an escort.

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, privilege passes are easily abused and organisations may wish to restrict their use where possible.



Any 'no camera' or 'no-mobile' telephone policy 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.

Steps to consider:

- Only allow staff members to host visitors if they have provided full details to security or reception.
- Restrict visitors access to the most basic level (additional access can only be provided by an approved member of staff)
- Screen visitors for electronic equipment and remove any mobile phones, cameras and laptops which are not approved or legitimately required.

Couriers

An organisation may wish to employ its own secure couriers to transport mail and other items between locations. The level of security used will depend on the sensitivity or value of the items being moved. However, even basic measures such as using tamper-proof packaging can be used to prevent employees from interfering with the contents.

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. Items should be stored in fireproof cupboards or safes, for example. The combination or keys for these areas should be tightly controlled and reviewed when an employee moves on or leaves the organisation.



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, or to all personal items and papers, or could include every removable item on the desk. The latter of which may be useful in an environment where desks are shared.

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.

Steps to consider:

- Assign each employee with particular daily responsibilities within the clear desk policy, for example, their own desk and a number of cupboards.
- Provide employees with a secure area to store their belongings when out of the office.
- Use a locking checklist to help employees secure the whole office before they leave and ask the last employee out to initial that final checks have been made.

Document removal



Organisations may wish to prevent staff from taking commercially sensitive material out of the office unless it is absolutely necessary. In such cases an organisation could ask employees to log the removal and return of these documents, which could be numbered or bar-coded. They may also wish staff to hold sensitive papers within locked containers while they are out of the office.

If an organisation works with protectively marked material, then no classified document should be removed from the building unless with prior agreement from management. Where approval is obtained each document's removal and return should be logged and papers should be held securely at all times, according to organisational policy.

Where an organisation is concerned about the loss of sensitive material, it could also restrict photocopier access and lock these completely out of hours. Measures could include requiring a PIN before use and using a copier which keeps a record of items copied. All of these measures should be supported through appropriate security checks (see [Security culture](#)) and robust disciplinary policies for any employee contravening these regulations.

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 below, to act undetected against organisational interests.

This policy can be supported through the use of motion alarms and cameras linked through to security guards. The system could be programmed to give security a few seconds warning before the alarm actually goes off to enable any false alarm to be overridden. This would also permit security to approach any suspicious individual without raising their awareness beforehand.

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.

Another option is to use software which forces the shutdown of desktops on any given network at the end of the day, for example. This makes it much easier to detect any PC started up out of hours.

Steps to consider:

- If work is required in a sensitive area out of normal office hours require two employees to be present or use additional monitoring, for example, CCTV.
- Alarm access points to sensitive areas and ensure security can respond out of hours.
- Inform employees where areas are alarmed at specific times, so that they do not set them off accidentally.

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 or if an employee tries to access the premises outside normal office hours (see also [Monitoring employee access](#)).

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

Steps to consider:

- Restrict entry to organisation out of office hours, unless particularly required.
- Program the system to alert and reject any attempt to use a pass twice in a row.
- 'Lock out' any pass where the PIN code is entered wrongly on three consecutive occasions.

Electronic access

The need for firewalls and anti-virus software is obvious in today's environment where computer hackers can remotely access, change or remove large volumes of data. However, such measures may not protect against legitimate employees abusing their IT access for unauthorised purposes. The following section provides an overview of this area but is not definitive. This is a complex area of expertise and organisations are advised to consult an IT security expert before attempting to implement any measure.



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 also [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, for example.

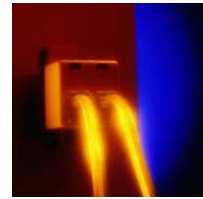
Nevertheless, it is equally important to assess and review access rights regularly and particularly when an employee changes jobs or leaves the organisation (see [Exit procedures](#)). An individual's access rights should not be allowed to accumulate unnecessarily over time and, where appropriate, access 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.

Steps to Consider:

- Standardise role based access across departments and locations.
- Set a time limit on access privileges and passwords, according to requirements.
- Remove access as soon as it is no longer required.

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 at 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 also [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.

Internet use

Many organisations provide staff with some form of internet access in the workplace. However, it may be advisable to restrict access to employees with an approved requirement. Furthermore, to protect the organisation from external attack (and perhaps in the interest of productivity), it may be useful to restrict or prevent access to certain sites such as social networking sites and web-based email accounts, or even to use a separate system for internet use.

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 program to be run or downloaded, for example Java script. Any persistent attempts to override these constraints should be logged and raised with the system administrator.

In some instances, staff may legitimately require access to blacklisted sites. For example, human resources may wish to search sites such as Facebook in order to further assess potential employees. Stand-alone machines not linked to the organisation's network could be used for such activities, in order to reduce the threat to the overall system.



Steps to consider:

- Provide internet access only when it is required, by permission of management.
- Require employees to sign an acceptable usage policy before access to the internet is provided.

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.

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. Any storage device should be equipped with a sufficient level of encryption for the data held upon it. If an employee is working abroad, generally they should avoid carrying any sensitive data or electronic encryption device (see CPNI website for further guidance).



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.

Steps to consider:

- Issue identifiable electronic items to individual employees who are responsible for their safekeeping, content and use.
- Conduct an annual muster of issued electronic items, for example USB sticks and laptops, to ensure they are safe and being used properly.
- Secure removable IT using wire locks.

Passwords

This case study 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.

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.

There are a number of websites which offer guidance as to what constitutes a secure password. Generally, it is agreed that 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 also 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 prevented from changing back to a previous password or altering only one character. Employees should also be able to change their passwords independently. For example, if they believe someone has seen them inputting their password.

Steps to Consider:

- Provide guidance to employees about secure and insecure passwords.
- Ask employees to avoid writing passwords down, sharing them or inputting passwords while others are watching.

Screen locks

To avoid unauthorised personnel from hi-jacking 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.

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.

Steps to consider:

- Challenge employees who fail to lock their terminals and ensure policy sets out measures to address persistent neglect in this area.
- Ask employees to lock screens when away from their desk or log out if they will be absent for an extended period.
- Automatically lock screens after a few minutes of inactivity and log out any locked screens which have been inactive for a long period.

Telephones



It may be that an organisation routinely records staff telephone calls for quality or training purposes, which can be useful in the event of an investigation or complaint from a colleague, for example. However, the fact that staff know this system is in place will reduce the likelihood that they will misuse their telephones or pass sensitive information in this way.

Conversely, 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. However, without any restrictions, such equipment may be misused by staff. Therefore, it is sensible to control access to such devices using a PIN code or by locking them within a secure room.

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>
- 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>
- International Organisation for Standardization. ISO 27001 sets out industry standards for security. <http://www.iso.org/iso/home.htm>

[Return to Contents](#)

Monitoring employee access

In the context of personnel security, monitoring employee access to physical or electronic assets is about establishing whether breaches of the organisation's internal policies are taking place. This is a specialised activity for which detailed guidance already exists both on the CPNI website and elsewhere; the aim of this chapter is to provide an overview of the subject.

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 subversion or 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.

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 any act would be very 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 open
- failure to observe 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.

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’. 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 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 occasionally 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.

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

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.*
- 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.

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. Activities which may appear malicious may be entirely innocent and so procedures in such instances must be thorough and fair.

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 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 and 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**

Again, 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, consider a threshold below which an investigation will not be carried out, in order to avoid adding to workloads – although all cases should still be assessed on their own merit, as many ‘low value’ incidents may still add up to cause for concern. An investigation may also sometimes be worthwhile purely for its deterrent effect.

- **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 and a sponsor should be identified. The lead investigator is responsible for carrying 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. The seniority of the lead investigator is usually related to the scale of the incident; in a leak enquiry, for example, it may be the sensitivity of the information leaked that informs the choice of investigator, as is the case in Government.

The sponsor’s key responsibility is one of ownership, ensuring that the appropriate steps will be taken according to the findings. They should be senior enough within the organisation to authorise disciplinary procedures and to promote internal changes depending on the outcome of the investigation.

Depending on the size and structure of the organisation, the roles of sponsor and 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. Providing there is no conflict of interests, both roles may be carried out by the same person.

Initial discussions between the investigations team and other parties such as Human Resources 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

Whether to run the investigation overtly or covertly

If there is a suspect, consider whether the nature of the incident dictates that they should be made aware of the investigation. 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.
- If the investigation concerns a planned unauthorised act that has yet to take place.
- The nature of the incident or suspicion.

Who should be involved?

The lead investigator will need to make certain people or business areas aware that an investigation is to take place and engage them in the process as appropriate, including:

- **Human Resources**

HR should be expected to assist both the investigation team and the employee under suspicion as the investigation proceeds, while remaining impartial. While liaison with HR is always important, it should be considered essential in cases where an employee is to be suspended while an investigation takes place.

- **Line management and colleagues**

It is usual to notify the employee's line manager or departmental management generally about the investigation. In certain cases it may also be necessary to inform a small number of the employee's immediate colleagues, although this is unusual and should only be considered where colleagues are likely to be interviewed later as witnesses, for example; given the sensitivities involved, Human Resources should certainly be consulted first.

- **Senior or executive management**

If an employee has committed a very high-profile unauthorised act, or if the investigation involves very sensitive information, it may be necessary to make the appropriate senior personnel in an organisation aware that the investigation is taking place.

- **Public Affairs**

If the nature of the incident is such that the media will take an interest, the organisation's Public Affairs department should be put on alert and appropriate responses drafted in advance.

- **Specialist investigators**

Accessing computer files on an employee's PC can cause data on the computer's hard drive to be overwritten, possibly resulting in the loss of vital evidence. Where specialised tools or knowledge such as PC forensics are required, consideration should be given to calling upon specialist investigators who can advise from the beginning of the investigation.

Independent investigators should be chosen for their credibility and established record of working on an investigation panel. This relationship will need to be carefully managed to ensure that the third party investigators comply with organisational procedures.

- **Legal advisers**

Before any steps are taken to investigate an individual, the lead investigator must consult an employment lawyer, who will be able to offer advice concerning the legal rights and responsibilities of all parties involved.

Depending on the nature of the incident it may also be appropriate to take legal action once the investigation has concluded, such as court injunctions to prevent publication of sensitive information in the press.

- **The police**

In most instances where a criminal act is suspected or has taken place, the police should be notified immediately and they will decide on the nature and extent of their involvement in the case. For cases involving only low-level losses or damage organisations may decide to deal with the matter internally. Again, this decision should be made in the light of legal advice.



If the police do become involved it is important that the organisation's internal investigation process continues. Criminal law and employee law differ in key areas such as the burden of proof and the organisation will need to be able to demonstrate that it has followed established procedures – such as the disciplinary process – if it intends to dismiss an employee, for example. Where both a police and an internal investigation are running concurrently, it is essential to have effective communication between the two investigating parties.

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?

This 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.

As with all matters affecting employees, this decision should be made in consultation with Human Resources and an employment lawyer.

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 bear in mind their legal obligations under the following legislation:

- **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. Although monitoring in general is covered in [Monitoring employee access](#), there are some specific issues to bear in mind in the context of an investigation.



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, including:

- 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.
- 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.

The advice of a specialist in employment law is essential.

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 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 office 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

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

[Return to Contents](#)

Exit procedures

Employees leaving the organisation take considerable knowledge about internal 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.

As the case of Vitek Boden shows (see panel), when an employee leaves an organisation their knowledge of the organisation’s assets and how to access them can remain at their disposal indefinitely, so it is vital that the appropriate physical, information and personnel security measures are in place to prevent it being used for unauthorised purposes.

The information that an employee acquires and the opportunity to act maliciously after leaving will differ according to the roles in which they worked. While an organisation’s exit procedures can consist of a comprehensive check list for every departing member of staff, it might be more efficient, particularly in larger organisations, to establish a set of role-based exit procedures. For example, when a member of the administrative support team leaves the locking codes on the confidential filing cabinets will need to be changed, while the departure of an IT systems administrator would require the expiry and renewal of all remote access codes.

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 Maroochydhore in Queensland, Australia.

Boden had previously worked on the Maroochydhore 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.



The development of role-based exit procedures should be driven by a personnel security risk assessment to determine the groups of employees that pose the greatest potential threat to the organisation. CPNI’s personnel security risk assessment model can be used for this purpose (see CPNI guidance **Risk Assessment for Personnel Security: A Guide** for more information).

Protecting the organisation

As soon as it is known that an employee will be leaving the organisation, their line manager, in consultation with Human Resources if appropriate, will need to consider how to manage the risk posed by an individual who may, depending on the circumstances, no longer be loyal to the organisation.



The first decision is how to handle the departure. The options will vary but are likely to include:

- Allowing the employee to carry on working during their contractual notice period, retaining their usual access to the organisation's assets.
- Allowing the employee to work their contractual notice period but with reduced access to assets (through constant supervision, for example, or the allocation of lower-level access codes).
- 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').

A supervised exit will minimise the potential insider risk but is likely to be seen as an overreaction if an employee is leaving on good terms. Allowing the individual to work their contractual notice period is less contentious but may provide opportunities for abuse of the organisation's assets. The decision will therefore be influenced by a number of factors, such as:

- Whether the employee is leaving voluntarily or as the result of a disciplinary process.
- If they are not leaving voluntarily, what they have done to cause their dismissal.
- Whether they are going to work for a competitor or hostile organisation.
- The nature of the role, and therefore the sensitivity of the organisational assets they can access.
- The output from a personnel security risk assessment, which will determine the threat they pose to the organisation.

The decision may not be straightforward. 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 leaving to take a job with a competitor organisation, for example, it may be appropriate to remove their access to commercially valuable information. If they are currently working in an extremely sensitive environment then it may be necessary to ask them to leave immediately after all.

Once a leaving date has been agreed, there is a need to reduce the employee's opportunity to carry out an unauthorised act. This begins with the removal of any organisational assets, access tools and identifiers that the employee no longer requires but could use to facilitate an insider attack, such as:



- uniforms
- security passes and identification cards
- mobiles/blackberries/pagers
- company credit cards
- business cards
- keys to secure areas or storage
- tokens for access to electronic systems
- laptops and other remote working equipment
- books, papers and commercially sensitive documentation belonging to the organisation.

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 – and 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 (see **Protecting the organisation**, above).

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 those employees:

- Working in branches.
- On sick leave.
- On paid leave pending an investigation.
- Working from home or at other (possibly third party) sites.
- On maternity leave.

If the organisation is to be protected as far as possible from the personnel security threat, many of the same items will need to be recovered and protective measures implemented when an employee dies in service. In these circumstances it is important that the procedures allow due sensitivity.

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 typical.

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.

[Return to Contents](#)

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** with legitimate access to **assets**, who exploits, or may exploit, their legitimate access for **unauthorised purposes**.

Insider activity

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

Organisation

A corporate body of any size in which people work in various roles to deliver a product or products.

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.

[Return to Contents](#)

Appendix A: 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. The first part (A) is completed by the employee and the second (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

- Employees 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 some kind of explanation regarding the purpose of the form. This may include updating HR files with any changes in personal circumstances and identify issues which may relate to an employee's personal security. Reassure staff that all responses will be held in confidence.

**ALL INFORMATION SHOULD BE HELD AND TREATED
IN CONFIDENCE**

PERSONAL CIRCUMSTANCES

The level of intrusion into an individual's personal circumstances will depend on the sensitivity of their employment. Examples of the kind of circumstances which may affect an individual's security profile include:

- 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 proceedings brought against you
- 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 circumstances above, there are a number of personal issues which could have an impact on an individual's resilience. If an employer is aware of these it may be possible to ensure that they do not present a security risk to the organisation.

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 FINANCES

Financial insecurity has been known to catalyse insider activity. Therefore 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.

- Has your debt or your ability to manage your debt increased significantly during the review period?
- Have you received, from any sources, sums of money or assets to the value of £5,000 or more during the review period?

EMPLOYMENT CONCERNS

Depending on the nature of an organisation's business, it may be appropriate to check 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 feelings of disaffection. Examples include;

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

It may be useful to remind employees at this point that all responses will be held confidentially.

DECLARATION

At this stage of the form it is helpful to include a statement to the effect that the employee understands their responsibilities and has completed the form accurately, to the best of their ability. There should be an option to request an opportunity to speak to a member of the security team and the form should be signed and dated by the employee.

Employee signature

Date

What happens next?

- *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 unless they are contacted.*
- *Quite often no further action will be required until the next review.*

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.

SUBJECT DETAILS

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

Sufficient room should be provided under each section for responses to be made (managers can be asked to continue on a separate sheet where necessary). Examples of areas to cover include:

PERSONAL QUALITIES

- Job career satisfaction (e.g. level of motivation, ethical concerns, feeling that his/her contribution is valued)
- Interpersonal skills (e.g. How do they get on with work / management colleagues? Are they a team player? Can they take constructive criticism?)
- Personality traits (e.g. reliability/stability/discretion, ability to cope with pressure, recklessness)
- Security awareness (e.g. attitude towards personnel, physical and IT security procedures)

BEHAVIOUR

- 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?
- Is there any indication that this individual has serious financial difficulties, or is inexplicably affluent?
- Is there anything about this individual that worries you, or that could indicate a matter of potential security concern?
- Is there any indication that this individual might have an alcohol or drugs problem?

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. Managers could, for example, be asked to circle the most appropriate response.

CURRENT CONTACT

Work contact, normally: DAILY WEEKLY LESS THAN WEEKLY

Social contact, normally: REGULAR OCASSIONAL NONE

It is also useful to ask managers whether they would be happy to supervise this person again as this can be a better endorsement than a glowing report.

DECLARATION – MANAGER

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

- Please indicate if you would like to discuss any issue further with a member of the HR team.

Signature Date

Name Position

COUNTERSIGNING MANAGER

Please comment below if there is any additional issue that you wish HR to be aware of, or indicate if you wish to speak to a member of the personnel security team.

Signature Date

Name Position

WE WILL CONTACT YOU IF AN INTERVIEW IS REQUIRED.

ALL INFORMATION WILL BE HELD AND TREATED IN CONFIDENCE.

[Return to Contents](#)