National Protective Security Authority

A Good Practice Guide – Edition Four

Ongoing Personnel Security

Contents

Introduction

The aim of this guidance

This guidance provides information about good practice in ongoing personnel security, focusing on the key elements of an effective security culture. It provides a useful supplement to existing procedures, and for those who are beginning to consider the role of the insider as part of their security regimes.

It is not intended to replace an organisation's existing ongoing personnel security procedures, or those specialist security manuals in use in certain sectors of the national infrastructure such as the Security Policy Framework. Nor, given the large numbers and the varied sizes and activities of organisations in the national infrastructure, is it possible to create a document detailed enough to become a handbook for ongoing personnel security in every organisation.

This guidance has been written for human resources (HR) and security managers and those with line management responsibilities, all of whom have a role in creating and maintaining a culture of effective ongoing personnel security.

NPSA recommends that organisations seek professional advice, especially on employment law, when implementing or amending their ongoing personnel security measures.

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

- Personnel Security Risk Assessment: a guide
- Pre-Employment Screening: a good practice guide
- Insider Data Collection Study
- Holistic Management of Employee Risk (HoMER)
- SeCuRE: Security Culture Review and Evaluation Tool – a guide for organisations
- Investigating Employees of Concern
- Managing the Disclosure of Employee-Related Information
- Online Social Networking
- Personnel Security in Remote Working
- Personnel Security in Offshore Locations
- Social Engineering – understanding the threat
- Motivation within the Security Industry
- Communicating Personnel Security Messages
- Security-Minded Comms – protecting your organisation through your corporate communications

These can be downloaded from http://www.npsa.gov.uk (see also *Appendix 1*).

Executive summary

Personnel security is a system of policies and procedures which seeks to:

- reduce the risk of recruiting staff who are likely to present a security concern;
- minimise the likelihood of existing employees becoming a security concern;
- 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;
- implement security measures in a way that is proportionate to the risk.

An insider is a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes. This can be a permanent, temporary, seconded, contract or agency worker (in this guidance, the terms employees and staff are used to refer to all these groups). As organisations implement increasingly sophisticated physical and information security measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.

Pre-employment screening plays an important part in recruiting staff who are unlikely to present a security concern. However, people and their circumstances and attitudes change, either gradually or in response to particular events. NPSA's *Insider Data Collection Study* shows that three-quarters of insider acts in this study were carried out by employees who had no malicious intent when joining the organisation, but whose loyalties changed after recruitment. The study also shows that, in many circumstances, the employee undertaking the insider act had been in their organisation for some years prior to undertaking the activity and opportunistically exploiting their access.

Some of the more common insider acts include: unauthorised disclosure of information, process corruption (where an employee has illegitimately altered an internal process for their own ends), corporate espionage and theft. Insider motivations vary greatly and are often a combination of factors. Examples include financial gain, revenge, notoriety, political or religious ideology and (where external pressure is exerted on an employee) fear or coercion.

Insiders are diverse, and no single set of countermeasures can guarantee protection. However, effective ongoing personnel security measures will help to mitigate the insider threat, and should include:

- a strong security culture, where everyone in the organisation is aware of their security responsibilities;
- effective line management, who can identify unusual behaviour early and intervene to prevent any problems becoming more serious;
- confidential systems where employees can report security concerns;
- effective access controls to sites, zones within sites and company systems;
- robust monitoring to identify unauthorised activity/access to sites and systems;
- established investigative procedures;
- good exit procedures.

The insider threat

NPSA's *Insider Data Collection Study* shows that insider behaviour is shaped by a complex mix of factors including life history and the work environment. It is 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. However, it is still likely that an innocent explanation may exist.

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

- inadequate personnel security measures during pre-employment screening;
- inadequate ongoing personnel security measures, limiting the organisation's ability to identify or prevent insider activity among its employees;
- poor management practices, which may reduce 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.

Circumstances surrounding an employee's work or personal life may increase their vulnerability to coercion, exploitation or duress, impair their judgement or precipitate their involvement in an insider act. Examples of such circumstances can include:

- uncertain employment conditions;
- poor or cavalier attitude towards security;
- decline in performance at work, friction with colleagues, disillusionment or dissent;
- significant physical or psychological problems, depression or emotional instability;
- personal problems, bereavement or lifestyle (or that of a partner or family member);
- addiction (e.g. gambling, alcohol or drugs) or other psychological dependence;
- personal finance difficulty e.g. debt, bankruptcy and other judgements, closure of bank accounts or withdrawal of credit facilities not done at the employee's initiation etc.;
- arrests, pending prosecutions, convictions, formal police cautions or police enquiries which may lead to prosecution (particularly if these relate to a post under the Notifiable Occupations Scheme, when these will be reported to the employer[1]);
- conflicts of interest e.g. ethical concerns or commercial interests;
- approaches by journalists or other persistent or unusual enquiries about employment.

[1] www.gov.uk/government/publications/the-notifiable-occupations-scheme-revised-guidance-for-police-forces

Security culture

An organisation's security culture is the style, approach and values that it wishes to adopt towards security, and it is essential to an effective personnel security regime. The benefits of an effective security culture include:

- employees are engaged with, and take responsibility for, security issues;
- levels of compliance with protective security measures increase;
- the risk of security breaches and incidents is reduced by encouraging employees to think and act in more security conscious ways;
- the risk of theft of materials or company information is reduced as employees are more likely to report behaviours/activities of concern, and procedures and processes are more robust;
- improved organisational performance through effective management, established reporting mechanisms, increased employee satisfaction and commitment to the organisation;
- the risk of reputational and financial damage to the organisation is reduced.

NPSA's *Insider Data Collection Study* shows that often a poor security culture existed in areas where insider acts took place, with a lack of adherence to security policies and practices by employees, and management being either unaware of malpractices or failing to deal with them effectively. The most common occurrences included:

- security containers not being closed or locked;
- the sharing of security passwords amongst colleagues;
- not locking computer terminals and allowing colleagues to use logged-on terminals;
- sensitive information left unsupervised on desks;
- pass access to restricted or secure areas not enforced.

The '**Employee Outlook Survey**' Autumn 2012 found that only 54% of employees believed that their organisation's values positively influenced people's behaviour at work. 55% felt fully or well informed on what was happening in their organisations.

CIPD, November 2012

An effective security culture requires the commitment of every member of staff, whether they are permanent, temporary or a contractor. If employees are clear about what is expected of them when there is a security incident, they are more likely to respond appropriately, and should be supported when they challenge or report those who do not.

Balancing risk and response

Any security measure, particularly those newly implemented, must be proportionate to the risks faced by the organisation (see NPSA's *Personnel Security Risk Assessment* guidance). Not only will excessive measures waste organisational resources, they could also undermine the implied duty of trust and confidence that employees have in their employer. Breaking this contract could alienate staff and reduce goodwill and confidence in the organisation. It also affects the 'psychological' contract between employer and employee (see the Chartered Institute of Personnel and Development (CIPD) factsheet on the Psychological Contract (July 2013) - a list of CIPD guides and factsheets can be found at *Appendix 2)*.

It is also important that security procedures do not get in the way of employees doing their job. If they do, employees are more likely to avoid complying with these procedures.

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 HR, management and IT and physical security

managers and staff representation/unions, for example. The presence of these experts should also increase the perceived authority of the process to employees not directly involved.

Culture management

An organisation must have a clear idea of the security culture it wants, this will vary according to the nature of the business and the work environment, for example:

- To what extent are individuals expected to make their own decisions about security practice?
- How will the organisation offer consistent guidance to employees so they take the 'right' kind of initiative?
- What level of risk is considered acceptable in the drive to achieve business results?
- To what extent should uniformity of approach be enforced?

The organisation should then 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.[2]

A mechanism that works well in one organisation may be unsuitable for another with a different culture, style and approach to managing security. It is crucial to clarify the desired culture at the outset so that the right mechanisms are adopted within the organisation. The same applies to implementing change in an organisation; the following principles are the same for both situations:

- clear explanations (briefings) to all involved;
- modelling of the desirable behaviours, particularly by senior managers;
- consistent implementation of policies and procedures;
- consultation with representatives of employee groups/representatives.

Management support and governance

Buy-in and commitment from senior management is vital in order to demonstrate the value placed on security. Their support or sponsorship may be crucial to securing the necessary resources to maintain or improve security within the organisation.

Top-down implementation is likely to promote compliance and consistency across all employee groups. Conversely, a lack of awareness of the insider threat at a senior level can undermine the process. Inadequate corporate governance and unclear policies in managing people risk and strengthening compliance can also make it difficult to detect and prevent insider activity.

Organisations should appoint a single, senior accountable owner of people risk to whom all managers with a responsibility for people risk can report.

Line managers also play a key role in the security culture of an organisation. As they are directly responsible for their staff, they are often best placed to commend individuals and pick up on behaviours of concern. The organisation should have objective monitoring mechanisms to support managers and provide performance feedback, as well as safeguarding employees against any manager holding a grudge.

[2] Based on the Culture Management Model developed by Competence Assurance Solutions (C.E. Johnson, 2008)

Clear policies and procedures

Organisations should have clear policies and procedures regarding security culture. They should explain the rationale behind their policies, outline any legal/regulatory requirements, outline compliance with relevant standards, and ensure that all employees understand and consent to these policies. They should also be easily accessible e.g. on a company intranet.

All policies and procedures should be followed openly and consistently, otherwise an organisation's security may be undermined. For example, if employees know that they will not be checked or disciplined for bringing unauthorised electronic devices onto a site, there is little incentive for them to adhere to such a policy.

Clearly defining such procedures enables an organisation to take action against persistent offenders without being partisan or unfair, or regarded as such. Taking a consistent approach will also reduce the likelihood of employees feeling they are being unfairly singled out or discriminated against unlawfully when action is taken. Disciplinary action should be taken in line with the organisation's misconduct procedures.

Organisations should consider incorporating the following in their security policies. This list is not exhaustive, and will vary according to the organisation, their operations, and the results of any Personnel Security Risk Assessment:

- Role-based access to sites, zoned areas within sites, and corporate IT systems.
- A clear desk policy requires documents and other items, including keys and removable objects of value, to be locked away in a secure cupboard or container when the office is unattended. This includes any papers left on printers, photocopiers or in meeting rooms.
- Employees should lock computer terminals when they are away from their desk, and should not share passwords with colleagues. Passwords should be changed as soon as possible if they become compromised.
- Sensitive, confidential or commercial documents should have clear instructions on handling. Employees should log the removal and return of documents.
- Employees should be made fully aware of their responsibilities when in possession of sensitive documents, e.g. working on the documents in public places, secure storage of documents away from site.
- Sensitive documents should be shredded, pulped or incinerated when no longer required, e.g. by complying with the NPSA Standard for the Secure Destruction of Sensitive Items[3]or BS EN 15713:2009[4] (the secure destruction of confidential material).
- A central point for returning old or obsolete IT equipment should be provided so that all data can be safely removed.
- Employees should be made aware of confidential reporting or welfare hotlines/emails.

Security awareness and training

The success of an organisation's security measures and procedures depends on how effectively they are communicated to employees. Individuals are more likely to engage if they understand why security measures are in place and their own responsibilities in relation to them.

Training and awareness provides excellent opportunities to ensure that employees are equipped with the required skills to perform their security responsibilities effectively. This can be achieved through a variety of measures:

[3] www.npsa.gov.uk/advice/Physical-security/secure-destruction-of-sensitive-items/

[4] British Standards Institution: https://knowledge.bsigroup.com

- An induction programme can stress the importance of the organisation's security culture to new staff. It can outline the organisation's security measures and procedures, demonstrate the organisation's commitment to them, and allow new staff to understand what is expected from them.
- Employees may be reminded of and prompted to abide by the employer's codes of conduct when logging on to IT systems.
- Security pages on a company intranet can house security policies, and should be easily accessible to employees. Regular articles and blogs can focus on either general or specific security issues, and can outline new or changes to existing policy. Security e-learning packages can also sit on these sites.
- Security awareness campaigns. These can include awareness days, roadshows, lunchtime briefings or discussions, and competitions. These can be conducted in an informal and relaxed atmosphere, and can be tailored to focus on specific issues.
- Periodic refresher training can tailor specific security messages to specific audiences. This can be done in a group, or by e-learning. Organisations should determine whether such training should be mandatory to all employees, and monitor attendance/completion rates.
- Bespoke DVDs, animations and poster campaigns (e.g. NPSA's *Communicating Personnel Security Messages*) can focus on specific security messages, and can be tailored to specific audiences e.g. senior management, line managers, guard force or the general staff.
- Applying a personal angle to security awareness and training (e.g. secure online banking or transactions to counter identity fraud, or child safety online to reinforce behaviour on social networking sites) can often result in increased appreciation and compliance of security measures by employees.
- Educating staff on the threats posed by social engineering, including methods used and applying effective countermeasures (see the chapter on *social engineering*).

Periodically gauging staff opinion about security standards within the organisation is a useful method of determining current attitudes and to monitor changing trends over time. This can be achieved by using NPSA's *Security Culture Review and Evaluation Tool (SeCuRE)* (see *Appendix 1*). It is important to highlight what the organisation is doing well, but also where it is falling short. The organisation should outline what measures are required to improve security standards, and obtain employees' support and engagement in implementing these measures.

Line management

NPSA's *Insider Data Collection Study* shows a lack of management supervision or oversight and a management failure to address and resolve issues within the workplace can often prevent early discovery of insider activity. Employee disaffection increases, while individual behaviours such as poor relationships with colleagues, absenteeism or anti-social behaviours become more frequent or extreme.

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

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

An effective line manager should:

- give their staff clear and definable goals;
- provide helpful and constructive support and feedback;
- give advice for managing change;
- maintain effective communication.

To help cultivate an atmosphere of loyalty and commitment, as well as reduce the threat of insider activity, line managers should possess the following skills:

- **Awareness** – line managers should know the basics of personality, what motivates people, why employees might become disillusioned and how leaders contribute to the problem of the insider threat.
- **Listening** – if something is beginning to go wrong managers need to identify and resolve the problem as early as possible.
- **Influencing** – having prior insight into what an insider might do, understanding their motivation and identifying potential difficulties early on is not helpful in isolation. Managers also need the skill and initiative to tackle issues quickly and effectively. They should also communicate difficult messages in a timely and appropriate fashion; this helps reduce uncertainty and anxiety among staff (which NPSA research has shown were factors behind some insider acts).

The ability of managers to identify and resolve unhelpful, unusual or suspicious behaviour in their staff will vary. It may be helpful to assess line managers' skills in these areas, and provide additional training and support as required. Security responsibilities should be included in each line manager's job description. If a line manager fails to attend to those responsibilities, then the organisation should address this as a disciplinary matter in line with its HR policies.

Employee welfare

An organisation with a strong welfare culture enables staff to share and address issues before they escalate; this may include providing access to professional support or advice. This is helpful as there are various life circumstances (e.g. 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 the organisation (see the chapter on *screening for the insider threat*).

There should be clear guidelines regarding what will and will not be tolerated by the organisation. If a manager needs to address any given employee behaviour it is important that this is done sensitively, adhering to relevant legislation (e.g. Equality Act 2010, Employment Rights Act 1996).

Addressing behaviours of concern

'Managing poor performance' is a competency frequently found wanting in organisations. While failing to act should not be an option for managers, it can often become the default position. Fellow employees can become dissatisfied because they have to carry a colleague who is not pulling their weight. However, they may also conclude that such conduct or poor performance is acceptable and follow their example.

Organisations should provide managers with the necessary tools and support to identify employees who may require additional attention, support and assistance to prevent their behaviour becoming a more serious concern. Where managers have concerns on an employee's lifestyle and behaviour, circumstantial vulnerabilities, adversarial mind-set or workplace behaviours, for example, these must be supported by evidence observed in the workplace. This will help determine the most appropriate course of action to be taken.

A manager may ask employees questions about their personal life when seeking an explanation for negative behaviour, where their work performance is suffering or there is a clear breach of organisational policy. It is imperative, however, that the focus of those questions centres on their performance or conduct in the workplace. Managers can make general enquiries concerning an employee's well-being or behaviour if it impacts upon the workplace. Although a manager's initial suspicion may be adverse, it is important to remember that there could be an innocent explanation.

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

Appraisals

Appraisals have traditionally been used to measure performance, but are also a useful way of ensuring that regular personnel security checks are conducted on all staff.

Every employee should be provided with the right tools to complete their role effectively. They should regularly agree, discuss and review SMART job and development targets with their management. Setting unrealistic targets or failing to offer employees development opportunities may cause employees to become disillusioned or to suffer from stress.

Specific
Measurable
Agreed
Realistic

Organisations should consider asking employees in sensitive roles to complete an annual security appraisal form (these roles can be identified by undertaking a *Personnel Security Risk Assessment*). 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 or are not appropriate for all employees, a simple checklist of items can be used to ensure that managers and employees are sharing the right information.

The checklist also provides a safeguard to employees by directing them to the range of appropriate questions that a manager may ask. The checklist could include:

- significant changes in financial position (positive or negative);
- change of address;
- significant changes in personal circumstances (e.g. marriage, separation or bereavement).
- any suspicious approach from third parties regarding the employee's work (see chapter on *social engineering*);
- raising awareness of the dangers of sharing too much personal information on the internet (see chapter on *social networks and use of the internet*).

Employees should be encouraged to report significant changes at the earliest opportunity. Appraisal and security forms should supplement and enhance communications between managers and their staff.

Remote working

Remote working, whether it is working from home, on the move or in clients' or satellite offices, is becoming increasingly commonplace. Whilst there are many advantages to these arrangements, there are increased risks in terms of personnel security:

- Direct supervision of remote workers is not possible and providing timely, reliable and constructive feedback is challenging for managers.
- Welfare or performance issues may not be identified or acted on until they develop into more serious problems.
- Remote workers can feel lonely, isolated and 'left out of the loop' when it comes to being informed of important information or development opportunities.

Organisations and managers should:

- agree the number and frequency of meetings with remote workers, and means of communication (i.e. face to face meetings, email, videoconferencing etc.);
- ensure remote workers are kept informed of news and change within the organisation;
- ensure remote workers receive the same training and development opportunities as office-based staff;
- arrange local management for those working at some distance or even abroad.

Further information can be found in NPSA's *Personnel Security in Remote Working*.

Further information

See *Appendix 2* for a list of organisations and websites which provide information and guidance on management and performance issues.

Access controls

Employee access controls should be proportionate to the scale and nature of the threats faced by the organisation. A *Personnel Security Risk Assessment* will determine whether the security measures in place are appropriate, and provide a clear rationale for identifying and implementing new measures.

Role-based access

A role-based access policy limits an employee's access rights within an organisation according to their job activities. This includes restricting access to physical zones (e.g. IT server or storage areas), cupboards, filing systems and IT systems. The 'need to know' principle, adopted by many government departments, allows them to restrict access to information/data etc. to only those who require it. This helps mitigate the risk of sharing sensitive information unnecessarily with colleagues, and allows organisations to detect unauthorised access to information or systems (see also the chapter on *protective monitoring*).

Where possible, access rights according to the role should be standardised across the organisation. This should be agreed with line management and the security department, and helps ensure the consistency of access security.

It is important that organisations assess and review access rights on a regular basis, in particular when an employee changes roles or leaves the organisation. An employee's access rights should not accumulate over time. Where appropriate, access rights and passwords should be set to expire at the end of a posting, or employment. Any extension should be applied for using the same procedures as for the initial application.

Security passes

If security passes are issued, wearing them should be mandatory for everyone in the organisation. Organisations should consider the following when issuing security passes:

- The issuing of passes should be controlled from a central location, preferably within the security department. This prevents employees bypassing the authorisation process, or fraudulently obtaining a pass on behalf of a third party.
- Security passes should include the name and a recent, high quality photograph of the pass holder. However, the information included on the pass should not present a security risk to the pass holder or the organisation should it be lost or stolen.
- Security passes should be tailored to distinguish between differing levels of employee clearance or access, and for zoned access. This can be achieved by colour coding passes or using different orientations.
- Organisations working across a range of different sites should ensure that the pass system is consistent throughout. This reduces confusion and the risk of security breaches if employees, contractors, visitors etc. are issued with inappropriate levels of access.

Organisations should have policies governing the loss or theft of security passes. This should include a reporting mechanism, which should also be available out of hours, depending on the risk posed. Once the loss has been reported, any electronic access should be removed immediately. Disciplinary action may also be appropriate; this should be in line with existing organisation policy.

Employees should be held accountable for inappropriate pass usage. Terms and conditions of use may include not sharing it with any third party, and storing the pass securely when not in use.

An electronic pass system can provide useful data regarding employee entry and exit patterns. It is possible for these systems to flag any attempted pass back (where an employee swipes in and then hands their pass to a third party to gain entry), or if an employee attempts to access the premises outside normal office hours, or an area of the premises to which they have no access rights (see also the chapter on *protective monitoring*). It is important that any flags are investigated fully, and appropriate action is undertaken.

Biometric verification

Biometric technologies refer to automated systems for recognising people based on biological and behavioural characteristics e.g. fingerprint, face, voice or iris characteristics. Biometric technologies can help to achieve a successful access control system, however they should be combined with access control passes/tokens to provide two-tier authentication.

Organisations should consider what additional safeguards biometric technologies might bring to their access control systems. If they are used at all, biometric systems should be used in secure locations within sites – ideally these should be targeted at areas where staff movement will be less than at perimeter access points and where staff access can be restricted to those with a genuine need to access these areas. Organisations should also consider whether the collection of such personal data is necessary or reasonable as employees may object to their personal 'specifications' being held on a security system. This information will be subject to the Data Protection Act 1998.

Visitors

Organisations should maintain a central record of visitors to any given site (this may also be useful or required 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 the identity of their 'host' employee (who should also be held accountable for their visitor while on site).

Visitor passes should provide only the most basic access rights to an organisation, and their accountable return should be mandatory on exit. Any prohibited items policy (e.g. cameras, mobile telephones, tablets) 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.

Network access

Within IT systems, each user can be provided with a separate account, password and access rights. Systems can also record actions, providing a useful audit trail and evidence in any investigation (see the chapters on *protective monitoring*, and *investigations*).

There is a risk in allowing employees to access multiple computer networks from a single workstation. If all networks are not protected to the same level, the connection could result in viral infections, data loss or file corruption to either party. Organisations should specify which connections can be made and by whom, and block any other connections, running and

downloading of executable programs etc. by default. Monitoring systems should capture and report any kind of anomalous behaviour (see *protective monitoring*).

Many organisations provide internet access in the workplace; however, it may be useful to restrict access to some sites in order to protect the organisation from external attack. Where employers have a legitimate requirement to view insecure sites, 'stand-alone' computers, not linked to the organisation's networks, could be used.

Organisations should have robust procedures for password setting and security, which all employees should adhere to. Employees should be prompted to change their passwords on a regular basis, and should be prevented from using obvious choices for passwords (e.g. an employee's own or partner's name and date of birth), or reverting to previous passwords.

Employees should lock their terminals when away from their desks, even for a short time. They should log out from IT systems if they are away from their desks for long periods, or if they leave the premises completely. Terminals should be set to lock or shut down if the terminals are inactive for some time – a *Personnel Security Risk Assessment* and local good practice will determine a reasonable time period for this.

Data or equipment removal

Some organisations will wish to control the removal of data from their systems. This could involve physically disabling the upload/download functions of every computer within the organisation. However, some employees will have a legitimate requirement to transfer sensitive data from one system to another. This could be achieved through the issuing of encrypted USB, which requires password authentication before they are accepted by the secure system, which should run virus checks on any content before it can be uploaded. Alternatively, the organisation's IT department could be responsible for the import/export of all data on the organisation's networks.

All IT equipment should be uniquely identifiable (e.g. by a serial number or barcode), and issued to a named employee who will remain accountable for it until its return. Each device should be equipped with a sufficient level of encryption for the data held upon it. The employee should sign a user agreement, including conditions on acceptable usage, and use of equipment in remote locations, or on the move. Equipment should be audited regularly to ensure it is being used correctly.

Bring your own devices

There is an increasing trend towards employees using their own devices in the workplace. This is referred to as 'bring your own device' (BYOD) and can include laptops, smartphones, tablets or USB-connected devices. Organisations often pay employees to purchase these devices themselves. While BYODs allow greater flexibility and enable the employee to work anywhere, they can provide a number of challenges for the organisation:

- The boundaries between personal and professional usage can become confused, making it difficult for organisations to monitor usage appropriately.
- Insufficient or inadequate security protection on devices.
- Malicious or inadvertent introduction of malware on to company systems.
- Loss of company data if the device is lost or stolen.
- Theft of company data.

- Employee timewasting through visiting websites or using applications on personal devices.
- Obligations of retaining and disclosure arising in litigation may apply to BYODs.

Organisations should decide whether it is appropriate to allow the use of personal devices in the workplace. If so, they should decide on the types of devices allowed, security protection, and who may use the devices (and for what purpose). This should be included in any acceptable usage policy. The organisation and employee should also agree on who is responsible for payment of the device and services, and on the monitoring of company business on the device.

For further guidance, please see the Get Safe Online website (www.getsafeonline.org), and the NPSA and NCSC websites.

Secure contracting

A 'contractor' or 'contract worker' is a worker who is not an employee. They include temporary staff, consultants, those on secondment and attachments. They may be engaged through an agency or by the organisation directly, and can be based on the organisation's premises, at home, or at a third party site.

Contractors are usually given access to the same organisational assets as employees in similar roles. As such, they can have the same impact if they use their access for unauthorised purposes. It is the employing organisation which owns the risk of granting the contractor access to its sites and assets, not the contractor organisation or agency.

Particular challenges in employing contractors can include:

- Timescales for recruiting contractors can often be tight. There can be pressure to overlook some pre-employment screening measures if it is anticipated they will be employed for a short time.
- Income from contract work can be irregular, which can be a motive for unauthorised activity for financial gain.
- A contractor's primary loyalty may not be to the employing organisation, and their commitment to security may be diminished.
- A contractor may work in competitor organisations consecutively or simultaneously.
- Contracts can be renewed or extended to the point where a contractor can work in an organisation for many years, often with little or no re-screening. They can build up an extensive knowledge of the organisation's activities.

In 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 subcontractors are hired, there is a risk that the organisation's security standards may become confused or diluted.

All contractors should therefore be subject to the same pre-employment screening and ongoing personnel security measures as their permanent counterparts. However, in some cases, a contractor may have to be in post without meeting the organisation's usual standards for security clearance e.g. where there is an urgent requirement for the contractor to begin work, or where 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.

A *Personnel Security Risk Assessment* will inform decisions about ongoing personnel security measures, helping to ensure that they are proportionate to the risk of contractors acting maliciously in post e.g. escorted access, restrictions on working hours.

When a contractor has been selected and screened by an agency, systems should be in place to confirm that the person arriving for work is the same person supplied by the agency, for example:

- the exchange of photographs and names between the agency and the organisation;
- confirming identity by document verification (see NPSA's Guide o*n Pre-Employment Screening – Document Verification*);
- industry-recognised arrangements e.g. the Construction Skills Certificate Scheme[5] or the Energy and Utilities Skills Register Card[6] can be an additional safeguard, though not as a replacement for pre-employment screening or document verification.

[5] www.cscs.uk.com/
[6] www.eusr.co.uk/

Inductions/briefings

Contractors should have some form of organisational inductions. Whilst these may not be to the same level as employees, it would be appropriate to give them the same security reminders and updates as employees. This will help them to understand why security is important, and how they can contribute to the organisation's security culture.

Access controls

Where possible, contractor access should be limited physically by zoned/controlled access. Contractors should be issued with a separate, distinguishable pass to permanent staff (i.e. colour and/or orientation), which should contain a recent photograph of the contractor. Organisations should consider:

- restrictions on the hours during which they will provide access;
- retaining contractor passes between visits – this requires the pass issuing team to know when the pass should be handed in and handed out;
- whether a contractor pass should be issued at all, but provide the contractor instead with a visitor pass, and the contractor escorted while on the organisation's premises. Escorted access should also be used where contractors have not been screened to the same standard as permanent staff.

To complement this, a challenge culture for non-compliance with access policies should be promoted and followed.

Contractor passes should be programmed to expire on a daily basis or when the contractor is no longer required on site. They should also be configured to flag any attempted unauthorised activity.

Sensitive IT systems, and the quantity and nature of information that can be accessed, should be restricted to those who require legitimate access, and should also flag unauthorised activity.

Ongoing security management of contractors

Local managers from the organisation's permanent staff 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.

Many contractors do not work on the organisation's premises but at home or at third party sites. They may, as a result, be subject to lower levels of supervision, and feel less involved with the organisation and their colleagues. Face-to-face meetings between contractors and their line manager should be held as often as is practical. This will reinforce the relationship between the contractor and the organisation, and provide a channel through which the contractor can voice any concerns before they develop into disaffection. Further information can be found in NPSA's *Personnel Security in Remote Working*.

The contract between the organisation and the contractor should set out standards of behaviour which the contractor is expected to observe. Contractors should be expected to commit to policies governing acceptable use of email and the internet, obligations toward data protection, security policies, and the organisation's gifts or hospitality polices (i.e. to report any they receive during the course of their contract connected with their employment for the organisation).

Contracts should outline the following personnel security provisions:

- 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.
- The right of the organisation to approve any subsequent choice of subcontractor.
- Where any work should be carried out and who should have access to specific assets.
- A requirement for contract staff to protect the organisation's assets, including restrictions on copying and disclosing company/customer information.
- Access control arrangements (physical and IT access).
- 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 a conflict of interest.
- The right of the organisation to audit the contractor's work in progress, and the contracting company's/agency's security procedures (and those of any sub-contractor).
- Arrangements for dealing with security incidents/breaches.
- A requirement that the contractor or the contracting company/agency must disclose any incident of expulsion from any relevant accrediting or professional body.
- An obligation to inform the organisation if a contractor is no longer employed by the contracting company/agency, has been dismissed, is undergoing any disciplinary procedures or has been arrested.
- Details of who is responsible for any lapses of security. This should be a single point of contact within the contracting company/agency.
- A clause that the contracting company/agency will be liable for financial penalties if it is discovered that the security provisions have not been adhered to (including pre-employment screening).

Organisations should always consult an employment lawyer when drafting contracts.

Contingency measures

The organisation and contracting company/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. The organisation should decide what additional personnel security measures are required e.g. restricted or supervised access, when the replacement contractor visits the premises.

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 true for former employees who are re-employed as contractors.

Steps should 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 that has 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 pose no greater threat to the organisation than previously, to a repeat of the entire pre-employment screening process. The requirement to undergo checks should be stipulated in the contract.

If the contractor has been employed through a contracting company/agency, they will usually carry out these re-checks. It is the responsibility of the employing organisation to stipulate the extent of the checks to be carried out, and to carry out audits as appropriate.

Exit procedures

These procedures should include provisions for revoking physical access to premises, return of all passes, keys and IT tokens, and the return of any company equipment and documents (physical and electronic) before the contractor leaves the organisation. Passes, passwords and IT tokens should also be de-activated. See the chapter on *exit procedures*.

Audits

Organisations should specify the right to audit pre-employment screening and ongoing security requirements with all companies/agencies in the contracting chain in any contract. The audit process should be as transparent and independent as possible.

The terms of reference should be agreed with the contracting company/agency before commencing the audit to ensure that the purpose and scope of the audit is clear. They should include the expected duration of the audit, which records and access to key staff will be required, and where the results will be reported at the end of the audit.

The contract should also contain sufficient compensatory terms (such as a termination clause) if the contracting company/agency is found to be in breach of procedures.

Social engineering

As organisations improve their physical and electronic defences external individuals/groups wishing to obtain confidential or sensitive information may attempt to exploit those within the organisation with legitimate access. This process is known as 'social engineering'.

NPSA's *Social Engineering – understanding the threat* provides guidance on understanding and countering the threat posed by social engineering to individuals and organisations. The following summarises key considerations in this process:

> In January 2013 a former business relationship manager at a communications company tried to persuade his former colleagues to allow him access to company premises and IT systems. The manager, who had left the company the previous year due to redundancy, told staff he was now working as a contractor for the company, and was awaiting his new pass and laptop. He also persuaded an employee to facilitate his access to the company IT systems using his own login.
>
> When confronted by a senior member of staff at the company, the manager stated he wanted to maintain personal relationships with company staff as he had known all of them prior to leaving the company. The manager was then escorted off the premises. The company then spoke to the manager's current employer (who were a vendor of the company's services) to remind them of their responsibilities. The manager was dismissed by his new

Social engineering can be mounted by commercial competitors, single issue groups, terrorist organisations, foreign intelligence services or criminals. Typically, the social engineer will find out as much as possible about the target individual or organisation before mounting an attack.

Social engineers may adopt a number of different techniques to achieve a successful outcome. These might include: emphasising their seniority or credibility to elicit a response; stating that other colleagues have provided information or allowed access previously; emphasising help the social engineer has given the target, leading the target to return the favour; pointing out the target has complied with similar requests in the past.

Name-dropping, appearing to be in a hurry and also simple flattery (even when the target is aware it is being used) are all powerful tools for encouraging people to divulge information.

Countermeasures

The most effective countermeasure available to organisations to protect themselves and employees from attack is education. Employees should be made aware of how social engineering works and the value of the information they hold.

Awareness on social engineering should include an overview of the range of possible methods 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;
- refraining from discussing sensitive working issues in social situations;
- not opening emails from unknown or suspicious senders;
- treating all email attachments with caution, including turning off the option to automatically download attachments.

Organisations should consider implementing the following steps to support its employees in keeping information secure:

- Developing corporate data strategies, ensuring that information relating to the organisation and its employees is handled and distributed in a considered and consistent manner.
- Adopting 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 trends or repeated attempts to acquire certain information, so that other colleagues can be made aware.
- Ensuring that information posted on the organisation's websites is sufficient to inform the public without offering superfluous details that will assist in the preparation of social engineering attacks. Further information can be found in NPSA's *Security-Minded Comms – protecting your organisation through your corporate communications*.
- Implementing policies covering the destruction of all hard copy documents and IT media (e.g. USB sticks, CD-ROMs etc.), particularly if they contain sensitive information.
- Requiring that employees declare gifts and hospitality, and reviewing lists frequently to identify unusual trends or inappropriate gifts or hospitality.
- Maintaining a clear desk policy and a culture where information is handled on a 'need to know' basis.
- Including awareness and training to detect and deter social engineering in both induction and regular ongoing security programmes. Articles in company newsletters and on the organisation's intranet sites can also help to reinforce this message.

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

- reminded of the control procedures which apply to their roles, in particular those governing how and when an enquirer's credentials should be checked, before responding to any requests for information;
- educated in identifying and responding to 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, but confident that they will have management support when they do so.

All suspected cases of social engineering should be reported, investigated fully and, where possible, resolved.

Social networks and use of the internet

For businesses and organisations, the internet and social networks are important media for the provision of goods and services, public engagement, promoting business, marketing and building confidence. For individuals, social networks have become an indispensable part of their lives, enabling them to keep in touch with friends and family, make new contacts and share information.

However, the internet and social networks bring a number of significant risks when used both in the workplace and at home:

- Users can download viruses, and access and download sensitive or unnecessary information.
- Excessive use can result in considerable timewasting and lost productivity.
- It is extremely difficult to remove content from the internet once it has been published. Shutting down a profile, for example, does not delete information.
- Businesses and organisations are at risk of considerable embarrassment if an individual's private life and opinions are linked to their employer, or if the individual posts sensitive or inappropriate material.
- An individual's personal profile of posts might reveal attitudes which might not fit in with the employer's values, and could lead to a potential conflict of interest.
- An individual's profile may contain large amounts of information which could be useful to criminals, commercial competitors, terrorists or hostile foreign intelligence services.
-

Managing the risks

Organisations should have policies and procedures on the use of the internet and social networking which are both practical and proportionate. Organisations should ensure that they are explained clearly to staff, that they have the agreement of staff and staff representative bodies, and that they are easily accessible (e.g. on a company intranet). Policies should be reviewed at regular intervals to ensure they remain current and fit for purpose. Always seek legal advice before introducing or amending policies.

Policies should include information on:

- the blocking of websites in the workplace (e.g. gaming, gambling or pornography websites) or have restricting access and usage. This may also reduce the risk of malicious software being installed on the system;
- implementing effective filtering across internet gateways (e.g. spam blockers, firewall and antivirus software), and ensuring that the latest updates to these and the operating system are promptly installed;
- acceptable usage, including posting content, password setting, performance issues, whether staff should agree to abide by a code of conduct, and inappropriate language or behaviour.
- guidance on the level of information staff should enter on their personal and professional profiles, privacy settings, and keeping their personal and professional profiles separate;
- staff should refrain from entering details of any security clearances or access to information or company sites on their profiles;
- appropriate sanctions for misuse;
- training and awareness programmes.

Organisations should also consider limiting the amount of information they publish on their websites about company sites, employees or senior management (including their contact details), research and development or work on sensitive contracts. This will reduce the risk of

state or commercial espionage, and social engineering (see also the chapter on *social engineering*, and NPSA's *Security-Minded Communications – protecting your organisation through your corporate communications*).

For further information, please see NPSA's *Online Social Networking*. The Get Safe Online website (www.getsafeonline.org) provides helpful and practical guidance for both organisations and individuals on acting securely online.

Screening for the insider threat

The purpose of screening is threefold:

- To identify individuals displaying types, levels of or clusters of behaviour which have been seen in previous insider cases. Identifying and acting upon such concerns is an integral part of effective ongoing personnel security management.
- To identify suspicious behaviours in the workplace (e.g. accessing databases or taking sensitive information offsite without authorisation).
- To assess the risk posed by an individual moving to a more sensitive role, where damage from insider activity would be greater.

The screening process

It is important that organisations have a clear justification for screening, identifying those roles where the risk is greatest, and ensure that the screening is carried out in a proportionate and transparent manner.

Identifying employees who may give cause for concern involves a basic level of screening for all employees, which can act as an initial filter. The tools and techniques used should be suitable for application across sizeable numbers of people and could include, for example:

- automated monitoring of employee activities to identify anomalous behaviour;
- using the appraisal process for managers to identify signs and behaviours of concern;
- application of more detailed assessment or tools by trained practitioners when concerns are raised by a line manager or colleague, which should be supported by evidence;
- raise awareness throughout the organisation on personnel security and the insider threat;
- providing mechanisms for employees to express their concerns.

Screening must be complemented by effective management and welfare to resolve and manage concerns as they arise (see also the chapter on *line management*). For example, it may be that there is an underlying welfare issue that requires employee assistance. This may involve a more direct approach, generally through face-to-face interaction such as an interview. Any suspicious concerns that persist should be addressed in more depth, usually by an internal investigation.

Organisations should run awareness programmes to ensure that line managers and employees do not overlook problematic or negative behaviour, and are comfortable in observing and reporting behaviours of concern. When concerns are raised, it is important not to overreact but to take swift and proportionate action in order to avoid any escalation. Organisational procedures should always be followed, to ensure that appropriate steps are taken in each case.

Reporting concerns

Providing a trusted resource for staff to report security concerns or suspicions, either anonymously or otherwise, is a positive way of nurturing a security culture within an organisation.

In organisations with a good security culture, the line manager will usually be the first point of contact for employees wishing to report unauthorised activity. Other avenues of receiving information may include speaking directly with a security or HR manager; receiving reporting from the public; or approaches from security authorities such as NPSA or the police (see NPSA's *Managing the Disclosure of Employee-Related Information*).

Employee hotlines

Where the above are not sufficient, the organisation should consider an employee hotline. This can take the form of a dedicated telephone line, internet/intranet contact site, or a dedicated company email address.

An employee hotline can serve two functions:

- Enable employees to report suspicions or actual incidents of illegal, unethical or improper conduct by their colleagues, employers, clients or third parties such as bullying, fraud, theft, or failure to adhere to security or health and safety procedures.
- Act as part of a staff welfare programme, enabling employees to seek advice on a range of issues e.g. financial difficulties.

Reporting hotlines are not designed to replace the line manager-employee relationship. They are intended to provide additional benefits e.g. out-of-hours reporting, where this is desirable.

Organisations should consider the following when implementing a hotline system:

- Organisations must seek legal advice prior to introduction.
- The hotlines 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.
- Employees should be made aware of all avenues open to them (including hotlines) to report concerns. These should all be readily available and easy to access.
- There should be clarity among employees on the procedures for reporting concerns, and the nature and content of calls that the hotline will accept.
- The hotlines should be available twenty-four hours a day. Employees may be less likely to use it while they are at work with the colleague(s) whose actions they wish to report.
- If the hotline is telephone-based, it should be free or at a low-rate tariff, as calls may be made from employees' own telephones.
- If the hotline is provided internally, it should be independent from the department responsible for investigating incoming reports.
- If the hotline is provided externally, there should be clear procedures on handling calls concerning criminal activity, including who should inform the police.
- The hotline provider should provide timely and meaningful information to management concerning the nature of incoming reports. This can be used to identify trends and influence organisational policy.
- Appropriate measures should be in place to support staff using the hotline. Effective sanctions, including disciplinary procedures, should also be in place to deal with malicious reporting.

The procedures for handling incoming incident reports must be clearly documented, and should be strictly adhered to in order to maintain employee confidence in the integrity of the system. To ensure a consistent response, the procedures should provide guidance on the handling of incoming reports (including dealing with irrelevant or malicious reports), and the next steps e.g. assessing the seriousness of the report, and ensuring that the details are forwarded to the appropriate party for further action.

Anonymity

Reporting hotlines can be anonymous. However, where possible, anonymous sources should be encouraged to provide their identity, particularly if the information is significant, and could lead to possible prosecutions.

Employers should provide assurances that anonymity will be preserved as far as possible. In some cases, it may be possible to carry out the entire investigation without revealing the employee's identity. However, this is unlikely to be achievable in every case. Depending on the severity of the reporting, it may be necessary to consult the employee making the report should an investigation reach the point of having to reveal their identity.

Data protection

Another consideration concerning anonymity results from a conflict between US and EU legislation on data protection, and how information recorded during reports to hotlines is processed (especially if the hotline provider is based overseas). In the US, the Sarbanes-Oxley Act 2002 requires organisations to implement an anonymous helpline to facilitate the reporting of accounting, auditing, banking and financial corruption. In the UK, organisations operating anonymous hotlines must collate and process information in line with the Data Protection Act 1998 (derived from the EU Data Protection Directive 95/46/EC).

Regulatory frameworks vary from country to country. Some countries do not allow personal data to be transmitted across their borders. Some government agencies have powers which enable them to access personal data stored on local servers. The confidentiality of hotline reports cannot, therefore, be guaranteed. For example the US-EU Safe Harbor Framework provides a way for US organisations to avoid interruptions in their business dealings with the EU or facing prosecution by European authorities under EU member state privacy laws.

Whistleblowing

The Employment Rights Act 1996 (ERA), amended by the Public Interest Disclosure Act 1998 (PIDA), provides employees with the right to complain to an employment tribunal if they are dismissed or suffer any form of detriment as a result of making a 'protected disclosure' (commonly known as 'whistleblowing').

A disclosure may qualify for protection if the person making it has reasonable belief that one or more of the following has occurred:

- 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.

The protected disclosure must be made to an appropriate person e.g. the employer, regulators, official bodies or other designated persons.

The Enterprise and Regulatory Reform Act 2013 introduced a number of amendments to ERA:

- A disclosure only qualifies for protection if the employee reasonably believes that it is being made in the 'public interest'.
- The Act removes the previous requirement under ERA for a protected disclosure to be made in 'good faith'. If an employer can show that the disclosure is not made for one or more of the reasons outlined above, an employment tribunal will dismiss an employee's claim for unfair dismissal or treatment.
- Employees may be personally liable if they victimise a colleague engaged in whistleblowing.
- Employers may be vicariously liable for those employees' acts against a whistleblower, although there will be a defence where the employer has taken all reasonable steps to prevent victimisation occurring.

Employers seeking to show that they have taken all reasonable steps to prevent victimisation by colleagues must demonstrate that they have clear and up-to-date whistleblowing policies in place. The policies should encourage openness, so that employees can raise issues without fear of reprisal or public exposure. They should include guidelines and time-limits for any consequent investigation. They should also outline sanctions and penalties for those making false or malicious accusations, and for those found to have victimised colleagues for whistleblowing.

Further information can be found in the CIPD factsheet on whistleblowing (May 2013), and the Publicly Available Specification (PAS) 1998:2008, the code of practice for whistleblowing arrangements.

See *Appendix 2* for websites explaining legislation and guidance referred to in this chapter.

Protective monitoring

NPSA's *Insider Data Collection Study* shows that some organisations had not made regular or systematic use of their own IT or financial auditing functions to spot irregularities or unusual behaviours. In others, counter-productive workplace behaviour was known in one part of the organisation but this knowledge was not shared with other sections. This can result in delays to the organisation taking mitigating action to reduce the risk, allowing insiders to act in the first place, and for some to continue acting without detection for longer than necessary.

To fully understand the level of risk an employee poses, organisations should access information held by HR concerning performance and welfare issues, IT for information about access to electronic data, and Security for physical breaches of security policies. A *Personnel Security Risk Assessment* should be used to ensure that monitoring is in proportion to the risks facing the organisation.

NPSA's *Holistic Management of Employee Risk* advocates a holistic approach to protective monitoring where information about employee risks (physical, electronic audit and personnel data) can be brought together under a single point of accountability. It provides advice on establishing effective protective monitoring and audit capabilities, and to act in a transparent, legal, ethical and proportionate manner.

Monitoring across networks

Most IT networks can be configured so that every event that takes place e.g. a user accessing a database file, generates an entry into a log. The entry will typically include the username or identifier, the date, time and other details relating to the event. An entry can also be recorded for failed events such as an unsuccessful attempt to open a file.

Although it is more usual for electronic systems to be monitored, organisations should also monitor physical access controls such as swipe cards or 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 of IT systems.

Monitoring and analysis can be carried out in either real time or offline, triggering an alert when a systematic effort to penetrate the organisation's access controls is detected. This can range from a single event, such as a rejected swipe card at a secure door, to patterns of events generated by various network components. For example, detecting the unauthorised removal of data from an organisation's database might require the examination of logs from the database, the firewall and the email system.

Monitoring of single channels

The following channels can also be monitored in isolation:

- **Email** – outgoing mail and attachments can be filtered for words denoting sensitive contents, and other terms that might indicate a leak of policy or the transmission of sensitive data, for example. The opening of email attachments and links can also be blocked to reduce the risk of introducing malicious software into the organisation's networks.
- **Internet use** can be monitored to detect attempts by employees to access inappropriate websites.

- **Telephone details** such as numbers dialled and the duration of calls, but could also be extended to the recording of telephone conversations (as is common in call centres).
- **Exfiltration of bulk data**.

Monitoring using closed-circuit television (CCTV)

A CCTV system uses a single or series of television cameras joined by a transmission link to relay images to a series of monitors, usually sited in the guard room or central control point. Depending on the sensitivity of the area under surveillance, CCTV may be used in isolation or in conjunction with other protective security measures such as intrusion detection systems.

CCTV can help clarify whether a security alert is genuine, and could be vital in any post-incident investigation. The monitoring and retention of CCTV footage must fully comply with relevant legislation (see below). If monitoring live CCTV, organisations should ensure there are adequate numbers of trained staff to carry out the monitoring. Any contract staff who operate CCTV equipment must be licensed by the Security Industry Authority.

Further information can be found on the NPSA (www.npsa.gov.uk/advice/Physical-security/CCTV/) and National Counter Terrorism Security Office (NaCTSO)[7] websites.

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:

- failure to observe a clear desk policy;
- unlocked drawers, key cupboards or safes;
- uncollected papers left on printers;
- unattended computers or laptops with users logged in;
- the use of removable media such as CD ROMs or USB sticks;
- security passes not being worn;
- doors to secure areas left or held open.

Please see *Appendix 3* for considerations on implementing protective monitoring. *Appendix 4* outlines relevant legislation covering protective monitoring.

[7] www.nactso.gov.uk/managing-the-risks

Investigations

Many organisations will at some point need to carry out some kind of internal investigation into a member of staff. However, not all organisations have dedicated investigation teams. When concern is raised about an employee, organisations can be unsure of how to react, particularly if an accusation of wrongdoing is hard to prove.

The primary duty for an investigator is to establish the true facts, and to be fair and objective when dealing with those raising concerns and the employee being investigated. In the event of an employee taking their employer to a tribunal, any hint of unfairness, lack of objectivity and thoroughness, or oppressive behaviour will significantly undermine a case.

Employers can react disproportionately to accusations; this can lead to costly employment tribunals or an unhappy and disaffected workforce. However, with correct procedures in place, employees who understand policies and regulations and competent investigative staff, organisations are better equipped to avoid potential pitfalls.

NPSA's *Investigating Employees of Concern* provides guidance to employers on the stages involved in conducting investigations. *Appendix 5* provides a summary of the main considerations explored in this guidance.

Exit procedures

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

The opportunity an employee will have to act maliciously after tendering their resignation or leaving the organisation will vary depending on their role; the exit procedures should reflect this. The example here shows the damage which can be caused if organisations fail to take appropriate steps to prevent employees abusing their knowledge and access privileges.

> In 2013, a company at a US airport had its contract terminated after it failed to collect or de-activate security passes of over 20 employees when they left the company. With the assistance of a colleague, one former employee gained access to restricted areas of the airport on at least two occasions.
>
> Press reporting

Protecting the organisation

If someone leaves an organisation feeling badly treated, ignored or unappreciated, they may be less restrained about what they say and may not feel guilty about damaging the organisation or disclosing company information. However, with the right handling and aftercare their inclination to be disloyal can be limited.

As soon as a line manager becomes aware that an employee is leaving an organisation they should, in consultation with security and HR departments, assess and where necessary manage the risk that the employee may pose in leaving the organisation. This will be influenced by a number of factors, for example:

- whether the employee is leaving voluntarily or as the result of a disciplinary process or redundancy;
- if they are not leaving voluntarily, the reason for their dismissal;
- whom they are going to work for (e.g. a competitor);
- their current role and the sensitivity of the organisation's assets they have access to.

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

- allowing the employee to continue working during their contractual notice period, retaining all their usual access to the organisation's assets;
- allowing the employee to work their contractual notice period, but with reduced access to assets (e.g. using additional supervision or allocating lower-level IT access);
- asking the employee to leave immediately, possibly under supervision, to prevent any unauthorised act while still on the premises. The employee should not return for the duration of their notice period (this is sometimes referred to as 'gardening leave').

The fact that an employee is leaving voluntarily does not necessarily mean that they can be allowed to continue working unsupervised for their notice period. If they are leaving to work for a competitor, if may be appropriate to remove their access to commercially valuable information. If they are employed in a sensitive position, it may be necessary to ask them to leave immediately; however this may cause ill-feeling, and should be used with caution. Where there is a risk but there is no justification for an immediate exit, it may be appropriate to reduce an employee's access and/or introduce additional safeguards for the remainder of their employment.

Once a leaving date has been agreed and regardless of the circumstances of the employee's departure, the organisation should ensure that all assets in the possession of the employee are returned. These may include:

- security passes and/or identification cards;
- company mobile/blackberry/pager(s);
- company laptop and other IT equipment e.g. memory sticks, mobile dongles, flash drives;
- any books, papers or commercially sensitive documentation;
- token(s) for access to electronic systems;
- keys to secure storage areas;
- company credit cards;
- any unused personal business cards;
- any protective clothing or clothing displaying the company logo;
- security containers such as security briefcases.

If the employee is leaving immediately, they should return all company property within the tightest possible timescales. However, if they are expected to continue performing their duties, or a limited subset of them, during their notice period, then this requirement should be amended accordingly. For items not recovered at this stage, a date and method of their return (in person or by post, for example) should be agreed with the employee.

Organisations should consider using an exit checklist to document all items requiring return, exit interviews etc., which should only be signed off once all actions have been completed and all assets returned. The contents will vary depending on the role and assets to be returned.

At the same time as the recovery of assets, the organisation should also consider additional steps to reduce the employee's access to assets, including:

- selectively or completely blocking the employee's user-ids to prevent system access;
- deleting organisation data from any personal devices;
- changing passwords to common systems;
- ensuring that measures are in place to protect the organisation's electronic systems from malware or hacking;
- selectively or completely blocking the employee's security pass to prevent physical access;
- changing door codes to common areas;
- changing combinations to storage areas and/or security containers;
- cancelling the employee's signature authority, credit card and expense accounts, ensuring that all relevant parties are notified;
- issue 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 outstanding actions should be scheduled and implemented as soon as is practical.

The exit procedures outlined above should also be used in more dispersed organisations where employees may not be in the same building as their line manager, security or HR department at the time of leaving. This would include employees working from home or at other sites (including overseas), on paid leave pending an investigation, or on sick or maternity leave.

Exit interviews

The exit interview is an opportunity to:

- ask and listen to the employee's reasons for leaving, particularly to any comment on how the organisation might have been responsible for their decision;

- recover as many of the organisational assets, access tools and identifiers as is reasonable at the time;
- obtain all passwords or encryption keys for files the employee has been working on;
- ask the employee if they have any comments or observations about the strength (or weakness) of the security culture, measures or procedures in place within the organisation;
- remind the employee of their security obligations under organisational codes of conduct concerning access to assets and intellectual property or (where appropriate) the Official Secrets Act. To reinforce this, some organisations ask the employee to read and sign a form summarising these points, which affirms their commitment to this process.

Where 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 HR manager should arrange the exit interview. However, 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 security issues.

The timing of the exit interview should be driven by the personnel security issues. Where the risk is high, the interview should be arranged promptly to ensure that the employee is aware of their security responsibilities at the very start of the notice period.

End of posting

If an employee is moving to a different post within the same organisation, the organisation should ensure that access to systems (including passwords) is revoked, and the return of any access tokens, if the employee will have no requirement to access them in their new role. Additionally, the employee should return any company assets (as described on the previous page), if they have no legitimate reason to keep them for the purposes of their new role.

Appendix 1: NPSA guidance

The following NPSA guidance and tools provide useful additional information on ongoing personnel security procedures:

- **Personnel Security Risk Assessment: a guide** – focuses on individuals (be they permanent employees, contractors, agency staff etc.), their access to an organisation's assets, the risks they pose to the organisation and the sufficiency of countermeasures implemented.
- **Holistic Management of Employee Risk (HoMER)** – guidance to manage the risk of employees' counterproductive behaviour whether inadvertent, negligent or malicious.
- **SeCuRE: Security Culture Review and Evaluation Tool – a guide for organisations** – a tool to shape the direction of an organisation's security procedures. It also provides a snapshot of how employees view security in the organisation.
- **Investigating Employees of Concern** - guidance on the stages involved in conducting investigations.
- **Managing the Disclosure of Employee-Related information** - guidance on how to manage employee-related information disclosed to organisations by the security authorities.
- **Online Social Networking** – Joint NPSA/CESG guidance on the risks associated with the use of online social networks and how they can be used safely.
- **Personnel Security in Remote Working** – guidance on the personnel security vulnerabilities in remote working, and how to reduce these risks.
- **Personnel Security in Offshore Locations** – guidance on the extent to which good practice personnel security measures, designed to mitigate the insider threat, can be applied effectively overseas.
- **Social Engineering: understanding the threat** – guidance to identify the threat from those who wish to extract information from employees or gain access to sites using psychological manipulation.
- **Motivation within the Security Industry** – also referred to as *Guard Force Motivation*, guidance to help those responsible for managing security personnel develop and maintain a security-effective and motivated guard force.
- **Communicating Personnel Security Messages** – six short animated films to promote interest in personnel security.
- **Security-Minded Comms** – guidance for an organisation's communication professionals on how to audit their internet profile, and how to publish information in a customer-focused way without giving away too much detail.

For further information please visit www.npsa.gov.uk.

Appendix 2: Useful websites

Chartered Institute of Personnel and Development (CIPD)

- Line management behaviour and stress at work (June 2009) – guidance for managers and HR departments: www.cipd.co.uk/hr-resources/guides/. The following factsheets (www.cipd.co.uk/hr-resources/factsheets/) are also of interest:
    - The Psychological Contract (July 2013)
    - The role of line managers in HR (April 2012)
    - Performance management: an overview (May 2013)
    - Employee communication (March 2014)
    - Employee engagement (August 2013)
    - Employee voice (September 2013)
    - Whistleblowing (May 2013)

Line management and performance

- **GOV.UK**: https://www.gov.uk/browse/working/redundancies-dismissals - Problems at work.

www.gov.uk/equality-act-2010-guidance - Legally protects individuals from discrimination in the workplace. The Act replaced a raft of anti-discrimination legislation including race, gender, age, disability, religion and sexual orientation.

- **Equality and Human Rights Commission**: www.equalityhumanrights.com
    - **Legislation.gov.uk**: www.legislation.gov.uk/ukpga/1996/18/contents - Employment Rights Act 1996. Organisations must not unfairly dismiss an employee. An employee who considered that the actions of their employer have breached the implied duty of mutual trust and confidence may resign and claim constructive unfair dismissal.
    - **Advisory, Conciliation and Arbitration Service (ACAS)**: www.acas.org.uk

Reporting concerns – data protection legislation

- **Sarbanes-Oxley Act 2002**: www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf
- **EU Data Protection Directive 95/46/EC**: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
- **US-EU Safe Harbor Framework**: export.gov/safeharbor/eu/eg_main_018476.asp

Whistleblowing – legislation/code of practice

- **Employment Rights Act 1996**: www.legislation.gov.uk/ukpga/1996/18
- **Enterprise and Regulatory Reform Act 2013**: www.legislation.gov.uk/ukpga/2013/24/part/2/crossheading/protected-disclosures/enacted
- **Publicly Available Specification (PAS) 1998:2008**: shop.bsigroup.com/forms/PASs/PAS-1998/

Appendix 3: Protective monitoring – considerations

Before monitoring takes place

- Always seek legal advice when introducing or updating protective monitoring policies or procedures.
- Be clear about the purpose of protective monitoring and that it is clearly justified by the risk, and ensure that any monitoring solution actually achieves its purpose.
- Employees should be fully aware of the policies and rationale behind protective monitoring within the organisation, and that all employees and employee representative bodies understand and support these measures. This can include training, information in staff handbooks or the company intranet, or message pop-ups when logging on to computers. If monitoring is used to enforce rules and standards, employees must know what these are.

Procedures

- For monitoring to be effective, each employee must have unique identities such as a swipe card and PIN for physical access, and user-id and password for systems access.
- Agree thresholds/flags for investigating unusual activity meriting further investigation. All monitoring systems are likely to produce 'false positives' – alerts where no suspicious activity exists. The extent to which systems can be fine-tuned to avoid these will vary from network to network. Alerts should be manually reviewed by somebody with a good understanding of normal access behaviour.
- Conversely, there is also a risk of 'false negatives'. The opening of a restricted file by a user name or identifier with appropriate access privileges, for example, 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 where the likelihood of employees sharing passes, passwords etc. is low.
- Covert monitoring should only be used on rare occasions, possibly as part of a wider investigation (see the chapter on *investigations* and NPSA's *Investigating Employees of Concern*).
- The frequency of event log analysis will depend on the organisation and the environment in which it operates. The more reliance an organisation places on monitoring, the more frequently the analysis will take place. In organisations with other ongoing personnel security measures in place, the dependence on monitoring may be reduced and analysis less frequent. However, analysis offline rather than in real time may result in unauthorised activity only being identified after the event.
- Arrangements must be made for the storage – sometimes over a considerable period – and efficient retrieval of data generated by monitoring. Depending on the quantity of data involved, a balance may have to be struck between the desired length of the audit trail and the cost of storage. A *Personnel Security Risk Assessment* can prioritise the risks faced by the organisation, and identify the key targets for monitoring e.g. specific entrances or exits, IT applications or transaction types.
- Event logs must be stored securely so that they cannot be tampered with, which is vital for evidential purposes.

Appendix 4: Protective monitoring - legislation

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

- **Data Protection Act 1998** (DPA) – www.legislation.gov.uk/ukpga/1998/29/contents - Almost all forms of monitoring will involve the collection of personal data. The DPA places responsibilities on organisations to ensure that personal data is collected lawfully and processed in a fair and proper way. Part 3 of the Act concerns monitoring at work.
- **Human Rights Act 1998** – www.legislation.gov.uk/ukpga/1998/42/contents - Article 8 of the Act provides for the right to respect for private and family life. Individuals' Article 8 rights extend to the workplace.
- **Employment Practices Code** – www.ico.org.uk - The Code is issued by the Information Commissioner's Office (ICO) and is intended to help employers comply with the DPA, and to encourage them to adopt good practice. Part 3 of the Code addresses monitoring in the workplace.
- **CCTV Code of Practice (revised edition 2008)** – This code is issued by the ICO and helps organisations to comply with the law when using CCTV to carry out monitoring.
- **Regulation of Investigatory Powers Act 2000** (RIPA) – www.legislation.gov.uk/ukpga/2000/23/contents - RIPA regulates the use of intrusive surveillance and investigation techniques, including the interception of communications.
- **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** – www.legislation.gov.uk/uksi/2000/2699/contents/made - These regulations provide for certain circumstances in which intrusive techniques such as the interception of communications can be used in the business context.

Appendix 5: Investigations - key considerations

Before the investigation

- Employers should offer their staff easy to use, non-confrontational and secure means of registering concerns about colleagues and security in general. These measures should be advertised to staff.
- Written guidance outlining the purpose of investigations is important to guide investigators through the process. If an organisation operates a zero tolerance policy, there is an obligation to investigate concerns no matter how awkward if might be for the organisation. However, any response must be proportionate.
- If it is suspected that a criminal act has taken place, law enforcement should be contacted as early as possible. They will be able to provide appropriate advice on proceeding with an investigation, or take over the investigation if required.
- Investigators should consider the motivation of those making an accusation, and decide how they wish to deal with any malicious reporting.
- Management support is essential to reduce potential repercussions at a later stage.
- The scoping of the investigation should begin with determining why an investigation is necessary and appropriate. The planning process should involve input from management, HR, legal and other stakeholders with knowledge or insight into the issue.
- To ensure impartiality, it is important that anyone involved, or suspected of involvement in the action being investigated is not involved in the investigation. If this is the case, suitable alternatives should instead be consulted.

During the investigation

- The number of people informed of the investigation should be limited to those who have a need to know. Any leaks may jeopardise the investigation.
- The investigators must decide whether the investigation should be conducted in an overt or covert manner. If the investigation is overt, the investigators should decide how much information can be disclosed to the individual being investigated.
- Agreement should be reached with HR and employment lawyers whether the individual being investigated should be suspended (if there is a chance that evidence might be removed or tampered with before the investigation team can assess it), restrict the employee's access or move them to another role for the duration of the investigation.
- Throughout the investigation, the investigators should record thoroughly all actions or enquiries taken, the reasons for doing so, and the results of those actions/enquiries. Investigators should seek legal advice throughout the investigative process.
- Consideration should be given as to whether physical searches and monitoring (e.g. CCTV, access control, access to/use of company systems) are required.
- Physical searches should only be conducted if there is reason to believe that information or evidence may be lost or destroyed. An independent person should be present during any physical searches, they can observe the search and record anything which is removed during the searches.
- Any monitoring must be done legally, proportionately, and in line with the organisation's policies. See also the chapter on *protective monitoring*.

- Interviews should be used to gather information, not to interrogate the subject of the investigation in a hostile manner. The interviewer should create an atmosphere which creates openness and increase the likelihood of information being offered.
- Interviews with those raising concerns or other witnesses can help establish facts, assess the credibility of those making the claims, and identify further areas for investigation.
- Employees should be offered the opportunity to have representation from a trade union official or colleague to accompany them. The organisation may be accused of not following correct procedures if this is not offered.

Following the investigation

- The investigators should consider outcomes of the investigation, and how they should be addressed. This may range from no action if no evidence of wrongdoing is found, through to disciplinary procedures or even dismissal if an offence has been committed.
- Following the conclusion of an investigation, a review should be conducted to identify how the investigation progressed, identify any problems that arose, and determine whether existing policies and procedures are sufficient, or require updating.