

PERSONNEL SECURITY IN OFFSHORE LOCATIONS

JUNE 2009

Disclaimer:

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

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. Nothing included herein should be interpreted as legal advice - you should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

This briefing note is based upon a research document compiled on behalf of CPNI by KPMG. This document, entitled '*Personnel Security in Offshore Centres; A summary of findings*' is available on CPNI's public website www.cpni.gov.uk. It was compiled during December 2008 – January 2009 and the information derived from this source was considered current at the date of publication.

Contents

Introduction	3
Overview	4
Making the decision to offshore	5
Establishing good communication with offshore staff	6
Cultural considerations	7
Impacts of offshoring on UK based staff	7
Managing the recruitment of offshore staff	8
Confirming identity	9
Nationality and immigration status	9
Verifying credentials	10
References	11
Finance checks	11
Health/drug screening	11
Ongoing personnel security offshore	12
Access controls	12
Protection of data	13
Employee monitoring	13
Reporting hotlines	14
Investigative techniques available offshore	15
Licensed investigators	15
Surveillance	16
Intercepting communications	16
Interview	16
Search/seizure	17
Involving the police in an investigation	17
Sources of information	18
Appendix A: Comparison table of pre-employment screening measures available	19
Appendix B: Comparison table of ongoing personnel security measures available	21
Appendix C: Comparison table of investigative techniques available	22

Introduction

Centre for the Protection of National Infrastructure

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

The national infrastructure

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

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

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

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

The aims of this guidance

This guidance has been written for UK government departments and organisations within the CNI who are already engaged in offshoring or who are planning to offshore some aspect(s) of their business. It considers the extent to which good practice personnel security measures, designed to mitigate the insider threat, can be applied effectively overseas.

CPNI does not attempt to define a single 'best practice' regime for offshore personnel security. Rather, this document aims to provide a useful starting point for a consideration of the issues involved with personnel security overseas, providing relevant factual information and examples from some of the most popular offshoring locations for UK organisations.

It is recommended that the current guidance should be read in conjunction with the following CPNI guidance documents which are referenced throughout and are available at www.cpni.gov.uk.

- Personnel Security Risk Assessment: A Guide
- A Good Practice Guide on Pre-employment Screening
- Ongoing Personnel Security: A Good Practice Guide

Overview

Addressing any security issue arising in an offshore business location is likely to bring particular challenges for UK organisations, not least due to the logistical difficulty of being separated geographically. The nature and severity of threats may differ from those experienced in the UK and organisations may not be familiar with local customs, security practice and legislation.

Personnel security measures aim to reduce the threat from 'insiders'; that is from an organisation's own employees who may exploit their legitimate access for unauthorised purposes. This guidance begins by considering the personnel security factors involved with the initial decision to relocate to an offshore environment, including possible cultural considerations and the potential impact on UK based employees.

The next section explores differences in pre-employment screening practices and legislation in eleven different countries (see list below), highlighting potential complications involved with confirming identity, nationality and immigration status, credentials and references. It also considers finance checks and medical screening. The table at *Appendix A* provides a full comparison of pre-employment measures undertaken by each country.

The focus then shifts to ongoing personnel security measures and considers the issues surrounding access control, data protection, employee monitoring and reporting hotlines. Finally, the document compares the investigative techniques available in different offshore locations, including the use of licensed investigators, surveillance, communications intercept, interview, search and seizure and local police involvement. Summaries of both the ongoing personnel security measures and investigative techniques available for the eleven countries detailed below are listed in *Appendix B & C*, respectively.

This guidance draws extensively on a research document commissioned by CPNI and completed by KPMG, '*Personnel Security in Offshore Centres; A summary of findings*', which is available on the CPNI website www.cpni.gov.uk and which looks at the current personnel security practices in what were considered to be eleven of the most popular offshore destinations for UK organisations:

- Bulgaria
- China
- Czech Republic
- India
- Ireland
- Philippines
- Poland
- Romania
- Singapore
- Slovakia
- South Africa

Making the decision to offshore

The term 'offshoring' refers to the relocation of some aspect of an organisation's business overseas. The process of transferring part of a business to any another organisation can be described as 'contracting' or 'outsourcing' and may occur within the UK or in an overseas/offshore location. An offshore business function may be fully operated in that country by UK staff (this is termed a 'captive' operation), managed by UK staff with a range of locally recruited employees, or entirely devolved to a local third party organisation.

The chapter on 'Secure Contracting' within CPNI's *Ongoing Personnel Security: A Good Practice Guide* discusses the issues involved with secure contracting in the UK and these are broadly similar in an offshore environment. However, there may be unique considerations involved with contracting in some offshore locations and some issues, such as retaining control of security practices and procedures, may be exacerbated by distance or language barriers.

Many organisations are attracted to the idea of offshoring due to the potentially significant cost savings involved. However, any decision to relocate some aspect of an organisation's business offshore should include a full personnel security risk assessment, enabling any cost saving to be weighed carefully against any potential threats. A number of factors will affect the risk faced, for example;

- The value of information, equipment or service being offshored, and predicted impact of the loss, disclosure, corruption or unavailability of these assets through insider activity.
- The threat level in-country. For example, is the country's intelligence service or a 'local' terrorist group known to target UK organisations or employees? What is the political relationship of the host country to the UK and how positive is local public opinion towards the UK and UK interests?
- The 'operating conditions' of any given country are established by its culture and legal framework. These determine the rights of the employer and employee and have an impact on the pre-employment, ongoing and investigative security measures available to organisations in that location.

If the offshore function is to be entirely contracted out to a local third party contractor it is important for the parent organisation to thoroughly assess their suitability before an agreement is reached. Ideally it would request written details of their personnel security policies, or undertake a 'partner evaluation' which considers how the third party's personnel security compares with that of the parent organisation.

Once the suitability of a third party has been established it is important to specify the parent organisation's requirements and expectations regarding personnel security within the contractual agreement. These may include:

- Details of the pre-employment screening and ongoing personnel security measures required, bearing in mind any legal or cultural considerations relevant to the particular country. These should specify whether each measure applies to a particular employee group or to all employees, determined by role and access.
- An assurance that the parent organisation retains the right to audit a third party's implementation of personnel security practices, either remotely or in person. This may include requiring access to current or historical data.
- Specification that third party contractors must seek approval from the UK management before entering into any sub-contracts, particularly with regard to any personnel security functions. Parent organisations must also ensure that the right to audit is included in any sub-contractual agreement.
- Requirement that third party contractors notify the UK management of the parent organisation if there is any personnel security breach in the offshore location, either as part of a regular report, or immediately as individual incidents occur.
- A contractual clause that specifies employees will be governed by UK law (although local laws may also still apply).

Establishing good communication with offshore staff

The fact that offshore employees are physically separated from the organisation's head office and other UK bases presents personnel security challenges. Research has shown that those who feel alienated from an organisation are less likely to engage with its values and culture and this may have an adverse impact on the loyalty of local employees to the parent organisation.

There are several ways in which an organisation can strengthen its links with its offshore locations and these may enable local employees to better identify with the wider organisation. Some examples include:

- Locating UK Head Office staff on the offshore site (ideally those who are also fluent in the local language). This can provide an oversight of work and any security issues, whilst increasing the flow of information between offices. This may be particularly helpful where there is a significant time difference.
- Assigning offshore staff with a UK-based mentor provides a mechanism for direct contact between the sites for work-related and personal queries.

Some organisations offer incentives in the form of short or longer term postings to UK offices in order to attract or retain high quality offshore staff. Where such policies exist it is important to ensure that any increased access is balanced by the security measures in place.

- Exchanging staff between locations, both for training/development and work opportunities. This may also act as an incentive for staff in both locations and will help to increase awareness of cultural diversity.
- Ensure senior staff members visit regularly and maintain frequent contact with offshore offices. This will facilitate a greater understanding of local issues and enable managers to establish a closer degree of oversight to ensure security and compliance.

Cultural considerations

Every country has its own unique culture which can vary between population groups and regions. The kind of cultural considerations relevant to the eleven countries listed on page four differ widely, though the following may be applicable;

- There may be a cultural expectation that women will not be in management roles, particularly where they may exert authority over men. Furthermore, there may be restrictions on their dress code.
- In some cultures, politeness will prevent a person from being at all negative, meaning that their answer may always be yes, even if the thing requested is totally impossible.
- Employees may expect or request facilities and/or time to practice a particular religion while at work, such as asking for a prayer room.
- In some cultures it is not acceptable for an individual to lose face publically. This may have significant implications for the way any disciplinary matter is conducted.
- Some cultures have different expectations regarding working hours; some may have a different work pattern, with Friday and Saturday forming the weekend instead of Saturday and Sunday, while others may expect a siesta during the day.

In the UK and many other countries, human rights legislation prohibits discrimination on the basis of gender, race or disability, for example. This may have implications for whether and how an organisation is able to accommodate cultural expectations such as those listed above.

Impacts of offshoring on UK based staff

Although this document focuses on the personnel security implications of operating overseas, it is important not to overlook the impact that such a decision may have on UK based employees. If the process of offshoring (moving business functions to another country) results in job losses at home, this may cause concern or anger among an organisation's UK workforce, particularly if this is communicated poorly.

Research indicates that uncertainty or perceived instability in the workplace can lead to disaffection amongst employees, which in turn could increase the risk of an employee engaging in insider activity.

Managing the recruitment of offshore staff

Pre-employment screening processes offshore should ideally be consistent with those undertaken in the UK (as set out by CPNI in '*A good practice guide on pre-employment screening*'). However, there will be some significant variations between countries in both the process of screening and nature of information returned. While such differences should not prevent a decision to offshore, they will need to be considered and addressed to maintain a good standard of personnel security.

Some of the issues organisations may encounter while attempting to assess potential local employees in an offshore location are:

- Lack of official infrastructure, which can make obtaining comprehensive information difficult or impossible.
- Confusing and overly bureaucratic legal, government and administrative frameworks, which are difficult to understand and negotiate. This can make pre-employment screening checks particularly hard for UK based human resource staff to obtain and interpret.
- The potential ease with which official documents in some countries can be forged may also affect the extent to which an organisation can trust the information it receives from a potential employee and the number and extent of checks required.

Where there are gaps in a prospective employee's data, due to the unavailability of information or verifiable information, an organisation may have to consider alternative means to mitigate the potential risks by increasing employee monitoring or supervision, for example, or by further restricting an employee's access. This may be for an established probationary period or for the duration of their employment. Please refer to *Appendix A* for a full comparison of measures used in the offshoring locations listed on page four.

Where there are concerns about counterfeit documents being presented as part of the identification process, this can be mitigated by requesting additional supporting documentation, or by making secondary enquiries to verify a document's authenticity.

Confirming identity

As with any pre-employment screening regime, the first step should be to gain assurance of the potential employee's identity. All of the countries listed on page four offer processes for verifying the identity of potential employees, although there is little consistency regarding the methods used or what is accepted as proof. Generally, the name and address of an individual are verified, although organisations also require a date of birth or tax details in some locations.

There are occasionally obstacles to some mechanisms of verifying identity. In China, for example, identity checks cannot invade the prospective employee's personal privacy, such as their domestic affairs.

There is a wide range of information available on foreign documents of identity, for example the European Union has made freely available detail on the security features of a number of European national passports (see **Sources of information**).

Nationality and immigration status

Establishing whether an individual is legally permitted to gain employment is an important part of pre-employment screening in the UK, as an employer who is found to have employed an 'illegal' worker may face legal action. Organisations located in each of the countries listed on page four also conduct nationality and immigration checks. However, it may be advisable to consult a legal expert in-country to confirm the local legal requirements and ensure that these are followed, even if the process is further subcontracted.

While there is an established exchange mechanism for employment migration within the European Union (EU) and European Economic Area (EEA), European organisations wishing to employ non-EU/EEA workers will require them to obtain the necessary documentation. For example in Ireland, any non-EEA national requires both a work permit and Garda National Immigration Bureau card.

Organisations based in countries from outside the EU or EEA may require all foreign workers to obtain a specified work permit and/or visa. This may need to be obtained by the employee, such as in South Africa, or by an organisation on behalf of an employee, as in Singapore.

Verifying credentials

The extent of other background checks carried out varies from country to country and according to the job role. In some countries, the mechanisms in place for sharing information may be less developed. In China, for example, records are generally held on paper rather than electronically, which may have an impact on recruitment timescales and the resources required to complete comprehensive checks.

For these reasons, some organisations may find that offshore pre-employment screening is too time consuming and resource intensive for their own staff to undertake. In such circumstances there may be value in engaging an experienced offshore screening company to undertake checks on the organisation's behalf. This issue is discussed within chapter eleven of the third edition of CPNI's *A Good Practice Guide on Pre-employment Screening*.

There are systems in place within all of the countries listed on page four to facilitate criminal records checks. Whether this is done or not is largely dependant on the role applied for. As a supplement to the Pre-employment screening guidance CPNI commissioned a KPMG research document entitled '*Disclosure of Criminal Records for Overseas Jurisdictions*'. This document, available on the CPNI website, provides details about obtaining criminal records from a wide range of countries. It also demonstrates how overseas crime categories correspond to those in the UK.

In some countries certain types of information are much more readily available than in the UK, (although the degree of reliability held by such data may vary from country to country). To illustrate this first point; a criminal records check in India will reveal *all* an individual's convictions, while under UK law convictions which are considered 'spent' are generally not visible¹. Therefore, it may not be appropriate to use previous conviction data as a basis for excluding an individual from employment.

It is recommended that organisations seek local advice, including legal advice when appropriate, to establish the most effective way of verifying an individual's credentials. Such individuals may also be able to provide some indication of a source's reliability.

¹ Rehabilitation of Offenders Act. <http://www.crb.gov.uk/Default.aspx?page=313>

References

Generally, official employer references will only contain basic information about when and where an individual has been previously employed. However, in some countries it is possible for a prospective employer to obtain further information. In none of the eleven countries listed on page four is there any obligation on an individual to provide a character reference.

There is great variation among the eleven countries listed with regard to the uptake and availability of character references from previous employers or persons of standing in the community. For example in Romania these are possible, but extremely uncommon in practice, while in Singapore, the main consideration of this common practice is to ensure that the referee is not a friend or family member.

Finance checks

As the table in *Appendix A* indicates, financial screening is not a routine part of pre-employment screening in the countries listed, unless the position applied for is of a senior or more responsible nature. However, there are a number of commercial companies which can provide assistance if financial screening is sought. There are also several public sources of financial 'sanctions' data, regarding individuals and companies (see **Sources of information**).

Health/drug screening

In Bulgaria, China, Czech Republic and Romania, health screening is a mandatory part of the employment process, often defined under a labour code; while in South Africa, such screening can only be conducted if it is directly relevant to the position and is not discriminatory. Generally, health screening seems to be an acceptable addition to the pre-employment process, where it is a clear requirement of the post. However, in most cases explicit consent of the individual is required.

Drug screening is much less common and much more controversial, perhaps due to the associated stigma of drug abuse. Even where permitted (usually for high risk posts), explicit consent is usually required and caution should be exercised. For example in China, an employee may claim reputational damages if they believe the (inappropriate) actions of the organisation have marred their reputation.

Ongoing personnel security offshore

It is important that organisations are attuned to cultural differences and understand that the implementation of UK personnel security policies may not be possible, practical or acceptable in an overseas location. Alternatives may be required for either legal or cultural reasons and the organisation should be flexible enough to meet this need. A wide range of potential measures are outlined in CPNI's ongoing personnel security guidance.

Maintaining a high standard of ongoing personnel security measures and ensuring that employees are well treated will raise morale and may also increase the psychological commitment of local staff to the organisation, reducing the likelihood of insider activity. This may be particularly so in countries which do not have any trade unions to represent employee groups or those with poor human rights records.

All personnel related security measures should be directly proportionate to the threat faced, as determined by a personnel security risk assessment (see CPNI's *Personnel Security Risk Assessment: A Guide* for further information). This is equally important in an offshore environment and organisations should remember that just because a particular security measure is *permissible* in a given country, does not necessarily mean that it will be useful or proportionate.

Access controls

None of the eleven countries listed within Appendix B have any legal restriction in the use of physical access controls to buildings or zones, other than where biometric data is restricted by a Data Protection Act. Physical screening is permitted in all countries, but is often restricted to same-gender searching protocols and is not widely used.

In the UK, CPNI recommends using a role based access approach which determines the physical and informational access an employee will have, according to their job role. These access rights should be regularly reviewed and automatically re-evaluated when an employee changes jobs.

The same approach is recommended in offshore locations, particularly where there is potentially less assurance regarding an employee's background and integrity, due to an absence of verifiable information. In addition, where staff are transferred or promoted within the offshore location or between the offshore base and the UK, the risk assessment should be reviewed and amended as required.

Protection of data

In the UK organisations have a duty to ensure, where appropriate, that employees are aware of their obligations regarding the protection of sensitive or valuable information, for example, to ensure compliance with the Data Protection Act 1998². Although there may be variations in the law in different locations, the same principles apply offshore. Access should be limited, according to an employee's role, and where a high level of access is needed, additional safeguards may be required to limit an employee's ability to disclose, print or copy this information. The following measures may be considered:

- Requiring staff to sign a confidentiality agreement as part of their employment contract. This should specify that corporate information must not be disclosed to anyone outside the organisation and clearly outline the consequence of any breach of this agreement.
- Restricting employee access to printers, photocopiers, data storage devices and email, particularly where sensitive data is involved.
- Searching employees (either 100% or at random) as they enter or exit the building. This can act as a deterrent and contribute to the detection of any unauthorised items and/or the removal of assets or information.

Employee monitoring

The subject of employee monitoring can be a sensitive one, with a pervasive idea that we do not like 'big brother watching us'³. Consequently, if the rationale for adopting such measures is not well communicated, they may undermine staff trust and morale. However, most monitoring systems do not actually focus on a single individual, but rather take in a large volume of data across a wide group of employees, enabling security staff to spot anomalous patterns, compared to a norm. This kind of monitoring is generally more palatable.

In many of the countries listed on page four, there is legislation in place regarding the use (or prohibition) of overt and covert monitoring systems (see Appendix B for a comparison of ongoing personnel security measures used in each country). It is, of course, important to comply with local legislation and legal advice should be sought before implementing any new measure to monitor employees, particularly in the context of monitoring telephone communications or covert IT monitoring.

In the UK, public authorities covered by the Human Rights Act 1998⁴ must ensure that any interference with privacy is necessary and proportionate for a legitimate purpose (listed in the Act) and in accordance with the relevant law (for example, the Regulation of Investigatory Powers Act 2000⁵).

² Data Protection Act 1998

http://www.ico.gov.uk/what_we_cover/data_protection/legislation_in_full.aspx

³ See 'employee monitoring' chapter within CPNI's *Ongoing personnel security: A good practice guide*.

⁴ Human Rights Act 1998. http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1

⁵ Regulation of Investigatory Powers Act 2000.

http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

Reporting hotlines

None of the eleven countries listed on page four prohibit the use of reporting hotlines. However, their deployment is not common practice in Poland, Romania, Bulgaria, the Czech Republic or Slovakia, if they are used at all. The reason for this may be due to cultural sensitivities or perhaps due to negative associations held with reporting hotlines.

There is also an ongoing issue of compatibility between the United States' Sarbanes-Oxley Act 2002, which requires organisations to provide an anonymous reporting mechanism for accounting or auditing matters, and EU data protection legislation, which stipulates that a hotline must be confidential but not anonymous. To overcome this dichotomy, some countries (for example, Ireland) have suggested that a whistleblower's report should be specific to an issue but not an individual.

Investigative techniques available offshore

Maintaining the ability to investigate and resolve security-related concerns about an individual or incident in an offshore location is a key aspect of personnel security. However in some offshore locations the legislation surrounding investigation is vague and it may be unclear whether a particular investigative activity is permitted. In such circumstances an organisation should consult a legal expert and proceed with caution.

It may be useful to have a security (and possibly HR) capability in situ, as it can be very difficult to oversee security and disciplinary procedures remotely. However, it may be necessary for at least some security and HR employees to be drawn from the local community. Where this is the case, the parent organisation should ensure that such individuals are subject to the same level of pre-employment screening as their UK counterparts. Where not possible, additional ongoing security measures may be required, according to an individual's responsibility and access.

Prevention of insider activity is always preferable to the cure and an investigation is likely to be more resource intensive than most other personnel security measures. For this reason, an investigation should be viewed as a necessary means to resolving unpreventable insider incidents, rather than as a preventative measure in its own right (although a good investigative capability will also act as a deterrent for insider behaviour).

The purpose of an investigation will inform and may dictate the course of events (for example, the process of collecting evidence for a criminal prosecution case involving a law enforcement agency will differ from that of an internal disciplinary event). Investigative activities, as outlined on the following pages, may be undertaken by the organisation, a private investigator, or local police authorities, depending on the location and circumstances.

Licensed investigators

With the exception of Bulgaria, China, Czech Republic and the Philippines, each of the eleven countries listed on page four have legislation in place regulating the work of private investigators. The capability for an organisation to conduct its own investigations can be extremely useful, particularly where there are finite resources available to the local police. However, this process can be resource intensive and the powers of such investigations may be limited. Moreover, serious incidents must be referred to the local or state authorities.

In China, legislation concerning the private investigations industry is developing and activities which are currently permissible may not be under the new laws. Companies conducting their own investigations should be alert to these potential changes and consult local legal experts to ensure that their investigative endeavours are compliant.

Surveillance

Some forms of surveillance do not focus on one individual but look across a number of employees. For example, some CCTV systems store data which can be scrutinised retrospectively if an insider incident later comes to light. In Romania, only the state authorities can perform surveillance of any type, regardless of the suspected or alleged offence. While in China, the Czech Republic, Ireland and the Philippines, the use of the different forms of surveillance are restricted according to the severity of the incident and the intrusiveness of the surveillance.

Most countries do not prohibit transactional surveillance; for example, telephone call records, email logs and financial transaction data, although some restrict this to information obtained directly from company premises or systems (see Appendix C for a comparison of the investigative techniques used within the countries listed on page four).

Intercepting communications

Most countries regulate, restrict or prohibit the use of intercept as an investigative tool, with the exception of Singapore, where there are currently no legal restrictions. In India and Poland, employee intercept is limited to that involving company systems, equipment or property. In China 'bugging devices' are illegal, but it is unclear whether other forms of intercept, such as telephone call monitoring, are permitted.

Although Appendix C indicates that the Czech Republic, Ireland, Philippines and Romania prohibit intercept, it should be noted that this generally only applies to private or internal company investigations. If the police were involved in a more serious criminal case, intercept may be permitted, if authorised and conducted by the law enforcement agencies.

Interception conducted from the UK of employees abroad may still be regulated by the Regulation of Investigatory Powers Act 2000 and, if not properly authorised, could constitute a criminal offence under that Act. If in doubt, legal advice on the specific situation should be sought.

Interview

None of the eleven countries indicated that an interview was not a permitted method of investigation, though the response for Romania (see Appendix C) highlights that an interview conducted internally by an organisation could not be used evidentially in a criminal case.

Nevertheless, an informal interview (conducted in accordance with the local legal framework, company policy, human rights and health and safety legislation) can be an extremely cost-effective way of determining whether an individual is worthy of closer scrutiny or if there is an innocent explanation of the circumstances which have elicited the initial suspicion.

Search/seizure

Neither Ireland nor Romania permits search or seizure by any other than the police, and in the other nine countries the procedure is restricted or regulated. Even the most permissive countries limit such activity to company equipment, systems and property.

Any employee subject to such a procedure is likely to be alienated by the experience and it is important that it is only conducted at a stage of an investigation when it becomes clearly necessary. If deployed sooner than this, there is a danger that such an individual may become, or become more, disaffected with the organisation and may be more likely to engage in insider activity.

Involving the police in an investigation

The expectation as to whether and when local police should be involved in an insider investigation varies between countries and depends on both police resources in situ and the nature of the incident. For example in Poland, any insider incident occurring within the public sector must be reported to the police as a matter of course and at the earliest opportunity, while private industry is under no obligation to report any insider incident. In contrast, for an organisation in Singapore, one of the main considerations is whether there is enough evidence for the police to prosecute, and in Ireland the police must be involved from the outset if a criminal prosecution is the desired outcome.

Generally, the police only need to be informed where it is clear that a criminal offence has occurred⁶ or where the matter is sufficiently serious to require their involvement. However, in many instances it may be more appropriate for an organisation to investigate insiders internally, without involving the police. Whatever course of action is undertaken, it is important to ensure the response is legally compliant within the country concerned, taking local legal advice where necessary.

⁶ Most countries are subject to the Anti-Money laundering Act, which states that suspected money laundering must be reported to the authorities.

Sources of information

Data Protection Act and outsourcing (in the UK and offshore)

Further details regarding the Data Protection Act and outsourcing can be found on the Information Commissioner's website;

http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Good Practice Note: Outsourcing – a guide for small and medium businesses

http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/good_practice_notes.aspx

Useful advice on government good practice on procurement, projects, contracting and information assurance is available at:

<http://www.ogc.gov.uk>

The European Commission has proposed a series of standard contractual clauses aimed at safeguarding personal data that is transferred to an offshore provider. For more information visit the EC website:

http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm

Overseas Security Information for Business (OSIB)

<http://www.fco.gov.uk/en/business-trade/sisbo-osib>

Overseas ID checks

The European Union has listed the security features of a number of European national passports;

<http://www.consilium.europa.eu/prado/EN/searchByIssuingCountry.html>

Financial sanctions sources

United States Treasury, Office of Foreign Assets Control – Specially Designated Nationals List (SDN list): <http://www.treas.gov/offices/enforcement/ofac/sdn/>

HM Treasury, financial sanctions list:

http://www.hm-treasury.gov.uk/fin_sanctions_index.htm

European Union – economic Combined Targeted Financial Sanctions List (eCTFS) or “EU Freeze List”:

http://ec.europa.eu/external_relations/cfsp/sanctions/list/version4/global/e_ctlview.html

Appendix A: Comparison table of pre-employment screening measures available

	Bulgaria	China	Czech Republic	India	Ireland	Philippines	Poland	Romania	Singapore	Slovakia	South Africa
Identity check	Yes	Yes, but cannot be invasive	Yes	Yes, some documents can be verified	Yes	Often	Possible, usually on first day (Po 1)	Often	Yes - no restrictions	Yes - no restrictions	Often
Residency check	Yes	Not usually	Yes	Common practice - ideally physically verified	Yes	Often, certificate issued to individual	Yes - usually on first day.	Yes	Yes - ID cards/employment documents only	Yes, at employers discretion	Often
Work permit and nationality checks	Sometimes, non EU and certain jobs	Yes - foreign workers require permit	Yes - foreign workers require permit	Yes - foreign workers require permit	Yes - Non EEA nationals require permit and GNIB card (Ire 1)	Yes – Foreign workers must get pre-arranged permit / visa (Ph 1)	Yes - Non EU/EEA nationals require permit	Yes - Visa & work permit required for non EU/EEA workers	Yes - foreign workers require permit - obtained by employer	Non EU/EEA nationals require permit - obtained by employer	Yes - all foreign workers, individual to obtain
Criminal record checks ★	Sometimes	Possible, with consent, but issues	Possible - issued to individual or legal representative	Double layer of records - procedure varies	Individual can apply locally for Police certificate.	Employer can request National Bureau of Investigation record clearance	Limited - employer generally not allowed to request /require	Usually required, mandatory for sensitive posts, obtained by individual	Can be part of pre-employment process. Not available to third parties	Sometimes, for sensitive positions, individual to apply.	Yes, individual or third party application
Education checks	Often	Possible, with written consent.	Sometimes - consent required	Often	Yes - consent generally required	Employee usually required to provide certificates	Sometimes - checked with institution on first day	Sometimes - can be requested of employees	Often, with individual's consent	Often, with individual's consent	Often, consent required
Qualification checks	Yes	Possible, consent may be required	Sometimes - consent required	Regular - consent generally required	Yes - consent generally required	Yes - often used, consent generally required	Sometimes - checked with institution on first day	Yes - where applicable	Regularly – where applicable	Often, with individual's consent	Often, consent required
Employment references	Normally	Possible – no obligation	Mandatory verification from previous employer (Cz 2)	Yes – normally confirm basic information	Yes - confirm basic information. Consent generally required	Employee may require certificate from previous employer	Sometimes, with consent - done directly between employers	Normal practice - basic information only, with consent	Normal practice - generally only basic information, with consent	Basic information on CV, not common for previous employer to comment	Normal practice - generally only basic information, with consent of individual
Character references from previous employers	Sometimes	Sometimes - not always provided	Sometimes, but no obligation	Possible - but not common	Common but not compulsory	Yes - generally three references required, limited detail.	No restrictions	Not common	Sometimes - no obligation	Sometimes, no obligation	Sometimes, no obligation. Cannot discriminate
Character references from persons of standing in the community	Yes - known for min 3 yrs	Possible - but not common	Sometimes, but no obligation	Yes - known for min 3 yrs	Possible - but not common	Yes - but must ensure referees are independent	No restrictions or obligations	Not established practice	Yes - no restriction, but must ensure referees are independent	Possible - but not common	No restrictions - but must be independent - known for min 2 years (Sa 1)
Financial/ credit checks	limited - senior/sensitive roles	limited - senior/sensitive roles	Not permitted unless directly relevant (Cz 3)	Not common practice, limited to senior / sensitive roles permission required	Prohibited unless absolutely necessary. explicit consent required	Not common - except in finance industry	Not common - no infrastructure in place to undertake such checks	Only available to financial / leasing / insurance institutions	Only for more senior / financial roles, consent required	Only used for more senior / financial roles, consent required	Not allowed, except for sensitive financial roles. Explicit consent required
Substance abuse screening	Permitted, but not common. Consent required	not common - risk of reputational damage, explicit consent required	Not common, explicit consent required	Not common, explicit consent required	Limited use - if suspicion held	Not common, only for high risk roles	Not common	Not established practice, except in high risk positions - explicit consent required	No legal restrictions, but not common, explicit consent required	Not common, explicit consent required	Only if relevant to position. Cannot discriminate
Occupational health checks	Mandatory type determined by role and age.	Yes - mandatory	Yes - mandatory (Labour code)	Not common, explicit consent required	Not common, explicit consent required	Permitted	Only after offer of employment has been made - subject to passing check	Yes - mandatory (Labour code)	No legal restrictions, but not common, explicit consent required	Common, but not part of pre-employment screening	Only if relevant to position. Cannot discriminate

★ Separate, detailed guidance on overseas criminal records checks available on CPNI website: <http://www.cpni.gov.uk/ProtectingYourAssets/overseas.aspx>

Key to references in Appendix A

- Ch 1: Not all criminal offences are recorded due to the lack of standard record-keeping procedures. The check cannot therefore guarantee that an employee does not have a criminal record.
- Cz 1: Further information available at <http://www.mn.domavcr.cz/advices-for-living-in-the-czech-republic/employment>
- Cz 2: Under s. 313 (1) of the Labour Code, on the termination of an employment relationship or an agreement on working activity, an employer is obliged to issue the employee a verification of his/her employment
- Cz 3: Under s. 316 of the Labour Code an employer may not require (directly or indirectly through third parties) from an employee such information that does not relate directly to work performance and to employment (labour) relationships, including information concerning an individual's family or property situation.
- Ire 3: Employees must provide employers with their permit documentation as well as their Garda National Immigration Bureau (GNIB) card which shows the right of the individual to reside in Ireland.
- Ph 1: More information is available at the website below:
http://immigration.gov.ph//index.php?option=com_content&task=view&id=25&Itemid=36
- Po 1: Labour Code Act of 26 June 1974 - employers have the right to request name, DoB, and address details for purpose of establishing identity.
- Sa1: <http://www.bcct.ca/Teacher/InternationalCountrySpecInfo.aspx?xmlfilename=southafrica.xml&imgfilename=southafrica.png&countryname=South%20Africa>

Appendix B: Comparison table of ongoing personnel security measures available

	Bulgaria	China	Czech Republic	India	Ireland	Philippines	Poland	Romania	Singapore	Slovakia	South Africa
Restriction of access to the premises	Yes	Yes (Ch 1)	Yes	Yes (In 1, 2 & 3)	Restricted (biometrics - ★DPA)	Yes	Yes (biometrics - ★DPA)	Yes	Yes	Yes (Sv 1)	Yes (Sa 1, 2)
Restriction of access to certain rooms/zones on the premises	Yes	Yes	Yes	Yes (In 1, 2 & 3)	Restricted (biometrics - ★DPA)	Yes	Yes (classified – Po 1)	Yes	Yes	Yes (Sv 1)	Yes (Sa 1, 2)
Physical screening (on entry/exit)	Yes	Yes	Yes (Cz 1, 2)	Yes (In 1, 2 & 3)	Restricted (biometrics - ★DPA)	Yes	Yes	Yes, but not used	Yes	Yes (Sv 1)	Yes (Sa 3)
Prohibition of removal of data from the premises (hard-copy)	Yes (★DPA)	Yes	Yes (★DPA, Cz 1)	Yes (In 1 & 2,)	Yes (★DPA, Ir 1)	Yes (Ph 1)	Yes (★DPA, Po 1)	Yes	Yes	Yes (Sv 1, 2, 3)	Yes (Sa 2)
Prohibition of removal of data from the premises (electronic)	Yes (★DPA)	Yes	Yes (★DPA, Cz 1)	Yes (In 1 & 2,)	Yes (★DPA, Ir 1)	Yes (Ph 1)	Yes (★DPA, Po 1)	Yes	Yes	Yes (Sv 2, 3)	Yes (Sa 4)
Visual surveillance (CCTV or other cameras), either overt or covert	Yes (*Bu 1)	Yes (Unclear)	Restricted (Cz 1)	Yes (In 2)	Restricted (★DPA)	Yes (Ph 2)	Yes (★DPA)	Yes (★DPA)	Yes	Yes (Sv 1, 4)	Yes (Sa 5)
Overt monitoring of access to IT and other equipment	Yes (★DPA)	Yes (Unclear)	Restricted (Cz 1)	Yes (In 1 & 2,)	Yes (★DPA)	Yes but restricted (Ph 2, 3)	Yes (★DPA)	Yes	Yes	Yes (Sv 2)	Yes (Sa 5)
Covert monitoring of access to IT and other equipment	Yes (★DPA)	Yes (Unclear)	Restricted (Cz 1)	Yes (In 1 & 2,)	Restricted	Yes but restricted (Ph 2, 3)	Yes (★DPA)	Yes	Yes	Yes (Sv 2)	Yes (Sa 5)
Use of alerts/automated warning systems to identify unusual employee behaviour (out of hours activities, duplicate payments)	Yes	Yes (Unclear)	Yes	Yes (In 2 & 3)	Yes (*DPA)	Yes	Yes (★DPA)	Yes	Yes	Yes (Sv 2)	(Sa 3, 5)
Overt or covert monitoring of internal or external communications (telephones, mail, e-mail or internet)	Yes (★DPA)	Yes (Unclear Ch 2)	Restricted (Cz 1)	Yes (In 2 & 3)	Restricted (★DPA)	Yes (Ph 4)	Yes (★DPA)	Yes, but company equipment only (Ro 1)	Yes	Restricted (Sv 2, 5)	Yes (Sa 4,5)
Reporting hotlines (anonymous)	Yes (★DPA)	Yes (Unclear)	Yes, but not widely used	Yes (In 2 & 3)	Yes	Yes, but not used	Yes, but not used	Yes - esp. to police, use limited	Yes	Yes (Sv 3) but not used	Yes (Sa 6)
Reporting hotlines (confidential)	Yes (★DPA)	Yes (Unclear)	Yes, but not widely used	Yes (In 2 & 3)	Yes	Yes, but not used	Yes, but not used	Yes, but use limited	Yes	Yes (Sv 3) but not used	Yes (Sa 6)

★DPA: Data Protection Act ★AMLA: Anti-Money Laundering Act

Appendix C: Comparison table of investigative techniques available

	Bulgaria	China	Czech Republic	India	Ireland	Philippines	Poland	Romania	Singapore	Slovakia	South Africa
Is there a licensing regime covering investigators?	No	Yes, but not private investigators	No	Yes (In 4)	Yes, (Ir 2)	No	Yes (Po 2)	Yes (Ro 2)	Yes (Si 1)	Yes (Sv 1)	Yes (Sa 7)
Physical surveillance (overt or covert)	Yes (Bu 1)	Restricted (Ch 3)	No (Cz 2)	Yes (In 2)	Restricted (★DPA)	Restricted	Yes (★DPA, Po 2)	No (Ro 3)	Yes (Si 1)	Yes (Sv 1, 4)	Yes (Sa 5)
Electronic surveillance (e.g. tracking devices)	Yes (Bu 1)	No (unclear)	No (Cz 2)	Yes (In 2)	Restricted (★DPA)	Restricted (Ph 2)	Yes (★DPA, Po 2)	No (Ro 3)	Yes (Si 1)	Yes (Sv 1, 4)	Yes (Sa 5)
Visual and communication surveillance (using cameras, video or CCTV)	Yes (Bu 1)	Yes (weak privacy laws)	No (Cz 2)	Yes (In 2)	Restricted (★DPA)	Yes (Ph 2, 4)	Yes - on company premises	No (Ro 3)	Yes	Yes (Sv 1, 4)	Yes (Sa 5)
Communication intercept (including oral, written and electronic communication including bugging devices)	Yes (Bu 1)	Restricted, bugging devices illegal (unclear)	No (Cz 2)	Restricted to company equipment, systems or property (In 1 & 2)	No (Ir 3)	No (Ph 4)	Restricted to company equipment, systems or property	No (Ro 3)	Yes	Yes (Sv 5)	Yes (Sa 5)
Computer or database surveillance (using either hardware or software tools, including forensic tools)	Yes (Bu 1)	Yes (unclear)	Restricted (Cz 2)	Yes (In 2)	Restricted	Yes (Ph 2)	Restricted to company equipment, systems or property	No (Ro 3)	Restricted to company equipment, systems or property	Yes (Sv 5)	Yes (Sa 5)
Formal interviews of staff	Yes (Bu 1)	Yes	Yes (Cz 3)	Yes	Yes	Yes	Yes (Po 3)	Yes, but not evidentially (Ro 3)	Yes, but voluntary	Yes (Sv 2, 4)	Yes (Sa 8)
Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)	Yes (Bu 1)	No, state sanctioned only	Yes	Restricted to company equipment, systems or property	Restricted	Yes (Ph 2)	Restricted to company equipment, systems or property	No (Ro 3)	Yes (Si 2)	Yes (Sv 5)	Yes (Sa 5)
Search and seizure of evidence, whether electronic or physical (overt or covert)	Yes (Bu 1, Health & Safety legislation)	Restricted (unclear)	Restricted (Cz 4)	Restricted to company equipment, systems or property	No, police only	Restricted (Ph 5)	Yes (★DPA)	No (Ro 3) (but Ro 6)	Restricted to company equipment, systems or property	Yes (Health & Safety legislation)	Yes (Sa 5)
Is it either usual or necessary to involve the police in investigations?	No	No, unless court action is required	No	Yes, for criminal offenses	Yes, for criminal offenses	Yes, for criminal offences	Yes - in public sector. No - in private sector	Yes, for criminal offences	Yes, for criminal offenses, but no immediacy	Yes, for certain criminal offences (Sv 6)	No obligation
If the police are involved, at what stage in the investigation does this generally occur?	-	-	-	From the outset	On discovery of crime		From the outset - public sector only		When there is sufficient evidence		
Are there any practical considerations to be aware of when involving the police / law-enforcement authorities?	Police have limited resources	Police have limited resources	Police have limited resources	Investigation should be conducted to evidential standards	Police must secure integrity of the crime scene.	Police have limited resources	When Police take over company will lose control of investigation	Police have limited resources	Is there sufficient evidence for Police to prosecute?	Employer must record any incident (Health & Safety legislation)	Police have limited resources (Sa 9)
What duties does the employer have to report information to local law enforcement authorities?	Criminality should be reported to police immediately	Unclear	Must report money laundering (★AMLA)	Duty to inform police (In 5)	Must report money laundering (★AMLA, Ire 4)	Must report money laundering (★AMLA)	Must report money laundering (★AMLA)	Must report money laundering (★AMLA, Ro 5)		Must report money laundering (★AMLA)	Must report money laundering (★AMLA, Sa 10)

★DPA: Data Protection Act ★AMLA: Anti-Money Laundering Act

Key to references in Appendix B & C

- Bu 1: Constitution of Republic of Bulgaria; the Convention for the Protection of Human Rights and Fundamental Freedoms and Private Security Business Act.
- Ch 1: Property rights in Chinese constitution
- Ch 2: However, caution and legal consultation is recommended as there have been cases where individuals have been successful in claiming damages
- Ch 3: Strictly, physical surveillance can only be carried out by official government investigators. However, "surveillance" is not well defined and therefore subject to legal interpretation.
- Cz 1: Labour Code, Act No. 262/2006
- Cz 2: Civil Code, Act no. 40/1964
- Cz 3: Constitutional act and the charter of fundamental rights and freedoms.
- Cz 4: Search/seizure of personal belongings not allowed without individual's consent
- In 1: Information Technology Act 2000
- In 2: Code of Business Conduct
- In 3: Certified Standing Orders
- In 4: Private Security Agencies (Regulation) Act 2005 [& Private Detective Agencies (Regulation) Bill 2007 - pending]
- In 5: Section 39 of the Code of Criminal Procedure, 1973 specifies the offences to be reported. Section 202 of the Indian Penal Code lists the punitive responses for the failing to report these.
- Ire 1: Criminal Justice (Theft and Fraud Offences Act), 2001.
- Ire 2: Private Security Authority [& Employment Regulation Order (Security Industry), 2005]
- Ire 3: Interception of Postal Packets and Telecommunication Messages (Regulation) Act, 1993.

- Ire 4: The Criminal Justice Act 1994
- Ph 1: The E-Commerce Act 2000 (Republic Act No. 8792)

- Ph 2: Rights to privacy in the Philippines are safeguarded under Article III of the Bill of Rights Section III of the Constitution of the Philippines
- Ph 3: The E-Commerce Act - imposes a duty of confidentiality on individuals.
- Ph 4: Anti-Wiretapping Act.
- Ph 5: A Search Warrant should be secured from the respective court prior to the search and seizure of evidence, whether physical or electronic (either overtly or covertly).
- Po 1: Confidential Data Protection Act
- Po 2: Act on Services of Private Detectives of 6 July 2001.
- Po 3: Interviews of staff are subject to Constitutional and Human Rights safeguards
- Ro 1: Monitoring of communications (overt / covert) is covered by Law 506/2004 concerning personal data protection over electronic communications.
- Ro 2: Private investigators in Romania are regulated by Law No. 329/2003.
- Ro 3: Such evidence is collected only by the Police and prosecutors. Evidence collected is subject to the Romanian Penal Code.
- Ro 4: Such evidence may be collected only by a specialised unit of the Romanian Information Services and is subject to the Romanian Penal Code.
- Ro 5: Under the Romanian Penal Code, any suspicions of money laundering, theft, fraud or forgery, or workplace accidents must be reported to the police.

- Ro 6: Procedures above (A3-10) can be conducted under the direction of a Court order when a mandate is issued by a Court Judge (*Ro 3, 4)
- Si 1: Private Security Industry Act which was enacted in September 2007
- Si 2: Financial transactional data and credit card activity are not available to third-parties under the Banking Act.
- SI 1: Private Security Service Act
- SI 2: Personal Data Protection Act
- SI 3: Labour Code Act No. 311/2001 (amended 2007)
- SI 4: Human Rights Act
- SI 5: Electronic Communications Act, 2003 (s55 refers).
- SI 6: The Penal Code requires reports to be made to the police for certain criminal acts.
- Sa 1: Mine Health and Safety Act 29 of 1996; Occupational Health and Safety Act 85 of 1993; National Key Points Act 102 of 1980
- Sa 2: Protection of Information Act 84 of 1982
- Sa 3: Constitution of the Republic of South Africa, 1996.
- Sa 4: The Electronic Communications and Transactions Act 25 of 2002.
- Sa 5: Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002.
- Sa 6: Protected Disclosures Act 26 of 2000 (Whistleblower Act). Section 6:2 of the Whistleblower Act makes provision for confidential hotlines.
- Sa 7: Private Security Industry Regulations, 2002
- Sa 8: Civil Proceedings Evidence Act No 25 of 1965
- Sa 9: Criminal Procedure Act No. 51 of 1977.
- Sa10: Prevention and Combating of Corrupt Activities Act No. 12 of 2004. Currently being amended by the Jurisdiction of Regional Courts Amendment Act, No. 31 of 2008.