ProtectUK

Personnel and people security

Original publication date
02/11/2020

1. What is personnel security?

Personnel security is a system of policies and procedures which aim to manage and minimise the risk of people exploiting legitimate access to an organisation's assets or premises for unauthorised purposes. These purposes can encompass many forms of criminal activity, from minor theft through to terrorism.

A first step to achieving this is to consider the 'people risks' within your organisation by conducting a personnel risk assessment. Consider the implementation of thorough pre-employment screening methods. This will support your organisation to employ only suitably qualified and reliable individuals. Once employed, manage them professionally to minimise the chances of staff becoming disgruntled. Finally, create a strong security culture, detect suspicious behaviour, and resolve security concerns once they become apparent.

1.1 The Insider Threat

Some external threats, whether from criminals, terrorists, or competitors seeking a business advantage, may rely upon the cooperation of an 'insider'.

An insider could be an employee, contractor, agency staff or even a business partner who has authorised access to your assets. They may already be working for you and see an opportunity to conduct an insider act for their own benefit, or may be someone newly joined who has infiltrated your organisation in order to seek information. They may be someone who has been coerced by a third party to exploit the access their job might provide, or be disgruntled and want to conduct an act of revenge.

1.2 Risk assessment process

Your organisation needs to have a risk assessment process in place which manages the consequences of an unauthorised or unlawful act and a process in place that helps you:

- identify and analyse the root cause of the incident
- identify the appropriate disciplinary actions or interventions that need to be undertaken
- assess the effectiveness of current control measures in place
- identify gaps in practice
- develop more effective control measures

These processes help your organisation learn from the incident and put in place measures to prevent the incident from occurring again.

Go the NPSA Reducing Insider Risk webpage.

2. Pre-employment screening

Personnel security involves a number of screening methods, performed as part of the recruitment process on a regular basis. Some methods of screening are very simple, others more sophisticated. These should be proportionate to the risk faced by the organisation. In each case, the aim of the screening is to collect information about potential or existing staff and to use that information to identify any individuals who present security concerns.

Pre-employment screening seeks to verify the credentials of job applicants and to check that the applicants meet preconditions of employment (e.g. that the individual is legally permitted to take up an offer of employment).

In the course of performing these checks, it will be established whether the applicant has concealed important information, or otherwise misrepresented themselves.

2.1 Pre-employment checks

Personnel security starts with the job application, where applicants should be made aware that supplying false information, or failing to disclose relevant information, could be grounds for dismissal and could amount to a criminal offence. Applicants should also be made aware that any offers of employment are subject to the satisfactory completion of pre-employment checks.

If an organisation believes there is a fraudulent application involving illegal activity, the police should be informed. Pre-employment checks may be performed directly by an organisation’s Human Resources Department, or this process may be sub-contracted to a third party. In either case, the organisation needs to have a clear understanding of the thresholds for denying someone

employment. For instance, under what circumstances would an application be rejected on the basis of their criminal record and why? Organisations using a third party for screening purposes should conduct regular audit checks to ensure the screening is meeting the standards required.

2.2 Data Protection Act and General Data Protection Regulation

The Data Protection Act (DPA) (2018) and the General Data Protection Regulation (GDPR) (2018) applies to the processing of personal information about individuals. Personnel security measures must be carried out in accordance with the data protection principles set out within the act.

3. Pre-employment screening policy

Your pre-employment screening processes will be more effective if they form an integral part of your policies, practices and procedures for the recruiting, hiring and where necessary, training of employees. If you have conducted a personnel security risk assessment, this will help you to decide on the levels of screening appropriate for different posts.

3.1 Identity

Of all the pre-employment checks, identity verification is the most fundamental. Two approaches can be used:

- A paper-based approach involving the verification of key identification documents and the matching of these documents to the individual
- An electronic approach involving searches on databases (e.g. databases of credit agreements or the electoral role) to establish the electronic footprint of the individual. The individual is then asked to answer questions about the footprint, which only the owner of the identity could answer correctly

Pre-employment checks can be used to confirm an applicant's identity, nationality and immigration status, and to verify their declared skills and employment history.

The Immigration, Asylum and Nationality Act 2006 means there are requirements for employers to prevent illegal working in the UK. These include an ongoing responsibility to carry out checks on employees with time-limited immigration status. Failure to comply with these regulations could result in a possible civil penalty or criminal conviction.

Go the NPSA Pre-employment Screening webpage.

3.2 Qualifications and employment history

The verification of qualifications and employment can help identify those applicants attempting to hide negative information such as a criminal record, poor performance or dismissal. Unexplained gaps should be explored during the recruitment process.

3.3 Qualifications

When confirming details about an individual's qualifications, it is always important to:

- consider whether the post requires a qualifications check
- always request original certificates and take copies
- compare details on certificates etc. with those provided by the applicant
- independently confirm the existence of the establishment and contact them to confirm the details provided by the individual

3.4 Employment history

For legal reasons it is increasingly difficult to obtain character references, but past employers should be asked to confirm dates of employment and the role undertaken.

Where employment checks are carried out, it is important to:

- check a minimum of three but ideally five years previous employment
- independently confirm the employer's existence and contact details (including the line manager)
- confirm details (dates, position and salary) with HR where possible, request an employer's reference from the line manager

3.5 Criminal record checks

A criminal conviction, either spent or unspent, is not necessarily a bar to employment. However, there are certain posts where some forms of criminal history will be unacceptable. To obtain criminal record information, a company can request that an applicant either:

- completes a criminal record self-declaration form, or
- applies for a Basic Disclosure certificate

Go the Government Disclosure and Barring Service webpage.

3.6 Role specific checks

For some posts it may be justifiable to carry out medical, financial or social media checks. For example where the employee's position requires the handling of money, financial checks would be appropriate. Interpreting the security implications of role specific checks is not straightforward and will require each organisation to decide where their thresholds lie (e.g. in terms of an acceptable level of debt) and specialist expertise in the area being checked.

3.7 Overseas checks

As far as possible, organisations should seek to collect the same information on overseas candidates and UK nationals who have lived or worked overseas as they would for longstanding UK residents (e.g. proof of residence, employment references, and criminal record). It is important to bear in mind that other countries will have different legal and regulatory requirements covering the collection of information needed to manage personnel security, therefore this step may be difficult.

A number of options are available to organisations wishing to perform overseas checks:

- request documentation from the candidate
- hire a professional / external screening service
- conduct your own overseas checks

In some circumstances, you may be unable to complete overseas checks satisfactorily (e.g. due to a lack of information from another country). In this case, you may decide to deny employment, or to implement other risk management controls (e.g. additional supervision) to compensate for the lack of assurance.

Go the NPSA Overseas Criminal Record Checks guidance.

4. Ongoing personnel security

Whilst pre-employment screening helps ensure an organisation recruits trustworthy individuals, people and their circumstances and attitudes change, either gradually, or in response to events. CPNI's insider data collection study identified:

- Over 75% of the insider acts were carried out by staff who had no malicious intent when joining the organisation, but whose loyalties changed after recruitment
- In many circumstances, the employee undertaking the insider act had been in their organisation for some years prior to undertaking the activity and exploited their access opportunistically. CPNI's collection of ongoing personnel security guidance and tools can be used to help an organisation develop and plan effective practices for countering the insider

threat and maintaining a motivated, engaged and productive workforce
- The application of good ongoing personnel security principles adds significant value to physical and technical security measures in a cost effective manner. It also promotes good leadership and management, maximising people as part of the whole security solution

Go the NPSA Reducing Insider Risk Guidance.

5. Investigation and discipline

Many organisations will at some point need to carry out an internal investigation into a member of staff. The primary duty for an investigator is to establish the true facts, whilst adhering to appropriate HR policy and employment law.

Organisations can react disproportionately to accusations, which can lead to costly employment tribunals or an unhappy and disaffected workforce. Conversely, organisations which fail to take any appropriate investigative and subsequent disciplinary action, can create a culture where staff actively disregard security policies and processes.

With correct procedures in place, employees who understand policies and regulations, and competent, trained investigative staff, your organisation will be better equipped to avoid such pitfalls and maintain trust.

6. Secure contracting

Contractors present particular personnel security challenges. For instance, the timescales for employing contractors are often relatively short and there is a greater potential for security arrangements to be confused or overlooked (e.g. due to further sub-contracting).

In managing the insider risks associated with contractors, it is important to:

- Ensure that pre-employment checks are carried out to the same standard as permanent employees. Where this is not possible due to tight deadlines or a lack of information available for background checking, the resulting risks must be managed effectively. The implementation of any additional security measures should be guided by a personnel security risk assessment
- Where pre-employment checks, or any other personnel security measures are carried out by the contracting agency rather than the employing organisation, a detailed account of the checks to be undertaken and the standards achieved must be incorporated into the contract. Furthermore, the pre-employment checking process conducted by the contractor should be audited regularly

- Confirm that the individual sent by the contracting agency is the person who arrives for work (e.g. using document verification or an electronic identity checking service)

Once the contractor has started working for the organisation, they will need to be managed securely. The following steps will help:

- Carry out a risk assessment to establish the threats and level of risk associated with the contractor acting maliciously whilst in post
- Verify the contract, and ensure it defines the codes of practice and standards required
- Provide photo passes to contract and agency staff and stipulate that they must be worn at all times whilst on site. Ideally, the employing organisation should retain contractors' passes between visits, reissuing them each time, but only after the contractor's identity has been verified. Ideally, there should be an expiry date visible on the pass. There should also be a policy for the surrendering of passes for both permanent and contracted staff, either once the member of staff leaves their employment or the contracted period ends
- The employing organisation and the contracting agency (or the contractor, should no agency be involved), should agree a procedure for providing temporary replacements when the contractor is unavailable. These arrangements should be included in the contract between the two parties. The employing organisation will need to decide what additional personnel security measures are required when replacement staff are on site
- Where a contractor is already in post, but the necessary pre-employment checks have not been carried out, or where the results of the checks fall below the acceptable standard, additional personnel security measures must be considered (e.g. continuous supervision) if they are to continue

Go the NPSA Secure Contracting Guidance.

7. Remote working

Remote working brings advantages for both the employer and employee, including the retention of motivated staff, increased flexibility and autonomy, and reduced costs for the organisation through consolidating and reducing office space. However, it also brings a number of people security issues, which, left unchecked, could lead to employee disaffection and increase the risk of counter productive work behaviours and malicious activity.

These might include:

- increased security risks resulting from the loss of IT equipment or sensitive company data,

particularly as a result of living in shared accommodation
- potential security or welfare concerns of employees going unchecked owing to a lack of direct supervision
- perception by the remote worker of loneliness and isolation, and being left ‘out of the loop’
- performance issues including the possibility of both under and over working, and resulting management issues

Go the NPSA Remote Working Guidance.

8. Security culture

Effective security relies on people behaving in the right way. This is enabled through an understanding of the threat and a clear understanding of what is required of them. In this way, people play a significant role in the detection, deterrence and prevention of security threats.

The development of an appropriate security culture, where the right security behaviours are adopted by the workforce, is essential to an organisation’s protective security regime. Used the right way, your staff, guardforce, contractors, visitors, suppliers and the general public can be a an effective resource at a relatively low cost, in strengthening your resilience to security threats and reducing your vulnerability to attack.

Security culture is defined by CPNI as ‘the set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security’. Without the right security values (i.e. culture), employees may exhibit poor security behaviours and operate a lack of compliance with protective security measures. This can lead to an increased risk of security incidents and breaches, resulting in reputational and financial damage, the development of a climate that facilitates insider threat, as well as potential harm to employees, customers, and/or business performance.

Before embarking on a change programme, however big or small, it is critical that an organisation is clear on the following:

- the objectives of the change (i.e. the vision or strategy)
- the size and scale of the change (i.e. the gap between where the organisation is now and where it wants to be)
- the actions required to implement the change (i.e. the interventions)
- whether the organisation is ready for the change (i.e. it has the necessary time, resources and buy-in)
- how to communicate the change to the target audience and other key stakeholders (i.e. the

communications strategy)
- how to review and evaluate the impact of the change (i.e. the measures of success and key performance indicators)

Embedding and maintaining change takes times. It also requires a clear vision, as well as a coordinated strategy to ensure the interventions are consistent, practical and meaningful.

There is no one right way to deliver change. The approach to take will depend on whether you are embedding behaviour change or culture change, the current climate in your organisation and what will resonate most with your target audience. A bespoke approach, suited to the particular needs and requirements of your organisation will ultimately work best.

Go the NPSA Security Culture and Behaviour Change guidance.

KEYWORDS
PERSONNEL SECURITY
RISK
PHYSICAL SECURITY
SECURITY CULTURE
RISK MANAGEMENT
HIRING SECURITY
VENUES AND PUBLIC SPACES
VENUES
PUBLIC SPACES