CPNI
Centre for the Protection of National Infrastructure

Personnel Security Maturity Model

Guidance Booklet

The purpose

The Personnel Security Maturity Model is issued by the UK's Centre for the Protection of National Infrastructure (CPNI) with the aim of providing a framework for organisations to assess their maturity in dealing with personnel security risks.

CPNI produces a wide range of tools and guidance covering various elements of personnel security (PerSec) practices and processes.These have grown organically as we have increased our understanding of insider acts and motivations over the last 10 years. Our PerSec Maturity Model provides a structured framework for the systematic and therefore more effective implementation of PerSec mitigations.

Our aim is to use the PerSec Maturity Model to assess and baseline an organisation's current level of PerSec Maturity from the information provided by the organisation (the maturity questionnaire) together with any additional evidence collected by the CPNI PerSec adviser in the course of their interaction with the organisation. The assessment will be compared with the maturity level that the organisation wishes to achieve, which may be directed by the lead government department or regulator.

Why use it?

Maturity Models are used in a number of industries to allow an organisation to assess their methods and processes according to best practice.

The CPNI PerSec Maturity Model has been designed to specifically assess an organisation's personnel security maturity. This is a key factor, in addition to physical and cyber security measures, in strengthening an organisation's resilience to insider and wider external security threats.

The model is based on comprehensive and robust research into insider acts[1], as well as extensive CPNI experience in PerSec mitigations (research and development programmes and close working with the CNI and overseas partners to test, refine and embed PerSec initiatives).

[1]*See CPNI Insider Data Collection Study – report of main findings available at* ***www.cpni.gov.uk/personnel-and-people-security***

The benefits of using the CPNI model are:

1. A starting point for developing a measurable PerSec improvement programme using the CPNI tools and guidance which are appropriate to the organisation's current level of PerSec maturity.
2. A common and consistent benchmark for PerSec performance across the Critical National Infrastructure (CNI), which will enable individual organisations to compare themselves with the rest of their sector, and wider CNI community.

The assessment will be used by CPNI to:

1. Target the use of existing PerSec advice, tools and guidance more effectively across the CNI.
2. Inform the development of PerSec improvement plans with organisations and CNI sectors.
3. Prioritise the development of new guidance and tools.
4. Track improvements in CNI sector-wide PerSec management practices.

How does it work?

The CPNI PerSec Maturity Model is based on seven core elements of effective PerSec processes, as identified through our insider data study and Research & Development programme:

- Governance and Leadership
- Insider Risk Assessment
- Pre-Employment Screening
- Ongoing Personnel Security
- Monitoring and Assessment of workers
- Investigation and Disciplinary Practices (Response)
- Security Culture and Behaviour Change

Annex A offers a detailed overview of these core elements.

How we assess your security

The core elements are evaluated against the six levels of PerSec maturity:

Annex B offers a detailed overview of these levels.

Key areas

The maturity questionnaire seeks evidence across four key areas and will be marked with the following icons to help you recognise what area of PerSec is being assessed in order to better focus your response on these areas:

EXISTENCE
of PerSec policies, processes and procedures

IMPLEMENTATION
of the PerSec mitlgations

CONSISTENCY
of the PerSec measures in place

EFFECTIVENESS
of the PerSec policies and processes that are in place

Using the questionnaire

The questionnaire is the primary evidence for assessing the level of maturity.

CPNI Advisers may require follow up discussions to clarify, or seek additional information to ensure a full and accurate assessment is made. The CPNI assessment will be internally quality assured to ensure commonality of benchmarking within and across CNI sectors.

The results of the assessment can then be used to:

- Have an informed discussion about the level of maturity the organisation wants to achieve (or maintain), and;
- Develop (in conjunction with their CPNI adviser) a PerSec improvement plan, which could involve attendance on CPNI run courses, briefing and awareness raising sessions, bespoke training and implementation of specific CPNI tools.

When you are at the stage to participate in the maturity assessment it may be helpful to consider the following:

- Identify a main point of contact within the organisation to work with CPNI.
- The assessment is based on the responses provided by the organisation. It is important to ensure that answers are as comprehensive as possible.
- Where applicable provide examples or evidence in support of the responses.

Access to the questionnaire

For access to the PerSec maturity questionnaire please contact your CPNI Adviser or email enquiries@cpni.gov.uk.

Maturity assessment questionnaire

The questionnaire is made up of the following seven sections:

1. Governance and Leadership

This set of questions assesses the level of corporate governance relating to PerSec, the level of engagement and commitment from the Board to PerSec, the reporting mechanisms up to the Board on PerSec and resourcing for PerSec from Board outwards across the organisation.

Example Questions:

EXISTENCE

Who has responsibility for managing your organisation's people risk?

IMPLEMENTATION

Is PerSec a standing agenda item at board level meetings?

CONSISTENCY

How are your PerSec policies integrated into your wider business?

EFFECTIVENESS

How do you review your PerSec policies (e.g after an incident, as part of an annual risk review)?

2. Insider Risk Assessment and Management

This set of questions assesses your insider risk process, the way in which insider risk is integrated into other organisational processes and the process for recording and reviewing insider risk decisions.

3. Pre-Employment Screening (PES)

This set of questions considers the policies and processes relating to Pre-Employment Screening within the organisation (employees and contractors), the competency of the people involved in the screening process and the central recording of screening decisions and the ability to review them as necessary.

4. Ongoing Personnel Security

This set of questions considers the policies, processes and procedures relating to PerSec and how consistently they are applied across the organisation, the competency of line management to apply the policies, the understanding and commitment of workers to the policies, and the process for reviewing personnel policy including exit procedures.

5. Monitoring and Assessment of Workers

This set of questions explores the effectiveness of monitoring processes, awareness of security procedures, reporting lines for workplace behaviours of concern and auditing arrangements and review of processes this section considers all workers whether they are contractors, consultants, part time, full time or temporary.

6. Investigation and Disciplinary Practices (Response)

This set of questions assesses the policies and procedures relating to investigating workplace behaviours of concern and the arrangements relating to security incident response, reporting mechanisms and analysis of incidents.

7. Security Culture and Behaviour Change

This set of questions considers the level of defined security culture across the organisation, workers' awareness, understanding of and engagement in PerSec and the ability of an organisation to respond and initiate change where required.

Annex A

CPNI definition of the Maturity Model core elements

Governance and Leadership

Positive and visible Board level support for protective security is vital to demonstrate to workers the value placed on personnel and people security policies and procedures.

As part of an overarching protective security strategy, strong security governance will develop (in conjunction with their CPNI adviser) a PerSec improvement plan. This could involve attendance on CPNI run courses, briefing and awareness raising sessions, bespoke training and implementation of specific CPNI tools.

Strong security leadership, at all levels across your organisation, will:

- Ensure consistency and clear lines of responsibility for the management of security risk.
- Foster a multi-disciplinary approach to countering the insider threat.
- Ensure proportionate and cost effective use of resources.
- Provide essential management information for the purposes of security planning and people management.
- Provide a strong example that both develops and underpins an effective security culture.

CPNI research has identified that a single accountable Board level owner of security risk and a top-down implementation of security policies and expected behaviours are likely to promote a more compliant and consistent security regime in your organisation.

Inadequate corporate governance structures and a lack of awareness of insider threat at a senior level can undermine effective security strategies and make it harder to detect, investigate and prevent insider activity.

Insider Risk Assessment

Understanding what security risks your organisation faces is essential for developing appropriate and proportionate security mitigation measures.

There are a range of risk assessment models available, which all follow the same principles:

1. Identify critical assets and systems in your organisation

2. Categorise and classify assets in relation to their level of criticality in supporting your business

3. Identify threats (based on the intent and capability of those who could carry out the threat)

4. Assess the likelihood of the threat occurring and impact should the threat transpire

5. Build a risk register to ensure all data gathered is recorded

6. The strategy of mitigating risks and reviewing the existing countermeasures

7. Development and implementation of new proportionate measures to reduce security risks

8. An iterative process of regularly reviewing risks

If you are carrying out a security risk assessment it is important that the results are factored into your wider corporate risk register

Next steps

The risks that have been identified are then used to inform the security mitigations you implement.

Carrying out a security risk assessment is crucial in helping security managers audit, and communicate to the executive Board, the security risks to which the organisation is exposed.

CPNI has developed a risk assessment model to help organisations centre on the insider threat. The process focuses on workers (their job roles), their access to their organisation's critical assets, risks that the job role poses to the organisation and sufficiency of the existing countermeasures.

Working through the CPNI insider risk assessment model will help organisations to:

- Conduct security risk assessments in a robust and transparent way.
- Prioritise the insider risk to an organisation.
- Evaluate the existing countermeasures and identify appropriate new measures to mitigate the risks.
- Allocate security resources (personnel, physical or cyber) in a way which is cost effective and proportionate to the risk posed.

Pre-Employment Screening

Pre-Employment Screening comprises the procedures involved in deciding an individual's suitability to hold employment in a given job role.

This is not limited to 'new joiners', but also individuals who are moving between job roles within an organisation. A suitable level of screening should be applied to all individuals who are provided with access to organisational assets including permanent, temporary and contract workers.

Robust Pre-Employment Screening policies and procedures are essential in organisations meeting their legal obligations and setting a foundation for a safe and secure workplace.

Appropriate screening measures help to provide cost effective and legally compliant assurance that only the right people, in the right job roles, are working within your organisation.

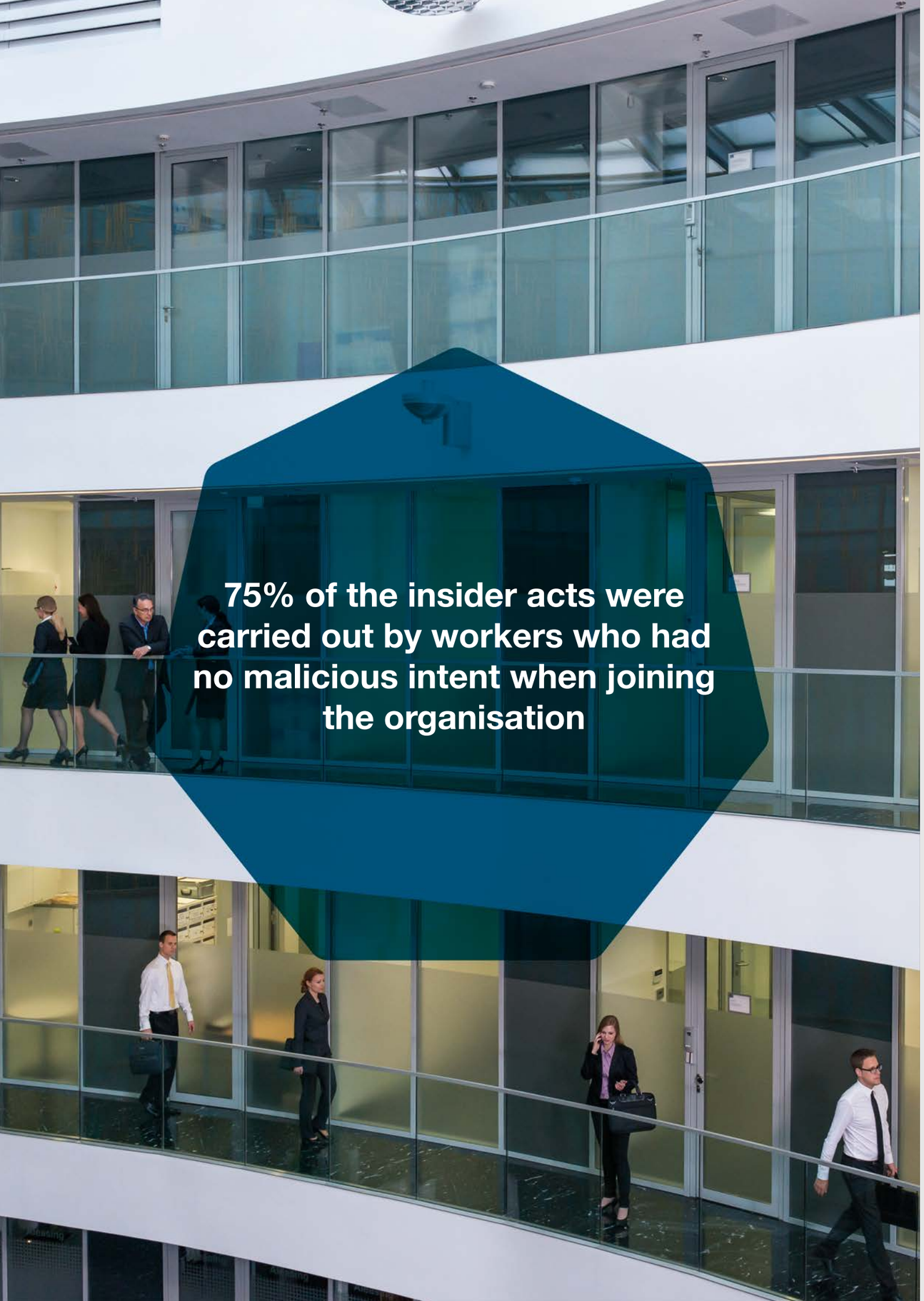
The application of screening measures will vary across organisations and across job roles. Basing screening decisions on thorough security risk assessments will ensure that any measures adopted will be proportionate to the risks and make best use of valuable resources.

As part of an overarching protective security strategy the appropriate application of PES will:

Deter applicants who may wish to harm your organisation from applying for employment.

Detect individuals with intent to harm your organisation at the recruitment or application phase.

Deny employment to individuals intending to harm your organisation and deny employment in roles for which the applicant is unsuitable.



Ongoing Personnel Security

While Pre-Employment Screening helps ensure that 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:

- 75% of the insider acts were carried out by workers who had no malicious intent when joining the organisation, but whose loyalties changed after recruitment.
- In many circumstances the worker 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 PerSec 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 PerSec principals adds huge value to physical and technical security measures in a cost effective manner, promoting good leadership and management and maximising people as part of the security solution.

Monitoring and Assessment

CPNI's Insider Data Collection Study indicated that some organisations had not made regular or systematic use of their own technical or financial auditing functions to spot irregularities or unusual workplace behaviours.

In other organisations, counterproductive workplace behaviours were known in one part of the organisation, but this was not shared with other sections, resulting in delays in the organisation taking mitigating actions to reduce the risk and allowing insiders to act in the first place, or for some, to continue their activity without detection for longer than necessary.

CPNI advocates a holistic approach to protective monitoring where information about workers' risks (physical, electronic audit and personnel data) are brought together under a single point of accountability and governance, to ensure a transparent, legal, ethical and proportionate protective monitoring capability.

Investigation and Disciplinary

Many organisations will at some point need to carry out some kind of 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 laws.

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, workers who understand policies and regulations, and competently trained investigative staff, your organisation is better equipped to avoid these pitfalls and maintain trust.

In addition to investigating an insider act your organisation needs to have a risk management process in place which manages the consequences of the act and a process in place that helps you:

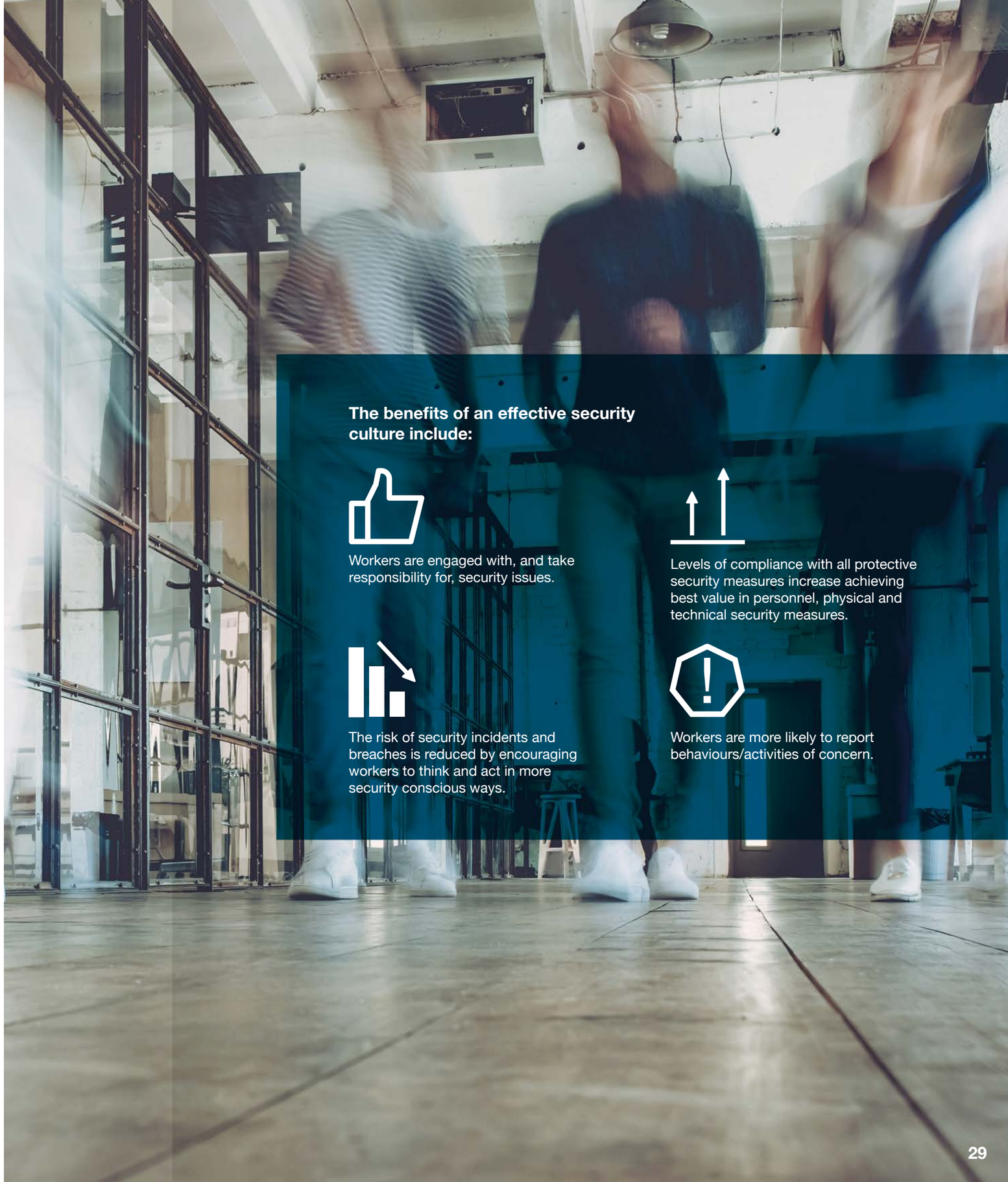
1. Identify and analyse the root cause of the incident.
2. Identify the appropriate disciplinary actions or interventions that need to be undertaken.
3. Assess the effectiveness of current control measures in place.
4. Identify gaps in practice and develop more effective control measures.

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

Security Culture and Behaviour Change

A good security culture in your organisation is an essential component of a protective security regime and helps to mitigate against insider threats and external people threats (such as hostile reconnaissance).

Security culture is the set of values, shared by everyone in an organisation, which determine how people are expected to think about and approach security, and is essential to the protective security regime as a whole.



The benefits of an effective security culture include:

Workers are engaged with, and take responsibility for, security issues.

Levels of compliance with all protective security measures increase achieving best value in personnel, physical and technical security measures.

The risk of security incidents and breaches is reduced by encouraging workers to think and act in more security conscious ways.

Workers are more likely to report behaviours/activities of concern.

Annex B

CPNI PerSec Maturity Model overview

Innocent

Level 0

Current Behaviours

Organisation is functioning at the most basic level. There are no formal PerSec policies, training or procedures. Senior Managers are unconcerned of the risks posed by people and have made no attempt to engage with CPNI. The organisation is at very high risk from operational, financial, and reputational damage due to PerSec threats.

Aware

Level 1

Current Behaviours

PerSec is defined in basic terms of technical or procedural solutions to meet UK employment legislation or regulation. No standardised threat mitigation processes, training or policy. No senior, board level, member of staff has been given responsibility for PerSec.

The organisation is at high risk from operational, financial and reputational damage due to PerSec threats.

Developing

LEVEL 2

Current Behaviours

PerSec is seen as a business risk, given management time and effort put into reducing security incidents. Security still defined in terms of adherence to rules, procedures and technical controls, however there is an acknowledged approach using standardised templates.

Security performance is measured in terms of lagging indicators (number of breaches, alarms). The organisation is at medium high risk from operational, financial and reputational damage due to PerSec threats.

Competent

LEVEL 3

Current Behaviours

There is an organisation wide, consistent approach to security with defined processes in place.

Organisation recognises the involvement of front line workers in security is critical. Managers recognise wide range of factors influence security and root causes can originate from management decisions.

Significant numbers of front line workers willing to work with management to improve security. The organisation is at medium risk from operational, financial and reputational damage from PerSec threats.

Effective

LEVEL 4

Current Behaviours

The Executive board recognises that security is important from a moral and economic point of view, and can provide business advantage. Governance arrangements are as concerned with monitoring and influencing precursor indicators as with lagging indicators.

Majority of workers accept the need for personal responsibility towards security. The importance of all workers feeling valued and treated fairly is recognised.

The organisation puts significant effort into proactive measures to prevent security incidents. Security performance is actively monitored, and statistics collected and analysed. The organisation is at medium low risk from operational, financial or reputational damage from PerSec threats.

Excellent

Level 5

Current Behaviours

The prevention of PerSec incidents is a core company value, and a board level member of staff has overall responsibility for PerSec. Security is part of “business as usual”.

The organisation recognises that the next threat is just around the corner and the PerSec risk assessment is reviewed at least once a year. Uses a range of indicators to monitor performance, but not just those which are performance driven.

Organisation has confidence in its security processes and is constantly striving to find better and innovative ways of improving security control. All workers accept personal responsibility for security. The organisation is at low risk from operational, financial and reputational damage due to PerSec threats.

Annex C

THRC PerSec definitions

Levels of Vulnerability

For Lead Government Departments and the relevant CNI, the Threats, Hazards, Resilience and Contingencies (THRC)[1] definitions of PerSec vulnerability are aligned to the CPNI maturity levels.

The following scale shows the level of vulnerability, the THRC sector-wide definition and the related maturity level. It is important to bear in mind that these definitions relate to the general state of the CNI sector rather than individual organisations.

HIGH

A lack of appropriate processes, arrangements or awareness and concern about people risk; operating only at the minimum required level for compliance.

LEVELS 0 & 1 INNOCENT, AWARE

MEDIUM HIGH

People risk seen as a business risk and resources allocated to reducing security incidents; security defined by adherence to rules and technical controls.

LEVEL 2 DEVELOPING

MEDIUM

Consistent approach within the sector to security, recognition of the variety of factors that influence security, solutions that involve managers and workers as part of the delivery mechanism.

LEVEL 3 COMPETENT

MEDIUM LOW

Significant effort put into proactive measures to prevent security incidents, security performance actively monitored; workers accept need for personal responsibility towards security.

LEVEL 4 EFFECTIVE

LOW

Prevention of PerSec incidents seen as a core value within the sector, has confidence in its security processes and constantly striving to find better and innovative ways of improving security control.

LEVEL 5 EXCELLENT

*[1]For more information on the National Resilience Capabilities Programme that THRC sits under please see **www.gov.uk/guidance/preparation-and-planning-for-emergencies-the-capabilities-programme.***

CPNI

Centre for the Protection of National Infrastructure

CPNI produces a wide range of tools and guidance covering various elements of recommended PerSec practices and processes.

These have grown organically as our understanding of insider acts, motivations and potential mitigations have over the last 10 years. The Maturity Model provides a structured framework for the systematic, and therefore more effective, implementation of an insider risk mitigation programme.