PA Consulting Group

National Protective Security Authority

HOLISTIC MANAGEMENT OF EMPLOYEE RISK (HoMER)

New guidance to help organisations to reduce the risk from their employees

Executive summary

Foreword by the Information Commissioner

The Information Commissioner's Office (ICO) has been involved with the HoMER project since its planning stages. It has been of particular interest to us because, on the one hand, we are concerned with the information rights of employees subject to workplace monitoring, and on the other, we have an interest in the security of personal data held by organisations. We recognise that keeping data secure inevitably involves making sure employees do not abuse their access to it – indeed, the Data Protection Act (DPA) requires organisations to take steps to ensure the reliability of any employees who have access to personal data.

Managing employee risk has become a critical issue for organisations, for which a fine balance is required between treating employees fairly and ethically, and ensuring comprehensive data security. This guidance is positive, pragmatic and business-led. It will help organisations to achieve a step change in their security and to strengthen their future position in the eyes of their people, customers and other relevant stakeholders.

Too often we have seen workplace monitoring schemes that are cloaked in unnecessary secrecy and that lack proper governance and senior-level accountability. The operation of such schemes can contribute to the negative and damaging behaviour that HoMER's principles are intended to prevent. We have therefore been impressed with HoMER's emphasis on the transparency and governance that must accompany any effective workplace monitoring scheme – this is very much along the lines of the ICO's 'Employment Practices Data Protection Code'.

We recognise that in some circumstances the procedural detail of a scheme – its precise methodology and scheduling – must be kept secret. However, the advantages of being as open as possible with employees about the operation of a workplace monitoring scheme are obvious.

Christopher Graham
Information Commissioner
August 2012

Helping you manage people risk

Holistic Management of Employee Risk (HoMER) is new guidance to help you manage the risk of employees' behaviour damaging your business.

'Employee risk' is defined as counterproductive behaviour, whether inadvertent, negligent or malicious, that can cause harm to an organisation.

The guidance sets out :

- good practice examples, principles, policies, and procedures which help manage the risk of counterproductive behaviour in the workplace
- ways to strengthen compliance with legal and regulatory frameworks
- a framework of measures to help improve trust amongst employees, customers and shareholders
- the importance of sound and engaged leadership, corporate governance and transparent policies.

Figure 1: Key stages of the HoMER guidance

The holistic use of targeted security measures and interventions (eg information, personnel and physical) will help you spot high-risk workplace behaviour and reduce the potential of employees carrying out malicious attacks.

This guidance is for board members and the managers of risk in your organisation.

HoMER has a pragmatic approach and a work-book style

The HoMER guidance leads organisations through the key stages of the people risk lifecycle.

Vision and leadership: the importance of sound and engaged leadership, corporate governance and transparent policies in managing people risk and strengthening compliance.

Assess: the importance of adopting a demonstrable risk-based approach and of having reliable asset, access and identity management.

Protect: the importance of developing compliant policies and procedures for protective monitoring.

Respond: the importance of advance 'response preparation' to an employee incident and guidance on how to do this in ways most likely to minimise damage and retain stakeholder trust.

Recover: effective steps for recovery following an incident while maximising lessons learned in order to improve security.

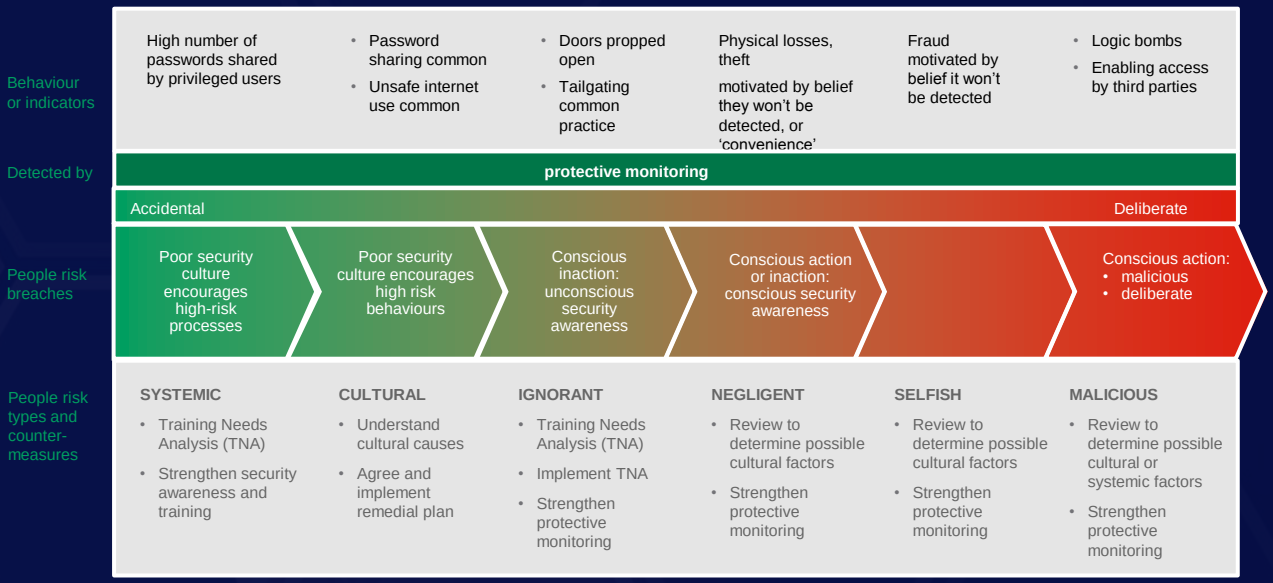
Key elements of HoMER:

- **A risk-based approach:** focus on assets and those who can access them. Understand where risks lie and allow your organisation to focus its investment in protective measures.
- **Holistic people management:** seek input from across your organisation to address the risk effectively.
- **A strong security culture:** make your values explicit and build a security culture where employees are committed to safeguarding security.
- **Single accountable ownership of people risk:** ensure that all functions with a responsibility for people risk report to a senior, single accountable owner.
- **Legality and transparency:** transparent policies and informed employees will gain trust and buy-in from stakeholders and strengthen compliance.

The full HoMER guidance is available from www.npsa.gov.uk (from 20 September 2012).

Build a strong security culture

Security breaches, what they say about the security culture and countermeasures



Studies show that most employees are not prepared to challenge colleagues who are not complying with policy. They are prepared to report breaches 'up the chain', but won't step in themselves. In some circumstances, the response to a report may be too late to prevent a security problem becoming an incident. Organisations should identify those policies which they want employees to actively enforce and provide the necessary training to empower them to do so in a non-confrontational manner which does not destroy the trust between colleagues.

Ensure your protective monitoring is ethical, legal and holistic

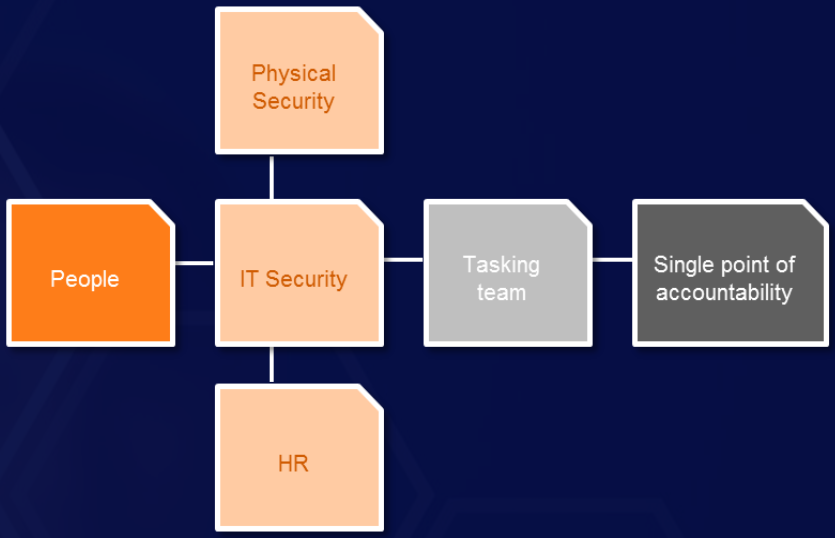
Monitoring should be both transparent and unpredictable

Employees being monitored should be aware of, and consent to, the monitoring.

For monitoring to be transparent, employees need clear guidance on the organisation's privacy policy.

Sensitivities of protective monitoring

Almost all forms of monitoring will involve the collection of personal data.



The Data Protection Act places responsibilities on organisations to ensure that such personal data is collected lawfully and processed in a fair and proper way.

It is essential to ensure transparency about the existence of protective monitoring but details of the monitoring should not be disclosed as this could allow it to be circumvented.

If your organisation is carrying out any form of monitoring in the workplace in the UK, you should obtain legal advice and consult relevant websites such as the Information Commissioners' Office (ICO) to ensure your monitoring is in line with legislation .

Emerge stronger

Your organisation does not have to suffer an incident to evolve: you can learn from the experiences of others.

The most effective organisations use their awareness of the external environment to anticipate new vulnerabilities, threats and risks.

As technologies change they bring new benefits but also new risks. Your organisation should be anticipating these environmental changes for business reasons but it is also encouraged to do so in the Data Protection Act.

By learning from each incident and feeding any 'lessons learned' into the risk assessment process your organisation can continually improve its holistic management of employee risk.

By applying this approach you will:

- mitigate identified people risks
- remain compliant with dynamic regulatory requirements
- anticipate regulatory trends
- anticipate the expectations of employees and wider stakeholders
- reflect, strengthen and contribute to the security culture of the organisation.

Further information

The HoMER guidance was produced jointly by CPNI and PA Consulting Group.

NPSA

NPSA protects national security by providing protective security advice. Our advice covers physical security, personnel security and cyber security/information assurance

Website: www.npsa.gov.uk

PA Consulting Group

We are a firm of over 2,000 people specialising in management and IT consulting, technology and innovation. We operate globally from offices across Europe, the Nordics, the United States, the Gulf and Asia Pacific.

Website: www.paconsulting.com

Email: cybersecurity@paconsulting.com

PA Consulting Group and NPSA are grateful for the comments and suggestions received from Field Fisher Waterhouse LLP.

Corporate headquarters
123 Buckingham Palace Road
London SW1W 9SR
United Kingdom
Tel: +44 20 7730 9000

www.paconsulting.com