Personnel Trustworthiness and Reliability

Adrian Freer

Director Civil Nuclear Security

Office for Nuclear Regulation

An agency of HSE

Focus of Presentation

- What is it?
- Why do we need it?
- How do we achieve it?

What is it?

- A system of policies and procedures which manages the risk of staff or contractors exploiting legitimate access to an organisation's assets or premises for unauthorised purposes.

The Layered Approach

- Prior to employment
- During employment
- Increasing levels of proportionate intrusiveness to accord with the access you require for your staff.

Basic level checks

- The most basic assurance layer is an absolute requirement for anybody who works for, or in conjunction with, government.
- It allows an assessment of honesty, integrity and values

Higher level checks (1)

- National Security Vetting clearances focus on susceptibility to subversion, criminality or compromise based on personal habits, financial stability or extreme political beliefs.

Higher level checks (2)

- Consideration given to:
  - involvement in illegal activities;
  - unspent criminal convictions;
  - false or unsubstantiated claims on the CV or application form;
  - unsubstantiated qualifications;
  - unexplained gaps in employment history;
  - adverse references;
  - questionable documentation;
  - Some medical conditions.

Why do we need it?

- Post employment, the greatest risk management challenge.
- ‘Attacks’ may rely upon the co-operation of an insider.

Why do we need it?

- Self initiated insider
- Recruited insider
- Deliberate insider

Why do we need it?

Insider Principles

- No common demographics of race, gender, or age;
- 58% employed in administrative and support positions of which 50% in leadership or supervisory roles.
- Nearly 50% exhibited inappropriate behaviour prior to the incident.
- 84% no previously recorded incidents or violations of organization policies.

Security During Employment

- Aftercare seeks to reduce the risk of insider activity, protect assets and resolve suspicions or provide evidence for disciplinary procedures.

Security During Employment

- I recommend “aftercare” in the context of “ongoing personnel security”:
  - **For higher level clearances**: Regular reviews of personal circumstances.
  - **For all categories of assurance**: The adoption of an holistic, flexible security culture.

Security Culture

- Maintenance of a robust security culture is critical to ensuring satisfactory aftercare.
- Provides assurance measures over and above those operated by other elements of the Critical National Infrastructure.

Security Culture - Principles

- Risk-based approach
- Holistic people management
- Strong security culture
- Single accountable ownership of people risk
- Legality and transparency

Principles

- Possible warning signs include:
  - drug or alcohol misuse;
  - expressions of support for extremist views, actions or incidents, particularly when violence is advocated;
  - sudden or marked change of religious, political or social affiliation
  - major unexplained changes in lifestyle or expenditure;
  - sudden loss of interest in work
  - stress such as excessively emotional behaviour;
  - changes in working patterns
  - unusual interest in security measures
  - frequent unexplained absences

Final Thoughts

- Be clear about the purpose of the protective monitoring and ensure that any solution achieves this purpose.
- Consider monitoring most acceptable to your employees.
- If monitoring is used to enforce rules and standards, make sure employees know what these are.
- Information collected through monitoring must be kept secure.
- Communicate clearly to employees.