Carol Higson

Insider Mitigation Programme

Who or what is an insider?

An insider is a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.

This can be a permanent, temporary, seconded, contract or agency worker (in this guidance, the terms employees and staff are used to refer to all these groups).

As organisations implement increasingly sophisticated physical and information security measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.

What does Personnel Security mean for Urenco UK?

Personnel security is a system of policies and procedures which seek to:

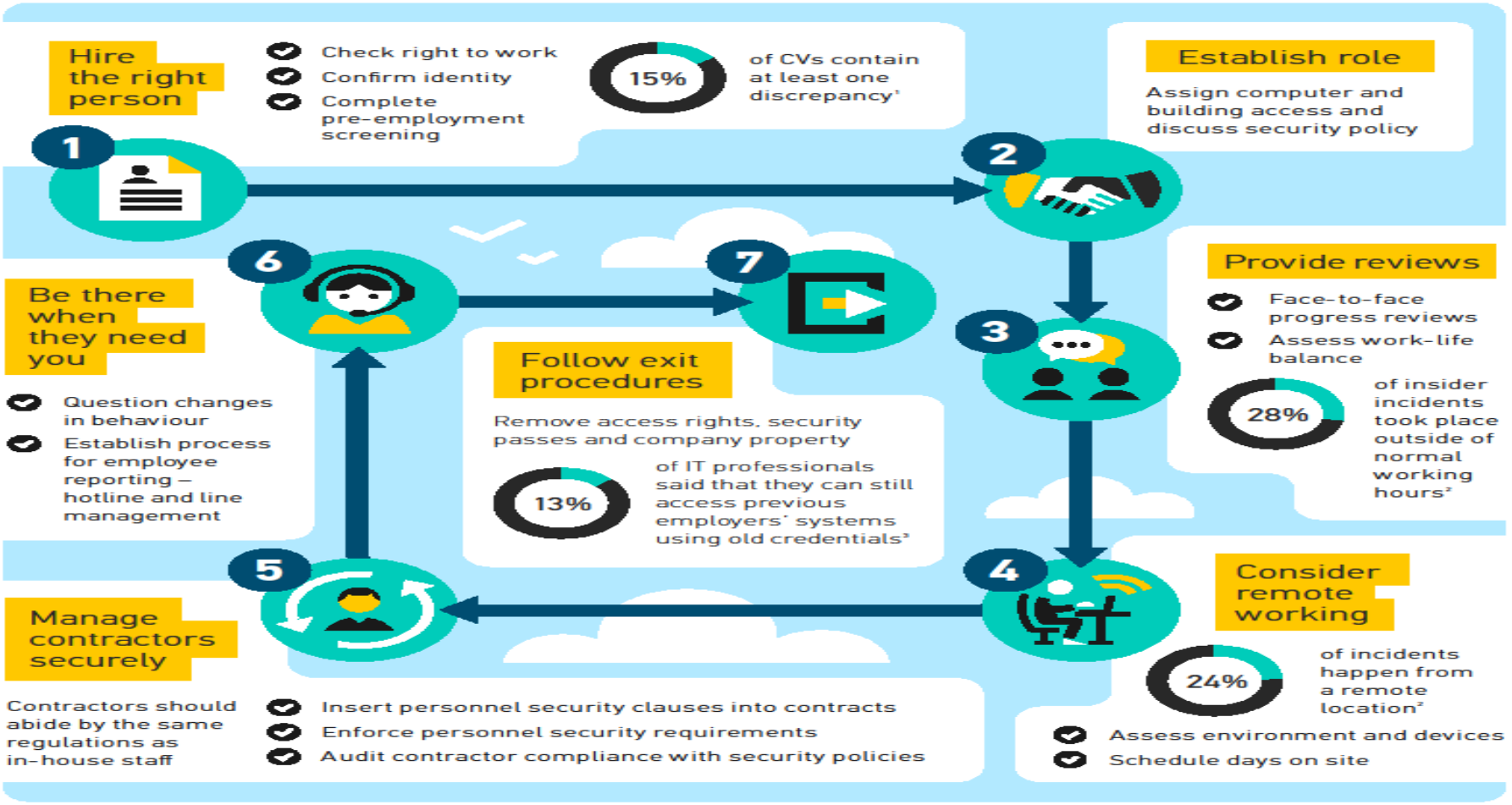
- Reduce the risk of recruiting staff who are likely to present a security concern
- Minimise the likelihood of existing employees becoming a security concern
- Reduce the risk of insider activity, protect the organisation's assets and, where necessary, carry out investigations to resolve suspicions or provide evidence for disciplinary procedures
- To implement security measures in a way that is proportionate to the risk

CPNI
Centre for the Protection of National Infrastructure

PERSONNEL SECURITY

Are you thinking about it?

Organisations should consider Personnel Security measures from the moment they employ someone to the moment they leave.



While pre-employment screening helps with recruitment, organisations need to monitor attitude changes and events that can affect employees over time.

FOR MORE INFORMATION PLEASE READ ONGOING PERSONNEL SECURITY: A GOOD PRACTICE GUIDE, AT WWW.CPNI.GOV.UK

REFERENCES: 1. CERT (http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=182); 2. The Security Company International (http://www.thesecurityco.com/media/40631/Whitepaper-insider-threat_January2013.pdf); 3. Lieberman Software (http://www.liebsoft.com/More-Than-1-in-8-IT-Security-Pros-Can-Access-Previous-Employer-Systems-Using-Old-Credentials/)

Why did UUK design a programme?

To mitigate against the insider threat which was posed in our Design Basis Threat.

The caveat to the company was that the programme could not eliminate the insider threat however it could significantly reduce the likelihood and mitigate the impact.

Which scenarios were reviewed;

- Staff working with company and customer sensitive information
- Staff working with classified information
- Protection of nuclear material/technology
- Those with access to IT and plant systems

Any breach at UUK could have significant and severe national security or financial/reputational consequence for both country and business.

Who was our programme aimed at?

Employees/Contractors

- Security culture

Supply chain

- How do their companies conduct vetting and employment checks, do they understand the insider/
- Malicious or accidental

All personnel who are authorised to enter the Urenco site

Line Managers and contract supervisors

The response force who have access to the whole site

How did we make an informed decision What data was collected/analysed?

Leading and lagging indicators

- Previous breaches
- Predicating behaviour from the data provided
- Data on security incidents, near-misses and reported vulnerabilities were analysed
- Root cause of any increase or decrease in reports of security near-misses

Performance data/feedback from the HR department / Occupational Health was used to inform the personnel appraisal process as well as the examples of interaction between security and support functions

Data from physical and cyber security teams on the control measures which were already in place concerning access electronically/physically

Key components of UUK's insider programme.

Multi discipline approach

- HR/Health/Sec/Operations

Identification of key assets/critical roles

- Shift manager
- Security manager

Transparency, governance and sign off by key stakeholders

- E.g. Head of compliance

Not to be reliant on the Government vetting system – we want to make our own decisions

Assured processes for:

- Recruitment, appointment, aftercare, leavers- essentially good housekeeping
- Increased controls- IT, physical etc.

The delivery

Line Managers

- Appraisal system
- Know their people

Whistleblowing and investigative procedures

- What is the process
- Are investigators qualified and experienced?

Effective access controls

- IT and physical systems

Good entry/exit procedures (HR process)

Management support and governance

Security awareness and training

Security Culture is key

Security culture was assessed through the Per Sec maturity model in order to identify cultural risk. This is a process identified by our regulator

Culture is about preventing accidental insider security breaches as well as preventing the deliberate insider breaches of security

Without an effective security culture other measures are unlikely to be effective

Urenco UK Risk register

Once the insider risk was identified it was then fed into the Urenco risk management process, forming part of our risk assessment

Urenco chose to follow the role-based risk assessment, which should flow from an organisational level risk assessment. This is the method supported by the UK government

Summary

Supply chain still remains a challenge

Are we perfect?..... NO.

Is the insider mitigation programme work in progress?

Is the programme visible to the organisation, yes.

Is the insider risk visible and accepted?

Is the programme a business enabler?..... YES.