Mitigating Insider Risks with IT Security

August 2016

This guidance is aimed at security managers that are responsible for insider[1] threat and have some responsibility for their organisation's IT security.

Types of insider crimes

An insider may be full or part-time, or a supplier. Insider crimes are far from new, but increasingly involve the misuse of corporate IT systems. Most research and guidance on this subject covers behavioural work, such as screening methods to identify problem staff, or IT security, focussing on hardening systems to make insider crimes difficult. Very little addresses both, but both are necessary, as insider crimes are holistic, involving people, organisations and IT. Examples of insider crimes that usually involve IT are:

- Fraud and rogue trading
- theft of sensitive information for personal use, public exposure, or for passing to a hostile state or rival company
- inappropriate access or use of databases
- system sabotage e.g. crashing servers, or deleting key data
- human-initiated cyber-attack
- theft of bulk data

Detecting insiders - relevant datasets

Insider risks should feature prominently and comprehensively on an organisation's wider risk assessment. Insider crimes should feature as personnel security and IT security risks. So, mitigating them requires expertise and data from both areas. The key to effective insider risk management lies with making good use of a range of relevant data from inside and outside the organisation. Examples of data that could be useful for detecting or investigating insider crimes are:

- HR data e.g. poor performance, previous investigations, pending departures, sensitive post holders
- IT system or application logs, physical access logs
- social media profiles, external contacts or conflicts of interest
- security breach information

[1] CPNI uses the following definition to describe an insider.
Someone who exploits or intends to exploit their legitimate access to corporate assets for unauthorised purposes

- personnel security e.g. anyone previously assessed as vulnerable from a security perspective
- use of portable media

Some suggested mitigations

The types of personality or circumstantial factors and access opportunities that contribute to increasing insider risk are numerous and complex. Many have been studied separately by CPNI's Insider Threat study[2] and Cyber Insiders[3] programme. In terms of unauthorised disclosure or theft of sensitive data, there may often be noted unusual behaviour, such as strong and unjustified sense of entitlement or being above rules, sympathies towards incompatible causes, or a strong and unjustified desire for recognition from the crowd. In many cases, these behaviours may be so extreme, as to have been noted by HR or management, through disciplinary processes, poor relations with colleagues and management, or general poor performance.

Staff who feel they have been passed over and have inflated perceptions of self- worth may be more motivated to disclose sensitive information or present significant work results more as their own, when they are really a team effort. In order to mitigate such risks, security teams might consider prioritising problematic staff or staff who have recently tendered resignations for closer IT monitoring.

Protective monitoring and analytics

Organisations should establish normal behaviour for roles or teams and develop rules or "use cases" that they are interested in detecting e.g. staff who suddenly email numerous sensitive reports to personal email accounts, when they would not normally do so. Organisations should identify the datasets that they need to alert on these rules e.g. external email and attachments, or database search records. Organisations should work with data owners to access these data and use analytical tools to study them.

Legality and governance

Legal sensitivities surrounding monitoring of staff exist in all countries, but vary in severity and rationality from country to country. Organisations should obtain legal advice at the outset, before collecting any data relating to their employees, giving careful consideration to what data is needed, how and why it will be used and stored. Organisations should develop governance and processes involving data owners, HR managers and get legal advice when considering how to manage insider casework.

Holistic risk mitigation

As well as aiming to Detect insider risks and activities, organisations should consider Deterrence and IT hardening or Prevention strategies. In fact, measures such as these may be easier and more effective ways of reducing risk than trying to detect or pre-empt insider acts by observing staff behaviour. Some suggested measures such as these are:

- Deterrence – producing comprehensive acceptable use policies, covering different applications, tools and networks, that stipulate what staff must not do and indicate that

[2] http://www.cpni.gov.uk/advice/Personnel-security1/Insider-threats/
[3] http://www.cpni.gov.uk/advice/cyber/Cyber-research-programmes/Cyber-insiders/

monitoring of these activities is in place. A good security culture is also key to good Deterrence.

- Prevention – disabling portable media, so that staff need authorisation to extract files onto media or external servers and that those transactions are centralised, recorded and audited.

These three strands – Detection, Deterrence and Prevention - should complement each other.

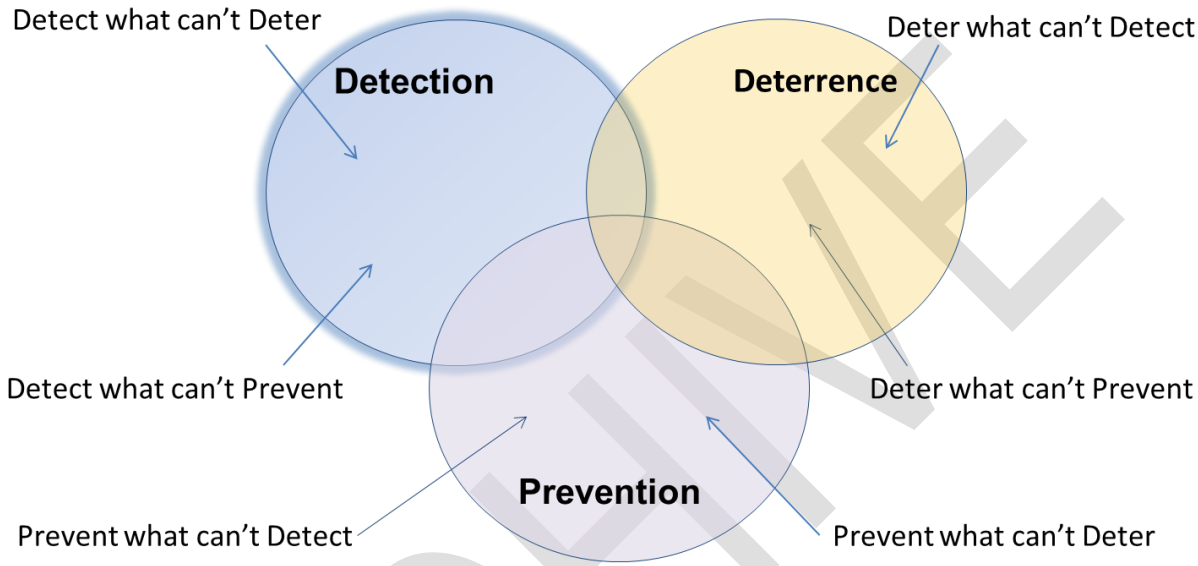

Figure 1: The three key components of insider threat mitigation should be geared to complement each other.