National Protective Security Authority

GUIDANCE

Quick Guide to gathering metrics for Personnel Security Maturity

The Selection of Metrics

The recommended approach to adopt, wherever possible, in selecting personnel security metrics is to:

- Identify a small number of different high-level strategic organisational goals which are likely to be affected by security e.g. performance, governance, staff capability etc.
- Identify, for each of these high-level strategic goals, a manageable set of specific, measurable indicators.
- Choose indicators which include a mixture of lead (predictive measurements) and lag (outcome measurements) indicators. See examples below.
- Do not use indicators which provide fundamentally unreliable information. For Example, any indicator based on very rare data occurrences.
- Choose indicators which are appropriate to several levels of security behaviour (individual/team/section/organisational). Although, depending on the circumstances of the organisation, it may not be necessary to have indicators for all levels.
- Where possible, choose at least one indicator which identifies counter-productive behaviour, e.g. security breaches.
- Make sure that the individual indicators chosen measure sufficiently different aspects of organisational performance so that they add value to each other.
- Choose indicators which are relevant to the work with security implications that your workforce carry out.

Types of Metrics

There are three dimensions on which metrics vary relevant to security maturity and behaviour:

- Metrics which are aimed at different stages of the development and occurrence of insider behaviour, i.e. pre-cursor, lead and lag indicators (see below for examples).
- Direct versus indirect indicators. Indirect indicators are those which although not explicitly about security there are nonetheless likely to be a strong relationship between them and security behaviours. For example, high levels of staff theft are likely to be associated with other types of counter-productive behaviour including security and insider acts.
- Quantitative versus qualitative indicators.

Use Lag indicators, such as security incidents or breaches, if they are available. However, for many organisations, they will be very rare events, so they do not provide reliable measures in which case rely upon other types of indicators.

Examples of specific indicators

Precursor indicators

- Staff surveys, employee engagement and employee pulse surveys.
- Staff performance measures, e.g. timekeeping, attendance (e.g. at meetings or briefings), productivity, staff disputes.

Lead Indicators

- Staff attitude and motivation indicators, e.g. requests for re-assignment, absenteeism rates, staff turnover and job hunting, staff complaints.
- Input and process measures, e.g. non-compliances and rule breaking, inclusion of security performance in risk registers and executive agendas, level of re-working required in security-related tasks, number of workforce reports on security issues, volume of training or retraining needed on security-related tasks.

Lag Indicators

- Security events, e.g. number of security incidents (e.g. cyber-attacks), number of security breaches (e.g. insider acts).
- Responses to security concerns, e.g. number of workforce security investigations, number of security clearance withdrawals.

Top Tips

- Use meaningful metrics which are already collected for other purposes.
- Ensure the measure is unambiguous. For example, a simple measure of volume of training is difficult to interpret. High levels of training can be a sign of good staff engagement and enthusiasm but can also be an indication that there are serious motivational and performance problems.
- Use metrics where you are clear what sorts of actions you might take to improve the situation.
- Choose metrics that are likely to endure so you can measure over time and monitor progress.