



## i-wareness<sup>®</sup> Management Information

The i-wareness<sup>®</sup> solution provides a range of supporting Management Information metrics which together provide strong evidence on both the effectiveness of your awareness programme and the level of behavioural change within your organisation. Information gained from the Management Information helps to validate your organisation's key security objectives and develop future campaign activity. Important for many organisations, the combined metrics also provide tangible evidence for compliance and audit requirements.

### The benefits

The i-wareness<sup>®</sup> Management Information:

- Provides tangible evidence for compliance and audit requirements
- Provides a detailed insight into the success of your awareness programme and guides future campaign activity
- Identifies the level of behavioural change within your organisation
- Allows management to validate and re-align your organisation's key security objectives
- Provides tangible evidence to support a business case for security awareness initiatives

### The metrics

The i-wareness<sup>®</sup> Management Information report is compiled using metrics from a number of different sources. Assessment of any of these elements in isolation will provide only a limited insight into the bigger security picture and overall organisational

security culture, however combined they give an excellent indication of progress made. The following metrics are analysed and presented:

- Security Awareness Survey results
- Knowledge Zone site hits
- Teach & Test results
- Incident Reporting metrics

### Security Awareness Survey

The Security Awareness Survey determines the current levels of security awareness within your organisation. It identifies employees' perception, attitudes and opinions and gives an insight of their behaviour in the workplace through their understanding of security policies and good practices.

The results of the survey will also identify your organisation's security strengths and weaknesses, provide tangible evidence to support a business case for security awareness initiatives and help direct your security awareness strategy.

## Knowledge Zone

The Knowledge Zone site hits provide you with a snapshot of the site's activity. Results allow you to:

- Filter the number of hits to the site (by unique users and page hits) on a daily, weekly, monthly, annual basis
- Distinguish areas or topics within the site that are most popular which can help guide future campaign activity
- Identify trends in site traffic and activity where a communications campaign has been active
- Review page ratings to guide content updates

## Teach & Test

Results from the Teach & Test allow you to measure your employees' understanding of security. This provides an accurate representation of the level of security knowledge among employees that can be used for compliance and audit purposes. Teach & Test results also act as a good indicator of the success of your communications campaigns. They identify gaps in employee knowledge and highlight hot security topics to direct future campaign direction.

## Incident Reporting

The incident reporting metrics often provide an insightful measure of the level of security awareness within your organisation. Following the launch of an ongoing awareness campaign, it is common for the number of incidents being reported to increase. This demonstrates the increased level of understanding by employees of the types of security incidents that they should be reporting and how they go about reporting such an incident.

Over time the trend will show that despite there being an increase in the number of incidents reported, the severity of these incidents have decreased as employees have a greater understanding of their security responsibilities.

These quantitative methods of measuring behavioural change and programme success provide a solid foundation for understanding the level of security awareness among your organisation and are tangible metrics for compliance and audit purposes.

In addition to these, there are qualitative methods of gathering opinions, perceptions, attitudes and behaviours to security awareness. These include:

- Focus groups
- Observation sessions

## Focus Groups

Focus groups allow an open discussion amongst a small representative of your audience. These encourage honest dialogues about employees' opinions, perceptions and attitudes towards security, their experiences to date (both personally and within your organisation), their concerns and also their ideas about communicating security messages. They are also useful in allowing you to explore and investigate particular issues so that you can find out more information.

Although they can be resource hungry, equally these groups are invaluable for gathering information from representative employee audiences and are a positive alternative for organisations where compliance is not the primary objective of an awareness programme.

## Observation sessions

Observation sessions provide the 'fly on the wall' measurement of behavioural change. Results from these sessions will provide detailed information on whether employees are demonstrating positive behavioural change as 'business as usual' with regards to their security responsibilities.