The Security Company International

INSPIRE. ENGAGE. PROTECT.

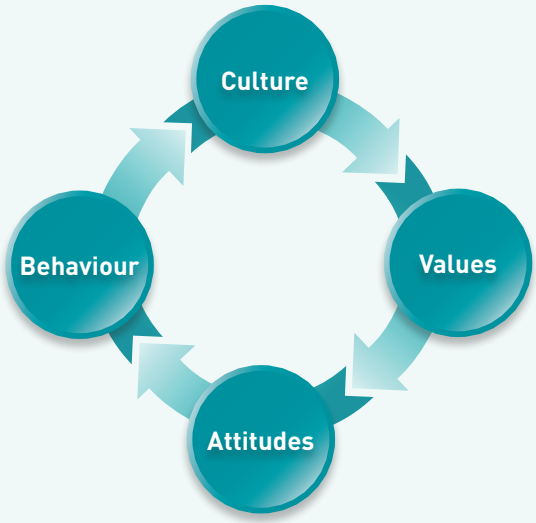
# Insight Programme

The Insight Programme assesses the company's security awareness culture and where the organisation scores in relation to other peer companies (where data is available).

The building blocks of culture are beliefs and values.

To change the security awareness culture there is an initial requirement to change the behaviours and attitudes of the people within the organisation.

To achieve this there must be understanding and acknowledgement of what their behaviours and attitudes are. Insight's methodology supports this by identifying the perception of security at the company, examples of best practice and any areas for improvement.




## The purpose

The Insight Programme provides:

- Evidence to create a business case and generate the backing of senior managers and directors to obtain budget and resource
- Intelligence of the security culture and a roadmap detailing how performance may be improved to achieve an agreed target for security awareness
- Inclusive thinking (at all levels throughout the organisation) to help lead open discussions on any issues and concerns raised
- A spotlight on any areas of high risk

## The structure

The Security Company assess the current state of security awareness performance by researching and asking key questions through a series of stakeholder interviews and focus groups. Key individuals are identified and interviewed to gather their expert opinion on the company's security stance.

Stakeholder interviews provide an opportunity to anonymously capture the opinions of the organisation's thought leaders. To focus on their security priorities and what's keeping them awake at night. This provides an objective overview of the opinions held which will be used to shape the security awareness strategy.

Focus groups are designed to encourage employees to think about security issues, share their views and opinions about the organisation. Discussions are focused on security priorities; what is working well and what is not; what security issues people really care about and what is going on behind the scenes. Anonymity is ensured so participants feel at ease that their ideas and opinions are shared in confidence.

The research provides a range of different Security Awareness Behaviour Indicators and will help to guide where enhancements should be made to deliver the maximum in behavioural change.

## Security Awareness Behavioural Indicators

| Existing behaviour | Password management | Classification | Clear desk clear screen |
|---|---|---|---|
| **Pre-contemplation – unaware of the need for change** | X | | |
| **Contemplation – thinking about changing but not yet acted** | | X | |
| **Preparation – making first steps towards a change** | | X | |
| **Action – taking regular action to change** | | | X |
| **Maintenance – getting results and feeling good about the change** | | | X |
| **Relapse – most people take about six attempts before they achieve long term change** | | X | |

This qualitative data focuses on the opinions, beliefs and attitudes of key members of the workforce and looks at the 'why' and 'how' of a situation.

The information can also be considered alongside the online Security Awareness Baseline Research (SABR) which is based on larger samples and provides statistical validity. Running in conjunction with the qualitative, or opinion based research, quantitative data is also collected as part of SABR.

## The report

The results of the assessment will map the security awareness 'landscape' – identifying areas of first-line risk and second-line concerns with recommendations for remedial activity.

The findings provide details about the thoughts, opinions, beliefs and views of security within the organisation. To provide a picture of what successful behavioural change would look like for the company and a roadmap to follow to increase security awareness performance.

It will help with:

- **Providing direction:** For the security awareness programme; ensuring an introduction to the right systems, processes and procedures to empower and reinforce a security-aware culture
- **Two-way dialogue:** Stakeholder engagement opens a dialogue with the business at all levels, from CEO to 'shop floor'. It empowers the security team to talk with authority to senior managers and deliver information in the way they require
- **Socialisation:** People who participate are more committed to implementing change, and any relevant information they have is integrated into the behavioural change plan
- **Landscape:** A picture to draw upon, to support security awareness planning and the creation of a strategy aligned to the company's business objectives
- **Evidence:** The gathered qualitative data provides evidence and support to take the security strategy forward
- **Building a business case:** Evidence to generate better understanding and the backing of senior managers and directors to obtain budget and resource

**"Culture is a shared set of beliefs, values and patterns of behaviour common to a group of people."**

Schermerhorn (1989)