The Security Awareness Survey

The Security Awareness Survey is designed to measure levels of awareness before, during and after your education programme. Use the results to prove changes in employee behaviour and demonstrate return on investment (ROI).

The benefits

The Security Awareness Survey will:

- Benchmark initial levels of awareness prior to and during your security education programme.
- Determine current employee perceptions, attitudes and opinions of security.
- Highlight security weaknesses that could put your organisation at risk.
- Identify security strengths that can enhance your organisation’s reputation.
- Support your business case for security awareness.
- Help direct your security awareness strategy.

The survey results will highlight any gaps in employee knowledge which could lead to insecure behaviour in the workplace. This, in turn, could put your organisation at risk. The data can be used to support your business case for funding security awareness initiatives. Benchmarking initial levels of awareness also assists with measuring any changes in behaviour that occur as a result of the programme.

The survey report will summarise the results, highlighting employees’ opinions about various areas of information security and how it is currently managed. This information is used to develop targeted security awareness campaigns that increase awareness of correct behaviours and address any gaps in knowledge.

The structure

The Security Awareness Survey is recommended for all types of education programme. It can be rolled out to the entire employee population or to a representative sample. Conducting the survey on an anonymous basis is often likely to elicit more honest responses.
The Security Awareness Survey focuses on common threats and uses a variety of question formats that require employees to indicate their opinions, behaviours and understanding.

A set of optional questions can be added to further enhance the survey data. These questions cover more specific topics, such as Mobile Workers, UK Government and Data Protection.

**The standard survey**

**The Security Awareness Survey is split into eight sections:**

**General Security Awareness:** This section asks your employees to rate their overall awareness of security including incident reporting.

**Your Information, Your Computer, Yourself and Your Workplace:** These sections ask your employees to agree or disagree with statements regarding their understanding of how to classify and handle sensitive information, device security (password, Internet and Email policy, mobile devices, etc.), travel security and workplace security ('clear desk clear screen' policy, ID cards, security incidents, etc.).

**Communication, training and development:** This section gathers information about employees' preferred communication channels and any training needs.

**Perceptions:** This section asks for employee opinions regarding current security practices within your organisation. This allows employees to express their thoughts about whether security is taken seriously and how information is currently managed. Perceptions are a good indicator of whether incorrect behaviour is due to lack of knowledge or cultural issues.

**Demographics:** You can determine how much demographic data you choose to collect. It is recommended that as a minimum the demographics associated with Role, Job Function and Business Unit are selected. This information can assist with targeting training and awareness activity.

**The survey report**

The survey data will be compiled and analysed in a comprehensive report that identifies:

- Gaps in knowledge of security responsibilities.
- Areas where employee understanding is good.
- Where employees currently go for advice and how they prefer to receive information.
- The recommended frequency of security communications and training and how this factor determines their effectiveness.
- Areas of concern regarding secure behaviour in the workplace.
- Where security is well-managed according to employees.