Service Definition
Staff Security Awareness Training

Intertek NTA's Information Security Awareness training package consists of the following components as standard. Modules are flexible depending on your organisational policy, and the desired outcome of the exercise.

Due Diligence:

- Pre-Delivery Call**:** The trainer will undertake a telephone call with the customer to get a feel for organisational policy, and the desired outcome of the training programme. It is paramount to NTA that the content of the training course marries up with organisational goals and does not conflict with exiting procedures or negatively affect office culture. Questions will be asked around existing information security policies (passwords, clear desk etc.), attack scenarios and who an incident should be reported to. This call usually takes about an hour but can take longer depending on customer requirements.

- Confirmation of Content**:** The trainer will then offer an overview of the course to the customer before it is delivered to attending staff. This can either be a remote session, or onsite shortly before the course is due to begin. This is to ensure that content is aligned with organisational goals.

The Training Course:

- Format**:** The course will be delivered in the form of a presentation in front of attending staff, rather than web or portal based. Slides will be used as collateral to support the trainer's topic of discussion. The session is designed to be interactive, and audience participation will be encouraged.

- Introduction**:** This will be a brief overview of what information security means, and its importance to those in attendance. This can be tailored to highlight the key areas that are of particular importance to your organisation i.e. protecting company assets, or ensuring customer data is stored securely. This section will also briefly provide recent statistics and stories as a way of highlighting the importance of staying secure, and the role played by your employees.

- Modules**:** These core modules contain the essentials for your employees to know in order to equip them with the necessary knowledge to help defend against information security breaches and change behaviours. For example, passwords, phishing, acceptable use of the internet and clear desk policy.

- Conclusion**:** This part of the session will draw upon the key areas highlighted in the training, tailored to meet your organisational requirements. It will also provide further reading for all attendees with links to both internal policies and procedures as well as links to external sites that will provide additional security tips.

Please note that the provision of electronic or hard copies of the presentation slides is not included within the service.

Course Format

The trainer will begin the session by introducing themselves and NTA as a company. Attendees will then be given an overview of what will be covered in the session.

What is Information Security?

The introduction will focus on educating attendees on information security; both its definition and its application in the world today. This section won't contain any complicated technical information - it will be a basic overview to help attendees understand the concepts behind the terminology.

Why is Information Security Important?

This section will aim to answer the question that many attendees on training courses have – "Why do I need to know this?". The trainer will focus on answering this question by stressing the importance of the role that employees play in maintaining a good security posture. This section will also include recent stories and statistics to highlight the reality of the issue, and how critical it is that all staff are aware of the risks faced by the organisation.

Passwords

This module will cover the basics on passwords - such as how passwords can be cracked, how often passwords should be changed, password storage and creating a strong password. Examples of bad passwords will be shown from real data dumps taken from hacked websites to highlight the seriousness of the problem.

This element can be tailored to your organisation's internal policies as necessary i.e. password length, how often they need to be changed etc.

Social Engineering

This module will detail the mechanics behind Social Engineering and the most common techniques used by Social Engineers. Social Engineering, such as phishing or an attempt to gain physical access to the office building, is a real world problem that can only be prevented by the correct response of individuals and thus is one of the most important aspects of staff security awareness.

Topics covered will be all forms of Social Engineering, including phishing via emails and phone calls, to tailgating. There will be real word examples of phishing, information on how to spot potential phishing attempts, what is meant by tailgating and also how to prevent it. This can be tailored to organisational policy, i.e. who to flag phishing emails to or who to notify should an unknown person be found in the office building.

This module works particularly well based on the results of an actual Social Engineering exercise, carried out by a third party such as NTA. Real world data and examples can be used to show attending staff that not only do these attacks happen, but that they already have.

Internet & Email Usage

This module will cover the acceptable use of internet and company email – including what personal use is accepted, safe browsing (i.e. being able to identify a compromised site) and how to keep personal and work life separate.

Social Media

This module will focus on the risks of using corporate social media, especially if employees have associated themselves with your organisation. There will be focus on what employees should/shouldn't say about your organisation on social media (and why), prevalent malware and the risks involved in making posts available to the public using real life spear phishing examples.

Removable Media

This module will focus on your organisational policy on removable media. It will cover the types of removable media that are permitted, the risks involved in using such devices, including recommendations on scanning for viruses and using only known media.

Altering Software

This module will cover recommendations for installing or modifying software on corporate devices. It will include procedures for requesting additional software to be installed, guidance on what file types are not permitted for download and the procedures for ensuring anti-virus is not tampered with, as well as recognising spoof download requests from malware.

Remote Working

This module will focus on remote working and will incorporate any organisational procedures covering this area. It will focus on the risks involved in working away from the office, including loss of corporate data and the vulnerabilities associated with public Wi-Fi.

Clear Desk Policy

This module will cover all aspects of a clear desk policy such as ensuring that all documents are lifted from printers and ensuring PCs are kept locked when unattended. This will reflect your organisation's clear desk policy and ensure that attendees are made aware of their obligations. An example image of an "unclear desk" is used in this section for comparison.

Incidents

The final module acts as a summary of what to do in the event of an actual information security breach – what procedures to follow and who to contact. Such information is paramount in staff security awareness, and attending staff should leave the session with a heightened awareness of the risks, things to look out for, what to do and what not to do, and who to report to should a breach be discovered.

Summary/Conclusion

The conclusion will be an overview of what has been covered within the session; it will summarise all the modules in brief with the most important points being drawn out and reinforced.