Information Security

Proposed Training on Information Security

30 April 2015

Introduction

Information security is everyone's responsibility and it is SCRA's duty to ensure that all their employees and contractors are aware of and fulfil their information security responsibilities.

SCRA does not have any specific information security training in place that satisfies SCRA's Information Security Policy Statement[1] that Information Security training will be available to all staff. Normally this training requirement is included within SCRA's staff induction training. Although both the Data Protection training and the eLearning course on Information Governance has some information security content there is no substitute to focused training to alert staff of the importance of security within the workplace.

This paper provides an understanding of the type of risks that SCRA is exposed to and proposes an information security training course to mitigate this risk.

Information Risk

Information security is all about minimising risk and SCRA's biggest risk to safeguarding their information is their staff.

The following examples are an illustration of some of the risks that SCRA is exposed to though their staff:

Threat	Staff Involvement	Potential Impact
Data Misclassification	Staff using OFFICIAL-SENSITIVE to mark all emails whether there are sensitive or not.	Causes confusion and can result in staff ignoring the protective marking increasing the risk of a data breach.
Unauthorised disclosure of case information	Staff not complying with SCRA's information security policies and practices as they unfamiliar with what they are.	Could cause a multiple data breach exposing SCRA to a fine from the ICO and/or considerable reputational loss.
Data loss through a cyber-attack	Clicking on a link or opening an attachment in a phishing email releasing malware into the SCOTS environment.	Major disruption to SCOTS/SCRA services (Malware can encrypt shared drives) Reputational damage and/or ICO fine
Unauthorised System access	Writing passwords down and not locking them away or using easy to guess passwords.	Another employee could release malware using their account causing major disruption and data loss to SCOTS/SCRA services. Reputational damage, ICO fine.
Unauthorised Service use	Staff downloading big files from the internet for personal use during core hours.	Reduction of SCOTS network performance causing slow system response resulting in lower productivity.

---

[1] As stated in the Information Security Handbook Version 3.1.

Proposal

To develop an information security PowerPoint presentation to strengthen staff information security knowledge and awareness of SCRA's information security policies as defined within the Information Security Handbook Version 3.1. The proposed course structure is :

1. Information Security Basics :- data confidentiality, integrity availability, information assets, types of threats, vulnerability, 'need to know' principle etc.;
2. Legislation & Government Security : SPF, SCOTS IT Code of Conduct, DPA, Computer Misuse Act etc.
3. Control Areas and Controls :- Governance, Physical, Personal, System, Network, etc.; administrative, technical and physical controls
4. SCRA information security organisational structure: Information Governance, information security roles SIRO, IAO, ISTAO, Accreditor etc.;
5. SCRA Policies - Data Classification, Data handling, Clear Desk/ clear screens locked print, mobile devices, email and internet usage, personal use password, USB sticks etc.;
6. Combatting against Cyber Attacks; Recognising a phishing email (demo), ransomware etc.;
7. Misuse, Monitoring, Forensics and Disciplinary procedures;
8. Business Continuity / Incident management.

There will be a need to prioritise some topics so that the presentation is not too long (about 75 minutes) while ensuring ample time is spent on specific areas where staff's understanding is vital. The presentation will be supplemented by pre-prepared exercises and a short quiz to aid understanding. The presentation and any additional course material will be provided to all trainees as printouts.

The approach to delivering the information security training to staff would need to be agreed once the course has been developed.

eLearning

As SCRA can develop their own eLearning courses it may be possible to create modules on some of the subject areas above allowing the training course to focus on raising staff awareness in specific areas where we have the biggest risks.