Cyber Security Awareness Training

Service Fact Sheet

Version: 1.2 **Date:** 12 June 2018

1. Introduction

This document details what the Ignite Systems cyber security awareness training will provide for an organisation. It outlines the purpose, what the deliverables are, expected outcomes, an overview of the content, and the costs.

2. Purpose

Cyber security awareness training is a formal process for educating staff about the importance of cyber security. To provide them with effective strategies, techniques and resources needed to stay safe online, so as to increase the resiliency of the organisation and also to improve their personal levels of cyber security.

3. Deliverables

The following deliverables will be provided as part of the training.

- ✓ A 1 hour face to face interactive training session on cyber security.
- ✓ Handout information comprising summary notes of the material covered in the course – provided in hard copy and PDF format.
- ✓ Ongoing access to an online resource page containing a wide range of cyber security related reference material, including:
  - copies of articles referenced in the training session.
  - links to online articles referenced in the training.
  - links to a wide range of online cyber security reference sites.
  - additional information that will be added from time to time – articles, case studies, reference material.

4. Outcomes

A person attending the training can be expected to achieve a level of understanding about cyber security in the following areas.

4.1. What is cybersecurity?

Participants will be able to explain what cyber security is and what it is intended to achieve.

4.2. The impact of cybercrime

Participants will recognise cybercrime as a real and present danger that could seriously damage their organisation, and impact their personal life.

4.3. The important role of employees

Participants will have an understanding of the importance of their role in cyber security and be able to identify how they contribute to cyber security.

4.4. Awareness about the main types of cybercrime

Participants will be able to explain in broad terms how the main types of cybercrime are carried out e.g. ransomware, phishing, identity theft, Business Email Compromise scams.

Participants will be able to explain and provide examples of how social engineering is employed in cybercrime.

4.5. Competency in preventing cybercrime

Participants can be expected to:

- Be alert to the use of social engineering and be able to recognise when it is being employed.
- Know how to identify email that is a potential risk and know how to respond to this type of email.
- Know not to open suspicious links or attachments in email – even if they know the source.
- Be alert to the potential risks of publishing and sharing certain types of information on social media.
- Know what constitutes good password practices.
- Be aware of options for securely sending Personal Information externally.
- Know to raise concerns regarding suspicious activities or events that may relate to cybercrime.

5. Content

The material to be covered in the training session is outlined below. The session will allow and encourage proactive participation, so the time and level of detail in each area will be to some extent dictated by this involvement.

5.1. The importance of cyber security

Set the scene by presenting an overview of how cyber security is being viewed by government institutions and professional bodies. This will be underlined with recent comments and advice from prominent and influential Australian people.

5.2. What is cybercrime?

An explanation about what cybercrime is, how it is carried out, and its scale and sophistication.

5.3. The impact of cybercrime

Some facts and figures about the impact of cybercrime, globally, in Australia, and its impact on businesses.

5.4. Cybercrime in action

Use of case studies to explain how the main types of cybercrime are carried out e.g. ransomware, phishing, identity theft, scams, hacking.

5.5. Cyber security and you

An explanation about why cyber security is more than the traditional focus on security services and systems. Information about the role that individuals can play in cyber security, and its relevance beyond the organisation – personal life, including family and friends.

5.6. How to avoid becoming a victim

Details of specific actions that people can take to play their part in cyber security.

5.7. Questions and Answers

An open forum to address any cyber security related questions.