TCG: **Telecommunications systems security**

Online course specification

Target audience:
This online course is aimed at those who have a role to play in reducing the vulnerability of telecommunication systems and databases to security breaches and fraudulent misuse.

Course aim:
To provide an overview of the protection of personal data held by telecommunications providers against misuse and the protection of telecoms systems against intrusion and fraudulent misuse.

Course level: Intermediate
An explanation of PTT course levels is given at the end of this document

Pre-requisites:
An appreciation of the services offered by telecommunications operators and the structure of the networks that provide such services. It is recommended that the PTT online courses TCA: "Telephony and data services" is studied before attempting this security course.

Course structure:
The course consists of the following five modules:

1. Protecting personal data
2. Digital security
3. Protecting databases
4. Internet security
5. Protecting telecoms services

Module 1: Protecting personal data

Module aim: To explain the need to protect information gathered about customers and employees and describe the role and relevance of risk analysis and a security policy.

After completing this module, a trainee will be able to:

- explain the terms confidentiality, privacy, integrity, and availability as applied to the protection of customer data and telecommunications service provision.
- describe the types of information gathered by telecoms service providers and why such data should be kept secure.
- describe the various types of electronic and social engineering attack on the confidentially of personal data.
- describe the motives of attackers and the potential effects of security breaches.
- explain the security aspects of recruitment and employment termination.
- describe the role and scope of data protection legislation in Europe.
- explain the role of risk analysis, security policies, security audits and security certification.

Module 2: Digital security

Module aim: Describe the methods of protecting digitally stored and transmitted information against unauthorised access and explain the factors that have increased the risk of intrusion in modern networks.

After completing this module, a trainee will be able to:

- describe the role and applications of symmetric and asymmetric encryption in the protection of stored and transmitted data.
- describe the role and applications of Authentication, Authorisation and Accounting in telecoms systems.
- describe how a man-in-the-middle attack can be used to gain unauthorised access to communications and describe ways of mitigating the risk of such an attack.
- explain the increased security risk in a competitive, converged and software driven telecoms environment.
- explain the factors that influence the trustworthiness of a network and the need for protection at the boundaries of a trusted network.

Module 3: Protecting databases

Module aim: To describe the threats to the security of information stored in databases and explain methods of ensuring the confidentially, integrity and availability of data.

After completing this module, a trainee will be able to:

- explain the importance of the management of access to confidential information and telecoms control systems.
- explain the role of audit trails as part of the management of access to data.
- explain methods of minimising unauthorised access to online databases including the use of strong passwords, two factor authentication, hashing, and prevention of SQL injection.
- describe how cross site scripting and a man-in-the-browser attack can compromise the security of an online communication.
- describe the role of the various databases employed in telecommunications systems.
- explain the importance of managing the disposal of equipment to prevent unauthorised access to data.
- describe methods of ensuring the availability and integrity of stored data.

Module 4: Internet security

Module aim: Describe the vulnerabilities of networks attached to the Internet and explain methods of protecting those networks and the services they provide from intrusion and data theft.

After completing this module, a trainee will be able to:

- describe the ways in which malware can affect confidentiality and availability and compare the ways in which the various forms of malware are spread from computer to computer.
- describe the various methods of avoiding the infiltration of malware into computer networks.
- describe the various ways apart from malware, that a hacker can employ to gain access to confidential information stored on or communicated over a network.
- describe methods of protecting networks against intrusion by hackers.
- describe the role of a security operation centre with reference to intrusion detection and transaction monitoring.
- describe the purpose of a denial of service attack and explain how such an attack is delivered.
- explain the various ways in which the disruption caused by a denial of service attack can be minimised.

Module 5: Protecting telecoms services

Module aim: To explain the obligations and commercial need of telecoms operators to protect their networks and services from possible threats and describe measures that can be taken to improve resilience and protect revenues against fraud.

After completing this module, a trainee will be able to:

- describe the role of the various governmental and industry organisations who have an interest in ensuring the security of telecommunications networks and services.
- explain the obligations of telecoms service providers to ensure their networks are resilient to physical and electronic threats.
- give examples of threats that can adversely affect the availability of telecommunications services.
- explain the obligations of service providers to co-operate with government agencies at times of emergency.
- give examples of network assets that require special protection and describe the electronic and physical measures that should be taken to protect those assets.
- describe the use of route, equipment and power diversity to improve the resilience of networks.

Course access requirements:
To access the course, a computer running a browser such as Google Chrome, Safari etc is required. The computer should have Internet access. A screen resolution of at least 1024x768 is necessary.

Learning facilities:
This online course employs interactive simulations, hypertext links to an online glossary and multiple-choice question sessions to fully involve the trainee in the learning experience. Each module provides revision links to previously studied, relevant topics. A record of progress and level of achievement is recorded for each trainee. Once studied as a structured, assessed course, the content can be browsed for revision or reference.

PTT course levels:
PTT online courses are categorised by one of three levels according to the depth of treatment they provide:

1. **Introductory:**

   PTT Introductory courses are designed for those with no previous experience or knowledge of telecommunications. These courses provide an overview of telecommunications or discuss the fundamentals of electronic communications. The study of general science at secondary (high) school is a typical pre-requisite for PTT Introductory courses.
   PTT Introductory courses are suitable for those joining the telecommunications sector particularly those in an apprenticeship programme.

2. **Intermediate:**

   PTT Intermediate courses are designed for technicians and engineers requiring an understanding of a certain aspect of telecommunications. Those planning to study an Intermediate course should have an understanding of the basic principles of electronic communications.
   The depth of treatment provided by Intermediate courses is typically equivalent to level 3 of a UK national vocational qualification (NVQ). PTT Intermediate courses can be used to support the attainment of a Communications Technology NVQ at level 3.

3. **Advanced:**

   PTT Advanced courses are designed for those who require an in-depth treatment of a certain aspect of telecommunications. Such courses are suitable for system designers as well as those who will be responsible for the maintenance of the system described in the course.
   Those planning to study a PTT Advanced course should have a background in telecommunications, and an understanding of telecommunications fundamentals and the principles of the type of telecommunications system described in the course.

PTT