Making IT good for society

BCS Level 4 Certificate in Cyber Security Introduction QAN 603/0830/8

Sample Paper A

Record your surname / last / family name and initials on the answer sheet.

Sample paper only 40 multiple-choice questions – 1 mark awarded to each question. Mark only one answer to each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either **A. B. C. or D**. Your answers should be clearly indicated on the answer sheet.

Pass mark is 26/40.

This qualification is regulated by Ofqual (in England).

1 Which of the following actions **BEST** describes a directive control?

A It instructs a user to do something in a particular way.
B It stops a user from doing the wrong thing.
C It identifies if a user has done something wrong.
D It corrects the erroneous input from a user.

2 Which of the following is a DNS technique used by botnets to hide phishing and malware delivery sites behind proxies?

A Fast flux.
B IP spoofing.
C Distributed denial of service.
D Logic time bomb.

3 Which of the following are required for a ransomware attack to be successful?

a) Sending an e-mail that looks genuine with an attachment to a user.
b) Luring a user to click a link and download a file.
c) Exploiting a poorly configured firewall.
d) Disrupting power supply of the server backups.

A a and b only.
B c and d only.
C a, b, c and d.
D b, c and d only.

4 What does CIA represent in relation to cyber security?

A Confidentiality, identity, availability.
B Confidentiality, integrity, availability.
C Confidentiality, integrity, accessibility.
D Criminality, integrity, availability.

5 How does SSL v3.0 provide better security against network interception than SSL v2.0?

A The derivation of session keys in SSL v3.0 takes place before the short window of verification stage.
B A man-in-the-middle adversary can influence the cryptographic suite in SSL v2.0.
C SSL v2.0 uses the negotiated authentication key to verify the contents of all messages sent.
D An attacker can only access the SSL 3.0 session authentication key during the verification stage.

6 During a recent security audit of a financial institution's networked printers, auditors found that separation of duties is particularly acute for check-printing printers. This is an example of which type of control?

A Detective control.
B Networked control.
C Financial control.
D Preventive control.

7 The following activities are parts of the attack chain principle. In which order do they **NORMALLY** happen?

a) Weaponsiation.
b) Actions on objective.
c) Delivery.
d) Reconnaissance.

A c, d, b, a.
B d, a, c, b.
C d, b, a, c.
D c, d, a, b.

8 Which of the following scenarios may result in a Cross-Site Request Forgery to occur?

A When HTTPS is used without a dedicated IP address, and therefore the SSL certificate contains a shared IP address.
B When a POST parameter performs an operation on behalf of a user without validation.
C When insecure direct object reference is made to those restricted resources that are to be requested.
D When firewalls are not properly configured or their default settings are not changed.

9 What sort of control is anti-virus software?

A Procedural.
B Perceptive.
C Protective.
D Primitive.

10 Which of the following are likely to be security implications of accidentally leaving ports open on a server?

A Increasing the attack surface.
B Providing a backdoor to a protected system.
C Need of deploying extra physical security solutions.
D Additional security awareness training for the staff.

11 What is horizon scanning?

A Looking at developments in technology to try and identify future trends or issues.
B Identifying known threats appearing on the boundaries of a company's network.
C Determining what new inventions in technology your competitors are bringing to market.
D Scanning for vulnerabilities in the software that has been installed on the company's networks.

12 Which of the following is a technical control?

A CCTV.
B An acceptable use policy.
C Locks on server room doors.
D User logon password requirements.

13 Which device is designed **PRIMARILY** to direct traffic on a network to a designated IP address?

A Hub.
B Firewall.
C Router.
D Scanner.

14 Which of the following **SHOULD** be considered when choosing where to locate physical IT resources?

a) Risk of a flood.
b) Risk of physical theft.
c) Risk of a power outage.
d) To avoid accidental data deletion.

A a, b and c only.
B a and d only.
C b, c and d only.
D a, b, c and d.

15 Which of the following is **TYPICALLY** a feature of a thick client?

A Uses a server for the main processing activity.
B Does the bulk of the processing activity rather than the server.
C Its designed for use by very inexperienced people.
D Uses web-based software through the terminals.

16 Which of the following may need to be reviewed when the threats landscape changes?

a) Security objectives.
b) Security requirements.
c) Security budget.
d) Security policy.

A b, c and d only.
B a, b and c only.
C a, c and d only.
D a, b and d only.

17 Which of the following is **LEAST LIKELY** to be an information security risk introduced by a Bring Your Own Device (BYOD) programme?

A BYOD devices could provide unauthorised access to office systems through their inter-connectivity.
B BYOD devices could be used to spread malware to office systems by transferring viruses through their connections to office networks.
C BYOD devices could provide accurate details of the user's location, thereby facilitating directed attacks on staff members.
D BYOD devices could have a serious effect on the volume of network traffic on an office system to which they are connected.

18 What **SHOULD** be the **MAIN** focus of information security practices in any organisation?

A Implementing security controls.
B Aligning with the business objectives.
C Remaining cost effective.
D Deploying long term solutions.

19 Which of the following security assurance models could **NOT** be evaluated by existing security evaluation criteria?

A Intrinsic assurance.
B Extrinsic assurance.
C Implementation assurance.
D Operational assurance.

20 What are the Common Criteria?

A An international standard for ICT product security certification.
B A way of checking if the most important security controls are in place.
C The easiest security controls to implement in an ICT system.
D Standard clauses expected to be seen in an outsourcing contract.

21 When are service providers required by UK law to notify the Information Commissioner's Office (ICO)?

A If a company's chief information officer is replaced.
B If a breach of personal data occurs.
C If a customer’s information is kept for more than 90 calendar days.
D If a customer's bank details are not received within 24 hours of a sale.

22 Which of the following are impacts of a cyber attack on a business?

a) Financial losses.
b) Reputational damages.
c) Use of office supplies.
d) Legal consequences.

A a and d only
B a, b and c only.
C a, b and d only.
D b and d only.

23 What do we call those parts of the World Wide Web whose contents are **NOT** indexed by standard search engines for any reason?

A Surface web.
B Darknets.
C Tor network.
D Unallocated spaces / clusters.

24 Which of the following is a commonly used tool for the analysis of risk severity and evaluations of the possible solutions?

A Certified Risk Analyst.
B Mind map.
C Capability Maturity Model.
D Risk register.

25 Fill in the blank:

The _____ is established during a Business Impact Analysis (BIA), by the owner of a process.

A Functional objective.
B Security objective.
C Recovery time objective.
D Security design objective.

26 Which of the following are part of Information Assurance?

a) Confidentiality.
b) Integrity.
c) Availability.
d) Non-repudiation.

A a, b, c and d.
B a, b and c only.
C b and d only.
D c only.

27 Poor system configuration issues can be identified by evaluating the system, using which of the following?

A Privacy enhancing techniques.
B Horizon scanning.
C Business impact analysis.
D Penetration testing.

28 What is it called when third-party streams of indicators are used to improve an organisation's threat awareness and response?

A Threat intelligence feeds.
B Security awareness training.
C SWOT analysis.
D Business Intelligence.

29 Fill in the blank:

Security **SHOULD** first be considered at the _____ phase.

A Requirements.
B Development.
C Testing.
D Maintenance.

30 Security requirements for a new product or system are **GENERALLY** driven from which of the following?

A Security solutions.
B Security objectives.
C Security functions.
D Security guidelines.

31 Which of the following is the **MOST** secure authentication protocol used for securing a WiFi connection?

A Extensible Authentication Protocol (EAP).
B Internet Protocol Security (IPSec).
C Challenge-Handshake Authentication Protocol (CHAP).
D WiFi Protected Access (WPA) protocol.

32 Fill in the blank:

_____ is a network topology where every node is connected to a central hub. The switch is called 'server' and the peripherals are called 'clients'.

A Client-server.
B Star.
C Peer-to-peer.
D Ad-hoc.

33 Which of the following is **MOST** frequently considered to be the weakest link within an organisation's cyber security?

A People.
B Third-party software.
C Insecure network connections.
D IT admin procedures.

34 Which of the following is a significant factor in the development of new attack techniques?

a) The rapid changes in technology.
b) The failure to patch old systems.
c) The increasing number of internet-enabled devices.
d) The failure of users to create complex passwords.

A a and c only.
B b and d only.
C a, b and d only.
D a, b, c and d.

35 Why is endpoint protection strategy **GENERALLY** considered as the **MOST** effective approach to contain malware attack chains?

A The endpoint protection strategy covers protection from insider threats and therefore offer a more comprehensive solution.
B Endpoint security products provide cheaper enterprise security solutions with minimal maintenance requirements.
C Businesses have no control over the development and spread of malware. Their best defence is to improve the security of their assets.
D This is often required by insurance companies to comply with the third-party protection requirements to cover losses from botnet attacks.

36 Fill in the blank with the **MOST LIKEY** answer.

If a company fails to deliver an agreed service to its customers, then it may be a breach of _____.

A Cyber law.
B Criminal law.
C Civil law.
D Contract law.

37 Fill in the blank:

Companies **SHOULD** be ready to meet General Data Protection Regulation (GDPR) compliance requirements by _____.

A 25th May 2018.
B 29th March 2019.
C 1st January 2019.
D 31st December 2018.

38 Fill in the blank:

Membership of a cyber security professional body (e.g. ISACA) requires you to adhere to their _____.

A Prescribed cryptographic tools for emails exchange.
B Code of professional ethics.
C Choice of cyber security tools.
D Approved suppliers of managed services.

39 Which of the following are **GENERALLY** considered to be reliable source of research outcomes and industry practice?

a) Peer reviewed journals.
b) Conference proceedings.
c) Professional body whitepapers.
d) Online chatting forums.

A a, b and c only.
B a, b, c and d.
C b, c and d only.
D a and d only.

40 Fill in the blank:

A technique used by risk managers for forecasting future events, such as accidental and business losses, is called _____.

A Competitor analysis.
B Risk analysis.
C Trend analysis.
D Cost benefit analysis.

-End of Paper-