Making IT good for society

BCS Level 4 Certificate in Cyber Security Introduction
Answer Key and Rationale QAN 603/0830/8

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**A**	Ransomware requires a system to be infected through a crypto virology attack. This is usually delivered through an attachment to an email. If the delivery email looks genuine, then clicking on the attachment to open it encrypts the victim's files. An attacker can also exploit poorly configured firewall to launch a ransomware attack. Disrupting power supply will affect the server backups but will not facilitate a ransomware attack.	6.1
2	**B**	CIA is a widely-applicable security model standing for Confidentiality, Integrity and Availability. This principle is applicable across the whole subject of Security. If any one of the three are breached it will have serious consequences.	2.1
3	**C**	Anti-virus software is a protective control. Procedural controls are things like policies. Deterrence is something that discourages wrong doing.	7.1
4	**C**	A router is designed to look at the address in a data packet and send it on to the appropriate part of a network to reach that address. A firewall is designed to limit the traffic coming into an organisation's IT systems and to protect from attackers. A DMZ is a zone designed to add an additional layer of security to an organization's local area network by "hiding" the internal network from the Internet or another network. A hub is a link between different networks or individual computers.	5.1
5	**B**	If all software is installed on the terminal, it is a thick client and this will require significant processing power in the terminal. Thin client is a terminal connected to a server network, where the device itself has very limited/ no processing power, nor software installed. There is no link to the ability of the users. The use of web-based software is called smart client and although there may not be much processing power in the terminal, it must have some.	5.2

Question	Answer	Explanation / Rationale	Syllabus Sections
6	**A**	Security objectives remain the same when the threats landscape is changed. However, the security requirements are directly related to the threats paradigm. There could be changes in the budgetary requirements to meet the new security requirements and also some changes in the security policy to reflect the changes.	4.1
7	**C**	A cyber-attack may impact a business in a number of ways including financial and social (reputational) losses and legal actions brought by the affecters. However, there will be no considerable difference in the use of office supplies.	1.3
8	**C**	Trend analysis is based on the idea that what has happened in the past gives an idea of what will happen in the future. Therefore, a risk manager can use trend analysis to predict the future events based on past data.	10.2
9	**B**	Darknets cannot be accessed through standard web browsers. Whereas a surface web is visible and is indexed by typical search engines (such as Google or Bing). Tor is a privacy-aware software to ensure anonymous communications. Unallocated space or clusters is the hard disk storage space that is not assigned to any drive.	2.4
10	**A**	Intrinsic assurance is the security quality and rigour provided by the developer of the system. It does not cover independent security evaluation and testing (such as in the Extrinsic assurance) and therefore it could not be evaluated by existing security evaluation criteria such as Common Criteria. Parameters of implementation and operational assurances can be evaluated by external auditors.	3.2
11	**A**	Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments. Common Criteria is more formally called 'Common Criteria for Information Technology Security Evaluation'.	8.3

Question	Answer	Explanation / Rationale	Syllabus Sections
12	**A**	Fast flux introduces numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records. Whereas in IP spoofing, a cracker masquerades as a trusted host to conceal his identity, spoof a Web site. In a DDoS attack, multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack.	6.1
13	**D**	Contract law consists of a large body of rules and guidelines that address contract formation and enforcement. When a party (a company in this question) fails to deliver the agreed service to the other party (customers in this question) than the most relevant legislation is the contract law.	8.2
14	**B**	Attack chain involves 7 activities in this order: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & control, Actions on objective.	7.1
15	**B**	Business should drive security controls so as to ensure alignment of security objectives with the business objectives. Costs and review needs depend on the business needs.	4.2
16	**A**	Reliability of a publication is measured through the quality of evaluation process used by the publisher. Conference proceedings, journals and whitepapers are peer-reviewed by the experts of their respective fields who evaluate the quality of the work presented in the manuscript. Whereas, open and unmoderated avenues such as online chat forums have no control over the quality of the contents being shared over there.	9.2
17	**D**	The amount of data transferred is likely to be small from smart phones and similar devices. However, the other options are realistic risks that organisations allowing staff to utilise BYOD need to consider very carefully.	10.1
18	**B**	This is a legal requirement for the companies operating in the UK to inform the ICO of any breach of personal data. They must also notify customers if the breach is likely to adversely affect customers' privacy, and keep a breach log.	1.2

Question	Answer	Explanation / Rationale	Syllabus Sections
19	**D**	Security vulnerabilities are usually introduced through poor configuration or inadequate patching policies or processes. Penetration testing is the process to identify these security vulnerabilities with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack.	3.4
20	**A**	Horizon scanning is a process which uses the idea of looking as far ahead as possible to look for trends, developments, research and related areas to help predict what threats we might face in the future. The OECD definition of horizon scanning is "a technique for detecting early signs of potentially important developments through a systematic examination of potential threats and opportunities, with emphasis on new technology and its effects on the issue at hand." http://www.oecd.org/site/schoolingfortomorrowknowledgebase/futuresthinking/overviewofmethodologies.htm	9.1