Practice Questions

Fundamental Concepts of Data Security

Contents

1 Security Systems

Question 1

Two of the key areas in security are data classification and security education. With the help of examples, explain why these particular areas are critical for security and describe at least two problems, for each area, that may arise if the security setup does not take them into account.

Question 2

Explain why continuous management of security is a critical issue and describe two aspects of the continuous management process.

Question 3

Explain why the current distributed nature of today's system poses new security challenges.

Question 4

Most organizations are putting a lot of effort into having an Internet presence as it offers the potential to reach a very large number of potential customers with minimal cost. Describe in detail at least two major drawbacks of having an Internet presence.

Question 5

The introduction of mobile devices such as iPhones and Android tablets has changed the way in which organizations deal with security. Explain two ways in which such mobile devices compound the problem of keeping a system secure.

Question 6

Explain with the help of an example why old equipment can pose a major security problem for an organization.

Question 7

A large number of software developers have introduced a patching system which is no longer under the control of the user (e.g. the patching system via STEAM). Explain the advantages and disadvantages of this approach from the point of view of system security.

Question 8

Consider the statement *"The availability of information has made system security a much more difficult task than in the past."* Argue for and against the statement.

Question 9

Decide whether the statement *"A software and hardware based security system solution will provide all the protection necessary for an organization's assets and day to day operations"* is true or false and explain your reasoning.

Question 10

What is the problem with an approach in which an organization is focused only on the business end and considers that information technology is solely the domain of the computer operators and system administrators?

Question 11

What is the management typically responsible for when developing a security system apart from providing the required resources?

Question 12

Explain why it is important that development of a security system is done in a top-down manner rather than bottom-up.

Question 13

Defining the ownership of information is a fundamental step in security planning. What are the responsibilities of a data owner?

Question 14

The integrity principle in the context of cyber security deal with the correctness of the data and the aim is to prevent damage from personnel inside or outside the organization. What is the first measure that needs to be put in place to help with the data integrity protection?

Question 15

Availability is most commonly compromised by either natural occurrences or denial attacks. Describe at least two issues each of physical, technical and administrative controls that one needs to to consider for a security system.

Question 16

In commercial organizations the concept of data integrity is further refined to provide more detailed definitions which are cover the aspects information and data integrity as well as origin or source integrity. Explain with the help of example difference between the three aspects of integrity.

Question 17

In the context of cyber security, define the following with the help of examples the terms: threat, risk and vulnerability.

Question 18

Three key concepts in cyber security are: identity, authentication, and authorization. With the help of examples, explain the concepts of identity, authentication, and authorization.

Question 19

Auditing is used for multiple purposes in a security system. Describe three major security issues addressed by the use of auditing.

Question 20

The CIA (or AIC) triad is a basis to develop a security system but one of the biggest challenges is provide a detailed enough coverage of the issues and threats that need to be addressed as part of the security solution. Describe two common concepts to security that are used to address with errors or omissions in the development stage and implementation stage of security system.

Question 21

Explain whether or not third parties be part of an organization's trust domains.

Question 22

Explain why it is very bad practice to follow a vendor's approach to secure a system.

Question 23

The integrity of the data needs to be safeguarded as best as possible and any reasonable security plan will ensure that the access to information is granted on a strictly need to know basis. However, this constraint alone is not sufficient to ensure the data integrity. Explain with the help of examples, two ways in which the data integrity can be further protected.

Question 24

Explain the concept of data integrity.

Question 25

USB portable storage devices have ever increasing capacities which significantly increases the availability of information. However, the storage devices are also posing significant challenges from a cyber security point of view with a common challenge being the fact that increasing amounts of data can be copied over to non-authorised portable devices. Describe two other major challenges posed by portable devices.

Question 26

Specify which of the AIC principles pose the most significant challenge if a cloud model is to be used by an organization? Explain your answer.

Question 27

Explain what a security model is.

Question 28

Explain the difference between a security model and security policy.

Question 29

Describe a security model designed to provide confidentiality protection.

Question 30

Describe a security model designed to provide integrity protection.

Question 31

Compare and contrast the Bell-LaPadula and Biba security models. Your answer should provide a description of each model, its aims and the differences and similarities between the models.

Question 32

Specify the three fundamental rules used by the Bell-LaPadula model to implement access control.

Question 33

Explain the concept of a state machine model in the context of cyber security.

Question 34

State machine models are used to develop operating systems and this means that specific restrictions are enforced in terms of processing and access to resources. However, often, the operating system or an application freezes completely. Why does the system freeze and can the frozen system be considered as a failure of the OS/application in a secure state? Explain your reasoning.

Question 35

Explain how the Bell-LaPadula model determines if a particular subject can access a requested object.

Question 36

With the help of an example, explain how the Bell-LaPadula model prevents confidential information from being revealed either by intent or by accident.

Question 37

Consider the case in which you have been hired as a security expert by a large accounting corporation to advise on the most appropriate security model to be used in the corporation's software. The options are the Bell-LaPadula model or the Biba model. Specify which model you would select and explain your reasoning.

Question 38

Explain how the Clarke-Wilson model works.

Question 39

Both the Clark-Wilson and Biba models address the issue of integrity. Given that integrity models have three major goals, specify the integrity goals and indicate the goals addressed by each model.

Question 40

Compare and contrast the Biba security model with the Clark-Wilson security model (your answer should specify how each model works).

Question 41

Compare and contrast the Bell-LaPadula and Clarke-Wilson security models. Your answer should provide a description of each model, its aims and the differences between the models.

Question 42

Explain what a backdoor attack is in the context of cyber security, why it is a security problem and how one can address it.

Question 43

Explain what a time of check/use attack is in the context of cyber security, why it is a security problem and how one can address it.

Question 44

Explain what buffer overflow attack is in the context of cyber security, why it is a security problem and how one can address it.

Question 45

Buffer overflow attacks are common but they require the hacker to have knowledge of a number of key bits of information. Describe the specific information that a hacker needs to have in order to carry out a successful buffer overflow attack.

Question 46

Consider the statement ”The C language is not susceptible to buffer overflow attacks as it provides a number of low level functions such as strncat or strncpy that do memory bound checking.” Specify whether or not the statement is true and explain your reasoning.

Question 47

Consider the statement ”The buffer overflow attack is popular because the same attack can be applied to different platforms and architectures (write once, use for multiple attacks)”. Specify whether or not the statement is true and explain your reasoning.

Question 48

The Bell-LaPadula security model compartmentalises the information based on two factors. Specify the two factors and explain why the approach is critical in restricting the flow of information.

Question 49

Describe the principles behind the Goguen-Mesequer security model and how information is protected under this model.

Question 50

Compare the Goguen-Meseguer model with the Clark-Wilson model. Your answer should cover the concepts behind the models, how the information is protected in the models and what are the key differences between the two models.

Question 51

Modern systems are largely distributed and though organizations actively try to secure their systems the very nature of the systems makes it difficult to have effective security solution. Apart from the proliferation of knowledge about systems and existing defences, specify two other factors that make cyber security a difficult problem to address overall and explain your reasoning.

Question 52

The business needs of organizations often make it imperative to have Internet presence as the Internet offers the chance of reaching potential clients and vendors for only a fraction of the cost when compared with more traditional means. The Internet has a number of fundamental problems from the point of view of security such the ease of access to resources/knowledge and the fact that it is a public space. From a business security point of view describe another fundamental problem with the Internet and explain whether it is possible for the problem to be addressed.

Question 53

Attacks can originate from outside or inside the organization. Explain why insider attacks are more difficult to handle and potentially more damaging when compared with outsider attacks.

Question 54

Describe an approach in which the threat of an insider attack can be reduced.

Question 55

Social engineering attacks are a huge problem in terms of cyber security because they bypass all the technological defences an organization may employ to secure its systems. Describe three types of social engineering attacks and suggest potential solutions.

Question 56

Consider the statement *"The Facebook page of an organization is treasure trove for an experienced hacker."* Specify whether the statement is true or false and explain your reasoning.

Question 57

Explain why the use of free services is a major concern from the point of view of security.

Question 58

How does the changing nature of the cyber attacks affect the design of security system of an organization?

Question 59

Specify the three conditions that may lead to a covert channel to be established.

Question 60

Explain the concept of a storage type covert channel from a cyber security point of view.

Question 61

Explain the concept of a timing covert channel from a cyber security point of view.

Question 62

Consider the case of two subjects A and B which have a trust relationship such that B trusts A. Assuming that A is part of a trust domain, does subject B also have to be part of A's trust domain? Explain your reasoning.

Question 63

The X.800 standard is focused on communications and this is underlined by the approach used to handle data confidentiality. Describe the different aspects of communication confidentiality covered by the X.800 standard.

Question 64

The X.800 standard is focused on communications and this is underlined by the approach used to handle data integrity. Describe the different aspects of communication in regards to data integrity covered by the X.800 standard.

Question 65

A key factor in developing a security system is data availability. Describe why availability is considered to be so important and explain why for most organizations and especially in cases such as Google and Microsoft which collect enormous amounts of information, data availability is one of two key aspects of associated with data.

Question 66

Describe the concept vulnerability in cyber security and give an example of a real-world software vulnerability you know of and describe briefly the weakness and potential exploit.

Question 67

Curtin ICT Appropriate Use Guidelines (as of 2015) describe the following Dos and Don'ts:

DO

- D1. Use only those ICT facilities and services for which you have authorisation.
- D2. Use ICT facilities and services only for their intended purpose.

- D3. Abide by applicable laws and University policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
- D4. Respect the privacy and personal rights of others.
- D5. Use Curtin ICT facilities and services in a manner which is ethical, lawful and not to the detriment of others.
- D6. Use Curtin ICT facilities and services for teaching, learning and academic purposes.
- D7. Use ICT facilities for personal use where such use is incidental and does not impose upon or adversely affect the University, such as using ICT facilities and services for occasional emails and web browsing.

DONT

- N1. Access, copy, alter or destroy information, electronic mail, data, programs, or other files without authorisation.
- N2. Use resources you have not been specifically authorised to use.
- N3. Use someone elses username and password or share your username and password with someone else.
- N4. Upload, download, distribute or possess pornography, pirated software, movies, or other unlicensed digital media.
- N5. Send unsolicited emails (spam).
- N6. Use electronic resources for harassment or stalking.
- N7. Possess any hacking tools such as packet sniffers, password crackers, vulnerability scanners without written authorisation from the Chief Information Officer (contact the Information Security team for assistance).
- N8. Wilfully waste resources associated with Curtins ICT facilities and services.

For each of the general security goals: Availability, Integrity, and Confidentiality, select at least one relevant example among the above list. For each example selected, justify your choice.

Question 68

Describe the availability principle in cyber security and discuss possible security programs that can be used to maintain availability against denial-of-service attacks.

Question 69

Having an Internet presence is common for many organizations, such as government agencies and financial institutions, to reach and provide conveniences to a large number of customers. However, it also makes information security more challenging and the organizations could become more vulnerable to cyber-attacks. In late 2013, a significant attack, known as Carbanak, was targeted at a number of banks and financial institutions world-wide. It was reported that the attackers used spear phishing emails to bank employees and exploited several vulnerabilities in Microsoft Office and Microsoft Word

so as to infect their machines with the Carbanak backdoor. Consequently this led to a large amount of financial losses to these organizations.

- Discuss possible avenues that having Internet exposure might cause organizations to have employees contact details revealed to cyber criminals in such spear phishing attacks. Suggest necessary security actions that prevent employee contacts from being revealed to cyber criminals.
-) It is known that administrative controls are one effective solution to combat phishing. Suggest at least three examples of administrative controls that can improve phishing awareness and prevention.

Question 70

Explain the fundamental difference between Authentication and Authorization.

Question 71

Modern security approaches nowadays use multi-factor authentication. Give an example of such an approach and explain why it offers improved security approach over the traditional authentication where only a single username and password combination needs to be presented.

Question 72

Give a specific example to illustrate that security can only be successful if support from top-level management is provided.

Question 73

Describe three (3) things security can obtain from management to enable successful security programs.

Question 74

Modern security approaches nowadays use multi-factor authentication. Give an example of such an approach and explain why it offers improved security approach over the traditional authentication where only a single username and password combination needs to be presented.

Question 75

Give a specific example to illustrate that security can only be successful if support from top-level management is provided.

Question 76

Confidential data leakage (aka data loss) is a large problem faced by security personnels. Give two possible causes of data leakage, and suggest relevant solutions to address them.

Question 77

Data integrity can be compromised by man-in-the-middle attack. Briefly explain this attack, and discuss how you would prevent or minimize the impact of such attacks.

Question 78

Give one example of email phishing, explain how it works, and suggest two (2) solutions to mitigate this type of attacks

Question 79

Explain what data security is.

Question 80

Briefly describe the term **privilege** in the security context. What does the *least* privilege principle mean?

Question 81

Can perfect data security be obtained? Explain your reasons.

Question 82

List six (6) components of an information system. For each component, give an example of vulnerability associated with it.

Question 83

You are in charge of security for a business whose websites are hosted in the cloud. List four (4) ways that you would consider to protect customer data, including orders, personal and financial information.

2 Security Controls

Question 84

Physical controls are often neglected when security systems are developed but they nonetheless are a critical component of an effective security solution. Describe two physical preventive types of controls as well as two physical detective types of controls and specify a scenario in which a combination of the two is necessary.

Question 85

Describe two types of technical controls and specify which one you would use for low security setup required to protect a generic PC lab.

Question 86

When developing a security system, it is important to plan for cases which the preventive measures in place fail thus the system integrity is compromised. From a security perspective what are the two main avenues that are generally considered for continuity/restoration of services?

Question 87

A small health organization has asked for advice in regards to improving its security system. The organization is already implementing a defense in depth mechanism which combines a firewall with a encryption of traffic to prevent confidential information being accessed by unauthorised personnel. The company has very limited funding and you can only suggest two additional security mechanisms to be considered. Describe the mechanisms you have selected and justify your selection.

Question 88

With the help of an example, explain the principle of failing securely.

Question 89

Many organizations develop security systems which are focused entirely on physical and technological security controls. Explain why this is insufficient and provide examples how the security could be compromised.

Question 90

Explain the difference between corrective and recovery controls.

Question 91

An organization is developing a security system but lacks the resources to implement the traditional five types of controls that are usually part of security solution. Specify which two types of controls you would recommend to leave out and explain your reasoning.

Question 92

With the help of an example, explain why the principle of minimization is important from the point of view system security.

Question 93

Administrative mechanisms are an integral part of preventive controls and a fundamental component are the security policies. Explain why just publishing the security policies is not an effective way of ensuring compliance with the new security rules.

Question 94

Describe at least for common security methods used to address the key requirements of the CIA triad.

Question 95

List the types of controls that are categorized by their functionality and list the types of controls that are categorized by nature/plane of applications. Give at least one example of each type of controls.

Question 96

You are asked to give security set-up advice for a medical research laboratory which has computer terminals connected to a server that stores sensitive information. a) Suggest two physical preventive controls and two physical detective controls that can be used and explain your choice. b) The laboratory is going to provide an Internet presence to assist researchers in finding information online. However, this raises a serious concern that the sensitive information is accessed by intruders from the outside world. Under the defense-in-depth principle, suggest specific security solutions for at least two layers of defense that may be deployed to mitigate the risk.

3 Business Continuity

3.1 Risk Management

Question 97

Risk analysis is an integral part of the process of developing a security system. What is risk analysis used for and how does it influences the overall security system.

Question 98

Describe the two main methods of risk analysis used in security systems. Which one of these risk analysis approaches would you select to develop a security system and explain your reasoning.

Question 99

The risk analysis process can be speeded up by using a variety of tools. Explain the advantages and disadvantages of using automated tools for risk analysis.

Question 100

Developing a security plan requires one to take into account both the current requirements and future developments in order to ensure that the security plan will suit the organization's needs. Outline the three levels of planning required and explain their role and importance in developing the security plan.

Question 101

Explain how you would measure risks? Do security staff need to address every risk? Explain your reasoning.

Question 102

Risk management generally consists of three (3) steps. What is the first step? Briefly what are involved in this step.

Question 103

Explain why periodic review is a fundamental requirement of any risk assessment strategy.

Question 104

Consider the statement *"Any security IT staff can carry out risk assessment"*. It it true or false. Explain your reasoning.

Question 105

List and briefly explain two factors that risk depends upon.

Question 106

Automatic risk assessment tools are widely available nowadays. Discuss when and where you would consider using them, and not using them.

Question 107

You have identified and evaluated the risk of an asset, and there are few controls for consideration. Discuss on which basis you would select one control over the others to address the risk.

Question 108

Explain why risk mitigation would not be successful without the involvement of top-level management.

Question 109

List five (5) common approaches to address risks. For each approach, give one example.

Question 110

List and briefly explain three (3) issues that need to be considered when assigning values to assets?

Question 111

Briefly describe four (4) main goals of risk analysis.

Question 112

Explain why it is often suggested that for a large organisation risk analysis is best carried out by a team rather than an individual.

Question 113

An important step in risk analysis is to determine the value of an asset. Give five (5) different questions you think might help with the task of determining the asset value.

Question 114

Give two (2) examples of intangible assets and explain why it is often more difficult to determine the value of an intangible asset than a tangible one.

Question 115

Suppose that a business sells goods only through its online store. In the event that the only webserver is attacked and taken offline for several days, what are potential losses?

Question 116

What is residual risk, and how is it related to total risk.

Question 117

An online retailer has performed risk analysis and concluded that the annualised loss expectancy is $1 million, mainly due to the likelihood of denial-of-service attacks. To reduce the annualised loss expectancy to $100,000, the retailer has subscribed to professional DoS protection services at the cost of $200,000 per annum. How much does the subscription save the retailer in loss expenses? What would you classify the retailer's approach to handling risk?

Question 118

A backup data centre is located in a remote area. It has been determined that in the event of a severe cyclone, which happened twice in the last 40 years, the backup data centre suffers 50% damage. The cost to rebuild the centre is currently $1 million. What is the single loss expectancy for the centre suffering from such a severe cyclone? What is the annualised loss expectancy? If the insurance premium for such events is $10,000 per annum, would it be wise to consider insuring the centre to address the risk? Explain your reasoning.

Question 119

Explain the following terms: security policy, standards, guidelines, procedures.

Question 120

Consider the following risk analysis of a software company

Threat category	Cost per incident	Occurrence frequency
Programmer mistakes	$5,000	1 per week
Loss of intellectual property	$75,000	1 per year
Software piracy	$500	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Theft of information (employee)	$5,000	1 per 6 months
Web defacement	$500	1 per month
Theft of equipment	$5,000	1 per year
Virus, worms, Trojan horses	$1,500	1 per week
Denial-of-service attacks	$2,500	1 per quarter
Earthquake	$250,000	1 per 20 years
Flood	$250,000	1 per 10 years
Fire	$500,000	1 per 10 years

- Calculate the SLE, ARO, and ALE for each threat category listed in the above table.
- How did the software company arrive at the values shown in the table?

- Assume that the company has implemented controls to address the risk shown in the analysis and the new figures after one year are shown below. Assume that the cost per incident figures are still the same. Recalculate SLE, ARO, and ALE values for each category. Comment on the results.

Threat category	Occurrence frequency	Cost of controls	Type of control
Programmer mistakes	1 per month	$20,000	Training
Loss of intellectual property	1 per 2 years	$15,000	Firewall/IDS
Software piracy	1 per month	$30,000	Firewall/IDS
Theft of information (hacker)	1 per 6 months	$15,000	Firewall/IDS
Theft of information (employee)	1 per year	$15,000	Physical security
Web defacement	1 per quarter	$10,000	Firewall
Theft of equipment	1 per 2 years	$15,000	Physical security
Virus, worms, Trojan horses	1 per month	$15,000	Antivirus
Denial-of-service attacks	1 per 6 months	$10,000	Firewall
Earthquake	1 per 20 years	$5,000	Insurance/backup
Flood	1 per 10 years	$10,000	Insurance/backup
Fire	1 per 10 years	$10,000	Insurance/backup

3.2 Change Management

Question 121

Explain the difference between a System-Specific Policy and a Program Policy.

Question 122

Explain why documentation is critical for developing an effective policy.

Question 123

Specify five key components of a policy.

Question 124

You have been asked to review a set of policies. How would you determine if any of the policies are in need of revision? What are the key aspects that you would consider in your evaluation (describe at least five such aspects)?

Question 125

Planning is the starting point for developing and deploying a security solution. Describe at least five key factors that need to be taken into account when into the planning process of a cyber security system.

Question 126

Describe at least four benefits offered by ISO27001.

MAGICKA 3D PRINT COMPANY INFORMATION

A printing company, ”Magicka 3D Print” consisting of three departments (Marketing, Press, Customer Services) is attempting to become ISO27001 compliant. The company information provided is as follows:

1) Each department has its own hierarchy with general staff the reporting to three specialised staff: the department leader, the department business manager and the department’s IT officer. The smallest department has only 30 employees (Marketing) while the largest department has over 55 employees (Customer Services). The company also has four directors with each director having a personal assistant.

2) Each department has its own wired network which is turn, connected to a central company server which handles the company’s email, web and financial services. The central server has its own dedicated IT staff which are reporting by the company’s overall chief IT officer. The central server is running SUSE Linux OS. The Press department is running a Windows 2003 server and all its staff use WINXP SP3 on the their individual PCs, while the Marketing and Customer Services departments are running different version of the UBUNTU Linux OS. The IT equipment is replaced in batches over a period of 36 months to ensure that no piece of equipment is more than 36 months old. The company is using a generic firewall solution and IT staff regularly monitor the firewall logs. Remote connections are allowed once permission has been granted by the appropriate department leader. The authentication is done at the local machine level only and no mobile devices are allowed to be connected to the company’s network.

3) The company considers its client details and latest graphical designs for printing (developed and stored in the Press department’s network) as its key assets.

4) All staff recruited for the IT needs of the company are interviewed and are sent to ”upskill” programs by rotation with each staff undergoing training every 4.5 years.

5) All staff are regularly informed about the security policies via notices posted on each department’s notice board.

6) Each department has a guideline on the proper use of computing resources.

7) The company is located in a large four story building in which it occupies the top three levels - the ground level is occupied by two coffee shops. The Marketing and Press departments have an open plan arrangement with only the specialised personnel having offices. The Customer Service department is designed to allows each member of the staff an office. All offices can be locked and only the department leaders as well as the company directors have copies of the master keys.

8) Access to the company’s levels is done via a token based entry, with each staff member being issued with a swipe card.

9) The company has 14 IT dedicated staff and their job is to ensure that the company’s system are running without significant interruptions. The primary aim of the IT staff in the company is to ensure the availability of its services via the web presence and only one low level IT staff has had any prior exposure to computer security. The company considers security important and for this reason it has regularly purchased high end computing equipment and running a firewall.

Question 127

You have been hired as a consultant to provide advice on how to handle the process leading to ISO27001/2 compliance.

Your first task is to provide the company with an rough outline of what is the basic requirement to get the process of ISO27001/2 compliance started. In short, you need to specify the steps required, provide the details for the initial step and provide basic information about the implementation of your proposal. Furthermore, you need to justify your recommendations and you need to into account that the resources available are limited.

Question 128

Describe an example wherein unmanaged changes to IT systems and networks can increase risk to enterprises. Describe how the risk can be minimized if changes are managed carefully.

Question 129

List and briefly describe two standards in the ISO27k suite that you are aware of?

Question 130

List and briefly the four (4) phases in the PDCA model when applied to ISMS processes.

Question 131

Describe how you would measure the success of a change management program?

Question 132

What are basic elements that you can expect to see in a change management and control policy. Briefly describe each of them.

Question 133

You are in charge of managing the upgrade of the operating system on the computers of a small organization. Give examples of key issues that you would consider before implementing the change.

Question 134

List four (3) things that ISO27001 advises every organisation to do when establishing the ISMS.

Question 135

Should training and awareness be part of the implementation and operation phase of ISMS? Explain why or why not.

Question 136

A change management team has performed all the preliminary assessments, identified and evaluated the risk, and made final decision of the change approach. Are there anything else the team needs to do before rolling out the necessary change. Explain your reasoning.

Question 137

After a change has been carried out, what is the next important step that the change management team need to be aware of.

Question 138

Which of the following is the the primary goal of change management? Explain your choice.

- A. Maintaining documentation
- B. Keeping users informed of changes
- C. Allowing rollback of failed changes
- D. Preventing security compromises

3.3 Planning and Disaster Recovery

Question 139

Explain the fundamental difference between business continuity planning (BCP) and disaster recovery planning (DRP).

Question 140

Which one of the following statements about Business Continuity Planning and Disaster Recovery Planning is **not** correct?

- A. Business Continuity Planning is focused on keeping business functions uninterrupted when a disaster strikes.
- B. Organizations can choose whether to develop Business Continuity Planning or Disaster Recovery Planning plans.
- C. Business Continuity Planning picks up where Disaster Recovery Planning leaves off.
- D. Disaster Recovery Planning guides an organization through recovery of normal operations at the primary facility.

Question 141

In which one of the following database recovery techniques is an exact, up-to-date copy of the database maintained at an alternative location?

- A. Transaction logging
- B. Remote journaling
- C. Electronic vaulting
- D. Remote mirroring

Question 142

What disaster recovery principle best protects your organization against hardware failure?

- A. Consistency
- B. Efficiency
- C. Redundancy
- D. Primacy

Question 143

What Business Continuity Planning technique can help you prepare the business unit prioritization task of Disaster Recovery Planning?

- A. Vulnerability Analysis
- B. Business Impact Assessment
- C. Risk Management
- D. Continuity Planning

Question 144

Which one of the following alternative processing sites takes the longest time to activate?

- A. Hot site
- B. Mobile site
- C. Cold site
- D. Warm site

Question 145

What is the top priority that either BCP and DRP addresses?

Question 146

What is a business impact analysis (BIA), and what is it used for?

Question 147

What is the fundamental difference between BIA and risk assessment?

Question 148

Explain why it is important for large organisations to have a proper BCP in place? What is the implication if a lack of BCP is found?

Question 149

Once BCP and DRP are clearly written down, what are the important steps that need to be taken to make sure the organisation is ready for unexpected situations?

Question 150

The following disruptive events which could have an impact on the operation and administration of a critical server of an organisation

- The only administrator falls sick and is unable to work for a week
- A sudden power outage for a day, which is beyond the power reserve of the UPS
- A sudden denial-of-service attack that totally brings down the main website of the organisation

Which event could be considered under BCP? DRP? Explain your reasoning.

Question 151

List and briefly describe four (4) components that every emergency action plan of an organisation should have.

Question 152

Order the following steps to reflect the right sequence that is used in business continuity management:

- business impact analysis
- strategy development
- plan development
- project initiation
- testing
- maintenance
- implementation

Question 153

What is usually considered the most important requirement in developing a BCP? Explain your reasoning.

Question 154

List and order the actions that are necessary to respond to an extended power outage to your critical server of a data centre. Assume that a reserve power can only sustain the server for a short period of time.

Question 155

Consider the statement *"Business continuity planning is only about recovery of computer systems."* Is it true or false? Explain your reasoning.

Question 156

Consider the statement *"Business continuity planning only addresses the Availability principle of security, not Integrity or Confidentiality"*. Is it true or false. Explain your reasoning with the help of an example.

Question 157

Does business continuity planning provide any additional benefits to an organisation apart from providing the ability to recover from major disruptive events.

Question 158

What is the recovery time objective (RTO)? Discuss an approach to reducing RTO.

Question 159

What is the recovery point objective (RPO)? Discuss an approach to reducing RPO.

Question 160

How do the cost to recover and cost of disruption relate to the length of disruption time. Sketch the relationships, and then explain where you would pick a targeted disruption time?

Question 161

In the context of backup and disaster recovery, explain the difference between cold sites, hot sites, and warm sites.

Question 162

Describe the advantages and disadvantages of hot sites.

Question 163

Describe the advantages and disadvantages of cold and warm sites.

Question 164

Describe how the objectives RPO and RTO influence the choice of cold, hot, or warm sites.

Question 165

Which areas that recovery plans are developed for: financially important areas, mission critical areas, or all areas? Briefly explain your choice.

Question 166

Explain why documentation is critical in BCP. List the benefits it provides.

Question 167

Explain why copies of data should be stored off-site?

Question 168

The first step in a BCP is to analyse potential threats in terms of both their *nature* and *extent*. Explain what nature and extent mean and give an example for each concept.

Question 169

List five (5) types of natural disasters. For each type, discuss the effects and suitable mitigation strategies.

Question 170

Testing is a very important phase of an effective BCP. Discuss how and when such tests should be carried out.

Question 171

How regular should BCP tests should be performed? Explain your reasoning.

Question 172

It is advised that records of important events need to be maintained/documented. What should be done to the records afterwards?

Question 173

Can preventive measures be of any use at all when addressing BCP? Describe your justification.

Question 174

What is the primary difference between preventive measures and recovery strategies?

Question 175

Where should an organisation keep its business continuity and disaster recovery plans? Explain your reasoning.

Question 176

Developing continuity and disaster recovery plans is a complex task. Recently, there have been automated tools to help with this planning process. List four (4) things that such an automated tool can help a team create.

Question 177

Explain the primary difference between a structured walk-through test and a simulation test.

Question 178

What need to be considered carefully before carrying out a full-interruption test?

Question 179

What are the the MTD, RPO, RTO values of the following scenario:

Susan is the new BCM coordinator and needs to identify various preventive and recovery solutions her company should implement for BCP/DRP efforts. She and her team have carried out an impact analysis and found out that the companys order processing functionality cannot be out of operation for more than 15 hours. She has calculated that the order processing systems and applications must be brought back online within eight hours after a disruption. The analysis efforts have also indicated that the data that are restored cannot be older than five minutes of current real-time data.

Question 180

Is it ok to declare emergency is over when all operations and people are safely moved to the offsite facility? Explain your reasoning.

Question 181

Is reciprocal agreement enforceable or not? Explain your answer.

Question 182

Explain the primary difference between a parallel test and a full-interruption test for disaster recovery planning.

3.4 Data Masking, Erasure, Backup, Incident Handling

Question 183

List three (3) issues one must consider before masking data.

Question 184

Describe two (2) situations where data masking is particularly important.

Question 185

Data involved in any data masking must remain meaningful at several levels. Explain what it means by ‘‘meaningful”.

Question 186

Suppose you need to mask the name, age, and address of customers before sending the database to a third-party software firm for testing of a new database application. Explain your choice to mask the above fields in the dataset. Be mindful of the fundamental requirements of data masking.

Question 187

One important requirement of data masking is that it must prevent reverse engineering, hence loosing the confidentiality of the data. Describe one example of a poor data masking practice that can be reverse engineered by a competent hacker.

Question 188

Explain the fundamental difference between two data masking techniques: substitution and shuffling.

Question 189

Comment on the strength of the shuffling method against the size of data.

Question 190

Briefly explain the numeric variance method. Give two examples of data fields that this method is applicable, and two examples of data fields that

Question 191

Discuss the pros and cons of the encryption method in the context of data masking.

Question 192

With the help of an example, explain the nulling out/deletion techniques for data masking. Where would you find this approach particularly suitable? What are the pros and cons of this approach?

Question 193

Explain the primary difference between the following two types of data masking: static vs on-the-fly. Give an example for each type.

Question 194

Explain the pros and cons of static data masking.

Question 195

Explain how dynamic data masking is different from static data masking? List four (4) advantages and four (4) disadvantages of dynamic data masking.

Question 196

Explain why data masking is so important to businesses who rely on cloud infrastructure.

Question 197

Which approach is more suitable for cloud data masking: static or dynamic? Explain your reasoning.

Question 198

Explaining why allowing employees to delete data and dispose their old work PCs themselves could pose a security risk? What would you suggest to do instead?

Question 199

It has been suggested that an old hard drive can be securely erased by encrypting the whole drive with a sophisticated algorithm and key, and then destroy the key. Discuss whether this software approach to data erasure is sufficient.

Question 200

Research and find out why wiping data off an SSD drive needs a little more consideration than regular SATA/PATA hard drives.

Question 201

Explain how you would securely erase data off a server storage volume configured as RAID-5?

Question 202

List four (4) questions you would need to ask before deciding on a particular backup strategy.

Question 203

Compare and contrast backing up data and buying insurance from a security management's point of view.

Question 204

Compare the two archiving choices: tape vs disk: Discuss the pros and cons of each approach, and explain where you would consider one but not the other.

Question 205

List the stages and necessary actions that you would consider for a plan in the event of a distributed denial-of-service attack to your data server.

Question 206

What is a computer security incident? Give three (3) examples of computer security incidents that compromise Availability, Confidentiality, and Integrity.

Question 207

A director of an organisation has accidentally clicked on the attachment of a phishing email and hence the computer is now infected with the latest virus not yet recognized by the existing antivirus programs. Soon after clicking the attachment, the director has suspected that email and its attachment. If a proper security incident response to this type of attack exists, discuss what would be an appropriate response procedure?

4 Ethics

Question 208

What is the difference between laws and ethics?

Question 209

An IT company, Pear Inc., is introducing a new set of policies for its forensics team. The policies have been emailed to all the team members thus ensuring that they are aware of the penalties of violating the newly introduced policies. Explain whether the new policies are enforceable by the company.

Question 210

A multi-national software developer with centres in US and Asia is considering developing a policy regarding the ethical use of work resources for personal use. A policy developed for the centres in the US has been very effective and the intent is to use it for all the remaining centres. Explain why the policy developed in the US is unlikely to have the desired outcomes when applied to all centres.

Question 211

Two of the common claims made by hackers are outlined below:

- a) A hacker provides a very valuable service to the community because by successfully comprising the security of a system, the hacker is exposing problems with the security setup, problems which need to be addressed.
- b) There is no actual harm done because everything that a hacker does takes place in a virtual world.

Argue with the help of examples against the claims made by the hackers.

Question 212

An investigation of successful attack on the servers of medical company has stalled because some of the files on the data drives are encrypted. You are part of the investigative team and your specialization is dealing with encrypted files. You are not sure that the files will help identify who was behind the attack but you cannot discount that possibility until you had a look at the files. However, while you do not have the key for the company's system (which is kept secret because of the medical nature of the data), you know of a friend who is a leading expert in the world of encryption and who can help with the problem of breaking the encryption. All you need to do is to send him a copy of the encrypted files. Explain the implications of ethical implications of getting your friend to break the encryption on the files.

Question 213

Company employee A is dismissed for login in using employee B details which he was using to read email messages and then pass them onto employee B who was sick at home and did not have access to the company's email system. Employee A had the permission of employee B to do so and lodged a lawsuit against the company claiming unfair dismissal. Explain whether or not the company's action was correct form an ethics point of view.

Question 214

An employee of a large company is dismissed after his Internet usage showed that he was downloading illegal software which he was in turn using to do his work. In his defense, the employee claimed that the practice of downloading illegal software was common in his area and could prove that all his colleagues had done the same. Explain whether his defense addressed the ethical component of his behaviour and describe what you feel the company needs to do in terms of the illegal downloads issue both from the point of view the employee's termination and the future behaviour of its employees. Justify your reasoning.

Question 215

Discuss why employees should be encouraged to join and/or maintain membership with professional organizations, explain the costs and the benefits involved.

Question 216

What are the three general causes of unethical and illegal behaviour and discuss general approaches to address these causes.

Question 217

John was assigned to develop a critical component of a commercial product for his software firm. Due to personal reasons, John was quite behind schedule and he was worried that if he could not meet the deadline, the company would lose the contract and thus his employment might be terminated. John found out that his colleague and also friend, Matt, had been working on a similar component during his employment with a previous firm and he had a personal copy of the source code. John decided to use part of the code to complete the task, but did not tell anyone.

Discuss ethical issues in this example. Suggest what actions you would recommend John to do instead.

Question 218

Suppose that you are doing a cyber-security assignment and you need to study different hacking tools. You have found some tools, including packet sniffers, password crackers, and vulnerability scanners, and you plan to install them in one of the lab computers for study. Discuss the necessary actions you need to take to comply with Curtin's ICT rules.