**Additional End of Chapter Short Question**

**Chapter 6**

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ helps in recommending risk-reducing strategies.

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ deals with the continuous evaluation of the risk management process such that ultimately successful risk management is achieved.

3. The risks identified at the requirements assessment stage feed into \_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_ trade-offs in systems development.

4. In the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ stage, re-accreditation and re-authorizations are considered.

5. Any system migration needs to take place in a secure and \_\_\_\_\_\_\_\_\_\_\_\_\_ manner.

6. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ reside in the motivations of humans to undertake potentially harmful activities.

7. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attacks can occur because of a malicious attempt to gain unauthorized entry to a system.

8. The nature and significance of certain kinds of attacks keeps on changing with \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

9. Accurate \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the first step towards accomplishing proper planning and accurate budgeting for software development projects.

10. There are \_\_\_\_\_\_\_\_ major types of cost estimation techniques available today.

11. The \_\_\_\_\_\_\_\_\_\_\_\_\_ make use of extensive past project data.

12. The \_\_\_\_\_\_\_\_\_\_\_\_\_ approach has led to overestimation or underestimation, each of which translates into a negative impact on the success of the project.

13. Software reliability, software usability, and software efficiency emerged as the factors that would cause the greatest impact on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

14. Besides an understanding of \_\_\_\_\_\_\_\_\_\_\_\_\_ aspects of the system, the related roles and responsibilities need to be understood.

15. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ information relates to the functional requirements of the system, the stakeholders of the system, and security policies and architectures governing the IT system.

**Chapter 9**

1. Sabotage typically results in \_\_\_\_\_\_\_\_\_\_ forms.

2. \_\_\_\_\_\_\_\_\_ sabotage ca be thought of as intentionally not doing something you should be doing, which through this interaction results in harm to the organization.

3. An employee who is \_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the workplace increases the chances of them committing an act of sabotage.

4. Acts of \_\_\_\_\_\_\_\_\_\_ sabotage among employees are rare.

5. \_\_\_\_\_\_\_\_\_\_\_ is a dangerous threat to any organization with respect to their own employees and can lead to tremendous devastation due to an employee’s familiarity with their information system and authorized access.

6. \_\_\_\_\_\_\_\_\_\_\_\_, even if it has no real evidence of wrongdoing, can still be harmful to an organization.

7. With the confidential customer data and intellectual property just the slip of a keystroke away from the \_\_\_\_\_\_\_\_\_\_\_\_\_\_, every organization should be considered at risk.

8. A careless or \_\_\_\_\_\_\_\_\_\_\_\_\_ employee may simply think they are doing their job or speeding up the process by sending secure information through an unsecured email attachment.

9. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ techniques are particularly effective because they are based on what can be considered a bug or flaw in the decision-making process of humans.

10. While most of the organizations have \_\_\_\_\_\_\_\_ filters intended to prevent phishing, it is impossible to stop all attempts, and it only takes one mistake to expose an entire organization.

11. Criminal organizations are driven by \_\_\_\_\_\_\_\_\_, rather than personal ambition or sheer boredom.

12. Parties engaging in the production or distribution of prohibited goods and services are therefore members of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

13. One of the weapons of choice in twenty-first century espionage is the \_\_\_\_\_\_\_\_\_\_\_\_\_.

14. A large number of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ acts conducted for social and political reasons have come to light over the past few years.

15. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ has added a new dimension to persecution and makes victims feel a palpable sense of fear.

**Chapter 10**

1. Security of informal systems is no more than ensuring that the integrity of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_ stays intact.

2. In terms of managing information systems security, it is important that we focus our attention on maintaining the behavior, values, and \_\_\_\_\_\_\_\_\_\_\_\_\_\_ of the people.

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ has been considered as the single most important factor leading to the success or failure of a firm.

4. A proper mix of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_ makes the difference in the success or failure of a firm.

5. Often, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are considered without an appreciation of the context, and hence solutions get developed in isolation of complete understanding of the problem.

6. Lack of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of control structures also results in security problems.

7. While the role of technical controls can not be underestimated, true \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ can only be achieved if the technical controls have been adequately institutionalized.

8. Security culture is the totality of patterns of behavior that come together to ensure protection of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of a firm.

9. Once well-formed, security culture acts as the glue that brings together the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of different stakeholders.

10. Many time the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ programs do not necessarily relate to the task at hand.

11. Security \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ensure that assets remain protected and the business flourishes.

12. The mismatch between corporate \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and professional practices leads to divergent viewpoints.

13. IT-based systems adversely affect the subsistence issues related to different \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ groups.

14. Many organizations use play as a means to prepare for possible \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

15. Organizations such as the \_\_\_\_\_\_\_\_\_\_\_\_\_\_ and government agencies are typically hierarchical in nature.

**Chapter 11**

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are the moral principles that guide individual behavior.

2. In order for a sound \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ strategy, the recognition of ethical principles is important.

3. While cybersecurity represents a blooming industry, there is a shortfall of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ graduates.

4. While outsourcing and offshoring may have played a role, a majority of the job losses can be attributed to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and automation.

5. The consequences of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are known to motivate individuals to circumvent controls and find shortcuts for monetary gain.

6. In robotic systems, it is possible to orchestrate an \_\_\_\_\_\_\_\_\_\_\_\_\_\_ that exploits intermediate network nodes.

7. While many do not acknowledge the ill effects of something like software piracy, the illicit sale is generating millions of dollars in sales, which is contributing to the underground \_\_\_\_\_\_\_\_\_\_\_\_ markets.

8. Because of the distributed nature of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, there are concerns that money launderers use them systematically.

9. Deviants have been characterized as greedy who typically lack \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

10. The lack of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ poses interesting challenges in terms of white-collar crime, money laundering, and the role of centralized clearing houses.

11. Simply issuing a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ or a credo, without following it up with training and publicity to reinforce the message, will not be enough to prevent employee transgressions.

12. Ethical training and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ campaigns can have the desired effect on the bulk of the employees of an organization.

13. Some employees evade \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ controls because of cultural idiosyncrasies.

14. Many organizations depend upon the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to ascertain the proficiency level of an individual.

15. Currently many organizations and institutions have made it mandatory for new \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ hires to acquire some form of certification.

**Chapter 12**

1. The fact that many computer and servers can be accessed via the \_\_\_\_\_\_\_\_\_\_\_ increases the risk of theft and misuse of data by anyone with sufficient skills in accessing and bypassing security safeguards.

2. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ passed a ruling that one country’s territory can not be used to carry out acts that harm another country.

3. The key elements of the CFAA are to provide \_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ for violating the law.

4. The implementation of the CFAA made it easier to prosecute complaints of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of sensitive information.

5. CFAA allowed a double-whammy against the \_\_\_\_\_\_\_\_\_\_\_\_\_, and allowed the \_\_\_\_\_\_\_\_\_\_\_\_\_\_ to attempt to recover more in damages.

6. Damage is defined as any impairment to the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of the computer data or information.

7. Motivation for the CSA was sparked by the escalating use of computer systems by the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and the requirement to ensure the security and privacy of unclassified, sensitive information in those systems.

8. The purpose of the CSA was to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and tighten security controls on computers in use throughout the federal government, and those in use by federal contractors.

9. Whether you are a large health care provider, insurance company, a small rural physician in practice or benefits consulting firm, you will have to consider a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ for personal history information to be in compliance with HIPAA.

10. HIPAA has important implications for all health care providers, payers, patients, and other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

11. The \_\_\_\_\_\_\_\_\_\_\_\_\_ assessment inventories an organization’s current security environment with respect to policies, processes, and technology.

12. The goal of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_ is to complete the current environment with the proposed regulatory one in terms of the level of readiness and to determine whether gaps exist and, if so, how large they are.

13. A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ should provide an analysis of both likely and unlikely scenarios in terms of probability of occurrences and their impact on the organization.

14. The SOX act increases the requirements that organizations must adhere to for financial \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

15. The FISMA security program requires the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of each federal agency to define and implement an information security program.

**Chapter 13**

1. Computer forensics is a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attempt to balance society’s need to protect itself and the rights of the individuals that are perceived as threatening society’s survival and prosperity.

2. It is almost impossible to enact effective \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the scope of the problem is revealed through real-life, everyday experience.

3. Like any other forensic science, computer forensics deals with the application of a science to a question of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

4. Computer forensics deals with the preservation, discovery, identification, extraction, and documentation of computer \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

5. The forensic process applies \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to the examination of computer related evidence.

6. Forensic is done through managing the investigation of the crime scene and its evidentiary aspects through a thorough, efficient, secure, and documented \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

7. The logical side of computer forensics deals with the extraction of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ from any relevant information resource.

8. Computer forensics does not \_\_\_\_\_\_\_\_\_\_\_\_ or \_\_\_\_\_\_\_\_\_\_\_\_\_ the evidence that was seized at the crime scene.

9. Computer forensics makes an exact \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ copy of the evidence, and analysis is performed on the mirror image copy while the original evidence is held in a secure environment.

10. Forensically \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ data is a mirror image of the humanly understandable information, such as time and date stamps.

11. The process of making a forensically acceptable copy of data for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ involves a whole host of steps to ensure that the data copy is forensically identical to the data source.

12. Law enforcement officials have \_\_\_\_\_\_\_\_\_\_\_\_\_ responses when asked about how forensic evidence should be gathered.

13. “Don’t touch anything; call us!” – response springs forth from the law enforcements commitments to help those in need, to upholding the law, and to put their expertise to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ use.

14. The nuances of the law and the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of the treatment do not allow a full discussion of either the law or the procedures dictated by the law.

15. There are exceptions to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ that allow investigators to perform warrantless searches.

**Chapter 14**

1. While it may be prudent to focus on the ease pf use and functionality in some cases, in others, maintaining \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of private data may be the foremost objective.

2. Although \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a goal that most organizations aspire for, it is often not possible to have that.

3. Traditionally organizations have been viewed as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and security has for the most part not been considered part of the useful system designed for the purposeful activities.

4. Exclusive emphasis on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and designing it in a top-down manner is counterproductive.

5. Changes in technology and the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ nature of business makes most standards obsolete even before they get published.

6. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of a model is judged on the basis of the extent to which it represents a given subset of the reality.

7. Security problems arise as a consequence of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and managerial inability to balance the rule- and norm-based aspects of work.

8. Problems of overformalization are usually a consequence of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ syndrome.

9. In practice, controls have dysfunctional effects because \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ solutions are proposed for specific problems.

10. A mismatch between the \_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_ of the organization could potentially be detrimental to the health of an organization and to the information systems in place.