FINAL EXAM

Course # 571003
Computer Security: Crime and Fraud Protection

based on the electronic .pdf file(s):

Computer Security: Crime and Fraud Protection
by: Dr. Jae K. Shim, Ph.D., 2005, 289 pages

14 CPE Credit Hours
Technology &
Operations

This exam sheet is made available for your convenience in answering questions while offline. Please note that you will still need to enter your answers on the online exam sheet for grading. Instructions are provided at the end of this document.

Chapter 1 - Organizational Policy

1. A good manager will know the types and forms of information generated and how the information is used by the business before planning how to manage it. T F

   ☐ TRUE

   ☐ FALSE

2. In designing and implementing risk-management procedures and controls the manager is not responsible for:

   ☐ Identifying the risks and evaluating the risks

   ☐ Installing appropriate controls

   ☐ Designing the security hardware and software

   ☐ Preparing a contingency plan and continually monitoring the controls against the plan

3. Optional security policy that defines the limit of acceptable behavior should include:

   ☐ No playing unauthorized games on the corporate computers

   ☐ No visiting adult web sites

   ☐ No use of pirated software

   ☐ All the above

4. The responsibility of the risk-manager does not include:

   ☐ Identify the risk

   ☐ Evaluate the risk

   ☐ Security guards

   ☐ Install appropriate controls

5. Not every organization need define security policies and acceptable behavior. T F

☐ TRUE

☐ FALSE

6. Proper security safeguards includes all except:

☐ turn over employees to prevent over familiarization

☐ revoke passwords as soon as an employee is terminated

☐ use lists of authorized personnel to control entry into system

☐ constantly monitor logs generated by computer system

7. A security policy includes:

☐ No playing computer games on corporate computers

☐ No visiting adult web sites

☐ Prohibits taking copies of corporate electronic documents out of the office

☐ All of the above

8. For a security policy to succeed, it is not necessary for all individuals or departments to participate. T F

☐ TRUE

☐ FALSE

Chapter 2 - Physical Security and Data Preservation

9. The first line of defense for a computer system is to protect it physically: the plant, the equipment, and the personnel. T F

☐ TRUE

☐ FALSE

10. Safeguards that help protect computer facilities from accidents and

disaster like floods and fire include all except:

- [ ] Adequate lighting for safe evacuation
- [ ] Open windows for ventilation
- [ ] Fireproof containers to protect media (disks, tapes)
- [ ] User manuals for equipment and software for proper operations

11. Maintenance and preventive care logs should not contain:

- [ ] Type of equipment serviced
- [ ] Date of service
- [ ] Controlling access to the equipment
- [ ] Service performed and results of diagnostic tests

12. Computer facilities are rarely susceptible to damage from environmental factors. T F

- [ ] TRUE
- [ ] FALSE

13. Computer facilities are susceptible to damage from a variety of environmental factors except:

- [ ] Heat
- [ ] Water
- [ ] Air conditioning
- [ ] Humidity

14. Simple precautions to minimize static electricity do not include:

- [ ] Using shag carpeting on the floors
- [ ] Using anti-static sprays
- [ ] Grounding computer equipment

☐ Use anti-static floor and table mats

15. Data that is no longer needed must be destroyed. T F

☐ TRUE

☐ FALSE

16. Computer and terminal controls should include the:

☐ Manufacturer's name

☐ Automatic shut-off, call-back, and time locks

☐ Model number of the hardware

☐ Date of purchase and date that the warranty expires

17. Special fasteners can be used to protect RAM chips and internal components using cover locks on all except:

☐ Lock the computer

☐ Block access to the disk drive

☐ Block access to the mouse

☐ Block access to the cd-rom

Chapter 3 - Hardware Security

18. Software security depends on hardware security. T F

☐ TRUE

☐ FALSE

19. Which of the following is not one of the most common hardware problems:

☐ Equipment can be stolen or replaced

☐ Security can be circumvented

☐ Having a key or password protected configuration set up

☐ Systems can be booted by unauthorized users

20. Data integrity can be ensured by:

☐ Human error

☐ Backing up data regularly

☐ Software bugs or viruses

☐ Natural disasters, fires and floods

21. Data integrity is as important to protect as actual hardware. T F

☐ TRUE

☐ FALSE

22. According to computer crime surveys the biggest dollar loss occurs by:

☐ Denial of services

☐ Sabotage

☐ Unauthorized insider access

☐ System penetration

23. Major computer vendors offering security products to safeguard user hardware and software are:

☐ Smart cards, preset locks

☐ IBM, HP, DELL

☐ Firewalls, anti-virus software

☐ All of the above

24. Major vendors offer the following security features except:

☐ Smart Card Security Kits (IBM)

☐ Hard drive password feature (DELL)

☐ Fingerprint identification technology (COMPAQ)

☐ Centralized management of hardware

25. The banks use smart card systems for computer security because they are not vulnerable to high-risk attacks. T F

☐ TRUE

☐ FALSE

26. Smart Card vulnerabilities do not include:

☐ Attacks by the cardholder against the terminal

☐ Attacks by the cardholder against the data owner

☐ Attacks against single sign-on employees

☐ Attacks by cardholders against the software manufacturers

27. A biometric product that is created by sound waves generated by an individual speaking a given phrase or password is a:

☐ Handwritten acoustic emission

☐ Palm print

☐ Voice print

☐ Iris

Chapter 4 - Software Security

28. A computer virus is a clinically injected organism into a computer system. T F

☐ TRUE

☐ FALSE

29. A program that replicates itself but does not infect other programs is a:

- [ ] Trojan horse
- [ ] Worm
- [ ] Dropper
- [ ] Bomb

30. Viruses remain free to spread into other programs because most common viruses give off no symptoms of their infection. T F

- [ ] TRUE
- [ ] FALSE

31. The top information security products and services now in use do not include:

- [ ] Virus protection
- [ ] Backup storage
- [ ] Access controls
- [ ] Electrical avoidance shockers

32. Which of the following is not a type of viruses:

- [ ] Boot sector viruses
- [ ] File infectors or parasitic viruses
- [ ] Animal viruses
- [ ] Macro-viruses

33. Firewalls do not:

- [ ] Protect against malicious insiders
- [ ] Protect against unauthorized entry from outside and inside
- [ ] Protect against completely new threats

☐ Protect against viruses

34. A system that enforces an access control policy between two networks is a:

☐ Web shield

☐ Firewall

☐ Net shield

☐ Group shield

35. Encryption is the transmission of data into secret code. T F

☐ TRUE

☐ FALSE

36. Which one of the following is not a practical application of Security Socket Layer (SSL)?

☐ Client/server systems – securing database access

☐ Financial – develop remote banking programs

☐ Information systems – create remote access and administration applications

☐ Under water activities – control water pressure

Chapter 5 - Personnel Security

37. It is not necessary to screen or pre-screen potential employees because their resumes guarantee their qualifications and honesty. T F

☐ TRUE

☐ FALSE

38. when checking and screening for pre-employment backgrounds you do not have to check:

☐ Applicants previous addresses and employers

☐ Professional and bank references

☐ Applicant's acquaintances and relatives

☐ Credit history

39. Companies should insist that new employees in sensitive jobs sign employment agreements with non-disclosure provisions. T F

☐ TRUE

☐ FALSE

40. Formal performance evaluations should be used to routinely assess employees' performance and skill level. T F

☐ TRUE

☐ FALSE

41. Effective performance appraisals will not detect:

☐ Low quality or low production output

☐ Complaints

☐ Late arrivals

☐ Warranted overtime

42. When training new employees which one of the following should not be addressed:

☐ What data can be used for personal use

☐ The organization's data backup policy

☐ The type of data that should be encrypted

☐ How data encrypted keys are managed

43. Employees can cause considerable damage if terminated except for:

☐ Intentionally input erroneous data

☐ Erase data files and destroy backups

☐ Terminate access prior to informing an employee of termination

☐ Make copies of data for personal use or competitors

Chapter 6 - Network Security

44. An attacker that is able to read or copy confidential information has:

☐ Denial of service

☐ Write access

☐ Read access

☐ None of the above

45. Most local area network or communication software packages contain encryption and security features. T F

☐ TRUE

☐ FALSE

46. It is important to realize that simply keeping the telephone number secret is sufficient. T F

☐ TRUE

☐ FALSE

47. Which of the following is not a tool used to implement the security plan:

☐ Encryption tools

☐ Route filtering

☐ Firewalls

☐ Powerpoint

48. A saboteur's tools do not include:

☐ Piggybacking

☐ Geographic dispersion

☐ Data manipulation

☐ Viruses

49. Which one of the following is not a common type of network topologies:

☐ Hierarchical topology (tree structure)

☐ Horizontal topology (or bus topology)

☐ Physical topology (surface elevations)

☐ Star topology (data communication)

50. Risks related to software bugs cannot easily be reduced by:

☐ Keeping up-to-date on software fix patches

☐ Using products that have been around a while

☐ Using well known brand name products

☐ Allowing services for internet users not authorized

Chapter 7 - Security Policy

51. In formulating a policy you must first ask yourself the following questions except:

☐ What resources need to be protected

☐ Against whom must we protect our system

☐ Why not take lack of protection and losses as part of doing business

☐ How much can we spend to protect the system

52. Computer security risk analysis and management does not involve:

- [ ] Destruction of data or equipment
- [ ] Security risk of system but not reliability of the system
- [ ] Theft of data equipment
- [ ] Malfunction of equipment or bugs in the software

53. Which of the following is not an example of human factor threats:

- [ ] Personnel incompetence
- [ ] Indifference
- [ ] Negligence
- [ ] Distrust others, do not share

54. An account administrator is not intended to ensure:

- [ ] User is authorized
- [ ] User has access privileges appropriate to the job
- [ ] User should be threatened against illegal usage of system
- [ ] User is not engaged in unauthorized activities

55. Disruption in computer processing can be classified as all except:

- [ ] Malfunction – minor disruption that affects hardware
- [ ] Malfunction – that affects software or data files
- [ ] Disasters – disruption to entire facility
- [ ] Unknown risks

56. Specialists inside and outside organizations who cannot suggest improvements and modifications in contingency planning are:

- [ ] Professional hackers

☐ Internal auditors

☐ Finance and accounting departments

☐ Security department

57. Which of the following is not a part of contingency plans:

☐ Documents and records likely to be needed first

☐ Where vital records are stored

☐ On-site storage of back-up records

☐ Equipment and other resources that might be needed for recovery

58. Systems and program documentation that should be backed-up do not include:

☐ Source code for program

☐ DSL telecommunication system

☐ Flow charts

☐ Program logic descriptions

59. Fire damage can be reduced by:

☐ Storage safes

☐ Smoke and ionization systems

☐ Chemical extinguishing systems, automatic sprinklers

☐ All of the above

Chapter 8 - Contingency Planning

Chapter 9 - Auditing and Legal Issues

60. Security auditing by Information Technology (IT) auditors and financial auditors can enhance audit efficiency by all except:

- [ ] Specialized computer audit techniques
- [ ] Use of technical tools and expertise
- [ ] Use for manual controls
- [ ] Evaluates the adequacy and effectiveness of the central system

61. IT auditors typically do not review the following:

- [ ] System development standards
- [ ] Size of building
- [ ] Library control procedures
- [ ] Network system and contingency plans

62. Which one of the following is not a control technique at the environmental level:

- [ ] Quality assurance review of vendor software
- [ ] Segregation of duties
- [ ] Ensuring that software is virus free
- [ ] Recommending hardware and software products

63. Basic EDI security risks do not encompass:

- [ ] Access violations
- [ ] Communication enhancement
- [ ] Message modifications
- [ ] Interruptions or delays

Chapter 10 - Computer Crime, Cyber fraud, and Recent Trends

64. Penalties for violation of the U.S. Computer Fraud and Abuse Act include:

- [ ] 1 to 5 years in prison for a first offence
- [ ] 10 years for a second offence
- [ ] 20 years for three or more offences
- [ ] All of the above

65. Which one of the following statements is not included in the definition of The Association of Information Technology Professionals (ATIP) computer crime as?

- [ ] Unauthorized modification of software, data, or network resources
- [ ] Unauthorized distribution of freeware software
- [ ] Unauthorized copying of software
- [ ] Unauthorized release of information

66. Hacking is the obsessive use of computers, or the unauthorized access and use of networked computer systems. Which of the following is not considered a hacker?

- [ ] Outsiders who use the Internet to damage data
- [ ] Company employees who use the Internet to steal data and programs
- [ ] Company employees who use the Internet to damage data
- [ ] Outsiders who use the Internet to view a company's website

67. Many computer crimes involve the theft of money. In the majority of cases, they are:

- [ ] "Inside jobs" that involve authorized network entry and fraudulent alteration of computer databases to cover the tracks of the employees involved
- [ ] "Outside jobs" that involve authorized network entry and fraudulent alteration of computer databases to cover the tracks of the employees involved
- [ ] "Inside jobs" that involve unauthorized network entry and fraudulent alteration of computer databases to cover

the tracks of the employees involved

☐ "Outside jobs" that involve unauthorized network entry and fraudulent alteration of computer databases to cover the tracks of the employees involved

68. Which one of the following would not be considered as a way that a computer virus can enter a computer system?

☐ E-mail and file attachments

☐ Borrowed copies of software

☐ Downloaded copies of shareware

☐ Running antivirus programs

69. The unauthorized use of private and confidential personal information has seriously damaged the privacy of individuals. Which of the following is an example of using the Internet to violate a person's privacy?

☐ Accessing individuals' private e-mail conversations and computer records, and collecting and sharing information about individuals gained from their visits to Internet websites and newsgroups.

☐ Always knowing where a person is, especially as mobile and paging services become more closely associated with people rather than places.

☐ Using customer information gained from many sources to market additional business services.

☐ Collecting telephone numbers, e-mail addresses, credit card numbers, and other personal information to build individual customer profiles.

70. Individuals have been mistakenly arrested and jailed, and people have been denied credit because of their physical profiles. These are examples of:

☐ Computer profiling and computer matching

☐ Computer libel

☐ Censorship

☐ Privacy

Instructions for Submitting Answers Online:

- *Sign In at www.ApexCPE.com*

- *Click the "My CPE" tab at the top of the page.*
- *Click "My CPE Courses".*
- *Find the current CPE year and click "Go to My Courses".*
- *Find this course and click the "Go to Course" link.*
- *Step 2 on the Course Syllabus page is "Take the Final Exam". Click the "Begin Final Exam" link.*
- *Enter your answers on the online exam sheet.*
- *Click the "Grade Exam" button at the bottom of the page. Your exam will be graded automatically. If your score exceeds 70%, a "Create Certificate" button will display. Otherwise, you may continue to retake the exam until you pass.*
- *A short evaluation page will display. Please provide your feedback for the course.*
- *Once the evaluation is complete, click the "Submit Evaluation & Create Certificate" button at the top of the page.*
- *You may print your Certificate of Completion by selecting File Print from your browser. Certificates remain online for at least five years from the certificate date.*

If you have any questions, please call us at 1-877-317-9047
or send an email to support@apexcpe.com