Chapter 3 Answers to Review Questions and Exercises

[A HD]Review Questions

1. What is the difference between law and ethics?

   Laws are rules that mandate or prohibit certain behavior in society; they are drawn from ethics, which define socially acceptable behavior. The key difference between laws and ethics is that laws carry the sanctions of a governing authority and ethics do not. Ethics are based on cultural mores: the fixed moral attitudes or customs of a particular group.

2. What is civil law, and what does it accomplish?

   Civil law represents a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizations and people. Civil law encompasses family law, commercial law, and labor law.

3. What are the primary examples of public law?

   Criminal, administrative, and constitutional law are the primary examples of public law.

4. Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change?

   The National Information Infrastructure Protection Act of 1996 amended the Computer Fraud and Abuse Act of 1986. It modified several sections of the CFA Act and increased the penalties for selected crimes.

5. Which law was created specifically to deal with encryption policy in the United States?

   The Security and Freedom Through Encryption Act of 1999 clarifies use of encryption for people in the United States and permits them to buy or sell any encryption product.

6. What is privacy in an information security context?

   Privacy is not absolute freedom from observation, but a “state of being free from unsanctioned intrusion.”

7. What is another name for the Kennedy-Kassebaum Act (1996), and why is it important to organizations that are not in the healthcare industry?

   The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects the confidentiality and security of healthcare data by establishing and enforcing standards and by standardizing electronic data interchange. HIPAA affects all healthcare organizations, including doctors’ practices, health clinics, life insurers, and universities, as well as some organizations that have self-insured employee health programs or manage data related to health care.

   Beyond the basic privacy guidelines, the act requires organizations that retain healthcare information to protect it using information security mechanisms, policies, and procedures. It also requires a comprehensive assessment of the organization’s information security systems, policies, and procedures. HIPAA provides guidelines for the use of electronic signatures based on security standards that ensure message integrity, user authentication, and nonrepudiation. There is no

specification of particular security technologies for the security requirements, except that security must be implemented to ensure the privacy of healthcare information.

The privacy standards of HIPAA severely restrict the dissemination and distribution of private health information without documented consent. The standards provide patients with the right to know who has access to their information and who has accessed it. The standards also restrict the use of health information to the minimum necessary for the healthcare services required.

8. If you work for a financial services organization such as a bank or credit union, which 1999 law affects your use of customer data? What other effects does it have?

   The law that affects the use of customer data by financial institutions is the Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999. Specifically, this act requires all financial institutions to disclose their privacy policies on the sharing of nonpublic personal information. It also requires due notice to customers so they can request that their information not be shared with third parties. In addition, the act ensures that an organization's privacy policies are fully disclosed when a customer initiates a business relationship and then distributed at least annually for the duration of the professional association.

9. What is the primary purpose of the USA PATRIOT Act?

   The USA PATRIOT Act of 2001 modified a wide range of existing laws to provide law enforcement agencies with broader latitude to combat terrorism-related activities. The laws modified by the PATRIOT Act include some of the earliest legislation created to deal with electronic technology.

10. How has the PATRIOT Act been revised since its original passage?

    In 2011, the PATRIOT Sunset Extension Act of 2011 was signed into law to extend certain provisions of the USA PATRIOT Act. These provisions covered wiretaps, searching of business records, and surveillance of people with suspected ties to terrorism.

11. What is intellectual property (IP)? Is it afforded the same protection in every country of the world? What laws currently protect IP in the United States and Europe?

    Intellectual property is recognized as a protected asset in the United States. The U.S. copyright laws extend this privilege to published works, including electronic formats. Fair use of copyrighted materials includes their use to support news reporting, teaching, scholarship, and other related activities, as long as the use is for educational or library purposes, is not for profit, and is not excessive. As long as proper acknowledgement is provided to the original author of such works, including a proper citation of the location of source materials, and the work is not represented as one's own, it is entirely permissible to include portions of someone else's work as reference.

    U.S. Copyright law governs the protection of IP in the United States.

    The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), created by the World Trade Organization (WTO) and negotiated from 1986 to 1994, introduced intellectual property rules into the multilateral trade system.

The Digital Millennium Copyright Act (DMCA) is the American contribution to an international effort by the World Intellectual Properties Organization (WIPO) to reduce the impact of copyright, trademark, and privacy infringement, especially when accomplished via the removal of technological copyright protection measures. This law was created in response to the 1995 adoption of Directive 95/46/EC by the European Union, which added protection for individual citizens with regard to the processing of personal data and its use and movement. The United Kingdom has implemented a version of this law called the Database Right to comply with Directive 95/46/EC.

12. How does the Sarbanes-Oxley Act of 2002 affect information security managers?

    Executives in firms covered by this law will seek assurance for the reliability and quality of information systems from senior information technology managers. In turn, IT managers will likely ask information security managers to verify the confidentiality and integrity of the information systems in a process known as sub-certification.

13. What is due care? Why should an organization make sure to exercise due care in its usual course of operations?

    An organization increases its liability if it refuses to take measures known as due care. Due care has been taken when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. The more active an organization is in exercising due care, the less likely it will be held liable for its employees' illegal or unethical actions.

14. How is due diligence different from due care? Why are both important?

    Due diligence requires that an organization make a valid effort to protect others and continually maintain this level of effort. Due care has been taken when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. It is important for an organization to practice both due diligence and due care to decrease its chances of being found liable if an incident occurs.

15. What is a policy? How is it different from a law?

    A policy is a formalized body of expectations that describe acceptable and unacceptable employee behavior in the workplace. The difference between a policy and a law is that ignorance of a policy is an acceptable defense.

16. What are the three general categories of unethical and illegal behavior?

    Software license infringement, illicit use, and misuse of corporate resources are the three general categories of unethical and illegal behavior.

17. What is the best method for preventing an illegal or unethical activity?

    Deterrence is the best method for preventing an illegal or unethical activity. For deterrence to be effective, the affected parties must fear the penalty, have an expectation of detection or apprehension, and expect that if they are apprehended, the penalty will be applied.

18. Of the information security organizations listed in this chapter that have codes of ethics, which has been established for the longest time? When was it founded?

The Association of Computing Machinery (ACM), established in 1947.

19. Of the organizations listed in this chapter that have codes of ethics, which is focused on auditing and control?

    The Information Systems Audit and Control Association (ISACA) is focused on auditing and related control systems.

20. How do people from varying ethnic backgrounds differ in their views of computer ethics?

    Overall, there is general agreement among people of different nationalities for what constitutes acceptable or unacceptable computer use. However, there is a range of views for whether some actions are moderately or highly unacceptable, according to a 1999 study published in *The Journal of International Business Studies*. The study found little support for the popular media's portrayal of Asians as having a high tolerance for digital copyright infringement. In fact, higher piracy rates in Singapore and Hong Kong may be less a function of ethical considerations than the fact that the countries offer fewer legal and financial disincentives to engage in software copyright infringement. The Netherlands consistently ranked as the country least likely to honor copyrights of content creators—and although the Netherlands has a higher piracy rate than some nations, it still ranks behind Singapore and Hong Kong.

[A HD]Exercises

1. What does CISSP stand for? Use the Internet to identify the ethical rules CISSP holders have agreed to follow.

   CISSP stands for Certified Information Systems Security Professional. The requirements for CISSP certification are as follows:

   - Subscribe to ISC^2's Code of Ethics.
   - Have at least three years of direct, full-time security professional work experience in one or more of the 10 test domains of the information systems security Common Body of Knowledge (CBK). Valid experience includes information systems security-related work performed as a practitioner, auditor, consultant, vendor, investigator, or instructor, or work that requires IS security knowledge and involves direct application of that knowledge.
   - No affiliation with any organization is required for taking the CISSP certification examination.

   Once these requirements have been met, one may take the certification test. The CISSP certification examination consists of 250 multiple-choice questions. Candidates have up to six hours to complete the examination, which covers the 10 test domains of the information systems security Common Body of Knowledge:

   - Access control systems & methodology
   - Applications & systems development
   - Business continuity planning
   - Cryptography
   - Law, investigation, & ethics
   - Operations security

- Physical security
- Security architecture & models
- Security management practices
- Telecommunications, network, & Internet security

After the exam, the following maintenance is required:

- After passing your CISSP certification examination, you will receive a certificate and ID card. You are also eligible to be listed in the CISSP Directory, to participate in the Speakers' Bureau, and to serve on ISC^2 committees and participate in annual elections.
- CISSP recertification is required every three years, with ongoing requirements for maintaining credentials in good standing. Recertification is accomplished mainly through continuing professional education (CPE) and by earning 120 CPE credits every three years.

ISC^2 also charges an annual maintenance fee.

2. For what kind of information security jobs does the NSA recruit? Use the Internet to visit its Web page and find out.
   - Information assurance research with these skills:
     - Secure network technology
       - Biometrics
       - Intrusion detection
       - Wireless security
       - High-speed networking security
     - Secure systems research
     - Secure network technology
     - Cryptology research
   - Information Assurance Directorate with these skills:
     - Network security
     - Vulnerability analysis
     - Public key infrastructure (PKI)
     - Security testing/red teaming
     - Firewalls/router security
     - Security software design/development (object-oriented programming: C++/Java)
     - Firewalls/router security
     - Security hardware design/development
     - Customer support
     - Defense information operations (DIO)
     - Special Processing Laboratory (SPL, now part of IAD)
     - Microelectronics Research Laboratory (MRL, now part of IAD)
   - Networking with these skills:
     - Packet based
     - Internet/intranets
     - Protocol development
     - Optical network management

- Advanced research

Alternate answer

The NSA's ongoing mission involves monitoring, gathering, and decoding foreign communication signals from around the world, as well as information assurance. To meet this goal, the NSA actively recruits people with computer and engineering backgrounds as well as people who are conversant in foreign languages. Current job titles listed at the NSA's Web site include Inspector General Auditor/IT Specialist, Mathematician, Computer Scientist, Cryptanalyst, Electronic and Computer Engineer, Signals Analyst, Signals Intelligence (SIGINT) Systems Engineering Architect, and Linguist.

3. Using the resources in your library, find out what laws your state has passed to prosecute computer crime.

(Each state will have different answers. Answers from the state of Georgia are given as a representative example.)

The Georgia Computer Systems Protection Act was signed into law in 1991. It repealed and replaced an act of the same name 10 years earlier. The law establishes certain acts of computer fraud or abuse as crimes punishable by fines, imprisonment, or both. A modification to the law was passed by the 1996 session of the Georgia General Assembly.

The following computer crimes are defined by state law (Georgia Code 16-9-90 et seq.):

Computer theft—Includes theft of computer services, intellectual property such as copyrighted material, and any other property.
Computer trespass—Unauthorized use of computers to delete or alter data or interfere with others' usage.
Computer invasion of privacy—Unauthorized access to financial or personal data.
Computer forgery—Forgery as defined by other laws, but committed on a computer rather than on paper.
Computer password disclosure—Unauthorized disclosure of a password resulting in damages of more than $500. In practice, this includes any disclosure that requires a system security audit afterward.

Maximum penalties are a $5,000 fine and one year of imprisonment for password disclosure, and a $50,000 fine and 15 years of imprisonment for the other computer crimes, plus civil liability. The law also includes the following state codes:

- Code 16-9-91 contains the Georgia Assembly's findings that previous laws made it difficult to prosecute computer crimes.
- Code 16-9-92 includes definitions of computer, computer network, computer operation, computer program, data, financial instruments, property, services, use, victim expenditure, and without authority.
- Code 16-9-93 goes into detail about computer theft, computer trespass, computer invasion of privacy, computer forgery, computer password disclosure, articles of exclusion, civil relief damages, and criminal penalties.

- Code 16-9-94 sums up codes 16-9-90 through 16-9-93.

4. Using a Web browser, go to *www.eff.org*. What are the current top concerns of this organization?

   - Expanded government surveillance with reduced checks and balances
     - Be careful what you put in that Google search.
     - Nationwide roving wiretaps
     - ISPs hand over more user information.
     - New definitions of terrorism expand scope of surveillance
   - Excessive breadth of government power with a lack of focus on terrorism
     - Government spying on suspected computer trespassers with no need for court orders (Sec. 217)
     - Adding samples to DNA database for those convicted of "any crime of violence"
     - Wiretaps now allowed for suspected violations of the Computer Fraud and Abuse Act
     - Dramatic increases to the scope and penalties of the Computer Fraud and Abuse Act
   - Allows Americans to be spied upon more easily by U.S. foreign intelligence agencies
     - General expansion of FISA authority
     - Increased information sharing between domestic law enforcement and intelligence
     - FISA detour around federal domestic surveillance limitations; domestic detour around FISA limitations

   Alternate answer

   A top concern of the EFF is spearheading a movement to repeal the Children's Internet Protection Act of 2000 (CIPA). According to the EFF, the software being used is not effective at blocking out pornography and instead is blocking thousands of sites that should not be blocked, hurting students' ability to learn.

   The EFF is also leading a coalition of civil liberties groups in urging a secret appeals court to reject the Justice Department's bid for broadly expanded powers to spy on U.S. citizens. "At issue in the case—which has focused a spotlight on the ultra-secret Foreign Intelligence Surveillance Court—is whether the Constitution and the USA PATRIOT ACT adopted by Congress after the Sept. 11 terrorist attacks permit the government to use looser foreign intelligence standards to conduct criminal investigations in the United States."

   (*www.eff.org/Privacy/Surveillance/20020919_eff_pr.html*)

5. Using the ethical scenarios presented earlier in this chapter in the Offline feature called "The Use of Scenarios in Computer Ethics Studies," finish each of the incomplete statements and bring your answers to class to compare them with those of your peers.

   This question is meant to provoke discussion; no answers have been provided.