Appendix

Answers to Review Questions

Chapter 1 Review Questions

1. **List and define the principal security objectives.**

   Answer:

   - Authentication: The assurance that the communicating entity is the one that it claims to be.
   - Access control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
   - Data confidentiality: The protection of data from unauthorized disclosure.
   - Data integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
   - Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
   - Availability service: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

2. **Describe the uses of data encryption.**

   Answer: Encryption is the conversion of plaintext or data into unintelligible form by means of a reversible translation. It is an element of many of the services and mechanisms listed in Chapter 1.

3. **What are the essential ingredients of a symmetric cipher?**

   Answer: Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

4. **What are the two basic functions used in encryption algorithms?**

   Answer: Permutation and substitution.

5. **How many keys are required for two people to communicate via a symmetric cipher?**

   Answer: One secret key.

6. **Describe the two general approaches to attacking a cipher.**

   Answer: Cryptanalysis and brute force.

7. **What are the principal ingredients of a public-key cryptosystem?**

   Answer: Plaintext, encryption algorithm, public and private keys, ciphertext, decryption algorithm.

8. **List and briefly define three uses of a public-key cryptosystem.**

   Answer:

   - Encryption/decryption: The sender encrypts a message with the recipient’s public key.
   - Digital signature: The sender “signs” a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
   - Key exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

9. **What is the difference between a private key and a secret key?**

   Answer: A user’s private key is kept private and known only to the user; it is complemented by a corresponding public key. A secret key can be shared by two or more users.

10. **What is a message authentication code?**

    Answer: A MAC is a data element associated with a data block or message. The MAC is generated by a cryptographic transformation involving a secret key and, typically, a cryptographic hash function of the message. The MAC is designed so that someone in possession of the secret key can verify the integrity of the message.

11. **What is a digital signature?**

    Answer: A digital signature is a value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data’s origin and integrity.

12. **Describe the use of public-key certificates and certificate authorities.**

    Answer: A public-key certificate contains a public key and other information, is created by a certification authority, and is given to the participant with the matching private key. A participant conveys its key information to another by transmitting its certificate. Other participants can verify that the certificate was created by the authority.

13. **Describe the functions of the various components in Figure 1.9.**

    Answer: (1) The authority maintains a directory with a {name, public key} entry for each participant. (2) Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication. (3) A participant may replace the existing key with a new one at any time, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way. (4) Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widely circulated newspaper. (5) Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.

Chapter 2 Review Questions

1. **Explain the term *information privacy*.**

   Answer: Information privacy is the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

2. **What is personally identifiable information?**

   Answer: PII is information that can be used to distinguish or trace an individual's identity.

3. **Explain the manner in which privacy by design and privacy engineering operate together.**

   Answer: Privacy by Design is intended to ensure that information privacy considerations are considered at every stage of system development and that privacy protection measures be designed into the system during the system design and development process, rather than retrofitted. Privacy engineering is generally considered to be the implementation and operation of a system dictated by PbD principles.

4. **What are the commonly accepted foundational principals for privacy by design?**

   Answer: (1) Proactive not reactive; preventative not remedial. (2) Privacy as the default. (3) Privacy embedded into design. (4) Full functionality: positive-sum, not zero-sum. (5) End-to-end security; lifecycle protection. (6) Visibility and transparency. (7) Respect for user privacy.

5. **What elements are involved in privacy risk assessment?**

   Answer: Privacy-related asset; privacy threat; privacy vulnerability; privacy controls.

6. **Describe the various types of privacy controls.**

   Answer: Management controls deal with management structure and responsibilities and overall strategy and policy. Operational controls deal with techniques and practices in the implementation and operation of a system. Technical controls are hardware and software mechanisms.

7. **What issues should be considered in selecting privacy controls?**

   Answer: The risk assessment process should be considered. If new controls create new risks, then these have to be considered in selecting additional control.

8. **Explain the difference between privacy risk assessment and privacy impact assessment.**

   Answer: Privacy impact assessment includes not only considering risk but also determining protection mechanisms to reduce risk.

9. **What are the types of privacy testing?**

   Answer: Functional testing, penetration testing, user testing.

10. **What are the overlapping and non-overlapping areas of concern with respect to information security and information privacy?**

    Answer: Overlap: accountability, integrity, aggregation, confidentiality, destruction. Areas of distinct concern for information privacy deal with specific protections for PII.

11. **Explain the trade-off between privacy and utility.**

    Answer: Any access of data that contains or is derived from PII has the potential to leak information that the source of the PII wants to keep private, thus reducing utility. On the other hand, increasing the privacy restrictions on information increases the restrictions on the flow of potentially useful information.

12. **What is the difference between usability and utility?**

    Answer: Usability refers to the ease of use of privacy features. Utility refers to the functionality available for databases containing PII with privacy protection in place.

Chapter 3 Review Questions

1. **What is the GDPR definition of *personal data*.**

   Answer: Personal data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural ,or social identity of that natural person.

2. **Explain the distinction between sensitive PII and non-sensitive PII.**

   Answer: The implication of the designation of some PII as sensitive is that the release of such information would have greater impact of some sort than non-sensitive PII, and that therefore an organization should have stronger privacy controls for sensitive PII. There is no widely accepted definition of sensitive PII.

3. **Describe four categories of information that may relate to individuals.**

   Answer:

   - Personally identifiable information: This term has already been defined. Simply put, it is information that leads to the identification of a unique individual.
   - De-identified personal information: Information that has had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.
   - Anonymous personal information: Information not related to an identified or an identifiable person and cannot be combined with other information to re-identify individuals. It has been rendered unidentifiable.
   - Aggregated (group) information: Information elements abstracted from a number of individuals, typically used for the purposes of making comparisons, analyzing trends, or identifying patterns.

4. **What is re-identification and how is it accomplished?**

   Answer: Re-identification is a process that re-establishes the relationship between personally identifiable data and de-identified data. The organization can achieve this by using a code, algorithm, or pseudonym that is assigned to individual records, with the enabling information protected by encryption or other means. Another approach is to encrypt identifying elements within data records.

5. **Describe the FIPPs defined by OECD.**

   Answer:

   - Collection Limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
   - Data Quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
   - Purpose Specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- Use Limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification except:

  a) with the consent of the data subject; or

  b) by the authority of law

- Security Safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- Individual Participation: An individual should have the right to:

  a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him

  b) have communicated to him data relating to him within a reasonable time

  at a charge, if any, that is not excessive

  in a reasonable manner

  in a form that is readily intelligible to him

  c) be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

  d) challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended

- Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

6. Give a brief overview of GDPR.

Answer: The GDPR is an EU privacy regulation that applies to all EU countries. It reflects modern developments in information technology and privacy concerns. It provides a broad definition of PII and applies to all EU residents and all organizations that do business in the EU.

7. List some of the major privacy-related laws in the U.S.

Answer:

- The Privacy Act of 1974: Specifies the rules that a federal agency must follow to collect, use, transfer, and disclose an individual's personally identifiable information (PII).

- The Fair and Accurate Credit Transaction Act of 2003 (FACTA): Requires entities engaged in certain kinds of consumer financial transactions (predominantly credit transactions) to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft.

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA): Requires covered entities (typically medical and health insurance providers and their associates) to protect the security and privacy of health records.
- The Family Educational Rights and Privacy Act of 1974 (FERPA): Designed to protect students and their families by ensuring the privacy of student educational records.
- The Gramm Leach Bliley Act of 1999 (GLBA): Imposes privacy and information security provisions on financial institutions; designed to protect consumer financial data.
- Federal Policy for the Protection of Human Subjects: Published in 1991 and codified in separate regulations by 15 federal departments and agencies, outlines the basic ethical principles (including privacy and confidentiality) in research involving human subjects.
- The Children's Online Privacy Protection Act (COPPA): Governs the online collection of personal information from children under the age of 13.
- The Electronic Communications Privacy Act: Generally prohibits unauthorized and intentional interception of wire an electronic communications during the transmission phase and unauthorized accessing of electronically stored wire and electronic communications.

8. **What role does NIST play with respect to information privacy?**

   Answer: As part of its ongoing development of standards and guidelines for information security, the CSRC has extended its concern to information privacy. The documents produced by the CSRC fall into three broad categories: privacy controls, privacy engineering, and a privacy framework.

9. **What contribution has ISO made to privacy standards?**

   Answer: More recently, ISO has begun developing privacy standards that serve as companions to the requirements and guidelines standards in the 27000 series.

10. **Explain the purpose of the ISF Standard of *Good Practice for Information Security*.**

    Answer: This document is a business-focused, comprehensive guide to identifying and managing information security risks in organizations and their supply chains. The breadth of the consensus in developing the SGP is unmatched. It is based on research projects and input from its members, as well as an analysis of the leading standards on cybersecurity, information security, and risk management. The goal is the development of best practice methodologies, processes, and solutions that meet the needs of its members, including large and small business organizations, government agencies, and nonprofit organizations.

Chapter 4 Review Questions

1. **What is meant by the term *repurposing* collected data?**

   Answer: The use of PII that is collected for one purpose to satisfy other purposes.

2. **Describe the different means of collecting PII.**

   Answer:

   - Mandatory disclosure: There are a number of contexts in which individuals are required to provide PII, such as on tax returns and disclosures by convicted felons (fingerprints, DNA).
   - Incentivized disclosure: In this case, an organization provides an incentive to an individual to disclose information. For example, a retail business may offer a loyalty card, which entitles the user to discounts but enables the business to track purchases.
   - Conditioned disclosure: This is similar to an incentivized disclosure and refers to the case in which, in order to obtain some important good or service, an individual must supply PII. Examples are driving an automobile, traveling on an airplane, voting, and gaining employment. In all these cases, the individual must supply some PII.
   - Entirely voluntary disclosure: As an example, people may disclose personal information on social media.
   - Unannounced acquisition of information: This category covers cases in which an individual discloses PII without being aware of it. An example is the use of cookies on Web browsers.

3. **Describe each of the threats listed in the threat taxonomy of Figure 4.1.**

   Answer:

   - Information collection: Includes surveillance and interrogation.
   - Information processing: Includes aggregation, identification, insecurity, secondary use, and exclusion.
   - Information Dissemination: Includes disclosure, breach of confidentiality, exposure, increased accessibility, blackmail, appropriation, and distortion.
   - Invasions: Includes intrusion and decisional interference.

4. **Explain the NIST privacy threat model.**

   Answer: The NIST privacy threat model is based on these concepts:

   - Subjects: Encompasses an individual or a group of individuals, the identity of individuals and groups, and their rights, autonomy, and privacy desires.
   - Data: Encompasses the data and derived information about these individuals and groups.
   - Data actions: Any system operations that process PII. These include the various data collection, processing, analysis, and retention practices; controls that constrain such practices; and impacts (negative and positive) of the collection and use of data on individuals, groups, and society.
   - Context: The circumstances surrounding the system's processing of PII.

5. **Explain the difference between privacy threat, problematic data action, and privacy harm.**

   Answer: A privacy threat is traditionally defined as the potential for violation of privacy, which exists when there is a circumstance, capability, action, or event that could violate privacy and cause harm to an individual. Also traditionally, a threat action is a realization of a threat; i.e., an occurrence in which vulnerability is exploited as the result of either an accidental event or an intentional act.

   NIST 8062 uses somewhat different definitions: A problematic data action is a data action that causes an adverse effect, or problem, for individuals. A privacy harm is an adverse experience for an individual resulting from the processing of his or her PII. Thus, a privacy data action is essentially the same as a privacy threat action, and a privacy harm is the impact of that action.

6. **List examples of problematic data actions.**

   Answer:

   - Appropriation: PII is used in ways that exceed an individual's expectation or authorization. Appropriation occurs when personal information is used in ways that an individual would object to or would have expected additional value for.
   - Distortion: The use or dissemination of inaccurate or misleadingly incomplete personal information. Distortion can present users in an inaccurate, unflattering, or disparaging manner.
   - Induced Disclosure: Pressure to divulge personal information. Induced disclosure can occur when users feel compelled to provide information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or privilege to an essential (or perceived essential) service.
   - Insecurity: Lapses in data security.
   - Surveillance: Tracking or monitoring of personal information that is disproportionate to the purpose or outcome of the service. The difference between the data action of monitoring and the problematic data action of surveillance can be very narrow. Tracking user behavior, transactions, or personal information may be conducted for operational purposes such as protection from cyber threats or to provide better services, but it becomes surveillance when it leads to privacy harms.
   - Unanticipated Revelation: Non-contextual use of data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse datasets.
   - Unwarranted Restriction: Unwarranted restriction to PII includes not only blocking tangible access to PII, but also limiting awareness of the existence of the information within the system or the uses of such information.

7. **Describe the categories of privacy harms.**

   Answer:

   - Loss of Self-Determination: The loss of an individual's personal sovereignty or ability to freely make choices.
   - Discrimination: The unfair or unequal treatment of individuals.
   - Loss of Trust: The breach of implicit or explicit expectations or agreements about the handling of personal information.
   - Economic Loss: This can include direct financial losses as the result of identity theft, as well as the failure to receive fair value in a transaction involving personal information.

8. **What are the general sources of privacy threats?**

   Answer:

   - Adversarial: Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources; i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies.
   - Accidental: Erroneous actions taken by individuals in the course of executing their everyday responsibilities.
   - Environmental: Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
   - Structural: Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters.

9. **Describe the categories of privacy vulnerabilities.**

   Answer:

   - Technical vulnerabilities: Flaws in the design, implementation, and/or configuration of software and/or hardware components, including application software, system software, communications software, computing equipment, communications equipment, and embedded devices.
   - Human resource vulnerabilities: Key person dependencies, gaps in awareness and training, gaps in discipline, improper termination of access.
   - Physical and environmental vulnerabilities: Insufficient physical access controls, poor siting of equipment, inadequate temperature/humidity controls, inadequately conditioned electrical power.
   - Operational vulnerabilities: Lack of change management, inadequate separation of duties, lack of control over software installation, lack of control over media handling

and storage, lack of control over system communications, inadequate access control or weaknesses in access control procedures, inadequate recording and/or review of system activity records, inadequate control over encryption keys, inadequate reporting, handling, and/or resolution of security incidents, inadequate monitoring and evaluation of the effectiveness of security controls.

- Business continuity and compliance vulnerabilities: Misplaced, missing, or inadequate processes for appropriate management of business risks; inadequate business continuity/ contingency planning; inadequate monitoring and evaluation for compliance with governing policies and regulations.
- Policy and procedure vulnerabilities: Privacy policies and procedures that are inadequate to fully protect PII, including conformance with FIPPs.
- Dataset vulnerabilities: Weakness in de-identification measures, inadequate masking of PII in statistical datasets, inadequate protection against discovery of PII by analysis of multiple datasets.

10. **Where might privacy vulnerabilities be located in an IT infrastructure?**

Answer:

- External transfer of PII, including to and from:

  —The PII principal

  —A third party individual or organization

  —A cloud service provider

  —An IoT
- Storage and process of the PII within the organization’s IT infrastructure.
- Organizational vulnerabilities, such as human resource, physical, operational, business continuity, policy and procedure, and dataset.
- If the organization offloads some storage and processing functions to an external cloud service provider, there may be privacy vulnerabilities at the cloud site.
- If the organization maintains an IoT that extends beyond the organization premises, there may be privacy vulnerabilities within the IoT network.

11. **What are the National Vulnerability Database and the Common Vulnerability Scoring System?**

Answer: The NVD is a comprehensive list of known technical vulnerabilities in systems, hardware, and software; it covers both security and privacy vulnerabilities. The CVSS provides an open framework for communicating the characteristics of vulnerabilities. The CVSS defines a vulnerability as a bug, flaw, weakness, or exposure of an application, system device, or service that could lead to a failure of confidentiality, integrity, or availability.

Chapter 5 Review Questions

1. **Explain the difference between authorization, authentication, and access control.**

   Answer:

   - Authorization: Authorization is the process of deciding what an individual or process ought to be allowed to do. In the context of system access, authorization is the granting of specific rights to a user, program, or process to access system resources and perform specific functions. Authorization defines what an individual or program can do after successful authentication.
   - Authentication: Authentication is the process of establishing an understood level of confidence that an identifier presented to a system refers to a specific user, process, or device. Authentication is often a prerequisite to allowing access to resources in an information system. This function is typically referred to as user authentication, to distinguish it from message authentication or data authentication.
   - Access control: Access control is the process of granting or denying specific requests: 1) for accessing and using information and related information processing services; and 2) to enter specific physical facilities. Access control ensures that access to assets is authorized and restricted based on business and security requirements.

2. **What is the difference between need-to-know and need-to-use?**

   Answer: With need-to-know, you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile). With need-to-use, you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

3. **Describe the process for authorizing users.**

   Answer:

   - Associate access privileges with uniquely defined individuals; for example, by using unique identifiers such as UserIDs.
   - Maintain a central record of access rights granted to a user ID to access information systems and services.
   - Obtain authorization from the owner of the information system or service for the use of the information system or service; separate approval for access rights from management may also be appropriate.
   - Apply the principle of least privilege to give each person the minimum access necessary to do his or her job.
   - Access privileges for an individual should be assigned for individual resources based on information security levels and classification of information.

- In addition to information resources, such as files and databases, authorization should specify which networks and networked services may be accessed.
- Requirements for expiration of privileged access rights should be defined.
- Ensure that identifiers are not reused; that is, authorizations associated with UserID should be deleted when the individual assigned that UserID changes roles or leaves the organization.

4. **In the context of user authentication, what is the distinction between identification and verification?**

   Answer: Identification is the means by which a user provides a claimed identity to the system; verification is the means of establishing the validity of the claim.

5. **Describe the functions of the various components in Figure 5.2.**

   Answer:

   - Credential service provider (CSP): A trusted entity that issues or registers subscriber authenticators. For this purpose, the CSP establishes a digital credential for each subscriber and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use.
   - Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.
   - Relying party (RP): An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.
   - Applicant: A subject undergoing the processes of enrollment and identity proofing.
   - Claimant: A subject whose identity is to be verified using one or more authentication protocols.
   - Subscriber: A party who has received a credential or authenticator from a CSP.

6. **Describe the three principal authentication factors.**

   Answer:

   - Knowledge factor (something the individual knows): Requires the user to demonstrate knowledge of secret information.
   - Possession factor (something the individual possesses): Physical entity possessed by the authorized user to connect to the client computer or portal.
   - Inherence factor (something the individual is or does): Refers to characteristics, called biometrics, that are unique or almost unique to the individual.

7. **What is multifactor authentication?**

   Answer: Multifactor authentication refers to the use of more than one authentication factor in the process of authentication.

8. **Describe four common access control policies.**

   Answer:

   - Discretionary access control (DAC): Access control based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
   - Mandatory access control (MAC): Access control based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.
   - Role-based access control (RBAC): Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
   - Attribute-based access control (ABAC): Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.

9. **What is the difference between an access control list and a capability ticket?**

   Answer: An access control list (ACL) lists users and their permitted access rights for each object for which access is control. A capability ticket specifies authorized objects and operations for a particular user.

10. **What is the difference between role-based access control and attribute-based access control?**

    Answer: RBAC is based on the roles that users assume in a system rather than the user's identity. An ABAC model can define authorizations that express conditions on properties of both the resource and the subject.

11. **What is identity and access management?**

    Answer: Identity and access management (IAM) typically consists of several discrete activities that follow the stages of a user's life cycle within the organization. These activities fall into two categories:

    - Provisioning process, which provides users with the accounts and access rights they require to access systems and applications.
    - User access process, which manages the actions performed each time a user attempts to access a new system, such as authentication and sign-on.

12. **Describe three deployment approaches for identity and access management.**

    Answer:

    - Centralized: All access decisions, provisioning, management, and technology is concentrated in a single physical or virtual location. Policies, standards, and operations are pushed out from this single location.
    - Decentralized: Local, regional, or business units make the decisions for all access choices, provisioning, management, and technology. There may be enterprise-wide policies and standards, but these are guidance for the decentralized provider.
    - Federated: Each organization subscribes to a common set of policies, standards, and procedures for the provisioning and management of users. Alternatively, the organizations can buy in a service from a supplier.

13. **What is federated identity management?**

    Answer: Federated identity management refers to the agreements, standards, and technologies that enable the portability of identities, identity attributes, and entitlements across multiple enterprises and numerous applications and supporting many thousands, even millions, of users.

14. **What is meant by single sign-on?**

    Answer: When multiple organizations implement interoperable federated identity schemes, an employee in one organization can use a single sign-on to access services across the federation with trust relationships associated with the identity.

Chapter 6 Review Questions

1. **List some common types of malware.**

    Answer:

    - Virus: A computer program that can copy itself and infect a computer without permission or knowledge of the user.

- Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.
- Trojan Horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
- Spyware: Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.
- Rootkit: A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.
- Backdoor: An undocumented way of gaining access to a computer system. Typically, a backdoor is a program that has the ability to bypass a system's security control, allowing an attacker to access the system stealthily.
- Mobile code: Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
- Bot: Also known as a zombie.

2. **With reference to SP 800-83, what are some desired capabilities of good malware protection software?**

   Answer:

   - Scanning critical host components.
   - Watching real-time activities on hosts to check for suspicious activity.
   - Monitoring the behavior of common applications.
   - Scanning files for known malware.
   - Identifying common types of malware as well as attacker tools.
   - Disinfecting files and quarantining files.

3. **What is the difference between disinfecting and quarantining files?**

   Answer: Disinfecting files refers to removing malware from within a file. Quarantining files means that files containing malware are stored in isolation for future disinfection or examination.

4. **Name all the techniques that firewalls use to control access and enforce site's security policy.**

   Answer: Service control, direction control, user control, behavior control.

5. **What are some common types of firewalls?**

   Answer: Packet filtering, stateful inspection, application-level gateway, circuit-level gateway.

6. **What are some of the weaknesses of packet filters?**

   Answer:

   - Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, if a packet filter firewall cannot block specific application commands and if a packet filter firewall allows a given application, all functions available within that application will be permitted.

   - Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).

   - Most packet filter firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality by the firewall.

   - Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Many packet filter firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.

   - Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet filter firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy.

7. **What is an intrusion detection system?**

   Answer: Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding—and providing real-time or near-real- time warning of—attempts to access system resources in an unauthorized manner.

8. **Describe the placement of intrusion detection systems.**

   Answer:

   - Host-based IDS: Monitors the characteristics of a single host and the events occurring within that host for suspicious activity. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the OS. Furthermore, unlike network-based IDSs, host-based IDSs can more readily see the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

- Network-based IDS: Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

9. **What are two generic approaches to intrusion detection?**

   Answer: Misuse detection and anomaly detection.

10. **What is the difference between misuse detection and anomaly detection?**

    Answer:

    - Misuse detection is based on rules that specify system events, sequences of events, or observable properties of a system that are believed to be symptomatic of security incidents. Misuse detectors use various pattern-matching algorithms, operating on large databases of attack patterns, or signatures. An advantage of misuse detection is that it is accurate and generates few false alarms. A disadvantage it that it cannot detect novel or unknown attacks.
    - Anomaly detection searches for activity that is different from the normal behavior of system entities and system resources. An advantage of anomaly detection is that it is able to detect previously unknown attacks based on an audit of activity. A disadvantage is that there is a significant tradeoff between false positives and false negatives. Figure 6.5 suggests, in abstract terms, the nature of the task confronting the designer of an anomaly detection system. Although the typical behavior of an intruder differs from the typical behavior of an authorized user, there is an overlap in these behaviors. Thus, a loose interpretation of intruder behavior, which will catch more intruders, will also lead to a number of false positives, or authorized users identified as intruders. On the other hand, an attempt to limit false positives by a tight interpretation of intruder behavior will lead to an increase in false negatives, or intruders not identified as intruders.

11. **What are the typical locations for the sensors in network intrusion detection systems?**

    Answer:

    - Outside the main enterprise firewall. Useful for establishing the level of threat for a given enterprise network. Those responsible for winning management support for security efforts can find this placement valuable.
    - In the network DMZ (inside the main firewall but outside internal firewalls). This location can monitor for penetration attempts that target Web and other services generally open to outsiders. The DMZ adds an additional layer of network security between the Internet and an organization’s internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network. It provides external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

- Behind internal firewalls, positioned to monitor major backbone networks, such as those that support internal servers and database resources.
- Behind internal firewalls, positioned to monitor LANs that support user workstations and servers specific to a single department. Locations 3 and 4 in Figure 6.6 can monitor for more specific attacks at network segments, as well as attacks originating from inside the organization.

Chapter 7 Review Questions

1. **List and define the four types of attributes that may be present in a microdata file.**

   Answer:

   - Direct identifier: A set of attributes in a dataset that enables unique identification of a data principal. Recall from Chapter 3 that a data principal is a natural person to whom the personal information in the dataset relates. Examples of identifying variables include name, email address, home address, telephone number, health insurance number, and social security number. Direct identifiers are thus PII attributes.
   - Quasi-identifier (QI): QIs by themselves do not identify a specific individual but can be aggregated and linked with other information to identify data subjects. Examples of QIs include sex, marital status, postal code or other location information, a significant date (e.g. birth, death, hospital admission, discharge, autopsy, specimen collection, or visit), diagnostic information, profession, ethnic origin, visible minority status, and income. The example in Section 7.2 of the re-identification of William Weld's medical records used the QIs birthday, ZIP, and sex.
   - Confidential attributes: Attributes not in the PII or QI categories but contain sensitive data subject information (such as salary, religion, diagnosis).
   - Non-confidential attributes: Attributes that data subjects do not typically consider sensitive.

2. **Explain the differences between microdata tables, frequency tables, and magnitude tables.**

   Answer:

   - Microdata table: Consists of individual records, each containing values of attributes for a single individual or other entity. Specifically, a microdata table *X* with *s* subjects and *t* attributes is an $s \times t$ matrix where X_{ij} is the value of attribute *j* for data subject *i*.
   - Summary table: A summary table, also called a macrodata table, is typically two-dimensional, with the rows and columns representing two different attributes. Thus, if the two attributes are A and B, the table can be expressed as A×B. A summary table contains aggregated data about individuals derived from microdata sources. For

example, a table that presents counts of individuals by 5-year age categories and the total annual income in increments of $10,000 is comprised of statistical cells such as the cell (35-39 years of age, $40,000 to $49,999 annual income). Summary tables are of two types:

—Frequency table: Presents the number of units of analysis (persons, households, establishments) in a table cell (an intersection of a table row and column). An example of this is a (race × sex) table where the table cells show the counts of the number of people having these attributes for different attribute values. Equivalently, each cell may contain the percentage or fraction of the total population under study that fits in that cell.

—Magnitude table: Displays information on a numerical aggregate value in a table cell. An example of this is a (disease × town) table where the table cells show the average age of patients having these attributes for different attribute values.

3. **What is a re-identification attack?**

   Answer: For a dataset that has been de-identified, a re-identification attack attempts to recover identifying information.

4. **List and define three types of disclosure risk.**

   Answer:

   - Identity disclosure: Occurs when a record in an anonymized or de-identified dataset can be linked with an individual identity. Identity disclosure is relevant to a dataset of records on individuals. An adversary is able to match one or more records to specific individuals. For example, an adversary determines that the record with the label field 7 belongs to Mary Jones; this reveals that all the information in that record is associated with Mary Jones.

   - Attribute disclosure: Occurs when sensitive information about a data subject is revealed through the de-identified file. Attribute disclosure is relevant to a dataset of records on individuals. An adversary is able to obtain one or more attributes for a specific individual, even though the adversary may not be able to obtain the full data record. For example, if a hospital releases information showing that all current female patients aged 56 to 60 have cancer, and if Alice Smith is a 56-year-old female that is known to be an inpatient at the hospital, then Alice Smith's diagnosis can be inferred, even though her individual de-identified medical records cannot be distinguished from the others.

   - Inferential disclosure: The released data make it possible to determine the value of some characteristic of an individual more accurately than otherwise would have been possible. For example, with a mathematical model, an intruder may be able to infer a respondent's sensitive income information using attributes recorded in the data, leading to inferential disclosure.

5. **Explain the differences between pseudonymization, anonymization, and de-identification.**

   Answer:

   - Anonymization: A transformation of a dataset containing PII such that an adversary cannot recover personal identities from the anonymized data by reasonable efforts.
   - De-identification: A transformation in which a re-identification parameter is associated with the transformed data, such that personal identities can be recovered with the use of that parameter.
   - Pseudonymization: A form of de-identification in which direct identifiers are replaced with pseudonyms, allowing records referencing the same individual to be matched.

6. **List and define approaches to privacy-preserving data publishing.**

   Answer:

   - Suppression: Removes some of the QI values. The objective is to eliminate those QI values that have a higher risk of allowing re-identification of specific records.
   - Generalization: Involves transforming some QIs into less precise representations.
   - Perturbation: Replaces specific QI values with equally specific but different values.
   - Swapping: Exchanges QI values between records.

7. **Explain the differences between *k*-anonymity, *l*-diversity, and *t*-closeness.**

   Answer: A dataset provides *k*-anonymity protection if the information for each person contained in the dataset cannot be distinguished from at least *k* – *1* individuals whose information also appears in the dataset. A *k*-anonymous dataset satisfies *l*-diversity if, for each group of records sharing QI values, there are at least *l* distinct values for each confidential attribute. A *k*-anonymous dataset satisfies *t*-closeness if, for each group of records sharing QI values, the distance between the distribution of each confidential attribute within the group and the distribution of the attribute in the whole dataset is no more than a threshold *t*.

8. **What types of attacks are possible on summary tables?**

   Answer:

   - External attack: As an example of an external attack, consider a frequency table Ethnicity × Town that contains a single subject for ethnicity Ei and town Ti. Then if a magnitude table is released with the average blood pressure for each ethnicity and each town, the exact blood pressure of the only respondent with ethnicity Ei in town Ti is publicly disclosed.
   - Internal attack: If there are only two respondents for ethnicity Ei and town Ti, the blood pressure of each of them is disclosed to the other.

- Dominance attack: If one (or few) respondents dominate in the contribution to a cell in a magnitude table, the dominant respondent(s) can upper-bound the contributions of the rest. For example, if the table displays the cumulative earnings for each job type and town, and one individual contributes 90% of a certain cell value, that individual knows his or her colleagues in the town are not doing very well.

9. **List and define approaches to protecting privacy in frequency tables.**

   Answer:

   - Suppression: Cell suppression involves two steps: (1) Suppress all cells that meet the definition of sensitive (below the threshold). These are primary suppressions. (2) Suppress additional cells to prevent recovery of primary suppressions from marginal totals. These are secondary suppressions.
   - Random rounding: The value in each cell is randomly rounded up or down.
   - Controlled rounding: Involves random rounding, followed by an adjustment to some of the cell values so that all rows and columns add to the original row and column totals.
   - Controlled tabular adjustment: Modifies the values in the table to prevent inference of sensitive cell values within a prescribed protection interval.

10. **List and define approaches to protecting privacy online queryable databases.**

    Answer:

    - Query restriction: With query restriction, each query must pass through a series of filters that apply various disclosure limitation rules.
    - Response perturbation: Response perturbation modifies the response values to user queries while leaving the data in the microdata file untouched.

11. **What is differential privacy?**

    Answer: Differential privacy involves adding noise, or small random values, to response values.

Chapter 8 Review Questions

1. **What are the main elements of the online ecosystem for personal data?**

   Answer: Data collectors, data brokers, and data users.

2. **What security features are built into HTTPS?**

   Answer: Encryption, data integrity, and authentication.

3. **How does a web application firewall function?**

   Answer: A **web application firewall (WAF)** is a firewall that monitors, filters, or blocks data packets as they travel to and from a Web application. Running as a network appliance, server plug-in, or cloud service, the WAF inspects each packet and uses a rule base to analyze web application logic and filter out potentially harmful traffic.

4. **What are the main elements of the mobile app ecosystem?**

   Answer: Cellular and Wi-Fi infrastructure, public app stores, private app stores, device and OS vendor infrastructure, enterprise mobility management systems, and enterprise mobile services.

5. **List major security concerns for mobile devices.**

   Answer: Lack of physical security controls, use of untrusted mobile devices, use of untrusted networks, use of apps created by unknown parties, interaction with other systems, use of untrusted content, and use of location services.

6. **What is mobile app vetting?**

   Answer: The process of evaluation and approval or rejection of apps within an organization.

7. **List and briefly define major privacy risks for web applications.**

   Answer: Web app vulnerabilities; user-side data leakage; insufficient data breach response; insufficient deletion of personal data; non-transparent policies, terms, and conditions; collection of data not required for primary purpose; sharing of data with third party; outdated personal data; missing or insufficient session expiration; and insecure data transfer.

8. **What are some of the major privacy/security threats for the use of mobile apps?**

   Answer: Insecure network communications, web browser vulnerabilities, vulnerabilities in third-party libraries, and cryptographic vulnerabilities.

9. **What are the online privacy principles defined by the FTC?**

   Answer: Notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress.

10. **What are the elements and sub-elements of the FTC online privacy framework?**

    Answer:

    - Privacy by design: Principles and procedural protections.
    - Simplified choice for business and consumers: Practices that do not require choice, and practices that require choice.
    - Greater transparency: Privacy notices, consumer access to data, and consumer education.

11. **List and briefly describe the main factors that contribute to the ineffectiveness of current web privacy notices.**

    Answer:

    - Conflating requirements: Companies are faced with a number of requirements in the design of their online privacy notices. Users want clear, easy-to-understand, and brief statements about a company's privacy practices and privacy controls. Companies need to comply with legal and regulatory requirements concerning the content of the privacy notice, such as defined in Europe's General Data Protection Regulation (GDPR), the US Health Insurance Portability and Accountability Act (HIPAA), and the California Online Privacy Protection Act (CalOPPA). Additionally, companies use privacy notices to demonstrate compliance with privacy laws and regulations other than those related to the privacy notice itself, and in an attempt to limit liability by promising more than they are legally required to promise.
    - Lacking choices: Most privacy notices offer little choice, especially for mobile apps and IoT devices. Many websites and apps interpret user access as consent to use, regardless of whether the user has seen, read, and/or understood the privacy policy.
    - High burden/low utility: Most users are not willing to invest the time required to read and understand all the privacy notices they routinely encounter, much less take the time to make choices via user controls. This problem is compounded by the lack of user-friendliness and the lack of choices.
    - Decoupled notices: Privacy notices are generally separate from normal user interaction. Websites only link to a privacy policy at the bottom of the page; mobile apps link to a privacy policy in the app store or in some app submenu; and privacy policies for IoT devices are only available on the manufacturer's website.

12. **List and briefly define the dimensions of a privacy notice design space.**

    Answer: Timing (when it is presented), Channel (how it is presented), Modality (communication model used), and Control (how are the choices provided).

13. **Define the various types of cookies.**

    Answer:

    - Unidentified cookie: The only identifying information associated with the cookie is a unique ID assigned by the server.
    - Identified cookie: User information is associated with the cookie.
    - Session cookie: Remains on the user system only while the user has on open window to that website.
    - Persistent cookie: Includes an expiration date.

- First-party cookie: Set and read by the web server hosting the website the user is visiting.
- Third-party cookie: Belongs to a domain different from the one shown in the address bar.

Chapter 9 Review Questions

1. **Define *data loss prevention*.**

   Answer: Data loss prevention (DLP), also referred to as data leakage prevention, refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.

2. **Discriminate between data at rest, data in motion, and data in use.**

   Answer:

   - Data at rest: Data that resides in databases, file systems, and other structured storage methods.
   - Data in motion: Data that is moving through a network, including wireless transmission.
   - Data in use: Data in the process of being created, retrieved, updated, or deleted.

3. **Define the *Internet of Things*.**

   Answer: The term IoT refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors.

4. **List and briefly define the principal components of an IoT-enabled thing.**

   Answer:

   - Sensor: A sensor measures some parameter of a physical, chemical, or biological entity and delivers an electronic signal proportional to the observed characteristic, either in the form of an analog voltage level or a digital signal. In both cases, the sensor output is typically input to a microcontroller or other management element. Examples include temperature measurement, radiographic imaging, optical sensing, and audio sensing.
   - Actuator: An actuator receives an electronic signal from a controller and responds by interacting with its environment to produce an effect on some parameter of a physical, chemical, or biological entity. Examples include heating coils, cardiac electric shock delivery, electronic door locks, unmanned aerial vehicle operation, servo motors, and robotic arms.
   - Microcontroller: The “smart” in a smart device is provided by a deeply embedded microcontroller.

- Transceiver: A transceiver contains the electronics needed to transmit and receive data. Most IoT devices contain a wireless transceiver, capable of communication using Wi-Fi, ZigBee, or some other wireless protocol. By means of the transceiver, IoT devices can interconnect with other IoT devices, with the Internet, and with gateway devices to cloud systems.
- Power supply: Typically, this is a battery.

5. **Define *cloud computing*.**

   Answer: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

6. **List and briefly describe three cloud service models.**

   Answer:

   - Software as a service (SaaS): The capability provided to the consumer is to use the CSP's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser. Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains the same functions from the cloud service. SaaS saves the complexity of software installation, maintenance, upgrades, and patches.
   - Platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the CSP. PaaS often provides middleware-style services such as database and component services for use by applications. In effect, PaaS is an operating system in the cloud.
   - Infrastructure as a service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems.

7. **List and briefly define four cloud deployment models.**

   Answer:

   - Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The CSP is responsible both for the cloud infrastructure and for the control of data and operations within the cloud.

- Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. The CSP is responsible only for the infrastructure and not for the control.
- Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

8. **Describe some of the main cloud-specific security threats.**

   Answer:

   - Responsibility ambiguity: The enterprise-owned system relies on services from the CSP. The level of the service provided (SaaS, PaaS, IaaS) determines the magnitude of resources that are offloaded from IT systems on to the cloud systems. Regardless of the level of service, it is difficult to define precisely the security responsibilities of the customer and those of the CSP. If there is any ambiguity, this complicates risk assessment, security control design, and incident response.
   - Loss of governance: The migration of a part of the enterprises IT resources to the cloud infrastructure gives partial management control to the CSP. The degree of loss of governance depends on the cloud service model (SaaS, PaaS, IaaS). In any case, the enterprise no longer has complete governance and control of IT operations.
   - Loss of trust: It is sometimes difficult for a cloud service user to assess the CSP's trust level due to the black-box nature of the cloud service. There is no way to obtain and share the CSP's security level in a formalized manner. Furthermore, the cloud service users are generally unable to evaluate the security implementation level achieved by the CSP. This in turn makes it difficult for the customer to perform a realistic risk assessment.
   - Service provider lock-in: A consequence of the loss of governance could be a lack of freedom in terms of how to replace one CSP with another. An example of the difficulty in transitioning is if a CSP relies on proprietary hypervisors or virtual machine image formats, and does not provide tools to convert virtual machines to a standardized format.
   - Non-secure cloud service user access: As most of the resource deliveries are through remote connections, unprotected APIs (mostly management APIs and PaaS services) are among the easiest attack vectors. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities pose significant threats.

- Lack of asset management: The cloud service user may have difficulty in assessing and monitoring asset management by the CSP. Key elements of interest include location of sensitive asset/information, degree of physical control for data storage, reliability of data backup (data retention issues), and countermeasures for business continuity and disaster recovery. Furthermore, the cloud service users also have important concerns on exposure of data to foreign governments and on compliance with privacy laws.
- Data loss and leakage: This threat may be strongly related to lack of asset management. However, loss of an encryption key or a privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information, such as encryption keys, authentication codes and access privilege, will lead to sensitive damages, such as data loss and unexpected leakage to the outside.

Chapter 10 Review Questions

1. **Briefly differentiate between information security governance and information security management.**

   Answer:

   - Information security governance: The process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.
   - Information security management: The supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. Management of information security is expressed through the formulation and use of information security policies, procedures, and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

2. **List and describe the responsibilities of typical C-level executive positions.**

   Answer:

   - Chief executive officer (CEO): Responsible for the success or failure of the organization, overseeing the entire operation at a high level.
   - Chief operating officer (COO): Generally second in command to the CEO. Oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies that govern operations.
   - Chief information officer (CIO): In charge of information technology (IT) strategy and the computer, network, and third-party (e.g., cloud) systems required to support an enterprise's objectives and goals.

- Chief security officer (CSO) or chief information security officer (CISO): Tasked with ensuring data and systems security. In some larger enterprises, the two roles are separate, with a CSO responsible for physical security, while a CISO is in charge of digital security.
- Chief risk officer (CRO): Charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings. This role does not exist in most enterprises. It is most often found in financial service organizations. In enterprises in which a CRO is not present, organizational risk decisions may be decided by the CEO or board of directors.
- Chief privacy officer (CPO): Charged with developing and implementing policies designed to protect employee and customer data from unauthorized access.
- Chief counsel: Also called general counsel or chief legal officer (CLO). The chief lawyer in the legal department, responsible for overseeing and identifying the legal issues in all departments.

3. **List and describe the responsibilities of typical privacy positions.**

   Answer:

   - Chief privacy officer (CPO): Has the necessary authority to lead and direct the organization's privacy program, which involves the development and implementation of the organization's privacy policy.
   - Data protection officer (DPO): Has the responsibility to highlight any issues or concerns related to the organization's compliance with privacy regulations and laws.
   - Privacy counsel: An attorney who deals with legal matters related to privacy.
   - Privacy leader: Head of privacy compliance and operations and may be the most senior privacy official in the organization.
   - Privacy champion: Promotes a culture of privacy throughout the organization.

4. **What is a privacy program?**

   Answer: A privacy program consists of the management, operational, and technical aspects of protecting PII. It encompasses policies, procedures, and management structure and mechanisms for coordinating privacy activity.

5. **Briefly differentiate between privacy program plan, privacy plan, privacy policy, privacy notice, and acceptable use policy.**

   Answer:

   - Privacy program plan: Relates to the long-term goals for maintaining security for assets and to privacy governance.

- Privacy plan: Relates to security controls in place and planned to meet strategic privacy objectives.
- Privacy policy: Relates to the rules and practices that enforce privacy. Also referred to as a data protection policy. It is concerned with specifying the policies and procedures that regulate how employees and non-employed personnel conduct themselves in relation to PII handled by the organization.
- Privacy notice: Relates to the information provided concerning privacy protection to outside users. This document is often referred to as a privacy policy. To distinguish this document, this book uses the term privacy notice.
- Acceptable use policy: Relates to how users are allowed to use assets.

6. **Briefly describe the OASIS privacy management reference model.**

   Answer: OASIS has developed the Privacy Management Reference Model and Methodology, which is a methodology and analytic tool. The PMRM is in effect a detailed instruction manual for managing privacy by design. It is a step-by-step method of assuring that the system design process incorporates and satisfies privacy requirements.

7. **Briefly describe the OASIS privacy documentation for software engineers.**

   Answer: OASIS has published a specification for software engineers that translates the seven Privacy by Design (PbD) principles to conformance requirements for documentation, either produced or referenced.

Chapter 11 Review Questions

1. **What are the four factors that determine risk, and how are they related to each other?**

   Answer: Assets and threats determine impact. Threats, vulnerabilities, and existing controls determine likelihood. Impact and likelihood determine risk.

2. **Differentiate between qualitative and quantitative risk assessment.**

   Answer: Quantitative risk assessment uses specific numerical values to estimate costs and likelihoods. Qualitative risk assessment uses relative values such as low, medium, and high.

3. **Explain the term *residual risk*.**

   Answer: Any risk treatment plan can reduce but not eliminate risk. What remains is referred to as residual risk.

4. **Explain the steps in the NIST risk management framework.**

   Answer:

   - Categorize: Identify information that will be transmitted, processed, or stored by the system and define applicable levels of information categorization based on an impact analysis. The purpose of the categorization step is to guide and inform subsequent risk management processes and tasks by determining the adverse impact or consequences to the organization with respect to the compromise or loss of organizational assets—including the confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems. This is risk assessment.

- Select: Select an initial set of baseline security controls for the system based on the security categorization as well as tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- Implement: Implement security controls and document how the controls are employed within the system and its environment of operation.
- Assess: Assess the security controls using appropriate assessment procedures. Determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Authorize: Management officially authorizes a system to operate or continue to operate based on the results of the security control assessment. This decision is based on a determination of the risk to organizational operations and assets resulting from the operation of the system and the decision that this risk is acceptable.
- Monitor: Continuously monitor security controls to ensure that they are effective over time as changes occur in the system and the environment in which the system operates. This includes assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

5. **Describe the various risk treatment options.**

   Answer:

   - Risk reduction or mitigation: Actions taken to lessen the probability and/or negative consequences associated with a risk. Typically, an organization achieves risk reduction by selecting additional security controls.
   - Risk retention: Acceptance of the cost from a risk.
   - Risk avoidance: Decision not to become involved in, or action to withdraw from, a risk situation.
   - Risk transfer or sharing: Sharing with another party the burden of loss from a risk.

6. **What is the difference between privacy risk assessment and privacy impact assessment?**

   Answer: Privacy impact assessment consists of privacy risk assessment followed by privacy control selection.

7. **How do privacy impacts differ from information security impacts?**

   Answer: The principle concern with privacy impact is the harm to individuals, with a secondary concern with the cost to the organization. Security impact is concerned with the cost to the organization.

8. **What is privacy threshold analysis?**

   Answer: A privacy threshold analysis (PTA) is a brief assessment that requires system owners to answer basic questions on the nature of their systems and whether the systems contain PII, to identify systems that require a PIA.

9. **Describe recommended steps for preparing for a PIA.**

   Answer:

   - Identify the PIA team and provide it with direction: The privacy leader should have ultimate responsibility for the PIA. The privacy leader, together with other privacy personnel, should determine the scope of the PIA and the needed expertise. Depending on the size of the organization and the amount of PII involved, the team may need to include information security experts, a privacy counsel, operations managers, ethicists, business mission representatives, and others. The privacy leader or privacy team should define the risk criteria and ensure that senior management approves those criteria.
   - Prepare a PIA plan: The person in charge of the PIA (the PIA assessor) should create a plan that specifies human resources, business case, and budget for conducting the PIA.
   - Describe the system or project that is the subject of this PIA: This description should include an overview of the system or project, summarizing the system design, personnel involved, schedule, and budget. The description should focus on what PII are processed. The PII discussion should indicate what PII is collected/processed, the objectives, which PII principals are affected, what systems and processes are involved in the handling of PII, and what privacy policies govern the handling of the PII.
   - Identify stakeholders: The assessor should indicate those who are or might be interested in or affected by the project, technology, service.

10. **What should go into a PIA report?**

    Answer:

    - Clarify whether the PIA was initiated early enough so that there was still time to influence the outcome.
    - Identify who conducted the PIA.
    - Include a description of the project to be assessed, its purpose, and any relevant contextual information.

- Map the information flows (i.e., how information is to be collected, used, stored, secured, and distributed, and to whom and how long the data is to be retained).
- Check the project's compliance against relevant legislation.
- Identify the risks to or impacts on privacy.
- Identify solutions or options for avoiding or mitigating the risks.
- Make recommendations.
- Be published on the organization's website and be easily found there or, if the PIA report is not published (even in a redacted form), there should be an explanation as to why it has not been published.
- Identify what consultation with which stakeholders was undertaken.

Chapter 12 Review Questions

1. **What are the four levels of Cyber Security learning continuum?**

   Answer: Awareness, cybersecurity essentials, role-based training, education/certification.

2. **Briefly explain the difference between privacy awareness and privacy culture.**

   Answer: Privacy awareness is the extent to which staff understand the importance of information privacy; the level of privacy required for personal information stored and processed by the organization; and their individual privacy responsibilities. Privacy culture is the extent to which staff demonstrates expected privacy behavior in line with their individual privacy responsibilities and the level of privacy required for personal information stored and processed by the organization.

3. **Differentiate between malicious behavior, negligent behavior, and accidental behavior.**

   Answer:

   - Malicious behavior: Involves a combination of motive to cause harm and a conscious decision to act inappropriately (e.g., copying business files before taking employment with a competitor, leaking sensitive information, misusing information for personal gain).
   - Negligent behavior: Does not involve a motive to cause harm but does involve a conscious decision to act inappropriately (e.g., using unauthorized services or devices to save time, increase productivity, or enable remote working).
   - Accidental behavior: Does not involve a motive to harm or a conscious decision to act inappropriately (e.g., emailing sensitive information to the wrong/unauthorized recipients, opening malicious email attachments, or publishing personal information on publicly available servers).

4. **What topics should be covered by a privacy awareness program?**

   Answer:

   - Provide a focal point and a driving force for a range of awareness, training, and educational activities related to information privacy, some of which might already be in place but perhaps need to be better coordinated and more effective.
   - Communicate important recommended guidelines or practices required to protect PII.
   - Provide general and specific information about information privacy risks and controls to people who need to know.
   - Make individuals aware of their responsibilities in relation to information privacy.
   - Motivate individuals to adopt recommended guidelines or practices.
   - Privacy awareness programs should be driven by risk considerations. For example, risk levels can be assigned to different groups of individuals based on their job function, level of access to assets, access privileges, and so on.
   - The awareness program should provide employees with an understanding of the different types of inappropriate behavior—namely, malicious, negligent, accidental—and how to avoid negligent or accidental unwanted behavior and recognize malicious behavior in others.
   - Create a stronger culture of privacy, one with a broad understanding and commitment to information privacy.
   - Help enhance the consistency and effectiveness of existing information privacy controls and potentially stimulate the adoption of cost-effective controls.
   - Help minimize the number and extent of information privacy breaches, thus reducing costs directly (e.g., data damaged by viruses) and indirectly (e.g. reduced need to investigate and resolve breaches).

5. **What are some tools used to impact awareness training?**

   Answer: Events, such as a privacy awareness day; promotional materials; briefings (program-, system-, or issue-specific); and rules of behavior.

6. **What topics should be covered by a cybersecurity essentials program?**

   Answer:

   - Technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges.
   - Common information and computer system security vulnerabilities.
   - Common cyberattack mechanisms, their consequences, and motivation for use.
   - Different types of cryptographic algorithms.

- Intrusion, types of intruders, techniques, and motivation.
- Firewalls and other means of intrusion prevention.
- Vulnerabilities unique to virtual computing environments.
- Social engineering and its implications to cybersecurity.
- Fundamental security design principles and their role in limiting point of vulnerability.

7. **What is role-based training?**

   Answer: Role-based training is intended for all users, privileged and non-privileged, who have some role with respect to IT systems and applications. In this context, the term role refers to the responsibility and functions that a person is performing within their organization. Role-based privacy training allows employees in different roles, such as human resources and IT, to receive education tailored to their specialties.

8. **Explain the concept of an acceptable use policy.**

   Answer: An acceptable use policy applies to all employees and defines responsibilities and acceptable use of IT systems.

Chapter 13 Review Questions

1. **Differentiate between a security event and security incident.**

   Answer:

   - Security event: An occurrence considered by an organization to have potential security implications to a system or its environment. Security events identify suspicious or anomalous activity. Events sometimes provide indication that an incident is occurring.
   - Security incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

2. **For security event logging, what events should be captured in operating system logs, network device logs, and web server logs?**

   Answer:

   - Operating system logs: Successful user logon/logoff; failed user logon; user account change or deletion; service failure; password changes; service started or stopped; object access denied; object access changed.
   - Network device logs: Traffic allowed through firewall; traffic blocked by firewall; bytes transferred; protocol usage; detected attack activity; user account changes; administrator access.

- Web server logs: Excessive access attempts to non-existent files; code (SQL, HTML) seen as part of the URL; attempted access to extensions not implemented on the server; web service stopped/started/failed messages; failed user authentication; invalid request; internal server error.

3. **What information should a privacy event log record?**

   Answer:

   - Which PII was accessed.
   - Which PII principals' PII was accessed.
   - What action was performed (e.g., read, print, add, modify, transmit, delete) as a result of the event.
   - When the action occurred.
   - Who is the individual responsible for the action.
   - What level of privileged access, if any, was used (e.g., by system administrators or operators).

4. **What are key objectives for a security audit?**

   Answer:

   - Allows the adequacy of the security policy to be evaluated.
   - Aids in the detection of security violations.
   - Facilitates making individuals accountable for their actions (or for actions by entities acting on their behalf).
   - Assists in the detection of misuse of resources.
   - Acts as a deterrent to individuals who might attempt to damage the system.

5. **Define the terms *security audit* and *security audit trail*.**

   Answer:

   - Security audit: An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.
   - Security audit trail: A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

6. **What do you understand by external security audit? What should be its key objectives?**

   Answer: External audits are carried out by someone from outside the organization. The objectives of the external security audit should be to:

   - Assess process of internal audit.
   - Determine the commonality and frequency of recurrence of various types of security violation.
   - Identify the common causes.
   - Provide advisory and training inputs to tackle the neglect of procedures.
   - Review and update the policy.

7. **What topics should be covered by a privacy audit checklist?**

   Answer: Preliminary work, information collected from users, security issues, privacy policy assessment.

8. **List and describe the privacy-specific controls that are part of the SP 800-53 audit and accountability control set.**

   Answer:

   - AU-3 Content of Audit Records: The control enhancement AU-3(3) deals with limiting PII elements in the content of audit records. The organization should specifically list what elements may be recorded in an audit record. The AU-3(3) guidance in this regard is as follows: Limiting PII in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.
   - AU-11 Audit Record Retention: The organization should specify a time period for retaining audit records to provide support for after-the-fact investigations of security and privacy incidents and to meet regulatory and organizational information retention requirements.
   - AU-12 Audit Generation: The control enhancement AU-12(4) deals with query parameter audits of PII, expressed as: Provide and implement the capability for auditing the parameters of user query events for datasets containing PII. Query parameters are explicit criteria that a user or automated system submits to a system to retrieve data. Auditing of query parameters within systems for datasets that contain personally identifiable information augments an organization's ability to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.
   - AU-16 Cross-Organizational Audit: The organization should employ organization-defined methods for coordinating organization-defined audit information among external organizations when audit information is transmitted across organizational boundaries. Maintaining the identity of individuals who requested specific services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance and privacy ramifications.

9. **What should be the objectives for information privacy incident management?**

   Answer:

   - Detect privacy-related events and deal with them efficiently; in particular, deciding when they should be classified as privacy breaches.
   - Assess and respond to identified privacy breaches in the most appropriate and efficient manner.
   - Minimize the adverse effects of privacy breaches on the organization and its operations by appropriate controls as part of incident response.
   - Coordinate with relevant elements from crisis management and business continuity management through an established escalation process.
   - Assess and mitigate information privacy vulnerabilities to prevent or reduce incidents.
   - Quickly learn from information privacy incidents, vulnerabilities, and their management. This feedback mechanism is intended to increase the chances of preventing future information privacy incidents from occurring, improve the implementation and use of information privacy controls, and improve the overall information privacy incident management plan.

10. **Describe the four phases of the incident management process.**

    Answer:

    - Preparation: Select the right staff and developing a plan.
    - Detection and analysis: Determine whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.
    - Containment, eradication, and recovery: Contain the incident, eliminate the threat, and recover from the incident.
    - Post-incident activity: Conduct an evaluation process and take remedial action.

11. **What skills and training are important for selecting members of a PIRT?**

    Answer: Members of the team should be selected with the following background/skill sets:

    - Understanding of known threats, attack signatures, and vulnerabilities.
    - Understanding of the enterprise network, security infrastructure, and platforms.
    - Experience in privacy breach response and/or troubleshooting techniques.
    - Experience in forensic techniques and best practices.
    - Understanding of regulations and laws as they pertain to privacy and disclosure and evidentiary requirements.
    - Understanding of systems, threats and vulnerabilities, and remediation methods in their area of business responsibility.

12. **What topics should be covered by a privacy incident response plan?**

    Answer: Privacy incident response team, applicable privacy compliance documents, information sharing to respond to a breach, reporting requirements, risk assessment, mitigation, notification.

13. **What factors should be considered in assessing the severity of a privacy breach?**

    Answer:

    - Nature and sensitivity of the PII potentially compromised by the breach, including the potential harms that an individual could experience from the compromise of that type of PII.
    - Likelihood of access and use of PII, including whether the PII was properly encrypted or rendered partially or completely inaccessible by other means.
    - Type of breach, including the circumstances of the breach, as well as the actors involved and their intent.
    - Impact on the organization, including legal liability, financial liability, and reputational harm.

Chapter 14 Review Questions

1. **What is the difference between a natural person and a legal person?**

   Answer: A natural person is a human being. A legal person is a non-human entity—such as a corporation, partnership, or sole proprietorship—that is recognized as having privileges and obligations, such as the ability to enter into contracts, to sue, and to be sued. Sometimes the term legal person encompasses natural persons as well as non-human entities, but GDPR limits the term legal person to non-human entities.

2. **What is the difference between a controller and a processor?**

   Answer:

   - Controller: The natural or legal person, public authority, agency, or other body that determines the purposes and means of processing personal data, regardless of whether or not such data are collected, stored, processed, or disseminated by that party or by an agent on its behalf.
   - Processor: The natural or legal person, public authority, agency, or other body responsible for processing personal data on behalf of and in accordance with the instructions of a controller. The controller and the processor may be the same entity.

3. **List some of the key responsibilities of a DPO.**

   Answer:

   - Assist the controller or the processor to monitor internal compliance with the GDPR.
   - Provide advice where requested as regards to the data protection impact assessment and monitor its performance.
   - Cooperate with the supervisory authority and act as a contact point. A supervisory authority is a government entity with the authority to enforce the GDPR.
   - Prioritize their activities and focus their efforts on issues that present higher data protection risks.
   - Create inventories and hold a register of processing operations based on information provided to them by the various departments in their organization responsible for the processing of personal data.

4. **What is the difference between an article and a recital in the GDPR?**

   Answer: The articles are the specific rules set forth in the regulation. The recitals provide commentary and additional explanation.

5. **List and briefly describe the main objectives of the GDPR.**

   Answer:

   - Provide the fundamental right to the protection of personal data for every individual.
   - Harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.
   - Balance privacy rights against other fundamental rights, in accordance with the principle of proportionality.
   - Define a strong and more coherent data protection framework in the EU, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market.
   - Enable natural persons, to the extent possible, to have control of their own personal data.
   - Ensure consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data throughout the Union.

- Strengthen and set out in detail the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.
- Take account of the specific needs of micro, small, and medium-sized enterprises in the application of the GDPR.

6. **Explain the concepts of material scope and territorial scope.**

   Answer: The actions covered by a particular law or regulation. In the context of this chapter, material scope refers to the types of processing of personal data that are covered by the GDPR. Territorial scope refers to the jurisdictional reach of a law or regulation. In the context of this chapter, territorial scope refers to what physical locations of enterprises and data subjects are covered by the GDPR.

7. **List and briefly describe the GDPR principles.**

   Answer:

   - Fair, lawful, and transparent processing: The requirement to process personal data fairly and lawfully is extensive. It includes, for example, an obligation to tell data subjects what their personal data will be used for.
   - Purpose limitation: Personal data collected for one purpose should not be used for a new, incompatible, purpose. Further processing of personal data for archiving, scientific, historical, or statistical purposes is permitted, subject to appropriate laws and regulations.
   - Data minimization: Subject to limited exceptions, an organization should only process the personal data it actually needs to process in order to achieve its processing purposes.
   - Accuracy: Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data are either erased or rectified without delay.
   - Storage limitation: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Data subjects have the right to erasure of personal data, in some cases sooner than the end of the maximum retention period.
   - Integrity and confidentiality: Technical and organizational measures must be taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access.
   - Accountability: The controller is obliged to demonstrate that its processing activities are compliant with the Data Protection Principles.

8. **Explain the concept of fairness in the GDPR.**

   Answer: In general, processing that may cause injury to an individual or group of individuals may be unfair.

9. **List and briefly describe rights of data subjects enumerated in the GDPR.**

   Answer:

   - The right to be informed where personal data are collected from the data subject: The controller shall, at the time when personal data are obtained, provide the data subject with information about the collection and use of the subject's personal data, including identity and the contact details of the controller; contact details of the data protection officer; purposes of the processing for which the personal data are intended as well as the legal basis for the processing; recipients or categories of recipients of the personal data, if any; where applicable, the fact that the controller intends to transfer personal data to a third country or international organization, with reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

   - The right to be informed where personal data have not been collected from the data subject: The controller must provide the same information as listed in the preceding bullet within a reasonable time period of obtaining the personal data from another source.

   - The right of access by the data subject: The controller must allow a data subject access to personal data held by the controller. The GDPR requires the responses be within a month, generally without charge, and with additional information, such as data retention periods.

   - The right to rectification: Individuals have the right to have inaccurate personal data corrected, or completed if it is incomplete.

   - The right to erasure (right to be forgotten): Individuals have the right to have their personal data erased, subject to certain restrictions.

   - The right to restrict processing: Individuals have the right to request the restriction or suppression of their personal data. Methods by which to restrict the processing of personal data could include temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.

   - The right to data portability: The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.

- The right to object: The data subject has the right to object, on grounds relating to his or her situation, at any time to processing of personal data concerning him or her. The controller cannot process unless demonstrating legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject.
- Rights in relation to automated decision making and profiling: Profiling involves (a) automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. Specific examples include: analyzing or predicting aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. An organization can only carry out this type of decision-making where the decision is either:

  —Necessary for the entry into or performance of a contract; or

  —Authorized by Union or Member state law applicable to the controller; or

  —Based on the individual's explicit consent

10. **What is the difference between data protection by design and data protection by default?**

    Answer:

    - Data protection by design: The controller shall implement appropriate technical and organizational measures, both at the design phase of the processing and at its operation, that satisfy the requirements articulated in the data protection principles. De-identification is an example of a technical measure; privacy awareness is an example of an organizational measure.
    - Data protection by default: The technical and organizational measures should assure that, by default, only personal data that are necessary for each specific purpose of the processing are processed.

11. **What is meant in the GDPR by the term *processing on a large scale*?**

    Answer: An organization should consider the following factors in determining whether processing is on a large scale:

    - The number of data subjects concerned, either as a specific number or as a proportion of the relevant population.
    - The volume of data and/or the range of different data items being processed.
    - The duration, or permanence, of the data processing activity.
    - The geographical extent of the processing activity.

12. **Distinguish between the concepts of risk and high risk.**

    Answer: Risk is a combination of impact or privacy harm and likelihood. High risk is a subjective concept that indicates that either the impact, or the likelihood, or both are significant.

13. **List and briefly describe the key steps in carrying out a DPIA.**

    Answer:

    - Description of the envisaged processing: This is a systematic description of the processing operation and its purposes. This should include the following:

      —A description of how the organization will collect, use, store, and delete personal data and whether personal data will be shared with third parties. A useful way to describe the processing is a flow diagram, as described in Chapter 11 of this book.

      —A definition of the scope of the processing, including the nature of the personal data, how much will be collected and processed, how long it will be stored, and how many individuals will be affected.

    - Assessment of the necessity and proportionality: This is a justification of the details of the processing operation in relation to the purposes.
    - Measures already envisaged: This documents the security and privacy controls already planned for this processing.
    - Assessment of the risks: This is a risk assessment that considers impact and likelihood. Chapter 11 of this book addresses this process in detail.
    - Measures envisaged to address the risk: This is a risk treatment plan, which documents the security and privacy controls used to mitigate the risks. The treatment plan should document how the controls ensure the protection of personal data and comply with the GDPR.
    - Documentation: The summary should include a complete description of the risk treatment plan, a description of residual risks, and a summary of DPO advice, if any.
    - Monitoring and review: The DPO should monitor the DPIA process and the controller should carry out a review to assess if processing is performed in accordance with the data protection impact assessment.

Chapter 15 Review Questions

1. **What are some of the key differences between the information privacy environment in the United States and that in the European Union?**

   Answer: The U.S. privacy landscape consists of a variety of federal and state privacy laws and regulations, some dating back to the 1970s, as well as common law created by judicial precedent. The EU depends upon a single regulation, the GDPR, which is common across all member states, each of which has a single supervisory authority or data protection authority to monitor and enforce the regulation.

2. **Briefly describe the privacy aspects of the Fair Credit Reporting Act.**

   Answer: FCRA details the information that consumer credit reports may contain and how and by whom a consumer's credit information can be used.

3. **Briefly describe the privacy aspects of the Fair and Accurate Credit Transactions Act.**

   Answer: Requires entities engaged in certain kinds of consumer financial transactions to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft.

4. **Briefly describe the privacy aspects of the Right to Financial Privacy Act.**

   Answer: Entitles bank customers to a limited expectation of privacy in their financial records by requiring that law enforcement officials follow certain procedures before information can be disclosed. Unless a customer consents in writing to the disclosure of his financial records, a bank may not produce such records for government inspection unless ordered to do so by an administrative or judicial subpoena or a lawfully executed search warrant.

5. **Briefly describe the privacy aspects of the Family Educational Rights and Privacy Act.**

   Answer: Protects students and their families by ensuring the privacy of student educational records, while ensuring a parent's rights to access his or her child's education records, correct mistakes in those records, and know who has requested or obtained the records. Educational records are agency- or institution-maintained records containing personally identifiable student and educational data. FERPA applies to primary and secondary schools, colleges and universities, vocational colleges, and state and local educational agencies that receive funding under any program administered by the U.S. Department of Education.

6. **What are the main goals of HIPAA?**

   Answer:

   - Mandate continuous health insurance coverage for workers who lose or change their job.
   - Reduce the administrative burdens and cost of healthcare by standardizing the electronic transmission and protection of healthcare-related administrative and financial transactions.

7. **What is the HIPAA Privacy Rule?**

   Answer: Officially known as the Standards for Privacy of Individually Identifiable Health Information, this rule requires safeguards to protect the privacy of patient data by setting limits and conditions on what information can be used and disclosed without patient authorization.

8. **To what categories of personal health information does HIPAA apply?**

   Answer: The HIPAA Privacy Rule protects most individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral. Individually identifiable health information, also referred to as protected health information (PHI), is information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan employer, or health care clearinghouse.
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

   (i) That identifies the individual; or

   (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

9. **Under what circumstance may a HIPAA covered entity use or disclose PHI?**

   Answer: A covered entity is required to disclose PHI under one of the following conditions:

   - The individual who is the subject of the information (or the individual's personal representative) authorizes in writing.
   - HHS is undertaking a compliance investigation or review or enforcement action.
   - A covered entity is permitted to use or disclose PHI without an individual's authorization for the following purposes or situations:

     —To the individual

     —Treatment, payment, and health care operations

     —Opportunity to agree or object

     —Incident to an otherwise permitted use and disclosure

     —Public interest, law enforcement, and benefit activities

     —Limited dataset for the purposes of research, public health or health care operations, where direct identifiers relating to individuals, their families, and employers are removed

10. **Describe the two methods of de-identification permitted under HIPAA.**

    Answer:

    - Expert determination method: A person who is technically qualified applies de-identification or anonymization techniques and determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information.
    - Safe harbor method: Involves the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

11. **Under the HITECH Act, what risk assessment factors must a covered entity take into account in determining whether a breach notification is needed?**

    Answer:

    - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
    - The unauthorized person who used the PHI or to whom the disclosure was made.
    - Whether the PHI was actually acquired or viewed.
    - The extent to which the risk to the PHI has been mitigated.

12. **Describe the technical measures mandated by the HITECH Act for the protection of data at rest.**

    Answer:

    - Full disk encryption: Encrypts the entire disk, except for software needed to boot the disk. This scheme uses an authentication method to enable booting. Once the device is booted, there is no protection of the data.
    - Virtual disk encryption: Encrypts the contents of a container, which are protected until the user is authenticated for the container.
    - Volume encryption: The same protection as virtual disk encryption, but for a volume instead of a container.
    - File/folder encryption: Protects the contents of encrypted files (including files in encrypted folders) until the user is authenticated for the files or folders.

13. **Describe the technical measures mandated by the HITECH Act for the protection of data in motion.**

    Answer:

    - Transport Layer Security (TLS): TLS is designed to make use of the Transmission Control Protocol (TCP) to provide a reliable end-to-end secure service. TLS is a complex protocol that allows users to authenticate each other and to employ encryption and message integrity techniques across a transport connection. SP 800–52 (Guidelines for the Selection and Use of Transport Layer Security Implementations) is the NIST specification.
    - Virtual private networks (VPN) using IPsec: A VPN is a private network that is configured within a public network (a carrier's network or the Internet) in order to take advantage of the economies of scale and management facilities of large networks. VPNs are widely used by enterprises to create wide area networks that span large geographic

areas, to provide site-to-site connections to branch offices, and to allow mobile users to dial up their company LANs. From the point of view of the provider, the pubic network facility is shared by many customers, with the traffic of each customer segregated from other traffic. Traffic designated as VPN traffic can only go from a VPN source to a destination in the same VPN. It is often the case that encryption and authentication facilities are provided for the VPN. IPsec is a set of Internet standards that augment the Internet Protocol (IP) and enable the development of VPNs at the IP level. SP 800–77 (Guide to IPsec VPNs) is the NIST specification.

- Virtual private networks (VPN) using TLS: An TLS VPN consists of one or more VPN devices that users connect to using their Web browsers. The traffic between the Web browser and TLS VPN device is encrypted with the TLS protocol. TLS VPNs provide remote users with access to Web applications and client/server applications, and with connectivity to internal networks. They offer versatility and ease of use because they use the SSL protocol that is included with all standard Web browsers, so the client usually does not require configuration by the user. SP 800–113 (Guide to SSL VPNs) is the NIST Specification.

14. Describe the three technical measures authorized by the HITECH Act for media sanitization.

Answer:

- Clear: Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- Purge: Applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques. This can be achieved by performing multiple overwrites. For a self-encrypting drive, cryptographic erasure can be used. If the drive automatically encrypts all user-addressable locations, then all that is required is to destroy the encryption key, which could be done by multiple overwrites.
- Destroy: Renders target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data. Typically the medium is pulverized or incinerated at an outsourced metal destruction or licensed incineration facility.

15. How is PII defined for the purposes of COPPA?

Answer: The law defines personal information as any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

16. **What are the main requirements imposed by COPPA?**

    Answer: CCPA lists the following as the enforceable consumer rights with respect to their personal information:

    - The right of Californians to know what personal information is being collected about them.
    - The right of Californians to know whether their personal information is sold or disclosed and to whom.
    - The right of Californians to say no to the sale of personal information.
    - The right of Californians to access their personal information.
    - The right of Californians to equal service and price, even if they exercise their privacy rights.