Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 4 of the official CISSP study guide. Here are the top things that you need to know from this chapter on laws, regulations and compliance. Understand the differences between criminal law, civil law and administrative law.

Criminal law protects society against acts that violate the basic principles we believe in. Violations of criminal law are prosecuted by federal and state governments, civil law provides the framework for disputes between people or the transaction of business between people and organizations, violations of civil law are brought to the court and argued by the two affected parties, administrative laws are used by government agencies to effectively carry out their day-to-day business.

Be able to explain the basic provisions of the major laws designed to protect society against computer crime. The Computer Fraud and Abuse Act as amended protects computers used by the government or an interstate commerce from a variety of abuses. The Electronic Communications Privacy Act ECPA makes it a crime to invade the electronic privacy of an individual. Know the differences among copyrights, trademarks, patents and trade secrets.

Copyrights protect original works of authorship such as books, articles, poems and songs. Trademarks are names, slogans, and logos that identify a company, product or service. Patents provide protection to the creators of new inventions. Trade secret law protects the operating secrets of a firm. Be able to explain the basic provisions of the Digital Millennium Copyright Act of 1998. The Digital Millennium Copyright Act prohibits the circumvention of copy protection mechanisms placed in digital media and limits the liability of internet service providers for the activity of their users.

Know the basic provisions of the Economic Espionage Act of 1996. The Economic Espionage Act provides penalties for individuals found guilty of the theft of trade secrets. Harsher penalties apply when the individual knows that the information will benefit a foreign government. Understand the various types of software license agreements. Perpetual licenses allow indefinite use after a one-time fee, while subscription licenses are time bound with recurring fees. Open source licenses offer usage freedom with conditions and enterprise agreements provide licenses for large organizations. End-user license agreements to find user rights and restrictions.

Concurrent licenses set simultaneous user limits and named user licenses tie to specific users. Click-through agreements require active consent during installation and cloud service licenses pertain to online services with terms presented upon registration. Understand the notification requirements placed on organizations that experience a data breach. California's SB 1386 implemented the first statewide requirement to notify individuals of a breach of their personal information. All other states eventually followed suit with similar laws. Currently, federal law only requires the notification of individuals when a HIPAA covered entity breaches their protected health information.

Understand the major laws that govern privacy of personal information in the United States, the European Union, Canada, China and South Africa. The United States has a number of privacy laws that affect the government's use of information, as well as the use of information by specific industries such as financial services companies and healthcare organizations that handle sensitive information. The EU has a more comprehensive general data protection regulation that governs the use and exchange of personal information.

In Canada, the Personal Information Protection and Electronic Documents Act governs the use of personal information. China includes privacy protections in the Personal Information Protection Law, while South Africa's are embedded in the Protection of Personal Information Act. Explain the importance of a well-rounded compliance program.

Most organizations are subject to a wide variety of legal and regulatory requirements related to information security. Building a compliance program ensures that you become and remain compliant with these often overlapping requirements. Know how to incorporate security into the procurement and vendor governance process. The expanded use of cloud services by many organizations requires added attention to conducting reviews of information security controls during the vendor selection process and as part of ongoing vendor governance. Be able to determine compliance and other requirements for information protection.

Cybersecurity professionals must be able to analyze a situation and determine what laws and jurisdictions apply. They must be able to identify relevant contractual, legal, regulatory and industry standards and interpret them for their given situation. Know legal and regulatory issues and how they pertain to information security. Understand the concepts of cyber crime and data breaches and be able to apply them in your environment when incidents arise.

Understand what licensing and intellectual property protections apply to your organization's data and your obligations when encountering data belonging to other organizations. Understand the privacy and export control issues associated with transferring information across international borders. Those are the study essentials that you'll need to know for Chapter 4 Laws, Regulations and Compliance.

From:
https://www.trident365.com/ - 三叉戟

Permanent link:
https://www.trident365.com/doku.php?id=projects:cissp:chapter4

Last update: **2025/05/18 17:14**