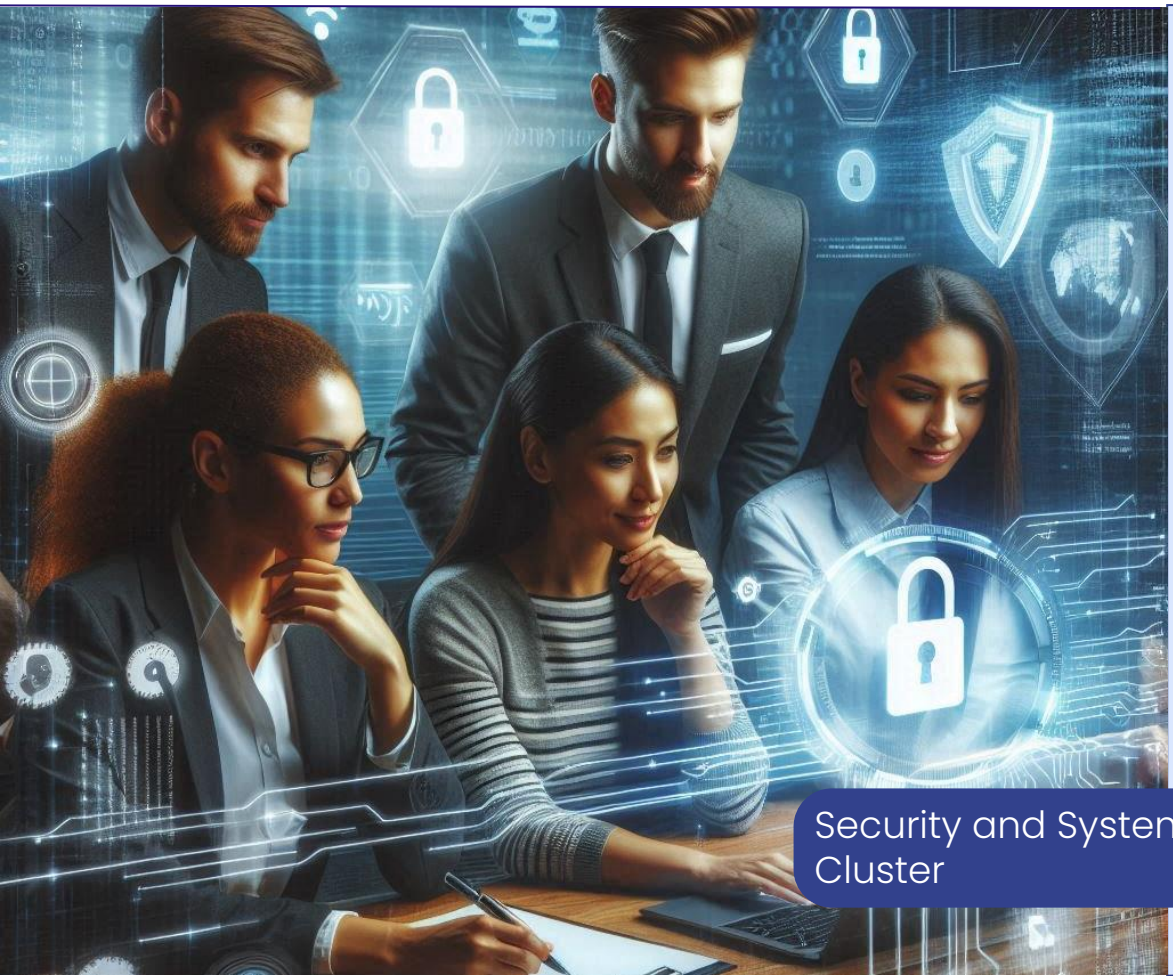
NATIONAL UNIVERSITY
COLLEGE OF COMPUTING AND
INFORMATION TECHNOLOGIES

VER 1.0

COURSE MANUAL

INFORMATION ASSURANCE AND SECURITY

This course provides students with the theoretical knowledge and practical skills in the implementation of Information Assurance and Security providing relevant solutions for security hardening and information protection through computer vulnerability assessment, secure coding, and computer security hardening techniques.



BS – COMPUTER SCICENCE

BS – INFORMATION TECHNOLOGY

Security and System Administration Cluster

MODULE 2

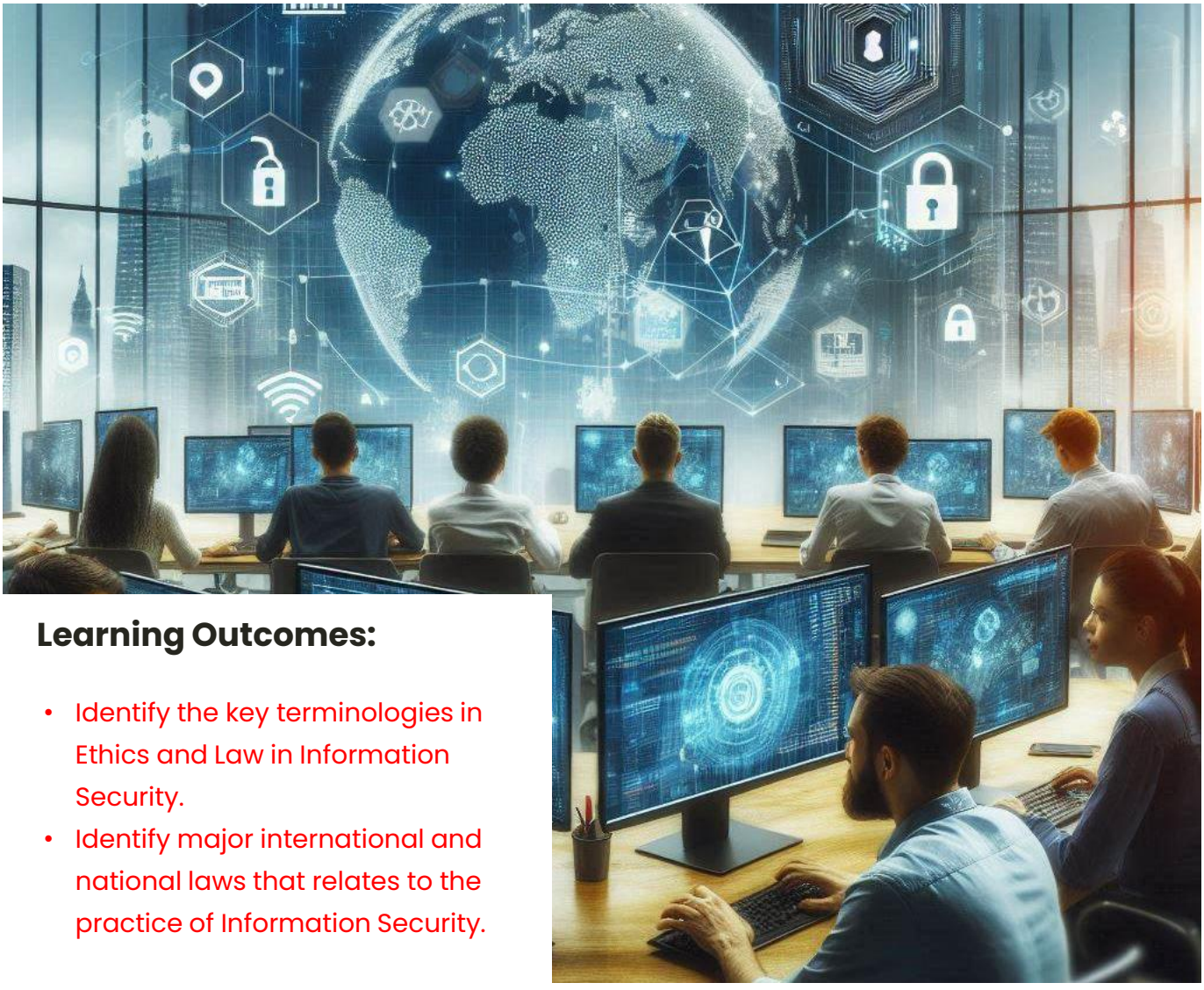
LEGAL, ETHICAL, AND PROFESSIONAL ISSUES

Table of Contents

Lesson Topics

LESSON 1

Laws and Ethics in Information Security



Learning Outcomes:

- Identify the key terminologies in Ethics and Law in Information Security.
- Identify major international and national laws that relates to the practice of Information Security.

Understanding Law and Ethics in Information Security

As a future information security professional, or an IT professional with security responsibilities, you must understand the scope of an organization's legal and ethical responsibilities. The information security professional plays an important role in an organization's approach to managing responsibility and liability for privacy and security risks. In modern litigious societies around the world, laws are sometimes enforced in civil courts, where large damages can be awarded to plaintiffs who bring suits against organizations. Sometimes these damages are punitive—a punishment assessed as a deterrent to future transgressions. To minimize liability and reduce risks from electronic and physical threats, and to reduce all losses from legal action, information security practitioners must thoroughly understand the current legal environment, stay current with laws and regulations, and watch for new and emerging issues. By educating the management and employees of an organization on their legal and ethical obligations and the proper use of information technology and information security, security professionals can help keep an organization focused on its primary business objectives.

In the first part of this module, you will learn about the legislation and regulations that affect the management of information in an organization. In the second part, you will learn about the ethical issues related to information security, and about several professional organizations with established codes of ethics. Use this chapter both as a reference to the legal aspects of information security and as an aid in planning your professional career.

Law and Ethics in Information Security

As individuals we elect to trade some aspects of personal freedom for social order. **Laws** are rules adopted for determining expected behavior in modern society and are drawn from **ethics**, which define socially acceptable behaviors. Ethics in turn are based on **cultural mores**: fixed moral attitudes or customs of a group. Some ethics are recognized as universal among cultures.

Organizational Liability and the Need for Counsel

Liability includes the legal obligation to make **restitution** for wrongs committed. The bottom line is that if an employee performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action, regardless of whether the employer authorized the act. An organization increases its liability if it refuses to take measures known as **due care** (or a standard of due care). Similarly, **due diligence** requires that an organization make a valid attempt to continually maintain this level of effort. Whereas due care means the organization acts legally and ethically, due diligence means it ensures compliance with this level of expected behavior. Given the Internet's global reach, those who could be injured or wronged by an organization's employees might live anywhere in the world. Under the U.S. legal system, any court can assert its authority over an individual or organization if it can establish **jurisdiction**. This is sometimes referred to as **long-arm jurisdiction** when laws are stretched to apply to parties in distant locations.

Policy Versus Law

Within an organization, information security professionals help maintain security via the establishment and enforcement of policies. The difference between a policy and a law, however, is that ignorance of a policy is an acceptable defense. Thus, for a policy to become enforceable, it must meet the following five criteria:

- **Dissemination (distribution)**: The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee.
- **Review (reading)**: The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for employees who are illiterate, reading-impaired, and unable to read English.
- **Comprehension (understanding)**: The organization must be able to demonstrate that the employee understands the requirements and content of the policy

- **Compliance (agreement)**: The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation.
- **Uniform enforcement**: The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Types of Law

Several categories of law affect organizations and their employees. Some of the more relevant categories include the following:

- **Civil law** comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizations and people.
- **Criminal law** addresses activities and conduct harmful to society, and is actively enforced by the state. Law can also be categorized as private or public.
- **Private law** encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations.
- **Public law** regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

Relevant U.S. Laws

Historically, the United States has been a leader in the development and implementation of information security legislation to prevent misuse and exploitation of information and information technology. Information security legislation contributes to a more reliable business environment, which in turn enables a stable economy. In its global leadership capacity, the United States has demonstrated a clear understanding of the importance of securing information and has specified penalties for people and organizations that breach U.S. civil statutes.

General Computer Crime Laws

Several key laws are relevant to the field of information security and are of particular interest to those who live or work in the United States. The **Computer Fraud and Abuse Act of 1986** (CFA Act or CFAA) is the cornerstone of many computer-related federal laws and enforcement efforts. It was originally written as an extension and clarification to the **Comprehensive Crime Control Act of 1984**.

The CFAA was amended by the **National Information Infrastructure Protection Act of 1996**, which modified several sections of the previous act and increased the penalties for selected crimes. The punishment for offenses prosecuted under this statute includes fines, imprisonment of up to 20 years, or both. The severity of the penalty depends on the value of the information obtained and whether the offense is judged to have been committed for the following reasons:

- For purposes of commercial advantage
- For private financial gain
- In furtherance of a criminal act

The preceding law and many others were further modified by the **USA PATRIOT Act of 2001**, which provides law enforcement agencies with broader latitude to combat terrorism-related activities. The full title of this act is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. In 2006, this act was amended by the **USA PATRIOT Improvement and Reauthorization Act**, which made permanent 14 of the 16 expanded powers of the Department of Homeland Security and the FBI in investigating terrorist activity. The act also reset an expiration date written into the law as a so-called sunset clause for certain wiretaps under the Foreign **Intelligence Surveillance Act of 1978 (FISA)** and revised many of the criminal penalties and procedures associated with criminal and terrorist activities.

Another key law, the **Computer Security Act of 1987**, was one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices. The **National Institute of Standards and Technology (NIST)**—known as the National Bureau of Standards prior to 1988—is responsible for developing these security standards and guidelines in cooperation with the National Security Agency.

Privacy

Privacy has become one of the hottest topics in information security at the beginning of the 21st century. In the context of information security, the right of individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality is called **privacy**. Many organizations collect, swap, and sell personal information as a commodity, and as a result many people are looking to governments to protect their privacy from such organizations. The ability to collect information, combine facts from separate sources, and merge it all with other information has resulted in databases that were previously impossible to create.

Relevant U.S. Laws: Customer Information

The Privacy of Customer Information Section of the common carrier regulation states that any proprietary information shall be used explicitly for providing services, and not for marketing purposes. Carriers cannot disclose this information except when it is necessary to provide their services. The only other exception is applied when a customer requests the disclosure of information, in which case the disclosure is restricted to that customer's information only. This law does allow for the use of aggregate information as long as the same information is provided to all common carriers and all of them engage in fair competitive business practices. Note that **aggregate information**—the "blinding" of data collected for the purposes of managing networks or systems—is different from **information aggregation**, which is the development of individual profiles by combining information collected from multiple sources.

- **Federal Privacy Act of 1974** regulates government agencies and holds them accountable if they release private information about individuals or businesses without permission.
- The **Electronic Communications Privacy Act (ECPA) of 1986**, informally referred to as the **wiretapping act**, is a collection of statutes that regulates the interception of wire, electronic, and oral communications. These statutes work in conjunction with the Fourth Amendment of the U.S. Constitution, which protects individual citizens from unlawful search and seizure.
- The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, also known as the **Kennedy-Kassebaum Act**, protects the confidentiality and security of healthcare data by establishing and enforcing standards and by standardizing electronic data interchange. HIPAA affects all healthcare organizations, including doctors' practices, health clinics, life insurers, and universities, as well as some organizations that have self-insured employee health programs.
- The **Financial Services Modernization Act** or **Gramm-Leach-Bliley Act of 1999** contains many provisions that focus on facilitating affiliation among banks, securities firms, and insurance companies. Specifically, this act requires all financial institutions to disclose their privacy policies on the sharing of nonpublic personal information. It also requires due notice to customers so they can request that their information not be shared with third parties. In addition, the act ensures that an organization's privacy policies are fully disclosed when a customer initiates a business relationship and then distributed at least annually for the duration of the professional association.

Relevant U.S. Laws: Identity Theft

Related to privacy legislation is the growing body of law on identity theft. Identity theft can occur when someone steals a victim's personally identifiable information (PII) and uses it to purchase goods and services, or conduct other actions while posing as the victim. PII is an information about a person's history, background, and attributes that can be used to commit identity theft. This information typically includes a person's name, address, Social Security number, family information, employment history, and financial information.

The U.S. Federal Trade Commission (FTC) now oversees efforts to foster coordination among groups, more effective prosecution of criminals engaged in identify theft, and methods to increase restitution made to victims.

The **Identity Theft Enforcement and Restitution Act of 2008**, which specifically addressed the malicious use of spyware or keyloggers to steal PII. This act also created a new designation of a level of identity theft that provided much stronger penalties for violators who used 10 or more computers to commit theft. The new law also created a mechanism by which victims of identity theft may receive restitution from criminals convicted under the act.

Relevant U.S. Laws: Export and Espionage Laws

To meet national security needs and to protect trade secrets and other state and private assets, several laws restrict which information, information management resources, and security resources may be exported from the United States. These laws attempt to stem the theft of information by establishing strong penalties for such crimes. Such laws have limited effectiveness in many cases because the theft is initiated from offshore and the ability to apply the law is reduced when perpetrators are from another jurisdiction.

- To protect American ingenuity, intellectual property, and competitive advantage, Congress passed the Economic Espionage Act in 1996. This law attempts to prevent trade secrets from being illegally shared.
- The Security and Freedom through Encryption Act of 1999 provides guidance for the use of encryption and provides protection from government intervention.

Relevant U.S. Laws: U.S. Copyright Law
Intellectual property is a protected asset in the United States. The U.S. Copyright Law extends this privilege to published works, including electronic formats. Fair use allows copyrighted materials to be used to support news reporting, teaching, scholarship, and similar activities, as long as the use is for educational or library purposes, is not for profit, and is not excessive. As long as proper acknowledgment is provided to the original author of such works, including a proper citation of the location of source materials, and the work is not represented as one's own, it is entirely permissible to include portions of someone else's work as reference.

Relevant U.S. Laws: Financial Reporting
The **Sarbanes-Oxley Act of 2002**, also known as SOX or the **Corporate and Auditing Accountability and Responsibility Act**, is a critical piece of legislation that affects the executive management of publicly traded corporations and public accounting firms. The law seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies. Penalties for noncompliance range from fines to jail terms. Executives in firms covered by this law seek assurance for the reliability and quality of information systems from senior information technology managers. In turn, IT managers will likely ask information security managers to verify the confidentiality and integrity of the information systems in a process known as sub certification.

Relevant U.S. Laws: Freedom of Information Act of 1966
The Freedom of Information Act (FOIA) allows any person to request access to federal agency records or information not determined to be a matter of national security. Agencies of the federal government are required to disclose requested information upon receipt of a written request. This requirement is enforceable in court. However, some information is protected from disclosure, and the act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA.

State and Local Regulations
A critical fact to keep in mind when reading federal computer laws is that the majority of them are written specifically to protect federal information systems. The laws have little applicability to private organizations. Thus, such organizations must be cognizant of the

state and local laws that protect and apply to them. Information security professionals must understand state laws and regulations and ensure that their organizations' security policies and procedures are in compliance.

Understanding International Laws and Bodies

IT professionals and information security practitioners must realize that when their organizations do business on the Internet, they do business globally. As a result, these professionals must be sensitive to the laws and ethical values of many different cultures, societies, and countries. When it comes to certain ethical values, you may be unable to please all of the people all of the time, but the laws of other nations is one area in which it is certainly not easier to ask for forgiveness than for permission. Several security bodies and laws are described in this section. Because of the political complexities of relationships among nations and differences in culture, few current international laws cover privacy and information security.

U.K. Computer Security Laws

The following laws are in force in the United Kingdom (U.K.) and are similar to those described earlier for the United States:

- **Computer Misuse Act 1990**: Defined three "computer misuse offenses":
    1. Unauthorized access to computer material.
    2. Unauthorized access with intent to commit or facilitate commission of further offenses.
    3. Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
- **Privacy and Electronic Communications (EC Directive) Regulations 2003**: Revoked the Data Protection and Privacy Regulations of 1999, and focuses on protection against unwanted or harassing phone, e-mail, and SMS messages.
- **Police and Justice Act 2006**: Updated the Computer Misuse Act, modified the penalties, and created new crimes defined as the "unauthorized acts with intent to impair operation of computer, etc.,"
- **Personal Internet Safety 2007** action in protecting personal Internet safety.

Australian Computer Security Laws

The following laws are in force in Australia and its territories, and are similar to those described earlier for the United States:

- **Privacy Act 1988**: Regulates the collection, storage, use, and disclosure of personal information. Applies both to private and public sectors. Contains 11 information privacy principles for handling personal information by most public sector agencies, and 10 national privacy principles for handling of personal information by nongovernment agencies.
- **Telecommunications Act 1997**: Updated as of October 2013; contains regulation related to the collection and storage of privacy data held by telecommunications service providers.
- **Corporations Act 2001**: Updated by the Corporations Regulations of 2001 and 2002; focuses on business relationships, but similar to SOX, contains provisions related to financial reporting and audits.
- **Spam Act 2003**: Legislation designed to regulate the amount of unwanted commercial marketing materials, especially via e-mail. Requires businesses to obtain consent of recipients, ensure that businesses accurately identify the recipients, and provide a mechanism by which the recipients may unsubscribe from commercial messages.
- **Cybercrime Legislation Amendment Bill 2011**: Designed to align Australian laws with the European Convention on Cybercrime (see next section); the bill specifies information that communications carriers and Internet service providers must retain and surrender when requested by law enforcement.

Council of Europe Convention on Cybercrime

The Council of Europe adopted the **Convention on Cybercrime in 2001**. It created an international task force to oversee a range of security functions associated with Internet activities and standardized technology laws across international borders. It also attempts to improve the effectiveness of international investigations into breaches of technology law. This convention has been well received by advocates of intellectual property rights because it emphasizes prosecution for copyright infringement. However, many supporters of individual rights oppose the convention because they think it unduly infringes on freedom of speech and threatens the civil liberties of U.S. residents. Thirty-four countries attended the convention signing in November 2001, and 41 nations, including the United States and the United Kingdom, have ratified the convention as of January 2014.

The United States is technically not a member state of the Council of Europe, but it does participate in the convention. As with much complex international legislation, the Convention on Cybercrime lacks any realistic provisions for enforcement. The overall goal of the convention is to simplify the acquisition of information for law enforcement agencies in certain types of international crimes. It also simplifies the extradition process. The convention has more than its share of skeptics, who see it as an overly simplistic attempt to control a complex problem.

World Trade Organization and the Agreement on Trade-Related Aspects of Intellectual Property Rights

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), created by the World Trade Organization (WTO) and negotiated from 1986 to 1994, introduced intellectual property rules into the multilateral trade system. It is the first significant international effort to protect intellectual property rights. It outlines requirements for governmental oversight and legislation of WTO member countries to provide minimum levels of protection for intellectual property. The WTO TRIPS agreement covers five issues:

- How basic principles of the trading system and other international intellectual property agreements should be applied
- How to give adequate protection to intellectual property rights
- How countries should enforce those rights adequately within their own borders
- How to settle disputes on intellectual property between members of the WTO
- Special transitional arrangements during the period when the new system is being introduced

Digital Millennium Copyright Act

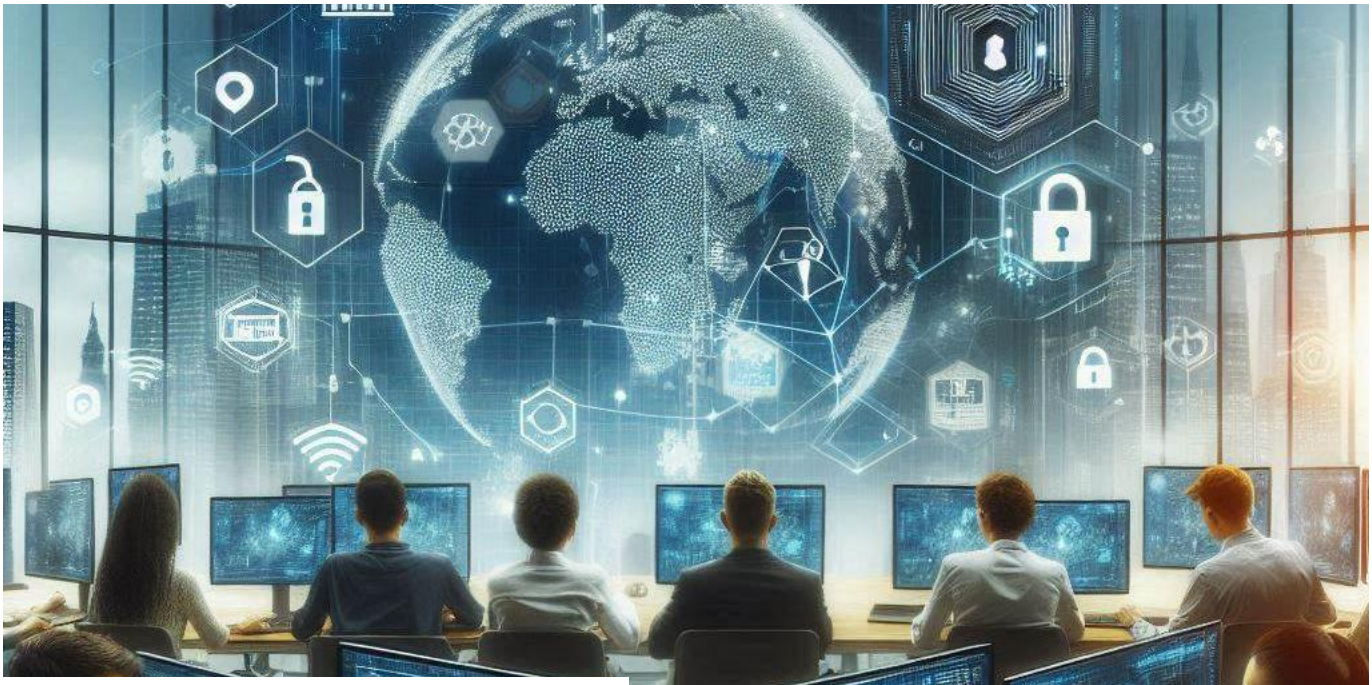
The Digital Millennium Copyright Act (DMCA) is the American contribution to an international effort by the World Intellectual Properties Organization (WIPO) to reduce the impact of copyright, trademark, and privacy infringement, especially when accomplished via the removal of technological copyright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

The DMCA includes the following provisions:

- Prohibits the circumvention of protections and countermeasures implemented by copyright owners to control access to protected content
- Prohibits the manufacture of devices to circumvent protections and countermeasures that control access to protected content
- Bans trafficking in devices manufactured to circumvent protections and countermeasures that control access to protected content
- Prohibits the altering of information attached or embedded into copyrighted material
- Excludes Internet service providers from certain forms of contributory copyright infringement

LESSON 2

Code of Ethics

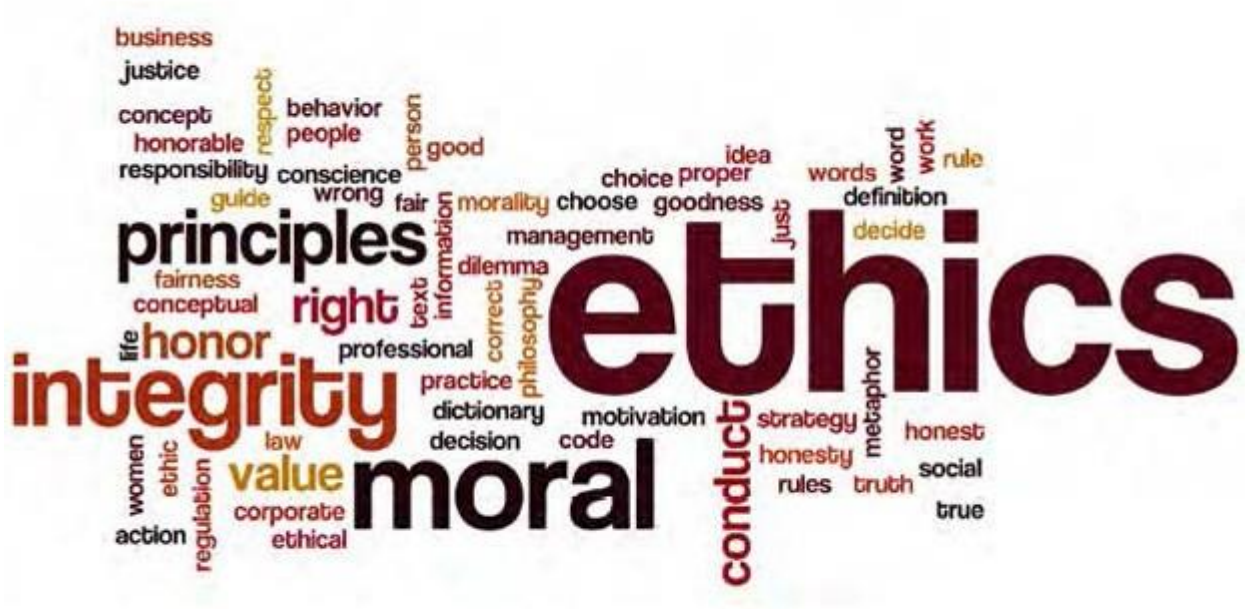


Learning Outcomes:

- Identify the Code of Ethics in a professional organization.

Understanding Ethics in Information Security

Introduction



Ethics are a structure of standards and practices that influence how people lead their lives. It is not strictly implemented to follow these ethics, but it is basically for the benefit of everyone that we do. Ethics are unlike laws that legally mandate what is right or wrong. Ethics illustrate society's views about what is right and what is wrong.

Computer ethics are a set of moral standards that govern the use of computers. It is society's views about the use of computers, both hardware and software. Privacy concerns, intellectual property rights and effects on the society are some of the common issues of computer ethics.

Ethics in Information Security

Many professionally regulated disciplines have explicit rules that govern the ethical behavior of their members. The information technology and information security fields do not have binding codes of ethics. Instead, professional associations such as the ACM and ISSA, and certification agencies such as (ISC)2 and ISACA, work to maintain ethical codes of conduct for their respective memberships. While these professional organizations can prescribe ethical conduct, they do not have the authority to banish violators from practicing their trade.

The Ten Commandments of Computer Ethics[22] from the Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Ethical Differences Across Cultures

Cultural differences can make it difficult to determine what is ethical and what is not—especially when it comes to the use of computers. Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality's ethical behavior violates the ethics of another national group. For example, to Western cultures, many of the ways in which Asian cultures use computer technology amount to software piracy. This ethical conflict arises out of Asian traditions of collective ownership, which clash with the protection of intellectual property.

Ethics and Education

Attitudes toward the ethics of computer use are affected by many factors other than nationality. Differences are found among people within the same country, within the same social class, and within the same company. Key studies reveal that education is the overriding factor in leveling ethical perceptions within a small population. Employees must be trained and kept aware of many topics related to information security, not the least of which is the expected behavior of an ethical employee. This education is especially important in information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal. Proper ethical and legal training is vital to creating an informed and well-prepared system user.

Deterring Unethical and Illegal Behavior

There are three general causes of unethical and illegal behavior:

- **Ignorance**: Ignorance of the law is no excuse; however, ignorance of policy and procedures is. The first method of deterrence is education, which is accomplished by designing, publishing, and disseminating an organization's policies and relevant laws, and obtaining agreement to comply with these policies and laws from all members of the organization. Reminders, training, and awareness programs keep policy information in front of employees to support retention and compliance.
- **Accident**: People who have authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. Careful planning and control help prevent accidental modification to systems and data.
- **Intent**: Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders. Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Understanding Code of Ethics in Professional Organizations

Many professional organizations have established codes of conduct or codes of ethics that members are expected to follow. Codes of ethics can have a positive effect on people's judgment regarding computer use. Security professionals have a responsibility to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society. Likewise, it is the organization's responsibility to develop, disseminate, and enforce its policies.

Professional organization	Web resource location	Description	Focus
Association of Computing Machinery	*www.acm.org*	Code of 24 imperatives of personal and ethical responsibilities for security professionals	Ethics of security professionals
Information Systems Audit and Control Association	*www.isaca .org*	Focus on auditing, information security, business process analysis, and IS planning through the CISA and CISM certifications	Tasks and knowledge required of the information systems audit professional
Information Systems Security Association	*www.issa.org*	Professional association of information systems security professionals; provides education forums, publications, and peer networking for members	Professional security information sharing
International Information Systems Security Certification Consortium (ISC)²	*www.isc2.org*	International consortium dedicated to improving the quality of security professionals through SSCP and CISSP certifications	Requires certificants to follow its published code of ethics
SANS Institute's Global Information Assurance Certification	*www.giac.org*	GIAC certifications focus on four security areas: security administration, security management, IT audits, and software security; these areas have standard, gold, and expert levels	Requires certificants to follow its published code of ethics

Professional Organizations of Interest to Information Security Professionals

© Cengage Learning 2015

Major Information Security Professional Organizations

The **Internet Activities Board(IAB)** is the organization that creates and defines Internet RFCs(Request for Comments) which forms the bedrock of most standards and protocols today.

In 1987, they published RFC1087– Ethics and the Internet. It is a policy relating to Ethical behaviour associated with the Internet.

According to IAB, the following practices would constitute unethical behaviour if purposely done.

- Seeks to gain unauthorized access to the resources of the Internet
- Disrupts the intended use of the Internet
- Wastes resources (people, capacity, computer) through such actions
- Destroys the Integrity of Computer-based Information
- Compromises the Privacy of users

The **Computer Ethics Institute** is a research, education and public organization focused on the interface of advances in information technology within ethical frameworks. CEI developed a very short and straightforward "Ten Commandments of Computer Ethics.

The **International Information Systems Security Certification Consortium (ISC)2** is a non-profit organization that focuses on the development and implementation of information security certifications and credentials. The code of ethics put forth by (ISC)2 is primarily designed for information security professionals who have earned a certification from (ISC)2.

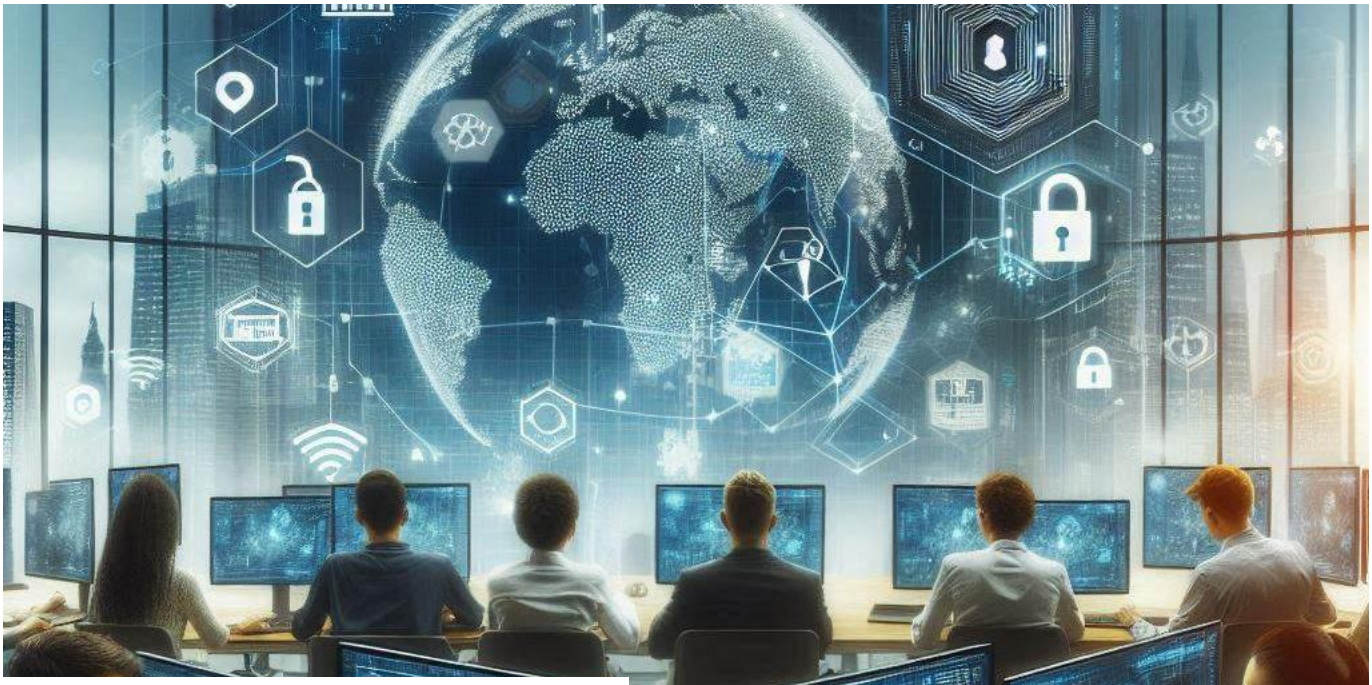
The **Association of Computing Machinery ACM** (www.acm.org) is a respected professional society, originally established in 1947 as "the world's first educational and scientific computing society." The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. The code contains specific references to protecting the confidentiality of information, causing no harm, protecting the privacy of others, and respecting the intellectual property and copyrights of others.

The **System Administration, Networking, and Security Institute, or SANS** (www.sans.org), is a professional organization with a large membership dedicated to the protection of information and systems. SANS offers a set of certifications called the Global Information Assurance Certification or GIAC.

The **Information Systems Audit and Control Association or ISACA** (www.isaca.org) is a professional association with a focus on auditing, control, and security.

Primary mission to bring together qualified IS practitioners for information exchange and educational development. Promotes code of ethics similar to (ISC)2, ISACA, and ACM

Privacy



Learning Outcomes:

- Describe the difference of GDPR and DPA.

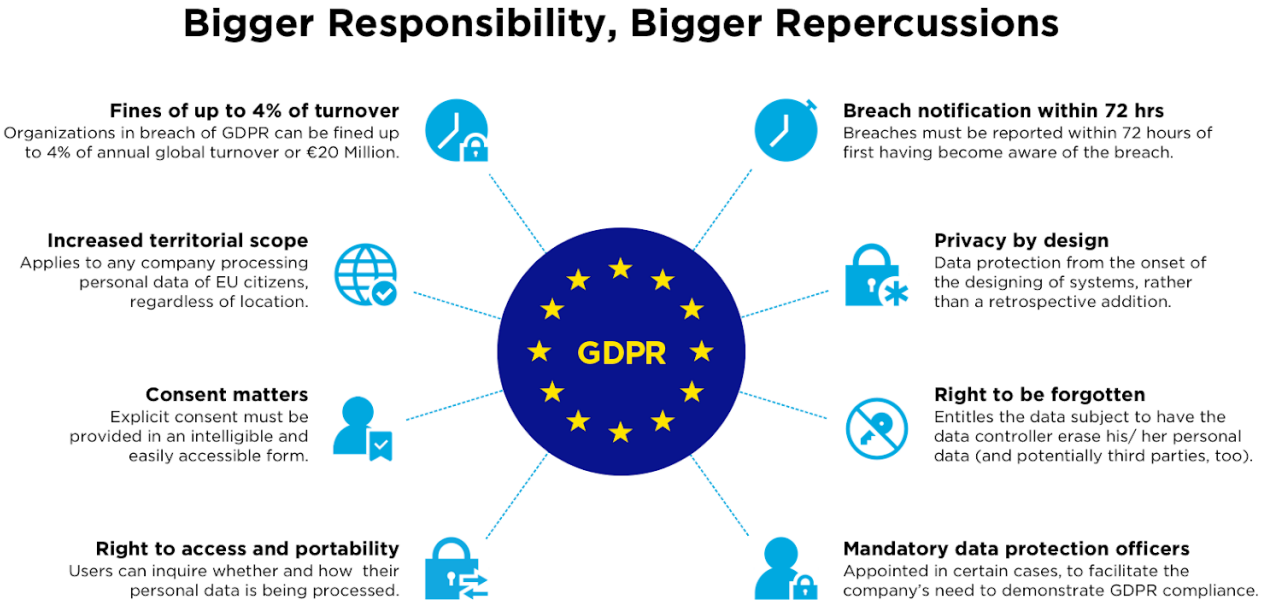
Understanding Privacy

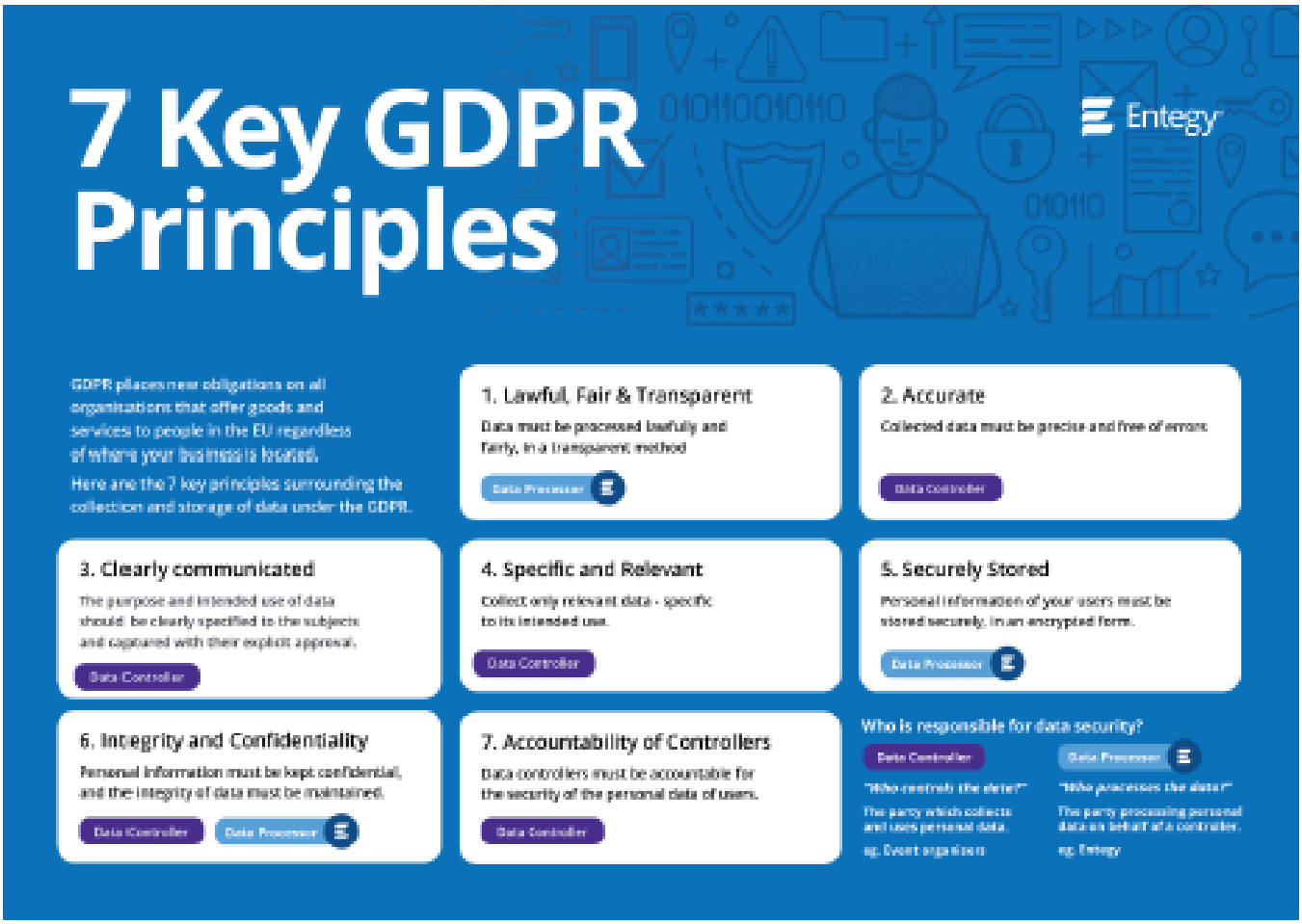
Privacy is the protection of the confidentiality of Personal Data. Organizations typically acquire and keep Personally Identifiable Information (PII) such as Social Security Numbers, Financial Information (i.e. Salary, Bank Account Information, Company Loans, etc.), and health care Information.

E.U. General Data Protection Regulation

The **General Data Protection Regulation (EU) 2016/679 (GDPR)** is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of

personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of data subjects inside the EEA.





PH Data Privacy Act of 2012

The **Data Privacy Act** is broadly applicable to individuals and legal entities that process personal information, with some exceptions. The law has extraterritorial application, applying not only to businesses with offices in the Philippines, but when equipment based in the Philippines is used for processing. The act further applies to the processing of the personal information of Philippines citizens regardless of where they reside.

The Republic Act No. 10173, also known as **The Data Privacy Act of 2012**

1. Protects the privacy of individuals while ensuring free flow of information to promote innovation and growth
2. Regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data.
3. Ensures that the Philippines complies with international standards set for data protection through National Privacy Commission (NPC).

ACTS PUNISHABLE	PENALTY
Unauthorized processing of personal information	Imprisonment-1 to 3 years Fine- P500K to P2M
Unauthorized processing of sensitive personal information	Imprisonment- 3 to 6 years Fine- P500K to P4M
Accessing personal information due to negligence	Imprisonment-1 to 3 years Fine- P500K to P2M
Accessing sensitive personal information due to negligence	Imprisonment- 3 to 6 years Fine- P500K to P4M
Improper disposal of personal information	Imprisonment-6 months to 2 years Fine- P100K to P500k
Improper disposal of sensitive personal information	Imprisonment-1 to 3 years Fine- P100K to P1M

ACTS PUNISHABLE	PENALTY
Unauthorized disclosure of sensitive personal information	Imprisonment-3 to 5 years Fine- P500K to P2M
Combination or series of acts	Imprisonment-3 to 6 years Fine- P1M to P5M

Perpetual or temporary absolute disqualification from office in addition to the above penalties.

LESSON SUMMARY

Laws: rules that mandate or prohibit certain behaviour in society; drawn from ethics

Ethics: define socially acceptable behaviours; based on cultural mores (fixed moral attitudes or customs of a particular group)

Many organizations have codes of conduct and/or codes of ethics

Organization increases liability if it refuses to take measures known as due care

Due diligence requires that organization make valid effort to protect others and continually maintain that effort

Studies have determined that people of differing nationalities have varying perspectives on ethical practices with the use of computer technology.

Deterrence can prevent an illegal or unethical activity from occurring. Deterrence requires significant penalties, a high probability of apprehension, and an expectation that penalties will be enforced.

KEY TERMS

- Laws
- Ethics
- Cultural Mores
- Due Care
- Due Diligence
- Jurisdiction
- Liability
- Restitution
- Policies
- Privacy
- Aggregate Information
- Identity Theft
- Personally Identifiable Information (PII)
- General Data Protection Regulation (GDPR)
- Data Privacy Act (DPA)
- Ra 10173

REFERENCES

Electronic Books

- Whiteman, et.al. “Principles of Information Security”, 3rd Edition

Online Sources

- Intersoft consulting, “General Data Protection Regulation”, https://gdpr-info.eu/
- NPC, “Data Privacy Act of 2012”, https://www.privacy.gov.ph/data-privacy-act/