**Module 3: Legal, Ethical, and Professional Issues in Information Security**

|  |  |
| --- | --- |
| 1. Laws and Ethics in Information Security  * Organizational Liability and the Need for Counsel * Policy versus Law * Types of Law  1. International Laws and Legal Bodies  * Council of Europe Convention of Cybercrime * Agreement on Trade-Related Aspects of Intellectual Property Rights * Digital Millenium Copyright Act (DMCA) | 1. Ethics and Information Security  * Ten Commandments of Computer Ethics * Ethical Differences across Cultures * Deterring Unethical and Illegal Behavior * Laws in the Philippines in Information Security |

|  |
| --- |
| **LAWS AND ETHICS IN INFORMATION SECURITY** |
| **Laws**   * Rules that mandate or prohibit certain behavior. * Drawn from ethics.   **Ethics**  Define as socially acceptable behaviors. |
| **Key Difference**   * Laws carry the authority of a governing body, ethics do not. * Ethics are based on cultural mores which is a fixed moral attitudes or customs. * Some ethics standards are universal. |
| **ORGANIZATIONAL LIABILITY AND**  **THE NEED FOR COUNSEL** |
| **Liability**   * Legal obligation for organization. * Extends beyond criminal or contract law. * Include legal obligation to restitution. * Employee acting with or without the authorization performs and illegal or unethical act that causes some degree of harm. * Employer can be held financially liable. |
| **Due Care**   * Organization makes sure that every employee knows what is acceptable or unacceptable. * Knows the consequences of illegal or unethical action |
| **Due Diligence**   * Requires that an organization make a valid effort to protect others to continually maintains this level of effort. |
| **Jurisdiction**   * Court's right to hear a case if a wrong is committed. * This is sometimes referred to as long arm jurisdiction, which is the long arm of the law reaching across the country or around the world to pull an accused individual into its court systems. |
| **POLICY VS. LAW** |
| **Policies**   * Guidelines that describe acceptable and unacceptable employee behaviors. * Functions as organizational laws. * Has penalties, judicial practices, and sanctions. |
| **Difference between policy and laws**   * Ignorance of policy is **acceptable.** * Ignorance of law in **unacceptable.** |
| **Keys for a policy to be enforced**   * Dissemination * Review * Comprehension * Compliance * Uniform enforcement – No one is above the law |
| **TYPES OF LAW** |
| * **Civil Law** – Govern a Nation of state. * **Criminal Law** - Addresses activities and conduct harmful to public. * **Private Law** - Encompasses family, commercial, labor, 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. |
| **INTERNATIONAL LAWS AND LEGAL BODIES** |
| * It is important for ***IT professionals*** and ***information security practitioners*** to 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. * While it may be impossible to please all of the people all of the time, dealing with the 'laws of other states and nations is one area where it is certainly not easier to ask for ***forgiveness*** than for ***permission.*** |
| **COUNCIL OF EUROPE CONVENTION**  **OF 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 for 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. |
| **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 over the years 1986-1994, introduced intellectual property rules into the multilateral trade system. * It is the first significant international effort to protect intellectual property rights. |
| **5 issues covered by WTO TRIPS Agreement**   1. How basic principles of the trading system and other international intellectual property agreements should be applied. 2. How to give ***adequate protection*** to intellectual property rights 3. How countries should enforce those ***rights*** adequately in their own territories. 4. How to ***settle disputes on intellectual property*** between members of the WTO. 5. Special transitional arrangements during the period when the new system is being introduced. |
| **DIGITAL MILLENIUM COPYRIGHT ACT (DMCA)** |
| **DMCA Provisions**   1. Prohibits the circumvention protections and countermeasures implemented by copyright owners to control access to protected content. 2. Prohibits the manufacture of devices to circumvent protections and countermeasures that control access to protected content. 3. Bans trafficking in devices manufactured to circumvent protections and countermeasures that control access to protected content. 4. Prohibits the altering of information attached or imbedded into copyrighted material. 5. Excludes Internet service providers from certain forms of contributory copyright infringement. |
| **ETHICS AND INFORMATION SECURITY** |
| **Computer Ethics**   * is a field of applied ethics that addresses **ethical issues** in the **use**, **design**, and management of information technology and in the formulation of ethical policies for its regulation in society. |
| **10 COMMANDMENTS OF COMPUTER ETHICS** |
| 1. Thou shall **not use Computers 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 create difficulty in determining what is **ethical** and **unethical**. * Difficulties arise when nationality's ethical behavior conflicts with ethics of ahother national group. * **Example:** to Western cultures, many of the ways in which Asian cultures use computer technology is software piracy. |
| 1. **Software License Infringement**  * Licensing infringement is the act of using another person's protected intellectual property (IP) without permission. * Copyright infringement is tried in federal court and governed by the U.S Legal Code, Title 17. |
| 1. **Illicit Use**  * The study respondents unilaterally condemned viruses, hacking, and other forms of the system abuse. * The low overall degree of tolerance for illicit system use may be a function of the easy correspondence between the common crimes of breaking and entering, trespassing, theft, and destruction of property and their computer-related counterparts. |
| 1. **Misuse of Corporate Resources**  * The scenarios used to examine the levels of tolerance for misuse of corporate resources each presented a different degree of noncompany use of corporate assets without specifying the company's policy on personal use of company resources. * It is interesting to note that only participants among the two Asian samples, Singapore and Hong Kong, Treported generally intolerant attitudes toward personal use of organizational computing resources. The reasons behind this are unknown. |
| **THREE DETERRING UNETHICAL AND ILLEGAL BEHAVIOR** |
| 1. **Ignorance**  * Ignorance of the law is no excuse. * First method of deterrence is education |
| 1. **Accident**  * Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. |
| 1. **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 rosecute offenders. |
| **LAWS IN THE PHILIPPINES**  **IN INFORMATION SECURITY** |
| **RA 10173 – DATA PRIVACY ACT OF 2012**   * Regulates the collection and processing of personal information in the Philippines and of Filipinos, including sensitive personal Information. * NATIONAL PRIVACY COMMISION (NPC) |
| **RA 10175 – CYBERCRIME PREVENTION ACT OF 2012**   * Offences against the confidentiality, integrity and availability of computer data and systems, computer related offences. * **NBI, PNP, CICC** |
| **RA 8792 – E-COMMERCE ACT OF 2000**   * Provides for the legal recognition of electronic documents, messages and signatures for commerce, transactions in government and evidence in legal proceedings. |
| **RA 8484- ACCESS DEVICE REGULATION ACT OF 1998**   * Penalizes various acts of access devices fraud, such as using counterfeit devices. * **EX: ATM SKIMMING** |