

Lecture 5

Ethics and privacy

| | |
|--|--|
| Ethical standards | <ol style="list-style-type: none"> 1. <u>Utilitarian approach</u> An ethical action is the one that provides the most goods or does the least harm. 2. <u>Rights approach</u> An ethical action is the one that best protects and respects the moral rights of the affected parties. (i.e. customers, employees, shareholders, business partners and competitors) 3. <u>Fairness approach</u> An ethical action treats all humans equally, or if unequally, then fairly, based on some defensible standard. 4. <u>Common good approach</u> An ethical action is the one that best serves the community as a whole and is important to the welfare of everyone, not just some members. It emphasizes the common conditions that are important to the welfare of everyone, including a system of laws, effective police and fire departments, health care, a public educational system and even recreation areas |
| Five steps in ethical decision making | <ol style="list-style-type: none"> 1. Recognize the issue 2. Get the facts 3. Evaluate alternatives 4. Make a choice 5. Reflect your decision |
| Ethics in corporate environment | <ol style="list-style-type: none"> 1. <u>Responsibility</u> - Means that you accept the consequences of your decisions and actions 2. <u>Accountability</u> - Refers to determining who is responsible for actions that were taken 3. <u>Liability</u> - A legal concept that gives individuals the right to recover the damages done to them by other individuals, organizations, or systems |
| Code of ethics | <p>Various organizations that promote fair and responsible use of information systems often develop a code of ethics.</p> |
| Privacy issues | <p>Privacy issues involve collecting, storing, and disseminating information about individuals.</p> |
| Information security | |
| Threat | <p>Any danger to which an information resource may be exposed</p> |
| Information security | <p>Protecting an organization's information resources from unauthorized access, use, disclosure, disruption, modification, or destruction</p> |
| Vulnerability | <p>The possibility that the system will be harmed by a threat.</p> |
| Exposure | <p>The harm, loss or damage that can result if a threat compromises that resource</p> |
| Factors that is increasing the threats to information security: | <ol style="list-style-type: none"> 1. smaller computing devices 2. downstream liability 3. the internet |
| IT Law | <ul style="list-style-type: none"> • Spam Act 2003 • Privacy Act 1998 • Copyright Act 1968 • Surveillance Devices Bill 2014 |
| Viruses | <p>Segments of computer code that attach to existing computer programs and perform malicious acts</p> |