Objectives

What key characteristics distinguish a professional from other kinds of workers, and what is the role of an IT professional?

What relationships must an IT professional manage, and what key ethical issues can arise in each?

How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?
What are the key tenets of four different codes of ethics that provide guidance for IT professionals?

What are the common ethical issues that face IT users?

What approaches can support the ethical practices of IT users?
Profession is a calling that requires

- specialized knowledge
- long and intensive academic preparation
Partial list of IT specialists

- programmers
- systems analysts
- software engineers
- database administrators
- local area network (LAN) administrators
- chief information officers (CIOs)
Legal perspective

- IT workers are not recognized as professionals
- not licensed
- IT workers are not liable for malpractice
IT professionals have many different relationships with:

- employers
- clients
- suppliers
- other professionals
- IT users
- society at large
Relationships Between IT Professionals and Employers

IT professionals must set an example and enforce policies regarding the ethical use of IT.

Software piracy is the act of illegally making copies of software or enabling others to access software to which they are not entitled.

Software piracy is an area in which IT professionals can be tempted to violate laws and policies.

The Business Software Alliance (BSA) is a trade group that represents the world’s largest software and hardware manufacturers.

- Its mission is to stop the unauthorized copying of software produced by its members.
- Penalties can be up to $100,000 per copyrighted work.
## Members of BSA (as of July 2005)

<table>
<thead>
<tr>
<th>Adobe</th>
<th>Apple</th>
<th>Autodesk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avid</td>
<td>Bentley Systems</td>
<td>Borland</td>
</tr>
<tr>
<td>Cadence</td>
<td>Cisco Systems</td>
<td>CNC Software/Mastercam</td>
</tr>
<tr>
<td>Dell</td>
<td>Entrust</td>
<td>HP (Hewlett-Packard)</td>
</tr>
<tr>
<td>IBM</td>
<td>Intel</td>
<td>Internet Security Systems</td>
</tr>
<tr>
<td>Macromedia</td>
<td>McAfee, Inc.</td>
<td>Microsoft</td>
</tr>
<tr>
<td>PTC</td>
<td>RSA Security</td>
<td>SAP</td>
</tr>
<tr>
<td>SolidWorks</td>
<td>Sybase</td>
<td>Symantec</td>
</tr>
<tr>
<td>The Mathworks</td>
<td>UGS Corp.</td>
<td>VERITAS Software</td>
</tr>
</tbody>
</table>
Trade secret

- information used in business
- generally unknown to the public
- company has taken strong measures to keep confidential
- examples are the formula for Coke, Intel manufacturing process for P4 chip
- employees must sign a non-disclosure agreement (NDA)
- problems due to high IT employee turn-over

Whistle-blowing

- attracts attention to a negligent, illegal, unethical, abusive, or dangerous act that threatens the public interest
Relationships Between IT Professionals and Clients

IT professional provides
- hardware, software, or services at a certain cost and within a given time frame

Client provides
- compensation
- access to key contacts
- work space

Relationship is usually documented in contractual terms
Ethical problems arise if a company recommends its own products and services to remedy problems they have detected

• but a company is unable to provide full and accurate reporting of a project’s status
• company hired as consultants may recommend its affiliated products
Legal Overview

Fraud, misrepresentation

• crime of obtaining goods, services, or property through deception or trickery
• fraud is proven in court

Breach of contract

• one party fails to meet the terms of a contract
• schedule slippage, cost overruns, better product may be released by competitor during contract execution
• can generate trials which are often settled out of court to minimize reputation damage
Develop good relationships with suppliers

- deal fairly with them
- do not make unreasonable demands

Bribery

- providing money, property, or favors to someone in business or government to obtain a business advantage
- U.S. Foreign Corrupt Practices Act (FCPA) makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office

IT projects are joint efforts in which vendors and customers work together

- difficult to assign blame
Bribery

- at what point does a gift become a bribe?
- no gift should be hidden
- perceptions of donor and recipient can differ
Distinguishing Between a Bribe and a Gift

<table>
<thead>
<tr>
<th>Bribes</th>
<th>Gifts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are made in secret, as they are neither legally nor morally acceptable</td>
<td>Are made openly and publicly as a gesture of friendship or goodwill</td>
</tr>
<tr>
<td>Are often made indirectly through a third party</td>
<td>Are made directly from donor to recipient</td>
</tr>
<tr>
<td>Encourage an obligation for the recipient to act favorably toward the donor</td>
<td>Come with no expectation of a future favor for the donor</td>
</tr>
</tbody>
</table>
Professionals owe each other adherence to a profession’s code of conduct

- there is a sense of mentorship and community

Ethical problems between members of the IT profession

- résumé inflation
- inappropriate sharing of corporate information due to IT access
Relationships Between IT Professionals and IT Users

IT user is a person for whom a hardware or software product is designed

IT professionals’ duty

• understand users’ needs and capabilities
• deliver products and services that best meet those needs
• establish an environment that supports ethical behavior by users
Relationships Between IT Professionals and Society

Actions of an IT professional can affect society

• society expect professionals to not cause harm (=trust)
• society expects professionals to provide benefits
• so there must be a sense of responsibility, also not to damage a professional sector’s reputation
Corporations are taking actions to ensure good business ethics among employees.
A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group

- a law does not provide complete guide to ethical behavior

Main parts:

- outlines what the professional organization aspires to become
- lists rules and principles by which members of the organization are expected to abide

Benefits for individual, profession, and society

- improves ethical decision making
- promotes high standards of practice and ethical behavior
- enhances trust and respect from the general public
- provides an evaluation benchmark
Professional Organizations

No universal code of ethics for IT professionals

No single, formal organization of IT professionals has emerged as preeminent

Professional organizations enable

• building of professional and working relationships
• sharing of useful information (stay up-to-date)
• provides a stamp of adhering to defined standards

Most prominent organizations include:

• Association for Computing Machinery (ACM)
• Association of Information Technology Professionals (AITP)
• Computer Society of the Institute of Electrical and Electronics Engineers (IEEE-CS)
• Project Management Institute (PMI)
Certification

Indicates a professional possesses a particular set of skills, knowledge, or abilities in the opinion of a certifying organization.

Can also apply to products.

Generally voluntary.

Carries no requirement to adhere to a code of ethics.

Can serve as a benchmarks for mastery of a certain skill set and knowledge.

- Good way to document and structure the acquisition of new skills and knowledge.
- Get re-certified to stay up-to-date.
Vendor certifications

- Cisco, IBM, Microsoft, etc.
- some certifications substantially improve IT workers’ salaries and career prospects
- relevant for narrowly defined roles
  - or certain aspects of broader roles
- require passing a written exam
- workers are commonly recertified as newer technologies become available
Industry association certifications

- require a certain level of experience and a broader perspective than vendor certifications
- lag in developing tests that cover new technologies
Government Licensing

Generally administered at the state level in the United States

- examples: CPAs, doctors, lawyers, etc.
- but also engineers that perform engineering services for the public

Case for licensing IT professionals

- encourage IT professionals to follow the highest standards of the profession
- practice a code of ethics
- violators would be punished by law
- without it there is no incentive for heightened care and no concept of malpractice
- licensing of IT professionals may improve today’s very complex IT systems
Adverse issues associated with government licensing of IT professionals

- there are few international or national licensing programs for IT professionals
- no universally accepted core body of knowledge
- unclear who should manage content and administration of licensing exams
- no administrative body to accredit professional education programs
- no administrative body to assess and ensure competence of individual professionals
IT Professional Malpractice

Negligence:

- not doing something that a reasonable man would do, or doing something that a reasonable man would not do

Duty of care:

- the obligation to protect people against any unreasonable harm or risk

Courts consistently reject attempts to sue individual parties for computer-related malpractice
Employees’ ethical use of IT is an area of growing concern
Common Ethical Issues for IT Users

Software piracy
  • copying work software for use at home (even when doing *some* work at home) is considered piracy

Inappropriate use of computing resources
  • surf work-unrelated websites
  • send questionable email
  • etc

Inappropriate sharing of information
  • private data
  • confidential information
Supporting the Ethical Practices of IT Users

Policies that protect against abuses:

- establish boundaries of acceptable and unacceptable behavior
- enable management to punish violators

Policy components include:

- defining and limiting the appropriate use of IT resources
- establishing guidelines for use of company software
- structuring information systems to protect data and information
- installing and maintaining a corporate firewall
Manager’s Checklist of Items to Consider when Establishing an IT Usage Policy

<table>
<thead>
<tr>
<th>Questions</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a statement that explains the need for an IT usage policy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the policy provide a clear set of guiding principles for ethical decision making?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is it clear how the policy applies to the following types of workers?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part-time workers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the policy address the following issues?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection of the data privacy rights of employees, customers, suppliers, and others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limits and control of access to proprietary company data and information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The use of unauthorized or pirated software</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Manager’s Checklist of Items to Consider when Establishing an IT Usage Policy

<table>
<thead>
<tr>
<th>Does the policy address the following issues?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee monitoring, including e-mail, wiretapping and eavesdropping on phone conversations, computer monitoring, and surveillance by video</td>
</tr>
<tr>
<td>Respect of the intellectual rights of others, including trade secrets, copyrights, patents, and trademarks</td>
</tr>
<tr>
<td>Inappropriate use of IT resources, such as Web surfing, e-mailing, and other use of computers for purposes other than business</td>
</tr>
<tr>
<td>The need to protect the security of IT resources through adherence to good security practices, such as not sharing user IDs and passwords, use of “hard-to-guess” passwords, and frequent changing of passwords</td>
</tr>
<tr>
<td>The use of the computer to intimidate, harass, or insult others through abusive language in e-mails and by other means</td>
</tr>
<tr>
<td>Are disciplinary actions defined for IT-related abuses?</td>
</tr>
<tr>
<td>Is there a process for communicating the policy to employees?</td>
</tr>
<tr>
<td>Is there a plan to provide effective, ongoing training relative to the policy?</td>
</tr>
<tr>
<td>Has a corporate firewall been implemented?</td>
</tr>
<tr>
<td>Is the corporate firewall maintained?</td>
</tr>
</tbody>
</table>
A professional from a legal standpoint
  • has passed the state licensing requirements
  • has earned the right to practice there

IT professionals have many different relationships
  • each with its own set of ethical issues and potential problems

Professional code of ethics
  • states the principles and core values essential to the work of an occupational group
Licensing and certification of IT professionals

• many people feel that certification will increase the reliability and effectiveness of information systems
• raises many issues

IT-related professional organizations have developed a code of ethics

IT usage policy defines appropriate and inappropriate IT user behavior