Chapter 9
Ethical Guidelines for Information Use

Managing and Using Information Systems: A Strategic Approach

by Keri Pearlson & Carol Saunders

WILEY
Publishers Since 1807

Learning Objectives

- Understand how ethics should be framed in the context of business practices and the challenges surrounding these issues.
- Define and describe the three normative theories of business ethics.
- List and define PAPA and why it is important.
- Identify the issues related to the ethical governance of information systems.
- Understand security issues of organizations and how organizations are bolstering security.
- Describe how security can be best enacted.
- Define the Sarbanes-Oxley Act and the COBIT framework.

Real World Examples

- TJX Co. discovered the largest security breach of its computer system in the history of retailing.
- As many as 94 million customers were affected.
- TJX had to decide between notifying their customers immediately, or waiting the 45 days allowed by the jurisdictions.
- If they waited their customers might be further compromised by the breach.
- If they notified them immediately they might lose customer confidence and face punishment from Wall Street.

NORMATIVE THEORIES OF BUSINESS ETHICS

Introduction

- Managers must assess initiatives from an ethical view.
- Most managers are not trained in ethics, philosophy, and moral reasoning.
  - Difficult to determine or discuss social norms.
- Three theories of business ethics are examined to develop and apply to particular challenges that they face (see Figure 9.1):
  - Stockholder theory
  - Stakeholder theory
  - Social contract theory

Stockholder Theory

- Stockholders advance capital to corporate managers who act as agents in advancing their ends.
- Managers are bound to the interests of the shareholders (maximize shareholder value).
- Manager's duties:
  - Bound to employ legal, non-fraudulent means.
  - Must take long view of shareholder interest.

Stakeholder Theory

- Managers are entrusted with a responsibility (fiduciary or other) to all those who hold a stake in or a claim on the firm.
- Stakeholders are –
  - Any group that vitally affects the corp. survival and success.
  - Any group whose interests the corp. vitally affects.
- Management must enact and follow policies that balance the rights of all stakeholders without impinging upon the rights of any one particular stakeholder.

Social Contract Theory

- Consider the needs of a society with no corporations or other complex business arrangements.
- What conditions would have to be met for the members of a society to agree to allow a corporation to be formed?
- Corporations are expected to create more value to society that it consumes.
- Social contract:
  - 1. Social welfare – corporations must produce greater benefits than their associated costs.
  - 2. Justice – corporations must pursue profits legally, without fraud or deception, and avoid actions that harm society.

Theory	Definition	Metrics
Stockholder	Maximize stockholder wealth, in legal and non-fraudulent manners.	Will this action maximize stockholder value? Can goals be accomplished without compromising company standards and without breaking laws?
Stakeholder	Maximize benefits to all stakeholders while weighing costs to competing interests.	Does the proposed action maximize collective benefits to the company? Does this action treat one of the corporate stakeholders unfairly?
Social contract	Create value for society in a manner that is just and nondiscriminatory.	Does this action create a “net” benefit for society? Does the proposed action discriminate against any group in particular, and is its implementation socially just?

Figure 9.1 Three normative theories of business ethics.

CONTROL OF INFORMATION

Privacy

- Those who possess the “best” information and know how to use it, win.
- However, keeping this information safe and secure is a high priority (see Figure 9.2).
- Privacy – “the right to be left alone”.
- Managers must be aware of regulations that are in place regarding the authorized collection, disclosure and use of personal information.
  - Safe harbor framework of 2000.

Area	Critical Questions
Privacy	What information must a person reveal about one's self to others? What information should others be able to access about you – with or without your permission? What safeguards exist for your protection?
Accuracy	Who is responsible for the reliability and accuracy of information? Who will be accountable for errors?
Property	Who owns information? Who owns the channels of distribution, and how should they be regulated?
Accessibility	What information does a person or an organization have a right to obtain, under what conditions, and with what safeguards?

Figure 9.2 Mason's areas of managerial concern.

Accuracy

- Managers must establish controls to insure that information is accurate.
- Data entry errors must be controlled and managed carefully.
- Data must also be kept up to date.
- Keeping data as long as it is necessary or legally mandated is a challenge.

Property

- Mass quantities of data are now stored on clients.
- Who owns this data and has rights to it is are questions that a manager must answer.
- Who owns the images that are posted in cyberspace?
- Managers must understand the legal rights and duties accorded to proper ownership.

Accessibility

- Access to information systems and the data that they hold is paramount.
- Users must be able to access this data from any location (if it can be properly secured and does not violate any laws or regulations).
- Major issue facing managers is how to create and maintain access to information for society at large.
  - This access needs to be controlled to those who have a right to see and use it (identity theft).
  - Also, adequate security measures must be in place on their partners end.

PAPA and Managers

- Managers must work hard to implement controls over information highlighted by PAPA.
- Limit access to data – avoid identify theft, and respect customer's privacy.
- FTC requires more disclosure of how companies use customer data.
  - Gramm-Leach-Bliley Act (1999)
- Information privacy guidelines must come from above: CEO, CFO, etc.

Security and Controls

- PAPA principles work hand-in-hand with security and controls
- Executives reported that hardware/software failures, and major viruses, had resulted in unexpected or unscheduled outages of their critical business systems (Ernst & Young).
- Technologies have been devised to manage the security and control problems (see Figure 9.3).
- RFID is being used to control access and manage assets.
- Employees require proper training and education.

IT GOVERNANCE AND SECURITY

IT Governance and Security

- Weill and Ross Framework for IT governance (Chap 8) offers a new perspective for assigning responsibility for key security decisions.
- Same archetypes can be expanded for security.
- Figure 9.4 shows an appropriate governance pattern for each decision.
  - 1. Information Security Strategy
  - 2. Information Security Policies
  - 3. Information Security Infrastructure
  - 4. Information Security Education/Training/Awareness
  - 5. Information Security Investments
- The archetypes clearly define the responsibilities of the major players in the company

Information Security Decision	Recommended Archetype	Rationale
Information Security Strategy	Business monarchy	Business leaders have the knowledge of the company's strategies, upon which security strategy should be based. No detailed technical knowledge is required
Information Security Policies	IT duopoly	Technical and security implications of behaviors and processes need to be analyzed and tradeoffs between security and productivity need to be made. Need to know the particularities of company's IT infrastructure.
Information Security Infrastructure	IT monarchy	In depth technical knowledge and expertise is needed.
Information Security Education/Training/ Awareness	IT duopoly	Business buy-in and understanding are needed; Technical expertise and knowledge of critical security issues is needed in building programs.
Information Security Investments	IT duopoly	Requires financial (quantitative) and qualitative evaluation of business impacts of security investments. Business case has to be presented for rivaling projects.

Figure 9.4 – Matching information security decisions and archetypes

Sarbanes-Oxley Act of 2002

- The Sarbanes-Oxley (SoX) Act of 2002 was enacted to increase regulatory visibility and accountability of public companies and their financial health.
  - All companies subject to the SEC are subject to the requirements of the act.
  - CEO's and CFO's must personally certify and be accountable for their firm's financial records and accounting (stiff penalties).
  - Firms must provide real-time disclosures of any events that may affect a firm's stock price or financial performance.
  - IT departments realized that they played a major role in ensuring the accuracy of financial data.

IT Control and Sarbanes-Oxley

- In 2004 and 2005 IT departments began to identify controls, determined design effectiveness, and validated operation of controls through testing.
- Five IT control weaknesses were uncovered by auditors:
  1. Failure to segregate duties within applications, and failure to set up new accounts and terminate old ones in a timely manner.
  2. Lack of proper oversight for making application changes, including appointing a person to make a change and another to perform quality assurance on it.
  3. Inadequate review of audit logs to not only ensure that systems were running smoothly but that there also was an audit log of the audit log.
  4. Failure to identify abnormal transactions in a timely manner.
  5. Lack of understanding of key system configurations.

Frameworks for Implementing SoX

- **COSO -** Committee of Sponsoring Organzations of the Treadway Commission.
  - Created three control objectives for management and auditors that focused on dealing with risks to internal control
    - **Operations** – to help the company maintain and improve its operating effectiveness and protect the assets of shareholders
    - **Compliance** – to assure that the company is in compliance with relevant laws and regulations.
    - **Financial reporting** – to assure that the company's financial statements are produced in accordance with Generally Accepted Accounting Principles (GAAP).
  - Five essential control components were created to make sure a company is meeting its objectives.

Frameworks (continued)

- COBIT (Control Objectives for Information and Related Technology)
  - IT governance framework that is consistent with COSO controls.
  - Issued in 1996 by Information Systems Audit & Control Association (ISACA)
    - A company determines the processes that are the most susceptible to the risks that it judiciously chooses to manage.
      - Control objectives are then set up with more specific key indicators
    - Advantages - well-suited to organizations focused on risk management and mitigation, and very detailed.
    - Disadvantages – costly and time consuming
  - Figure 9.5 lists the components of COBIT and examples of each component

Component	Description	Example
Domain	One of four major areas of risk (Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate); Each domain consists of multiple processes	Delivery and Support
Control Objective	Focuses on control of a process associated with risk; There are 34 processes	DS (Delivery and Support) 11 - Manage Data: ensures delivery of complete, accurate and valid data to the business
Key Goal Indicator	Specific measures of the extent to which the goals of the system in regard to a control objective have been met	“A measured reduction in the data prepartion process and tasks”
Key Performance Indicator	Actual, highly-specific measures of the for measuring accomplishment of a goal	“Percent of data input errors” (Note: the percentage should decrease over specified periods of time)
Critical Success Factor	Describes the steps that a company must take to accomplish a Control Objective. There are 318 Critical Success Factors.	“Data entry requirements are clearly stated, enforced and supported by automated techniques at all level, including database and file interfaces”
Maturity Model	A uniquely-defined six-point ranking of a company’s readiness for each control objective made in comparison with other companies in the industry	“Data is not recognized as a corporate resource and asset. There is no assigned data ownership or individual accountability for data integrity and reliability. Data quality and security is poor or non-existent”

Figure 9.5 – Components of COBIT and their examples

IT and the Implementation of Sarbanes Oxley Act Compliance

- Section 404 of SoX deals with management's assessment of internal controls making implementation considerable.
- CIO works with auditors, CFO, and CEO.
  - CIO must tread carefully
  - Braganza and Franken provide six tactics for working effectively in these relationships (Fig 6.9).
  - The extent to which a CIO could employ these various tactics depends upon the power that he or she holds relating to the SoX implementation

Tactic	Definition	Examples of Activities
Knowledge Building	Establishing a knowledge base to implement SoX	Acquiring technical knowledge about SoX and 404
Knowledge Deployment	Disseminating knowledge about SoX and developing an understanding of this knowledge among management and other organizational members	Moving IT-staff with knowledge of 404 to parts of the organization that are less knowledgeable Creating a central repository of 404 knowledge Absorbing 404 requriements from external bodies Conducting training programs to spread an understanding of SoX
Innovation Directive	Organizing for implementing SoX and announcing the approach	Issuing instructions that encourage the adoption of 404 compliance practices Publishing progress reports of each subsidiary's progress toward 404 implementation Putting drivers for 404 implementation in place Directing 404 implementation from top down and/or bottom up
Mobilization	Persuading decentralized players and subsidiaries to participate in SoX implementation	Creating a positive impression of SoX (and 404) implementation Conducting promotional and awareness campaigns
Standardization	Negoitating agreements between organizational members to facilitate the SoX implementation	Using mandatory controls, often embedded within the technology, to which users must comply Indicating formal levels of compliance or variance from prescribed controls Establishing standards of control throughout the organization Creating an over-arching corporate compliance architecture
Subsidy	Funding implements' costs during the SoX implementation and users' costs during its deployment and use	Centralizing template development Developing web-based resources Investing in developing the skills of IT staff to implementing 404 Funding short-term skill gaps Investing in tracking implementation Managing funds during implementation to achieve specific IT-related 404 goals.

Figre 9.6 CIO Tactics for implementing SoX compliance

Other Control Frameworks

- ISO
  - ISO (International Organization for Standardization) is the world's **largest developer** and publisher of **International Standards**
- Information Technology Infrastructure Library (ITIL)
  - Set of concepts and techniques for managing IT
  - Offers 8 sets of management procedures

FOOD FOR THOUGHT: GREEN COMPUTING

Green Computing

- Concerned with using computing resources efficiently.
- Gartner put Green Computing at top of list of upcoming strategic technologies.
  - Due to increasing energy demands to run IT infrastructure.
  - Largest 5 search companies use more power that generated by Hoover Dam.
- Companies are working to become more efficient by:
  - Replacing older systems with more energy efficient ones.
  - Moving workloads based on energy efficiency.
  - Using most power inefficient servers only at peak usage times.
  - Improving data center air flows.
  - Turning to virtualization.

Green Computing

- Green programs have a triple bottom line (TBL or 3BL):
  - Economic
  - Environmental
  - Social
- Can be considered from the Social Contract Theory perspective.
  - People and Planet motivations
- Stockholder Theory Perspective

SUMMARY

Summary

- Ethics - decisive action rooted in principles that express what is right and important and about action that is publicly defensible and personally supportable.
- Three important normative theories describing business ethics are: Stockholder Theory, Stakeholder Theory and Social Contract Theory.
- PAPA is an acronym for the four areas in which control of information is crucial: privacy, accuracy, property, and accessibility.
- Issues related to the ethical governance of information systems are emerging in terms of the outward transactions of business that may impinge on the privacy of customers.
- Security looms as a major threat to Internet growth.
- Sarbanes-Oxley Act (2002) - enacted to improve internal controls