Database Design and Entity-Relationship Models

Database Design

- Databases store data
- Design reflects the organization that exists within the data
- Model: representation of reality that retains only selected details
  - Powerful tool for validating necessary details and eliminating irrelevant ones
  - Associate or map elements in reality to elements in the model
- Data model: captures organization of the data in a logical representation of the data
- Database development steps:
  - Developers analyze forms, reports, queries to judge requirements for system
  - Requirements summarized in a data model, containing descriptions of data and relationships
  - Database design implemented
  - Database created and filled with user data
- To build a database, must first start with an *entity-relationship model* (ER diagram):
  - Visualization/diagram of the data
  - Describes the logical database
  - Graphical method of mapping the real world
  - Once ER diagram is built it is used as a blueprint for the real database

Entity Relationship Model

- Most popular for data modeling, introduced by Peter Chen in 1976
  - Now has many variants
- Consists of
  - Entities (with attributes)
  - Relationships (with attributes, cardinality, participation)
- Entity: represents a discrete object (person, place, thing, event) in rectangle
  - I.e. Western: Student, Course, Program, Professors, etc.
- Attributes: describe properties of the entity in oval
  - I.e. Student attributes: student number, name, address, phone, email, etc.
- Instances: set of data items that exist under the entities
  - I.e. instance of Student entity: 250615954, Tamara Grunberger, 695, etc.
- Key attributes: necessary to uniquely identify the instance of each entity <u>underlined</u>
  - I.e. SIN, student number, employee number, course number
- Relationship: association between two or more entities that captures how they are related in a diamond
  - I.e. person WORKS FOR company, student TAKES course
  - Can have attributes (i.e. hire date describes relationship, not person or company)
- Cardinality: indicates the number of instances involved in the relationship
  - 1:1 relationship: single entity to single entity
    - I.e. 1 faculty member is chair of 1 department
  - 1:M (M:1) relationship: one to many entities
    - I.e. MANY students registered to 1 faculty
  - N:M relationship: many to many entities

    - I.e. MANY students take MANY courses
- Participation: indicates whether all or only some of the instances of an entity are involved in the relationship
    - Total participation: all instances involved (marked with double line)
    - Partial participation: only some instances involved (marked with single line)
- Recursive relationship: relationship among the same entity
    - I.e. Supervision relationship (supervisor and supervisee) solely among employees

ER Diagrams—Crow's Foot

- Rectangles represent entities, relationships showing with lines
- Cardinality: crow's foot
    - Forks at the end of lines indicate many instances involved in relationship
- Participation: vertical line marks at least 1 entity of that type involved; oval marks that entities are optional

Normalization

- Process: converts table into two or more tables, changing from poorly to well structured
- Data integrity problems: different names for same entity produces incorrect/inconsistent data
- Normalized tables…
    - Eliminate duplicate data
    - Are slower to process
    - Have a single theme for each table

Database Elements

- Entity: anything about which an organization wishes to store data (i.e. Student info)
- Fields: information about attributes stored in fields (i.e. Student names stored under Name field)
- Record: consists of all the fields containing data about one entity instance
- File: a set of all related records
- Tables: consists of rows and columns, should always have a key attribute (primary key)

Relational Database

- Data model based on a relation represented in a 2D table
- Entities and relationships in ER diagram become tables in relational model
- Rows consist of *instances* of entity or relationship
- Columns consist of *attributes* of entity or relationship
- The table that stores a relationship inherits the key attributes from all entities involved in the relationship
    - I.e. TAKES relationship—Student TAKES Course
        - Key from Student table (student number) and key from Course table (course number) become information to be stored in Takes table

Converting ER Diagrams to Relational Databases

- Each entity becomes its own table with key attribute as primary key and other attributes as subsequent columns
- For each 1:1 relationship: choose one entity involved and make its key the foreign key in the other entity's table, and the relationship's attributes get moved as well
- For each 1:M relationship: take the key from the 1 side and make it the foreign key in the MANY table
- For each N:M relationship: create a new table that combines the relationship attributes, and the key attributes of both entities

Chapter 5: Database and Content Management

Content Organization and Management

- Content is related to intellectual property
  - A form of creative endeavor that can be protected through a trademark, patent, copyright, industrial design, or integrated circuit topography
- Content management challenge: processing and storing the right content, getting the right content to the right person in the right format and the right time
- Management of content data: Database Management System (DBMS)—effectively and efficiently stores and processes data
- Presentation of content: Content Management System (CMS)—organize documents and seek out documents to organize access
- Spreadsheet VS database: both keep track of things
  - Spreadsheet keeps lists of a single concept/theme
  - Database keeps lists involving multiple themes

Components of a Database

- Database= table/files + relationships among rows + metadata
- Relationships among records: values in one table relate to rows in other tables
  - Primary keys: columns that identify unique row in table, each table has a key
  - Foreign keys: primary keys from other tables
- Metadata: databases are self-describing—metadata is data describing the data
- Components of a database application system:
  - User
  - Database application: forms, reports, queries, application programs
  - Database Management System (DBMS): i.e. Microsoft Access
  - Database: tables, relationships, metadata

Database Applications

- Collection of forms, reports, queries, application programs
- Applications can have multiple users, databases can have more than one application
- Forms: read, insert, modify, delete data
- Reports: shows data in structured context, able to compute values
- Queries: comprehensive and robust method to ask/answer questions about data
  - Structured Query Language (SQL): international standard for processing databases

- Application programs: process logic specific to a business' needs
  - Enables database processing over the Internet
  - Intermediary between web server and database
  - Responds to events (reads, inserts, modifies, deletes data)

Multi-User Processing

- Lost update problem: locking used to coordinate activities of multiple users
  - Each change/modification/deletion of content overrides the past changes done and the initial value is lost with each new activity

Database Management Systems (DBMS)

- Functions:
  - Create tables and relationships in database
  - Process database
  - Administer security levels to access database
- Enterprise DBMS: process organizational and work group databases
  - Large databases that support many users
  - I.e. IBM's DB2, SQL Server, Oracle
- Personal DBMS: designed for smaller, simpler database applications
  - Supports fewer than 100 users
  - I.e. Access, dBase, FoxPro, Paradox, R: Base

Extension 5B: Access and SQL

Access Tables

- Primary key: makes each record unique
  - Default is the first AutoNumber data type added
- Properties: define characteristics of object
- Datasheet view: used to add, modify, delete, view records
- Design view: used to create and modify fields in a table
- Store data in smallest parts—i.e. instead of 1 field for full name make 2 for first/last
- Date arithmetic: data type date/time follows specific structure
- Normalization: use of multiple tables to reduce redundancy
- Field names have no spaces

Forms

- Form view: displays completed form, used to enter/modify data
- Layout view: visual representation used to create/modify form
- Design view: used to create/modify form with more options for controlling it

Reports

- Printed documents displaying information from database
- Layout data in useful and attractive format

- Can be based on one or more tables/queries, not all fields need to be included, allows data to be summarized
- Default graphic is Binder, but can be changed
- Report headers/footers: printed only once at beginning and end of report
- Page headers/footers: printed at the top/bottom of every page
- Group headers/footers: start/end of each grouping
- Unbound controls: no data source, displays titles, labels, lines, rectangles, graphics
- Bound controls: data source is a field in the table or query
- Calculated controls: data source is an expression usually consisting of values in fields, tables, queries (i.e. avg, sum)
- Report wizard: uses predefined report styles to create a report based on answers users provide
    - Choose fields, grouping level and order, sort and summarize, chose layout, style, name
- Establishing relationships: between primary and foreign keys from different tables/queries
    - Referential integrity: ensures data is relational database maintains consistency when data is changed (marked by infinity symbol)
        - Cascade update related fields OR cascade delete related fields

Queries

- Processed using SQL, provide a subset of a table based on specific criteria
    - Subset becomes an Access object
- Dataset: allow us to ask questions about data, the subset that answers the question
    - Questions formed using criteria, which restricts dataset to match parameters
- Select query: searches associated tables and returns a dataset that matches parameters
- Specifying criteria: use operands (i.e. <,>,=), wild cards (*, ?), null values, AND (must match all specified criteria), OR (must match only some of specified criteria)
- Run command (!): click this to run the query

SQL

- Structured Query Language statements retrieve and update data in a database
- ANSI: American National Standards Institute created standard computer language for accessing and manipulating database systems
- SQL works with database programs (Access, DB2, SQL Server, Oracle)
- Statement format: SELECT <attributes> FROM <tables> WHERE <conditions>
    - I.e. SELECT student.name, s-number, course.name, c-number FROM (Student INNER JOIN Takes ON Student. s-number=Takes. s-number) INNER JOIN Course ON Takes. c-number=Course. c-number WHERE s-number=”250615954”
- ORDER BY keyword: sorts results in ascending (“Asc”) or descending (“Desc”) order
- Nested queries: retrievals involving more than one query, make SQL statement for on then use that for the final SQL statement
- INSERT INTO statement: adds new instance of an entity or relationship to database
    - INSERT INTO <table> (<column1>, <column2>, etc.) VALUES (<v1>, <v2>, etc.)

- DELETE FROM statement: deletes instances
  - DELETE FROM <table> WHERE <instance condition>
- UPDATE statement: modifies attribute values
  - UPDATE <table> SET <column> = <new value> WHERE <instance conditions>

Chapter 7: Information Systems for Competitive Advantage

Information Systems affect Competitive Advantage

- To determine competitive strategies, businesses either…
  - Change the product: new or enhanced
  - Change business processes: use technology to secure customers, reduce costs, create barriers for competitors
- ISs make primary and support activities more productive than competitors
  - Holds true for commercial, non-profit, and government organizations
- Fundamental types of IS within organizations:
  - Calculation systems
  - Functional systems
  - Integrated/cross-functional systems

Calculation Systems

- Antiquated systems
- Relieved workers of repetitive calculations
- Labour-saving devices
- Produced little information
- I.e. computing payroll and writing cheques, inventory tracking

Functional Systems

- Facilitated work of single department or function
- Functions added to calculation system programs providing more value
  - I.e. payroll expanded to become human resources
- Functional silos: problem with system, designed to work independently of one another fostering isolation, BUT functional systems are interrelated which leads to data duplication, disjointed business processes across functions, limited information at any one source, inefficient decisions, increased cost to business
- Decisions that are appropriate for only single business function may be inefficient for an entire business process
- Reorganize Porter's Value Chain such that basic types of functional systems include…
  - Marketing and sales
  - Operations
  - Manufacturing
  - Human resources
  - Accounting

Marketing and Sales Information Systems

- Marketing IS: product and brand management that assesses…

    - Effectiveness of marketing messages
    - Advertising
    - Promotions
- Sales IS: involves…
    - Sales forecasting: planning production, managing inventory, financial reporting
    - Customer management: generate follow-up business, turn prospects into customers, manage customers
- Summary of functions of sales and marketing information systems:
    - Prospect generation
    - Lead tracking
    - Customer management
    - Sales forecasting
    - Product/brand management

Operations Information Systems

- Manage finished-goods inventory
- Used primarily by non-manufacturers
- Processes include…
    - Order entry
    - Order management
    - Finished-goods inventory management
    - Customer service

Manufacturing Information Systems

- Process data about inventory—manufacturing, scheduling, operations
- Support production and planning
- Manufacturing philosophies:
    - Push production planning: create schedule and push goods through manufacturing and sales
    - Pull production planning: respond to customer demand such that a reduction in inventory triggers production
    - "One-off" producers fall in neither category
- Inventory, manufacturing planning, manufacturing scheduling, and manufacturing operations facilitate production of goods

Accounting Information Systems

- General ledger, financial reporting, accounts receivable/payable, cost accounting, cash management, treasury management, budgeting applications
- Importance of legislation: creation of internal controls to prevent corporate fraud
    - Sarbanes-Oxley (SOX) Act (US)
    - Bill 198—Budget Measures Act (Canada)

Business Process Design/Redesign

- Does not simply automate or improve existing functional systems
- Paving the cow path: process of making what already exists more efficient

    - Making things easier without necessarily changing them
- Considers creation of new, more efficient business processes
    - Integrates activities of all departments involved in value chain
    - Cross-departmental business processes: takes advantage of an many activity linkages as possible
- Challenges:
    - Process design projects are expensive, difficult, and time consuming
    - Employees resist change
    - Ultimate outcome is uncertain

Industry Standard Processes

- Early business process design projects were tailor made
- 1990s software vendors designed integrated applications with built-in industry standard processes, which work to…
    - Integrate activities across departments
    - Save costs of tailor-made process design
    - I.e. Oracle, SAP
- Advantages: inherent business processes and use of tried and tested processes
- Disadvantages: may differ from pre-existing processes in the organization and may require it to change substantially

Integrated-Cross Functional Systems

- Operate across departmental boundaries—increased functionality and efficiency
- Transition from function systems is difficult, designed to overcome problems in functional systems
- Integrated processing requires a clear line of authority and the coordination of departmental activities
- Inter-organizational systems: used by 2 or more companies
- 2 cross functional systems:
    - Customer Relationship Management (CRM)
    - Enterprise Resource Planning (ERP)
- Most organizations have a mixture of functional and cross-functional systems

Customer Relationship Management (CRM) Systems

- Organization is customer-centered
- Support processes: attracting, selling, managing, delivering, supporting customers
- Includes only direct value chain activities involving customer
- Single repository for customer data
    - Eliminates inconsistent data
    - All departments have access to all customer data
- 4 customer life cycles:
    - Marketing sends message to target market
    - Prospects order and need to be supported
    - Support and resale increases value to existing customers
    - Win-back processes categorize customers according to value

Enterprise Resource Planning (ERP) Systems

- Enterprise wide, cross-departmental
- Support processes: primary business processes, human resources, account support
- Integrates sales, orders, inventory, manufacturing, customer service activities
- Based on documented, tested business models:
  - Provide software, pre-designed databases, procedures, and job descriptions for organization-wide process integration
- Provides cross-functional process view of organization through a formal approach based on formal business models
- Maintains data in centralized database
- Advantages:
  - Organizations don't need to reinvent processes, they are tried and tested
  - Inventory reduction due to better planning
  - Lead time reduction
  - No data inconsistency problems as it creates an integrated database
  - Lower costs and higher profitability
- Disadvantages:
  - Costly
  - Change is challenging
- Implementation: determine current models and ERP models >> remove inconsistencies >> implement the ERP system

Enterprise Application Integration (EAI) Systems

- Solves problems of isolated systems
- Provides layers of software that connect applications together
- Enables existing applications to communicate
- Provides integrated information
- Leverages existing system
- Enables gradual move to ERP
- No centralized database—files of metadata describing where the data is

Inter-organizational Systems

- Systems that cross organizations
  - Involve selling and purchasing
  - Integrate multiple company operations
- Types of inter-organizational systems:
  - E-commerce
  - Supply Chain Management (SCM)

E-Commerce and Web 2.0

- Systems working across organizations
- Provides competitive advantage to both parties—but disparity makes hard to implement
- Web 2.0: concept introduced by Tim Reilly describing applications and platforms on web
  - Focuses on providing services, not simply software applications, that can be accessed by a large number of people

    - Recognizes the importance of the user as part of the system, providing data and information that makes the service better
    - Creation of unique and difficult-to-develop data improves when more people use the system (i.e. Facebook)
    - Natural evolution of e-commerce
- E-commerce: buying and selling good/services over private or public computer networks
    - Merchant type: sell their own goods and services
        - Business-to-business (B2B)—i.e. Grand and Toy
        - Business-to-customer (B2C)—i.e. Amazon
        - Business-to-government (B2G)
    - Non-merchant type: sell service of others, arrange the sale of goods
        - E-commerce auctions: online auctions—i.e. eBay
        - Clearing houses/electronic exchanges: matches buyers with sellers (i.e. Priceline)
- Benefits of e-commerce:
    - Greater market efficiency→ disintermediation: elimination of layer of supply chain
    - Improves flow of price information→ web based price comparisons
    - For the seller: knowledge of price elasticity
        - Price elasticity: measures amount demand rises or falls with price changes
        - Losing-bidder auction prices
        - Price experimentation
        - More information obtained directly from customer

<u>Supply Chain Management (SCM)</u>

- Supply chain: network of organizations and facilities
    - Transforms raw materials into products
    - Products delivered to customers
- Integrates primary inbound logistics business activity
- Involves…
    - Customers, retailers, distributors, manufacturers, suppliers
    - Transportation, companies, warehouses, inventories
    - Method for transmitting messages and information among organizations
- Supply chain performance: facilities, inventory, transportation, information
- Three factors of information:
    - Purpose: transactional (orders/returns), or informational (customer order data)
    - Availability: access and sharing
    - Means: methods of transmission (i.e. XML)
- Information systems involved in supply chain management:
    - Supplier Relationship Management (SRM)
    - Inventory
    - Customer Relationship Management (CRM)
- Supplier Relationship Management (SRM): business process for managing contacts between an organization and suppliers
    - Supplier: any organization that sells something to an organization with an SRM application

        - I.e. manufacturer supplies to distributor
    - Supports inbound logistics primary activity, and the procurement support activity
    - SRM processes: source >> purchase >> settle
- Benefits of IS on supply chain performance:
    - Reduced cost of buying and selling
    - Expanded supply chain speed
    - Reduced size and cost of inventory—enables just-in-time inventory
    - Fix bullwhip effect
    - Supply chain profitability not optimized
- Bullwhip effect: variety in the size and timing of orders increases at each stage up supply chain
    - Natural dynamic of multistage supply chain
        - Unrelated to erratic customer demand
        - Large fluctuations force distributors, manufacturers, suppliers to carry large inventory
        - Reduce overall profitability
    - Eliminate effect by giving participants access to consumer-demand information
        - Inter-organizational information systems share data

Chapter 8: Decision Making and Business Intelligence

Challenges of Making Decisions

- Factors making business decisions challenging:
    - Uncertainty and complexity
    - Information overload
    - Data quality

Information Overload

- Exabyte= 10^18 bytes
- Storage capacity increases while cost decreases
    - Basically unlimited today
- Exponential growth of information
    - Inside and outside of organizations
    - Can be used to improve decision making
- Ability to store any amount of data pertaining to customers
    - Allows for better understanding of customers
    - Data can be used for forecasting
- Provides competitive strength when making decisions
- Business manager's challenge: find appropriate data, incorporate data into decision making
    - Information systems can both help or hinder this process
- Data quality: processed data from operational systems can be used for basic reports (i.e. current sales, sales projection)

OLTP Support for Decision Making

- Online Transaction Processing (OLTP) System: collects data electronically, processes transactions online
- Backbone of all the functional, cross-functional, and inter-organizational systems in an organization
- OLTP systems support decision making by…
    - Providing raw information about transactions
    - Providing information about the status of an organization

Basic Methods for Processing Transactions

- Real-time processing: transactions are entered and processed immediately upon entry
    - I.e. airline reservation, personal online banking systems
- Batch processing: system waits until it has a batch of transactions before the data is processed and the information is updated
    - I.e. transfer of all daily branch transactions to central office
- Data resource challenge: while data may be collected in OLTP system, the data may not be used to improve decision making
- Asset: resource from which future economic benefits may be obtained
    - Treat data as an important asset

Online Analytic Processing—OLAP

- Focus on making OLTP-collected data useful for decision making
- Provides the ability to sum, count, average, and perform other simple arithmetic operations on groups of data
- Final report has measured facts and dimensions

Business Intelligence (BI) Systems

- Provide information for improving decision making
- Primary systems (bolded shit):
    - Reporting systems
    - Data-mining systems
    - Knowledge management systems
    - Expert systems
- **Reporting systems:** process supplier information to rank quality
    - Integrate data from multiple sources
    - Process data by sorting, grouping, summing, averaging, comparing
    - Results form the report
    - Improve decision making by providing right information to the right user at the right time
- **Data mining systems**: search patterns to predict delivery delays or quality problems
    - Process data using statistical techniques:
        - Regression analysis
        - Decision tree analysis
    - Market based analysis: look for patterns and relationships to anticipate events or predict outcomes
        - Predict donations
    - Represents convergence of disciplines

    - Takes advantage of developments in data management to process enormous databases
    - Unsupervised data mining: analysis run *before* model created
        - Technique applied, then results observed
        - Hypotheses created after analysis to explain results
        - I.e. cluster analysis: technique to identify groups of entities that have similar characteristics
    - Supervised data mining: analysis run *after* model created
        - Statistical techniques used to estimate parameters
        - I.e. regression analysis: measures impact of a set of variables on another variable
        - I.e. neural networks: predict values; make classifications (i.e. good or bad prospect customer?)
        - I.e. market-based analysis: computes correlations based on past performances
- Market-based analysis: technique for determining sales patterns, creates probabilities that two items will be purchased together
    - Confidence: probability of purchasing 2 items together
    - Lift: ratio of confidence to the base probability of buying an item
    - May need to consider multiple-item purchases
- **Knowledge management systems:** process that creates value from intellectual capital by collecting and sharing human knowledge
    - Rank suppliers and share experiences
    - Supported by information system technology and the 5 components of information systems with an emphasis on people
    - Fosters innovation
    - Improves customer service
    - Increases organizational responsiveness
    - Reduces costs
- **Expert systems:** rule-based systems that encode human knowledge gathered from human experts
    - Contain rules for supplier selection
    - Improve diagnosis and decision making in non-experts
    - Expert system shells: program that processes the "if" side of the rules until no value gets returned, and reports the values of all variables
    - Difficult and expensive to develop
        - Labour intensive, ties up domain experts
    - Difficult to maintain, don't really live up to expectations
    - I.e. expert systems for pharmacies
        - MYCIN developed in 70s to diagnose certain infectious diseases
        - DoseChecker verifies appropriate doses
        - PharmaADE ensures patients not prescribed drugs with harmful effects

<u>RFM Analysis</u>

- Way of analyzing and ranking customers according to their purchase patterns

- Simple technique that considers…
  - How *recently* (R) a customer has ordered
  - How *frequently* (F) a customer orders
  - How much *money* (M) a customer spends per order

Data Warehouse

- Extracts and cleans data from operational system
- Prepares data for BI processing
- Data warehouse DBMS:
  - Stores data
  - May also include data from external sources
  - Contains metadata concerning data stored in the warehouse meta-database
  - Extracts and provides data to BI tools

Data Mart

- Maintain information on inbound logistics and manufacturing
- Data collection to address particular needs (business function, problem, opportunity)
- Smaller than data warehouse
- Users may not have data management expertise, so must have knowledgeable analysts for special functions
- Complete implementation is costly, and it requires data management expertise and knowledgeable analysts

Chapter 9: IS Strategy, Governance, and Ethics

Organizational Strategy and Information Systems

- Information systems help organizations achieve their goals and support a competitive advantage
- Effectively managing information systems requires a significant amount of IT planning
  - Developing plans requires understanding of the organization and the technology
  - Misalignment can occur as this is a difficult process
- Enterprise architect: creates blueprint of organization's information systems and the management of these systems
  - Organizational objectives, business processes, databases, information flows, operating systems, applications and software, supporting technology
- Popular method created by John Zachman (1980s) that divides system into 2 dimensions:
  - 6 reasons for communication (what? Data, how? Function, where? Network, who? People, when? Time, why? Motivation)
  - Stakeholders (planner, owner, designer, builder, implementer, worker)

Alignment

- Process of matching organizational objectives with IT architecture
- Not a straightforward process but an ongoing, continuous challenge fitting IT architecture with business objectives

- Measured as the degree to which the IT department missions, objectives, plans overlap with the overall business missions, objectives, plans
- Most important indictor of alignment is successful communication between the business and IT executives

Information Systems Governance

- Ensures organizations produce "good" results and avoid "bad" results
- Development of consistent management policies and verifiable internal processes
- Establishment of rules applying to sourcing, privacy, security, and internal investment
- Goal is to improve the benefits of an organization's IT investment over time
- Organizational governance associated with Information Technology Architecture
- Laws: Sarbanes-Oxley (SOX) Act in America, Bill 198- Budget Measures Act in Canada
    - Laws force companies to comply with collecting, reporting, discussing standards

Sarbanes-Oxley Act (US) and Budget Measures Act (Canada)

- SOX (2002): revision of Exchange Act (1934)
    - Governs reporting of publicly held companies
    - Enacted to prevent corporate fraud (i.e. WorldCom and Enron cases)
- Bill 198—Budget Measures Act
    - Similar legislation introduced in Canada
    - Increased level of responsibility and accountability of executive management of publicly held Canadian companies
- Both require management to create internal controls
- Organization's external auditor: issue an opinion on the quality of controls and management statements
- Expose manager and external auditor to financial and potentially criminal liability if events show the internal controls were defective
- I.e. setting Internet controls: separation of duties and authorities in accounts payable
    - Someone to authorize expense, one to issue cheque, one to account for transaction
- Computer-based accounting systems used for the production of financial statements
    - Appropriate controls in place to ensure reliability
- IS production of assets tat are subject to liability (i.e. order processing IS for customer information—must ensure only authorized access to information)
- Goal is to strengthen and upgrade financial reporting and thus maintain and improve trust in public companies' financial reports
- Large companies expect to divert more than 15% of IT budget to SOX compliance, which will in turn provide full employment to internal and IT auditors

Information Systems Audit

- Examination and verification of a company's information resources that are used to collect, store, process, and retrieve information, including the organization's IS policies and procedures
- Many firms offer IS audit services (i.e. Information Systems Audit and Control Association—ISACA)

- Control Objectives for Information and Related Technology (COBIT): framework of the best practices for IT management
  - COBIT 4: latest edition (December 2005)
  - Allows management to benchmark the security and control practices for IT control
  - Allows users of IT services to be assured security and controls exist
  - Allows auditors to substantiate their opinions on internal control and advise on IT security and control matters
  - Addresses issue of control from 3 dimensions:
    - Business objectives
    - IT resources
    - IT processes

Green IT

- Green computing: using IT resources to better support the triple bottom line for organizations
- Triple bottom line: expands traditional financial reports to take into account ecological and social performance
- Primary goals:
  - Improve energy efficiency
  - Promote recyclability
  - Reduce the use of materials that are hazardous to the environment
- Energy Star program: international government/industry partnership to produce equipment that meets high energy efficiency specifications or promotes the use of such equipment
- E-cycling: recycling of electronic computing devices

Chapter 10: IT Department

IT Departments and Operations

- Responsible for providing IT services to the organization
- 2 basic activities:
  - Maintaining current IT infrastructure
  - Renewing and adapting infrastructure
- IT operations maintain the current IT infrastructure
  - Demands large portion of the IT budget
- IT operations include delivery of service, maintenance, protection, and management of IT infrastructure
  - Stability, predictability, accountability, reliability, security
- IT professionals: specialize in particular technology—networks, operating systems, databases, administrators, hardware
- Information Technology Infrastructure Library (ITIL): collection of books providing framework of best practices for IT operations

IT Projects

- Renew and adapt the IT infrastructure to keep IT working effectively in the future

- Responsible for changing the production system rather than maintaining it
- May be funded from outside IT department
- Use of IT professionals to have broader skill set
- Project Management Body of Knowledge (PMBOK): provides accepted project management techniques and practices
    - Developed by the Project Management Institute in 1996, revised in 2008
- IT operations and projects are separate fields that rely on one another
    - Projects end, infrastructure must be maintained and replaced with new projects

Using the Web

- IT department supports the company's website servers and applications
- Important role in delivering IT services for internal employees and external customers
- Web design roles:
    - Project manager (interacts with customer, moves project along)
    - Lead designer/analyst (overall look and design)
    - Developer (design and create functioning site)
    - Technical architect (server/browser support, database integration)
- Company's Intranet website (internal) contains…
    - Frequently asked questions
    - Web-based service request forms
    - Web-based applications (i.e. help desk)
- Company's Internet website (external) contains…
    - Frequently asked questions
    - Customer support information
    - Company directory/contact information

IT Department Responsibilities

- Managing IT infrastructure: to provide IT services by managing and protecting IT, data resources, system applications
- Develop and adapt IS and IT infrastructure
- Align activities and services with primary goals and objectives of the organization
    - Facilitate business processes
    - Improve decision making
- Asses new technologies to determine possible applications
- Adapt infrastructure and systems to new business goals
- IT infrastructure: computers/servers and networks
    - Monitor, tune, repair
    - System outages are expensive
    - Respond to threats to infrastructure
- Data resource threats: human errors/mistakes, malicious human activity, natural events
    - IT department manages risk by…
        - Identifying risk
        - Estimating cost of risk
        - Specifying safeguards for risk
        - Determining the level of risk

- System applications: functional and cross-functional applications (i.e. ERP, CRM, SCM)
  - Support for applications built in-house
  - Managing system upgrades for purchased applications
  - Monitoring installation of systems and ensuring proper licensing of products
- Renewing IT infrastructure involves creating, developing, adapting IS and IS/systems infrastructure, and specifying standard computer systems

Decision to Adopt

- Decision based on analysis of costs and benefits (tangible, intangible)
- Tangible costs and benefits: directly measurable in dollars
  - I.e. labour, material, service/support cost savings
  - Service/support cost savings: value of not losing customers with support system
- Intangible costs and benefits: difficult to determine in dollars
  - I.e. cost of management's time to make decision, missed opportunities, customer bad will, value of email
- IS and IT expenditures: organizations justify expenditures by…
  - Computing costs
  - Computing tangible benefits
  - Performing financial analysis
  - If not justified, compute and consider intangible costs
- 5 innovation characteristics:
  - Relative advantage: performance of innovation relative to traditional products
  - Compatibility: ability to use it along with existing technology
  - Complexity: difficulty in using or understanding it
  - Triability: ability to use it before purchasing (i.e. 30 day trial)
  - Observability: extent that it can be demonstrated
- Technology Acceptance Model (TAM): 2 factors considered when adopting a technology
  - Perceived ease of use
  - Perceived usefulness

Costs in Typical IT Budget

- Operation costs: overlap in categories (i.e. operations personnel)
- Direct labour costs: applied direct to cost of project
- Indirect labour costs: management, data administration applied in personnel category
- Deployment costs: cost of setting up systems with little custom development
- Systems development costs: cost of creating new information
- Costs may be capitalized
  - Expense recorded as a depreciation against the capital expense
- IT budget typically developed incrementally, based on last year's expenses plus incremental changes

Who Pays for IT

- Small organizations: IT costs accumulated
  - Costs not assigned to departments or users
  - Treated as overhead expense

- Large organizations: chargeback expense
  - Costs allocated to users by department, number of users, number of computers
- Chargebacks: detailed allocation with complicated calculations
  - Trade-off between accuracy and cost of administration

IT Department Organization

- Chief Information Officer (CIO)
- Technology office
- Operations and development
- Outsourcing relations
- Data administration

Acceptable Use Policy (AUP)

- Set of rules restricting the use of information systems
- Written for corporations, businesses, universities, schools, and website owners
- Integral to the framework of information security policies

Chapter 11: Acquiring Information Systems through Projects

Acquiring Software for Information Systems

- 4 basic methods for acquiring *software applications*:
  - Buy it and use it
  - Buy it and customize it
  - Rent or lease it
  - Build it yourself
- Acquiring new software is NOT the same as acquiring new information systems
  - More to IS than just software
  - New software must be integrated into existing IS

Information Technology Projects

- Components: scope (objective), start and end dates, temporary use of resources, unique, accomplish change
- Large IT component in terms if budget or personnel
  - New email application requires CRM or ERP installation
- Require fundamental changes to business process—new IT supports changes
- Not exclusively about technology—impact on data, procedures, people
- Hard to estimate time, budget, scope

Project Management

- PMBOK: most recently published in 2008
  - Defines project as “consisting of a temporary endeavour undertaken to create a unique product, service, or result”
  - Compilation of the best practices, processes, techniques

    - 5 processes: stages in life of the project
        - Initiating
        - Planning
        - Executing
        - Monitoring/controlling
        - Closing
    - 9 knowledge areas: factors managed through life of project
        - Project integration
        - Scope
        - Time
        - Cost
        - Quality
        - Human resources
        - Communication
        - Risk
        - Procurement
- Information Technology Project Management (ITPM): collection of techniques and methods used to plan, coordinate, and complete IT projects
    - Methods include
        - Planning tools
        - Budgeting methods
        - Graphical scheduling methods (i.e. PERT, Gantt charts)
        - Risk management techniques
        - Communication planning
        - High-tech team development
    - Work breakdown structure: hierarchy of tasks required to complete project
        - Baseline WBS: final work-breakdown structure plan

<u>IT Project Risks</u>

- Not easy to represent graphically
- Lack of a good model
- Good estimates are difficult to develop because technology continually changes
- Difficult to monitor progress, estimate time, budget, and scope
- CHAOS report (1994): 16% of projects delivered on time, budget, scope; 30% were cancelled before delivering anything
- Sauer, Gemino, Reich report: 66% success rate (2/3); 25% general failure regardless of size

<u>Systems Development</u>

- Systems analysis and design—creation and maintenance of information systems
    - Development requires all 5 components (hardware, software, data, procedures, people), more than just programming or technical expertise
- ISs are never commercial-off-the-shelf (COTS), but adapted to fit needs of business and people
- Methodologies: no single process works in all situations (in detail further down)

- Systems Development Life Cycle (SDLC)
- Rapid Application Development (RAD)
- Object-Oriented systems Development (OOD)
- Extreme Programming (XP)

System Testing, Conversion, Maintenance

- Test plan: sequence of all actions taken when employing system
  - Includes all normal and error situations
  - Product Quality Assurance (PQA): testing specialists
  - Beta testing: future system users try out new system
- Conversion:
  - Pilot: entire system implemented on limited portion of business, so if system fails it only affects a limited boundary thus reducing exposure
  - Phased: new system installed in fields and tested after each phases, continues until it is installed in entire organization—can't be used in tightly integrated systems
  - Parallel: new system runs parallel to old one during testing expensive and time consuming, data must be entered twice, but benefit is the easy fallback system
  - Plunge: direct installation of new system and immediate discontinuation of old one with no backup—to be avoided at all costs
- Maintenance: tracks failures and enhancements
  - Corrections prioritized on severity, enhancements prioritized on business decision

Development Methodologies

- SDLC: classic process with 5 phases
  - Systems definition: management's statement defines new system's goals/scope
  - Requirements analysis: identify features and functions **most important phase**
  - Component design: based on approved user requirements (off the shelf, with alterations, custom made)
  - Implementation: implement, test, and install new system
  - System maintenance: repair, add features, maintain
  - Disadvantages:
    - SDLC Waterfall: phases get repeated when they aren't supposed to
    - Too many requirements
    - Hard to schedule and budget
- RAD: design/implement/fix development process
  - Iterative process with continuous active user involvement
  - Use of prototypes
  - Joint application design—conducted by teams
  - Use of computer-assisted software/system engineering tools (i.e. CASE)
- OOD: technique used is object-oriented programming (OOP)
  - OOP: designing and writing computer programs
  - Easier and cheaper to fix and adapt
  - Business applications slower process
  - Uses Unified Modeling Language (UML)
  - Unified Process (UP): designed for use with UML, 5 phases (3 similar to SDLC)

        - Inception
        - Elaboration
        - Construction
        - Transition
        - Maintenance
- XP: emerging technique for developing computer programs/applications
    - Extreme iterative development
    - Very short development cycle (only weeks)
    - Paired programming, customer-centric, just-in-time (JIT) design
        - Paired programming: unconventional method where 2 programmers work side-by-side on same computer continuously communicating, results in less errors and more easily maintainable

Outsourcing

- Process of hiring another organization to perform services
- Outsource any business activity in value chain (i.e. marketing and sales, manufacturing)
- Vendor can be domestic or international
    - Offshoring: vendor is overseas—tends to be less expensive, advantages of time difs
- Advantages: easier management, risk reduction, cost reduction
- Disadvantages: loss of control (vendor in control), benefits outweighed by long term costs (from vendor's costs and demands), no easy exit
- Alternatives:
    - Acquisition and operation of hardware and/or licensed software
    - Outsourcing entire system
    - Business function outsourcing (employee travel)
    - Application outsourcing (web-service hosting)

Application Service Providers (ASP)

- Special form of outsourcing
- ASP agreement: contract with vendor to "rent" applications from vendor on a fee-for-service basis
- Vendor maintains the system at its own web location and the client organization accesses the application on the vendor's website
- Payments: monthly or yearly, based on the number of employees or "users"

Chapter 12: Managing Information, Security, and Privacy

Identity Theft

- Fastest growing crime
- Stealing, misrepresenting, or hijacking the identity of another person
- With vital information, an identity thief can…
    - Take over a victim's financial accounts
    - Open new bank accounts and transfer money
    - Apply for loans, credit cards, and other services

Sources of Security Threats

- Human errors and mistakes: accidental problems, poorly written programs or designed procedures, physical accidents
- Malicious human activity: intentional destruction of data, destroying system components, hackers, virus and worm writers, criminals and terrorists
- Natural events/disasters: fires, floods, etc., initial losses of capabilities, losses from recovery actions

Unauthorized Data Disclosure

- PIPEDA: Personal Information Protection and Electronic Documents Act
  - Personal information defined as information about an identifiable self not including name, title, business address, or employee telephone number
  - Gives individuals the right to know what an organization collects, uses, or discloses their personal information
  - Requires organizations to identify anyone who is responsible for keeping personal information private and secure
- Pretexting: pretending to be someone else (i.e. credit card call)
- Phishing: obtaining unauthorized data using pretexting via email (i.e. banking info)
  - Create replica of webpage to fool user into submitting personal info
  - Email send from apparently legitimate source and advised to follow link—may install spyware, adware, malware
  - One way to check would be to enter wrong password, it will usually still accept it
- Sniffing: interception of computer communications
  - Wired network: requires physical connection
  - Wireless network: “drive-by” access gained through unprotected network
  - Packet sniffers: programs capturing data from information packets as they travel over internet or company networks, confidential info can be taken
- Breaking into networks allows malicious stealing of data

Incorrect Data Modifications

- Human errors leading to incorrect entries of information and procedural problems
- System errors
- Hacking: unauthorized access to and use of computer systems, often done using known flaws in operating systems, application programs, or access controls
- Faulty service: incorrect systems operations (human or technical)
  - Usurpation: unauthorized programs invade a system and replace a legitimate program by halting it and substitution their own processing

Denial of Service (DoS)

- Caused by human error or malicious attacks
- Forces the victim’s computer to reset or consume its resources such that it can no longer provide its intended service
- Obstruct the communication media between the intended users and the victim so they can no longer communicate adequately
- Denial of Service (DoS) attack: system performance degrades until system freezes

- Overloading and shutting down an ISPs email system by sending email "bombs" at rate of 1000 per second from a randomly generated email address
- Shutting down a web server by sending multiple requests for a webpage

Elements of a Security Program

- Senior management involvement
  - Set policies
  - Balance costs against risk
  - Responsible for information security
- Safeguards: technical, data, human
- Disaster preparedness
- Incident response

Elements of Computer Security

- Support mission of organization depending on nature and size of organization
- Cost effective: cost benefit analysis, direct (labour costs), intangible (customer anger)
- Explicit responsibilities and accountabilities assigned to individuals
- Responsibilities outside department—consequences can affect other units
- Comprehensive, integrated, periodically assessed

Elements of a Security Policy

- Senior management defines policy and manages risk
- General statement of security program:
  - Provides foundation for more specific security measures
  - Specifies goals and assets to be protected
  - Designates security management department
  - Ensures enforcement of policies
- Issue-specific policies: personal use of computers, use of email services, and Internet
- System-specific policies: addressed as part of standard systems development process
  - Customer data (sold or shared with others), processing employee data

Risk and Uncertainty

- Risk: likelihood of adverse occurrence
  - Known threats and consequences
  - Management must manage likelihood by limiting consequences, but reducing risk always costs
- Uncertainty: different from risk
  - Unknown threats and consequences
- Due to uncertainty, risk management is never exact

Assessment of Risk

- Define assets: sensitive data, computer facilities, trademark and brand (phishing), employee privacy
- Assess potential threats: likelihood of occurrence, consequences of occurrence
- Safeguard (technical, data, human): reduces vulnerability
- Vulnerability: opening or weakness in security system

- Consequences: damages when asset is compromised, tangible and intangible
- Likelihood: probability assets will be compromised
- Probable loss: bottom line of risk assessment

Technical Safeguards

- Hardware and software
- Usernames and passwords: identification and authentication
- Smart cards: magnetic strip or microchip contains identification information, can be used with Personal Identification Number (PIN) to be more effective
- Biometric authentication: authenticities with physical characteristics (fingerprints, facial and retinal scans)
- Single sign-on: typically multiple levels of authentication
    - Personal computer, LAN, database

Malware: Spyware and Adware

- Virus: computer program that replicates itself
- Worm: virus that propagates on internet or other computer
- Trojan horse: virus that masquerades as useful programs or files
- Spyware programs: installed on user's computer without user's knowledge or permission
    - Program observes user actions/keystrokes and monitors computer activity
    - Reports activity to sponsoring organization (i.e. marketing analysis, purchasing)
    - Maliciously used to obtain names, passwords, account numbers, sensitive information
- Adware programs: similar to spyware but typically not malicious
    - Watches user activity and produces pop up ads
    - Not illegal but many object to it
    - Can modify defaults (windows, search engine, search results)
- Symptoms:
    - Slow
    - Pop ups
    - Suspicious changes to computer
    - Unusual hard drive activity

Antivirus and Antispyware

- Install recommended software
    - I.e. Trends PC-Cillin, Norton AntiVirus, Lavasoft Adware, etc.
- Scan system frequently (automatically once a week)
- Update software definitions

Data Safeguards

- Data administration: organization-wide function that develops data policies
    - Enforce data standards
- Database administration: specific database function with procedures for multi-user processing
    - Control of changes to database structure and protection of database

- Establish user data rights and responsibilities
- Enforce rights with user accounts and passwords
- Encryption: protection for sensitive data
    - Key escrow: safety procedure where only trusted parties hold the key
- Back up copies: store off-site, check validity
- Physical security: lock and control access to facility, maintain entry log
- Third party contracts: periodically inspect premises and interview personnel

Human Safeguards

- People and procedure components
- Authorized users follow appropriate procedures for system use and recovery
- Restricting access requires authentication and user account management

Enforcement of Policies

- Responsibilities: define each position
- Accountability: hold employees accountable for violations
- Compliance: monitor employee activity
- Termination: create policies and procedures, mostly friendly

Non-Employee Personnel

- Temporary personnel and vendors: screening, training and compliance, contract, accounts with least privileges
- Public users: harden site and facility
    - Hardening a site: technical safeguard that locks down or eliminates unrequired features to reduce vulnerability
- Protect partners and public that benefit from system from internal company security problems

Account Administration

- Account management procedures: creation, modification, removal of accounts
- Password management
    - Strong passwords: 7+ characters, not a name or dictionary word, upper and lower case, special characters, constantly changed
- Help desk policies: can be security risk, must authenticate caller before providing information or access to it

Security Monitoring

- Activity log analyses:
    - Firewall log: dropped packets, infiltration attempts, unauthorized access attempts
    - DBMS log-in records: successful and failed log in attempts
    - Web server logs: documents web activities
- Analysis of logs: threat patterns, successful/unsuccessful attacks, evidence of vulnerability
- Security testing: in house and external security professionals
- Investigation of incidents

- Lessons learned for next time

Disaster Preparedness

- Disaster: substantial loss of infrastructure caused by acts of nature, crime, terrorism
- Best safeguard is location of infrastructure: so it is not prone to natural disaster
- Identify all critical systems that would cause organization to fall if lost, and identify all resources needed to run those systems (i.e. computers, OS, databases, etc.)
- Create backups for critical resources at remote processing centres
    - Hot site: remote site run by disaster recovery service
    - Cold site: empty space provided for customers to provide all the info needed
- Senior management decides based on balancing risk, benefits, costs

Three Types of Computer Crime

- Crimes committed using computer
- Crimes committed against computer
- Crimes where computer used to store data as evidence

Computer Crime Top Reported Losses

- Virus
- Unauthorized access
- Laptop theft
- Theft of proprietary data

Computer Forensics

- Forensics: use of science to obtain data for use by legal system
- Computer forensics includes identification, collection, examination, and preservation of digitally recorded data
- Complicated procedure: easy to damage data in the process
- Deleted data never really gone—system takes away space on disk but data still resides when overwritten
    - Software tools and read de-allocated space
- Data may be hidden in many locations on the network and can be disguised by name/type
- Steganography: messages hide by encoding them in files
    - Programs for finding them are fairly ineffective

Responding to Suspected Computer Crime

- Treat like any other security incident
- Develop incident response plan
- Balance liability against need to know full nature of attack
- Actions depend on nature of the crime
    - Constrain, eradicate, recover when dealing with a virus attack
    - Preserve evidence for prosecution

- May have to allow attack to continue in order to ;; gather evidence