Big Questions:

Chap 6

One

Problems with Traditional File Environments and the Solution

Traditional file environments can be cumbersome and inefficient, especially as data volumes grow. Here are some of the key problems:

- **Fragmented Data:** Files are often maintained by individual departments, leading to silos of information. This makes it difficult to get a holistic view of the data.
- **Data Redundancy:** The same data may be duplicated across multiple files, wasting storage space and increasing the risk of inconsistencies.
- **Data Inconsistency:** When data is scattered and redundant, it's more likely to have conflicting versions. This can lead to errors and unreliable information.
- **Program-Data Dependence:** Programs can become reliant on the specific structure of data files. If the file format changes, the program may need to be modified as well.
- **Limited Flexibility:** Traditional file systems are not very flexible when it comes to adapting to new data requirements or reporting needs.
- **Poor Security:** Since files are scattered around, it can be difficult to control access and ensure data security.
- **Restricted Sharing and Availability:** Sharing data effectively can be challenging due to fragmented storage and lack of centralized control.

The Solution: Database Management Systems (DBMS)

A Database Management System (DBMS) offers a more efficient and organized way to store and manage data. Here's how it addresses the problems of traditional file environments:

- **Centralized Storage:** A DBMS stores all data in a central location, making it easier to access and manage.
- **Reduced Redundancy:** The DBMS ensures data is stored only once, eliminating duplication and saving storage space.
- **Data Consistency:** The DBMS enforces data integrity rules to prevent inconsistencies.
- **Program-Data Independence:** Programs interact with the data through the DBMS, so they are not dependent on the physical structure of the data files.
- **Increased Flexibility:** The DBMS allows for easier data manipulation and reporting due to its structured query language (SQL).

- **Enhanced Security:** The DBMS provides user access controls and data security features.
- **Improved Sharing and Availability:** The DBMS facilitates data sharing and collaboration among authorized users.

By moving from a traditional file environment to a DBMS, organizations can improve data accuracy, efficiency, security, and overall data management.

TWO

COMPONENTS OF BUSINESS INTELLIGENCE

Business Intelligence (BI) relies on a powerful infrastructure to gather, store, analyze, and present data for informed decision-making. Here's a breakdown of the key components:

- **Data Warehouse:** This is the central storage unit for your BI system, acting like a giant pantry. It consolidates data from various sources into a single, organized location. Here, data is cleaned, transformed, and structured for analysis.
- **Data Mart:** A data mart focuses on specific business areas, like marketing or sales. Data marts contain a targeted subset of information relevant to a particular department, making it readily accessible for their analysis needs.
- **Hadoop:** For truly massive datasets, traditional data warehouses might struggle. Hadoop is a framework that distributes data storage and processing across clusters of computers, allowing you to handle big data efficiently.
- **In-memory Computing:** For super-fast analysis, especially with real-time data, in-memory computing comes into play. This approach stores data in the computer's memory for lightning-fast processing, ideal for situations requiring immediate insights.
- **Analytical Platforms:** These are the tools used by business analysts and other users to explore, analyze, and visualize the data stored in the BI system. Analytical platforms provide a user-friendly interface for data manipulation, allowing users to identify trends, patterns, and valuable insights for better decision-making.

Chap 8

ONE

Why Our Systems Are Vulnerable: A Breakdown of Threats

Our computer systems are like that – powerful tools, but with vulnerabilities that can leave them exposed. Here's a breakdown of the common culprits:

- **Network Accessibility:** Just like a castle with an open gate, easily accessible networks create a security risk. Hackers can exploit weaknesses in network security to gain unauthorized access.
- **Hardware Issues:** Physical hardware can malfunction (like breakdowns), be misconfigured (leaving settings insecure), or even be damaged by accidents, improper use, or even theft. These hardware problems can create openings for attackers or data loss.
- **Software Problems:** Just as a poorly built foundation can weaken a castle, buggy software with programming errors, faulty installations, or unauthorized modifications can create vulnerabilities in your system. These software problems can be exploited to introduce malware or steal data.
- **Natural Disasters:** Just like a powerful storm, natural disasters like floods, fires, or earthquakes can damage hardware and disrupt operations, potentially exposing or destroying data.
- **External Threats:** Information systems often connect to external networks or use devices outside the company's direct control (like public Wi-Fi). These external connections can introduce security risks if not properly managed.
- **Portable Device Risks:** Laptops, smartphones, and other portable devices are essential tools, but if lost or stolen, they can be a treasure trove of sensitive data for attackers. Strong data security practices are crucial for these devices.

TWO

Malicious Software: The Creeps in Your Computer

Imagine sneaky intruders trying to harm your computer. That's what malware, or malicious software, is all about. Here's a quick rundown of the different types and how they sneak in:

- **Malware (Malicious Software):** This is the umbrella term for all software designed to harm your computer or steal your data. Think of it as a general category of unwanted guests.
- **Viruses:** These replicate themselves and spread from one computer to another, often by attaching to files or programs.
- **Worms:** Similar to viruses, worms can spread quickly, but they exploit network vulnerabilities to jump from machine to machine without needing to be attached to a file.

How Malware Spreads: These malicious programs use various tactics to infiltrate your system:

- **Downloads & Drive-by Downloads:** Downloading infected files or visiting compromised websites can unknowingly install malware.
- **Emails & IM Attachments:** Opening malicious attachments in emails or instant messages can unleash malware.

- **Mobile Device Malware:** Just like computers, smartphones and tablets can be infected through app downloads or clicking on harmful links. Not all apps are created equal!
- **Social Network Malware:** Deceptive social media posts or messages with infected links can trick you into clicking and getting infected. Be skeptical of online offers that seem too good to be true.
- **Trojan Horses:** These disguise themselves as legitimate software, but once installed, they unleash their harmful effects. Think of a malicious program hiding inside a seemingly harmless gift horse.
- **Other Threats:** There are many other malware variations:
    - **SQL Injection Attacks:** These exploit weaknesses in website databases to steal data. Imagine someone breaking into a secret room through a hidden hatch.
    - **Ransomware:** This malware locks your files and demands a ransom to unlock them. Think of digital kidnappers holding your data hostage.
    - **Spyware:** This malware silently monitors your activity and steals your personal information. Imagine a secret spy gathering your information without you knowing.
    - **Keyloggers:** These programs record your keystrokes to steal passwords and other sensitive information. Think of someone spying on your fingers as you type.

Signs of Infection: If your computer is running slow, experiencing pop-ups, or behaving strangely, it might be infected.

Tools for Safeguarding Information Systems

Protecting your valuable data requires a layered defense, just like a well-fortified castle. Here's an overview of some key tools and technologies that act as your digital security guards:

- **Identity Management Software:** This software automates user accounts, assigns access privileges, and ensures only authorized individuals can enter your system.
- **Authentication: Verifying Who You Say You Are:** Here are some common methods:
    - **Password Systems:** The classic username and password combination. Choose strong, unique passwords and change them regularly.
    - **Tokens:** These small hardware devices generate unique codes for login, adding an extra layer of security.
    - **Smart Cards:** Similar to tokens, these embedded chip cards hold user information and require physical possession for authentication.
    - **Biometric Authentication:** Fingerprint scanners, facial recognition, or iris scans use unique physical characteristics for login.

    - **Two-factor Authentication:** This combines two methods, like a password and a code from your phone, for enhanced security.
- **Firewalls: Your Digital Wall:** Firewalls are hardware and software systems that monitor incoming and outgoing network traffic, blocking unauthorized access to your private network. They often use techniques like:
    - **Packet Filtering:** Inspecting data packets to ensure they come from authorized sources and follow security protocols.
- **Intrusion Detection Systems (IDS): Sentinels on the Walls:** IDS monitor network traffic and system activity for signs of intrusions and potential attacks.
- **Anti-malware and Anti-spyware Software: Your Digital Shields:** These programs act like shields against malicious software. They scan your system for malware and spyware, often able to remove them as well. Remember, these require regular updates to stay effective.
- **Encryption: Guarding Your Messages:** Imagine secret messages sent in code. Encryption scrambles data using algorithms, making it unreadable to anyone without the decryption key. This protects sensitive information during storage and transmission.

By using a combination of these tools and best practices, you can create a strong defense against cyber threats and safeguard your information systems.

THREE

Risk Assessment: Identifying and Mitigating Threats to Your Business

A business needs to be prepared for potential risks. Risk assessment is a crucial process that helps identify and analyze threats to your organization.

Here's a breakdown of what a risk assessment typically involves:

- **Understanding the Risk:** The goal is to determine the level of risk a specific activity or process poses to your business if not properly controlled.
- **Identifying Threats:** These are the potential events or situations that could cause harm. This might include security breaches, data loss, natural disasters, or even equipment failures.
- **Likelihood of Occurrence:** Here, you estimate how probable each threat is to occur within a given timeframe, typically a year. Consider factors like historical data or industry trends.
- **Potential Losses:** This involves estimating the financial impact of each threat if it materializes. Consider both direct losses, like replacing damaged equipment, and indirect losses, like revenue lost during downtime.
- **Expected Annual Loss (EAL):** This final step multiplies the probability of occurrence by the potential losses to estimate the average yearly cost you might

incur if the threat happens. This helps prioritize risks based on their potential impact.

By conducting a risk assessment, you can gain valuable insights into potential threats and take steps to mitigate them. This might involve implementing controls, like security measures or backup systems, to reduce the likelihood or impact of a threat.

Exposure	Probability of Occurrence	Loss Range (Average) ($)	Expected Annual Loss ($)
Power failure	**30%**	**$5,000 – $200,000 ($102,500)**	**$30,750**
Embezzlement	**5%**	$1,000 – $50,000 ($25,500)	$1,275
User error	98%	$200 – $40,000 ($20,100)	$19,698

FOUR

Encryption

Encryption scrambles data using algorithms, making it unreadable to anyone without the decryption key. This protects sensitive information during storage and transmission.

Here's a breakdown of the two main encryption methods:

- **Symmetric Key Encryption: Sharing a Secret Key**
  - In symmetric key encryption, both the sender and receiver use a single, shared secret key to encrypt and decrypt messages.
- **Public Key Encryption: A Two-Key System**
  - Imagine having a special lock with two keys: a public key that anyone can access and a private key that only you keep. Public key encryption uses two mathematically linked keys:
    - **Public Key:** This key is widely distributed and can be used by anyone to encrypt messages. It's like giving everyone a copy of the public lock.
    - **Private Key:** This key is kept secret by the recipient. It's the only key that can decrypt messages encrypted with the corresponding public key. Think of this as the only key that can open the lock created with the public key.

Here's how public key encryption works:

1. **The sender encrypts the message with the recipient's public key, which is readily available.**

2. **Only the recipient's private key can decrypt the message, ensuring confidentiality.**

CHAP 13

ONE

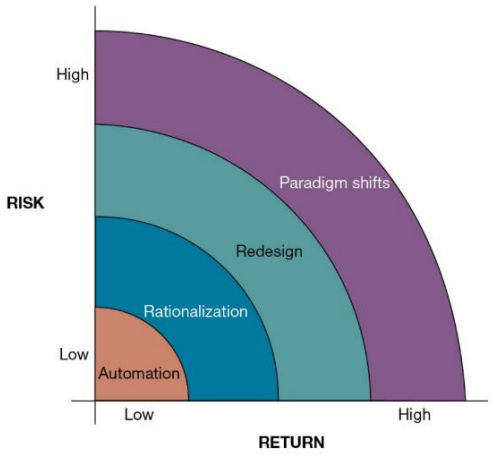
Systems Development and Organizational Change

The way we work is constantly evolving, and information technology (IT) plays a key role in driving organizational change. Here's how IT-enabled changes can transform your business:

- **Automation: Working Smarter, Not Harder:** Imagine replacing repetitive manual tasks with automated processes. IT systems can handle calculations, data entry, and other routine activities, freeing up employees for higher-level work. This increases efficiency and productivity.
- **Streamlined Operations:** Standardized operating procedures (SOPs) are the foundation for consistent work practices. IT can help rationalize these procedures by automating workflows, combining unnecessary steps, and eliminating duplication. Think of streamlining a factory assembly line for smoother production. This is often seen in programs for continuous quality improvement (CQI) initiatives.
- **Total Quality Management (TQM) & Six Sigma:** These methodologies focus on achieving excellence through continuous improvement. IT systems can support data collection, analysis, and reporting, allowing you to identify areas for improvement and track progress.
- **Business Process Redesign (BPR):** Sometimes, a complete overhaul is needed. BPR involves analyzing, simplifying, and redesigning entire business processes. IT tools can facilitate process mapping, workflow automation, and data-driven decision making for a more efficient organization. Imagine reorganizing an entire department for better collaboration and communication.
- **Paradigm Shifts: Rethinking the Game:** IT can sometimes lead to fundamental changes in how a business operates. This could involve defining a new business model, venturing into new markets, or fundamentally changing the nature of the organization. Think of a company transitioning from brick-and-mortar retail to a fully online model.

Remember, IT-enabled change is not just about technology. It's about using technology to empower people, streamline processes, and ultimately achieve your organization's goals

Figure 13.1 Organizational Change Carries Risks and Rewards



TWO

Business Process Redesign (BPR)

The way we work isn't set in stone. Business Process Redesign (BPR) is a powerful approach for organizations to analyze, improve, and fundamentally transform how they operate.

BPR falls under the umbrella of Business Process Management (BPM), which offers a variety of tools and methodologies to streamline and optimize business processes. Here's a breakdown of the key steps involved in BPR:

- **Identifying Opportunities for Change:** The first step is to pinpoint processes that could benefit from improvement. Are there areas with bottlenecks, inefficiencies, or a lack of clear ownership? Think of a cluttered workspace that needs reorganization.
- **Analyzing Existing Processes:** Once you've identified target processes, a deep dive is needed. This involves mapping the current process, identifying pain points, and understanding how tasks flow between departments.
- **Designing the New Process:** Now comes the creative part! Based on your analysis, redesign the process to eliminate inefficiencies and improve performance. This might involve automation, streamlining workflows, or even restructuring teams.
- **Implementation: Putting the Plan into Action:** Here's where the rubber meets the road. The redesigned process is rolled out, often in phases, to ensure a smooth transition. Communication, training, and change management are crucial during this stage.

- **Continuous Measurement: Tracking Progress and Adapting:** Change doesn't stop after implementation. It's important to continuously monitor the redesigned process, measure its effectiveness, and make adjustments as needed.

By following these steps and leveraging BPM tools, organizations can achieve significant improvements through BPR. This might include increased efficiency, reduced costs, improved customer satisfaction, or a competitive edge in the market.

THREE

The Power of Prototyping

- **What is a Prototype?** It's a **working but preliminary version** of your information system. Think of it as a rough draft or a scale model. It allows you to get early feedback and identify any issues before investing heavily in development.
- **The Prototype Process:**
    1. **Identify User Requirements:** Just like an architect needs blueprints, you need to understand what users need from the system. Gather their input and define the functionalities.
    2. **Develop the Initial Prototype:** This is a basic, but working model of the system. It might use simpler technologies or focus on core functionalities. Think of a basic sketch of the building layout.
    3. **Get User Feedback:** Put the prototype in the hands of your target users. Observe how they interact with it, gather their feedback, and identify areas for improvement.
    4. **Revise and Enhance:** Based on user feedback, refine the prototype. Add features, improve usability, and iterate until you have a solid foundation. Imagine revising the sketch based on feedback about functionality and flow.

- **Advantages of Prototyping:**

    - **Reduces Uncertainty:** If you're unsure about user needs or design solutions, a prototype allows for early testing and course correction. It's like checking the blueprint to ensure it aligns with your vision before construction begins.
    - **User-Centric Design:** Prototypes excel at user interface (UI) design. They allow users to interact with the system and provide valuable feedback on its usability and intuitiveness. Imagine testing furniture placement in a mock-up room to ensure user comfort before buying everything.
    - **Meeting User Needs:** By involving users early and often, prototypes increase the likelihood of the final system meeting their actual needs and

expectations. It's like ensuring the final building is functional and meets the needs of those who will use it.

- **Disadvantages of Prototyping:**
    - **Potential Shortcuts:** Sometimes, prototypes can lead to skipping essential design steps in favor of a quick build. Ensure the core functionalities are well-defined before prototyping.
    - **Scalability Limits:** Prototypes are often designed for limited data or users. They might not handle large-scale implementations effectively. Think of a small-scale model building that might not translate perfectly to a full-size structure.
    - **Testing and Documentation:** Prototypes may not undergo rigorous testing or extensive documentation. Remember, they are stepping stones, not replacements for thorough development processes.