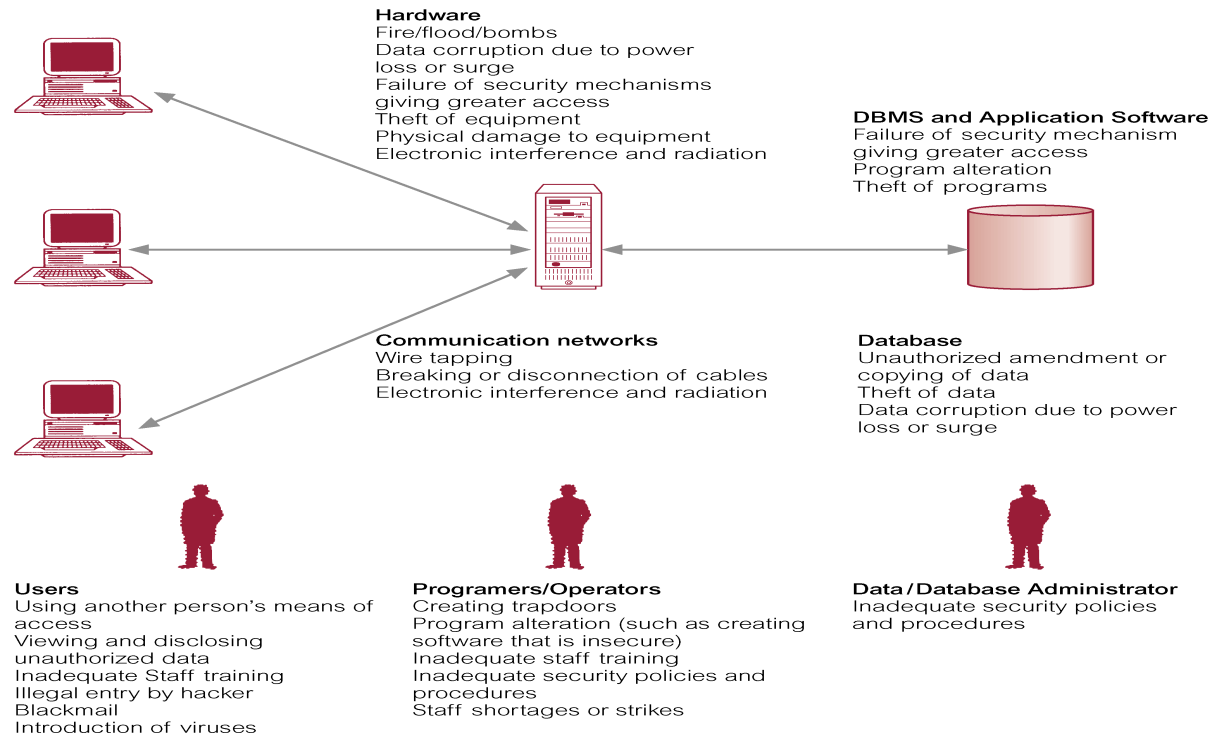
**Database Security**

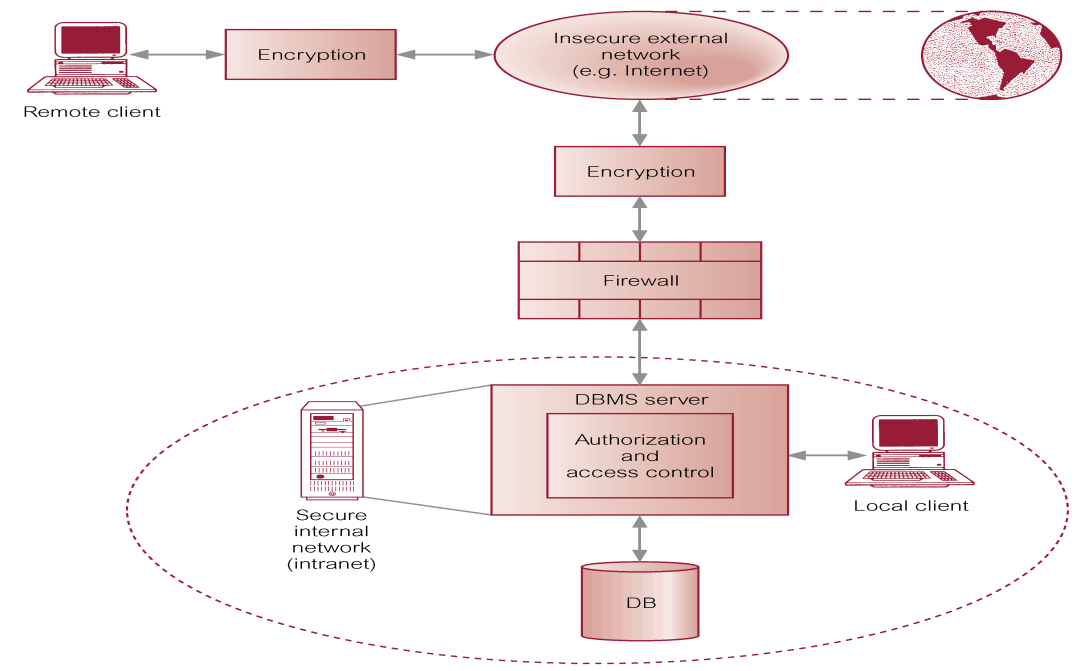
* Data is a valuable resource that must be strictly controlled and managed, as with any corporate resource.
* Part or all of the corporate data may have strategic importance and therefore needs to be kept secure and confidential.
* Mechanisms that protect the database against intentional or accidental threats.
* Security considerations do not only apply to the data held in a database. Breaches of security may affect other parts of the system, which may in turn affect the database.
* Involves measures to avoid:
  + Theft and fraud
  + Loss of confidentiality (secrecy)
  + Loss of privacy
  + Loss of integrity
  + Loss of availability
* **Threat**

Any situation or event, whether intentional or unintentional, that will adversely affect a system and consequently an organization.

**Summary of Threats to Computer Systems**



**Typical Multi-User Computer Environment**



**Countermeasures – Computer-Based Controls**

* Concerned with physical controls to administrative procedures and includes:
  + Authorization
  + Views
  + Backup and recovery
  + Integrity
  + Encryption
  + RAID technology
* **Authorization**
  + The granting of a right or privilege, which enables a subject to legitimately have access to a system or a system’s object.
* **Authentication**
  + A mechanism that determines whether a user is who he or she claims to be.
* **View**
  + Dynamic result of one or more relational operations operating on the base relations to produce another relation.
  + A virtual relation that does not actually exist in the database, but is produced upon request by a particular user, at the time of request.
* **Backup**
  + Process of periodically taking a copy of the database and log file (and possibly programs) to offline storage media.
* **Journaling**
  + Process of keeping and maintaining a log file (or journal) of all changes made to database to enable effective recovery in event of failure.
* **Integrity**
  + Prevents data from becoming invalid, and hence giving misleading or incorrect results.
* **Encryption**
  + The encoding of the data by a special algorithm that renders the data unreadable by any program without the decryption key.
* **RAID (Redundant Array of Independent Disks) Technology**
  + Hardware that the DBMS is running on must be *fault-tolerant*, meaning that the DBMS should continue to operate even if one of the hardware components fails.
  + Suggests having redundant components that can be seamlessly integrated into the working system whenever there is one or more component failures.
  + Main hardware components that should be fault-tolerant include disk drives, disk controllers, CPU, power supplies, cooling fans.
  + Disk drives are most vulnerable components with shortest times between failure of any of the hardware components.
  + One solution is to provide a large disk array comprising an arrangement of several independent disks organized to improve reliability and increase performance.
  + Performance is increased through *data striping*: the data is segmented into equal-size partitions (the *striping unit*), which are transparently distributed across multiple disks.
  + Reliability is improved through storing redundant information across the disks using a *parity* scheme or an *error-correcting* scheme.
  + There are a number of different disk configurations called RAID levels.
* RAID 0 Nonredundant
* RAID 1 Mirrored
* RAID 0+1 Nonredundant and Mirrored
* RAID 2 Memory-Style Error-Correcting Codes
* RAID 3 Bit-Interleaved Parity
* RAID 4 Block-Interleaved Parity
* RAID 5 Block-Interleaved Distributed Parity
* RAID 6 P+Q Redundancy

**DBMSs and Web Security**

* Internet communication relies on TCP/IP as the underlying protocol.
* However, TCP/IP and HTTP were not designed with security in mind. Without special software, all Internet traffic travels ‘in the clear’ and anyone who monitors traffic can read it.
* Must ensure while transmitting information over the Internet that:
  + inaccessible to anyone but sender and receiver (privacy);
  + not changed during transmission (integrity);
  + receiver can be sure it came from sender (authenticity);
  + sender can be sure receiver is genuine (non-fabrication);
  + sender cannot deny he or she sent it (non-repudiation).
  + Must also protect information once it has reached Web server.
* Download may have executable content, which can perform following malicious actions:
  + Corrupt data or execution state of programs.
  + Reformat complete disks.
  + Perform a total system shutdown.
  + Collect and download confidential data.
  + Usurp identity and impersonate user.
  + Lock up resources.
  + Cause non-fatal but unwelcome effects.
* Measures include:
  + Proxy servers
  + Firewalls
  + Message digest algorithms and digital signatures
  + Digital certificates
  + Kerberos
  + Secure sockets layer (SSL) and Secure HTTP (S-HTTP)
  + Secure Electronic Transactions (SET) and Secure Transaction Technology (SST)
  + Java security
  + ActiveX security.
* **Proxy Servers**
  + Proxy server is computer that sits between browser and Web server.
  + It intercepts all requests to Web server to try to fulfill requests itself.
  + Has two main purposes:
    - improve performance;
    - filter requests.
* **Firewalls**
  + Designed to prevent unauthorized access to/from a private network.
  + Can be implemented in both hardware and software, or a combination of both.
  + Several types of firewall techniques:
    - Packet filter.
    - Application gateway.
    - Circuit-level gateway.
    - Proxy server.
* **Message Digest Algorithms**
  + Message digest algorithm takes an arbitrary-sized string (*message*) and generates fixed-length string (*digest* or *hash*).
  + A digest has following characteristics:
    - Should be computationally infeasible to find another message that will generate same digest.
    - Digest does not reveal anything about message.
* **Digital Signatures**
  + Digital signature consists of two parts:
    - string of bits computed from data being ‘signed’;
    - private key of individual or organization wishing the signature.
  + Can be used to verify data comes from this individual or organization.
  + Digital signature has many useful properties:
    - Authenticity can be verified, using public key.
    - Cannot be forged (assuming private key is kept secret).
    - Function of data signed and cannot be claimed to be signature for any other data.
    - Signed data cannot be changed or signature will no longer verify data as being authentic.
* **Kerberos**
  + A server of secured user names and passwords.
  + Provides one centralized security server for all data and resources on network.
  + Database access, login, authorization control, and other security features are centralized on trusted Kerberos servers.
  + Has similar function to that of Certificate server: to identify and validate a user.
* **Secure Sockets Layer (SSL)**
  + Encryption protocol for transmitting private documents.
  + Designed to prevent eavesdropping, tampering, and message forgery.
  + Works by using private key to encrypt data that is transferred over SSL connection.
  + Layered between application-level protocols such as HTTP and TCP/IP transport-level protocol.
  + Thus, may be used for other application-level protocols such as FTP and NNTP.
* **Secure-HTTP (S-HTTP)**
  + Protocol for securely transmitting individual messages over Web.
  + Both SSL and S-HTTP use techniques such as encryption, and digital signatures, and:
    - allow browsers and servers to authenticate each other;
    - allow controlled access to Web site;
    - ensure data exchanged between browser and server is secure and reliable.
* **Secure Electronic Transactions (SET)**
  + Open, interoperable standard for processing credit card transactions over Internet, in simple and secure way.
  + Transaction is split in such a way that merchant has access to information about:
    - what is being purchased,
    - how much it costs,
    - whether payment is approved,
  + but no information on what payment method customer is using.
* **Secure Electronic Transactions (SET)**
  + Card issuer (e.g. Visa) has access to purchase price, but no information on type of merchandise involved.
  + Certificates are heavily used by SET, both for certifying cardholder and for certifying that merchant has relationship with financial institution.
* **Secure Transaction Technology (SST)**
  + Protocol designed to handle secure bank payments over Internet.
  + Uses DES encryption of information, RSA encryption of bankcard information, and strong authentication of all parties involved in transaction.
* **Java Security**
  + Sandbox ensures untrusted application cannot gain access to system resources.
  + Involves three components:
    - class loader;
    - bytecode verifier;
    - security manager.
  + Safety features provided by language and JVM, and enforced by compiler and runtime system.
  + Security is a policy built on top of safety layer.
* **ActiveX Security**
  + ActiveX security model places no restrictions on what a control can do.
  + Instead, each ActiveX control can be digitally signed by its author using system called Authenticode™.
  + Digital signatures are then certified by CA.
  + This security model places responsibility for the computer’s security on the user.