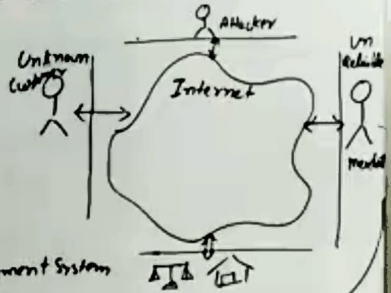
Security Threats to E-Commerce

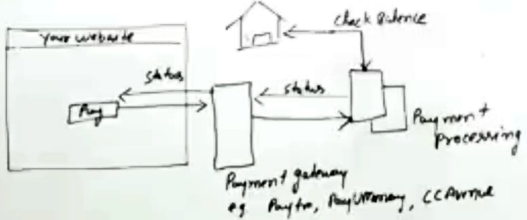
E-Commerce, also known as Electronic Commerce or Internet Commerce, refers to buying selling goods or services using internet and transfer money to execute this transaction.



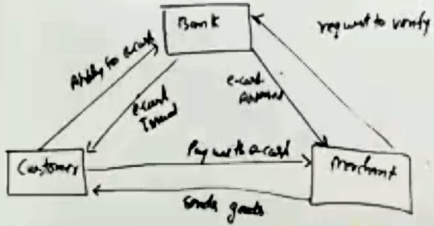
- E-commerce threats Can be
  1. Accidental
  2. Purposeful
  3. Human Error
- Threats are
  1. Electronic Payment System
  2. E-Cash
  3. Credit / Debit card
     (1) Skimming
     (2) Unwanted presence
     (3) Phishing
     (4) POS (Point of sale)

1. Electronic Payment System

transaction. It is user friendly and



(2) E-Cash: E-Cash is paperless cash System which facilitates the transfer of fund. It is stored in computer or mobile in form of softw wallet. eg. Paypal, paytm, google pay.



Digital Signature

A digital Signature is a mathmetical technique which validate the Authenticity and integrity of message, software or digital document.

Cyber Security provide following services.

1. Authentication
2. Non- Repudiation
3. Integrity
4. Confidentiality

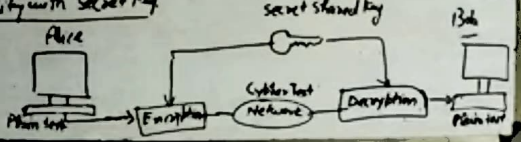
Algo in digital Signature

1. Key generation
2. Signing Algorithm
3. Signature Verifying Algo

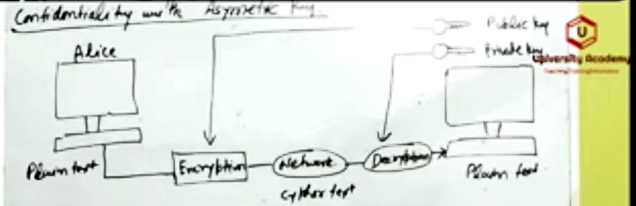
There are two type of key used in Cyber Security

1. Symmetric key (secret key)
2. Asymmetric key (Public key)

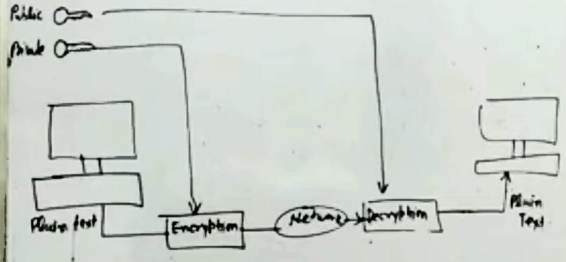
Confidentiality with Secret Key



Confidentiality with Asymmetric Key



Authentication, Integrity and Non- Repudiation using Asymetric key



Digital Signature

A digital Signature is a mathmetical technique which validate the Authenticity and integrity of message, software or digital document.

Cyber Security provide following services.

1. Authentication
2. Non-Repudiation
3. Integrity
4. Confidentiality

DS

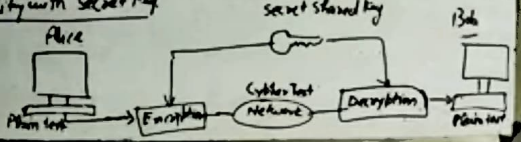
Algo in digital Signature.

1. Key generation
2. Signing Algorithm
3. Signature Verifying Algo

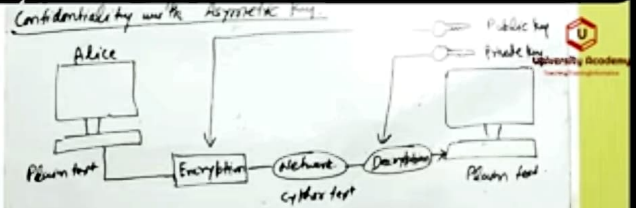
There are two type of key used in Cyber Security.

1. Symmetric key (secret key) one secret key.
2. Asymmetric key (Public key) two Public, Private

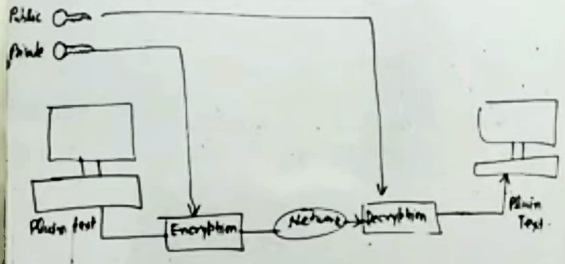
Confidentiality with Secret Key



Confidentiality with Asymmetric key



Authentication, Integrity and Non-Repudiation using Asymetric key



Digital Signature

A digital Signature is a mathmetical technique which validate the Authenticity and integrity of message, Software or digital document.

Cyber Security provide following services.

1. Authentication
2. Non-Repudiation
3. Integrity
4. Confidentiality

DS

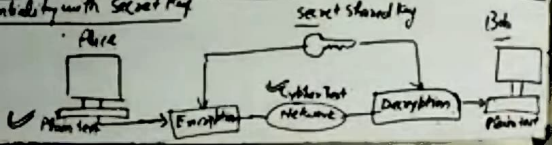
Algo in digital Signature

1 Key generation
2 Signing Algorithm
3 Signature Verifying Algo

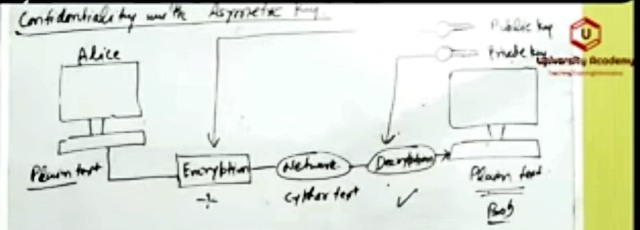
There are two type of key used in Cyber Security

1 Symmetric key (secret key) One secret key.
2 Asymmetric key (Public key) two Public, Private DS

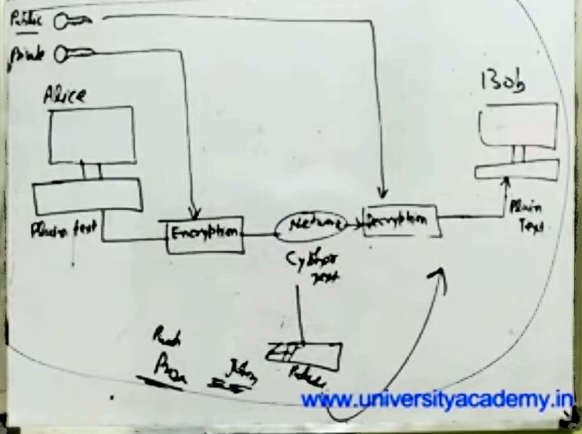
Confidentiality with Secret Key



Confidentiality with Asymmetric Key



Authentication, Integrity and Non-Repudiation using Asymmetric key



Secure Information System Development

During the SISD, stakeholders have to decide and select the Development Activity. Traditional development process do not take into Security Concern.

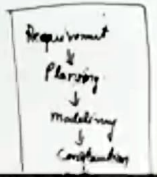
Therefore there exist approaches which focus on Security development techniques, method and tools.

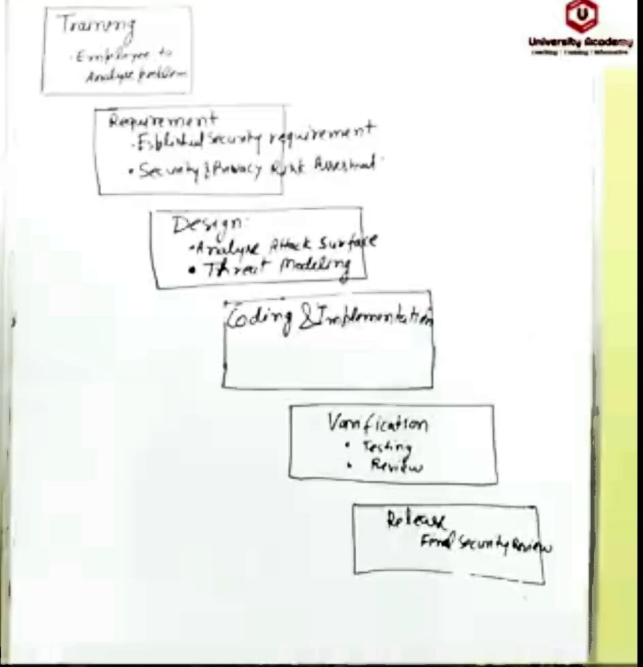
There are three SISD lifecycle

1. Mirosoft Secure Information System Development
2. Open web Application Security project
3. Comprehensive lightweight Application security process

Traditional s/w development process

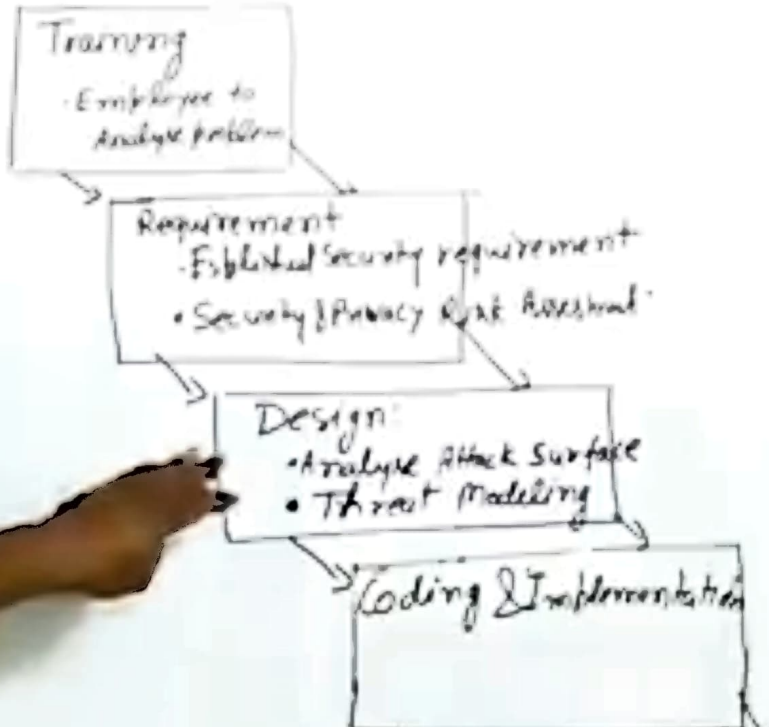
- Waterfall
- V- Model
- Spiral
- Incremental

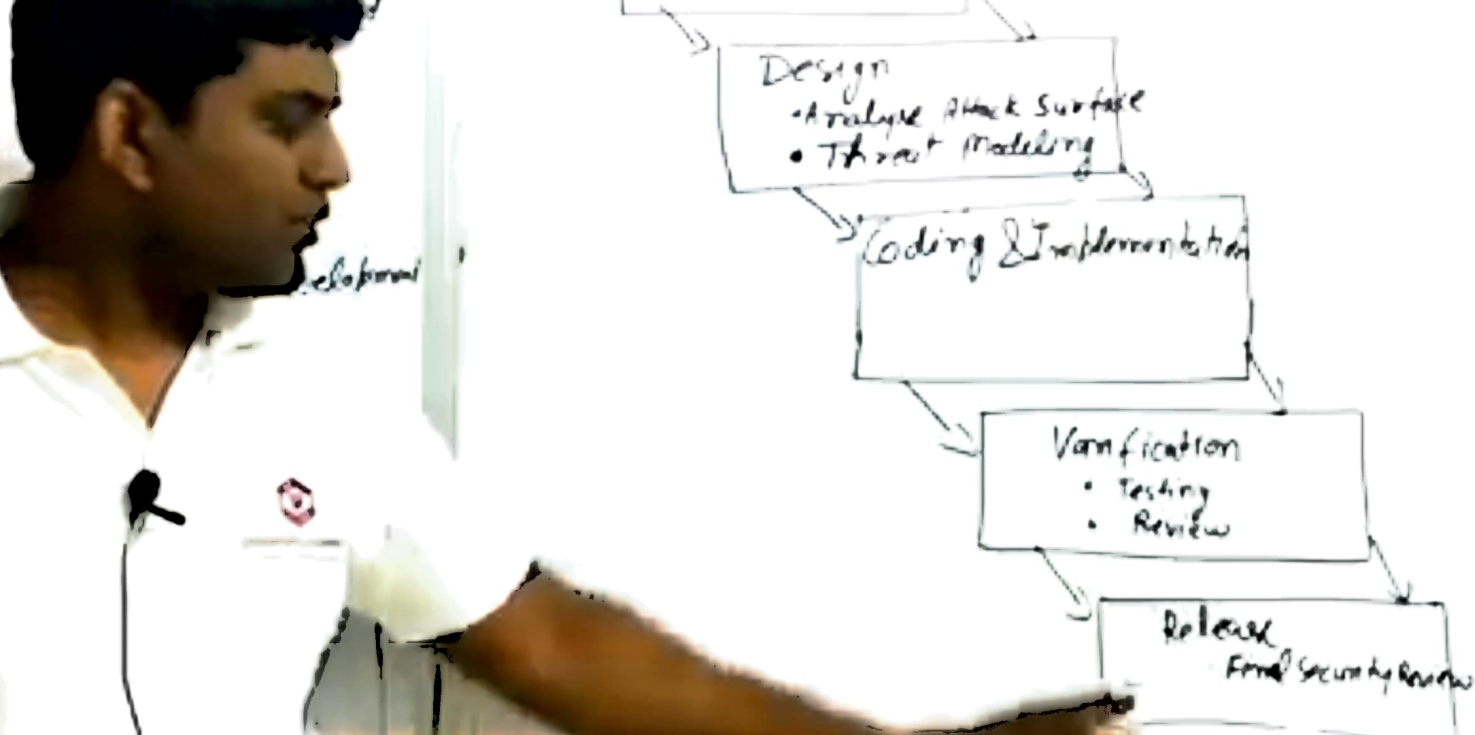




s have to decide and
Traditional develop-
nto Security Concern
st approaches which
techniques, method

SD Lifecycle




Design
• Analyse Attack Surface
• Threat Modeling
Coding & Implementation
Verification
• Testing
• Review
Release
Final Security Review

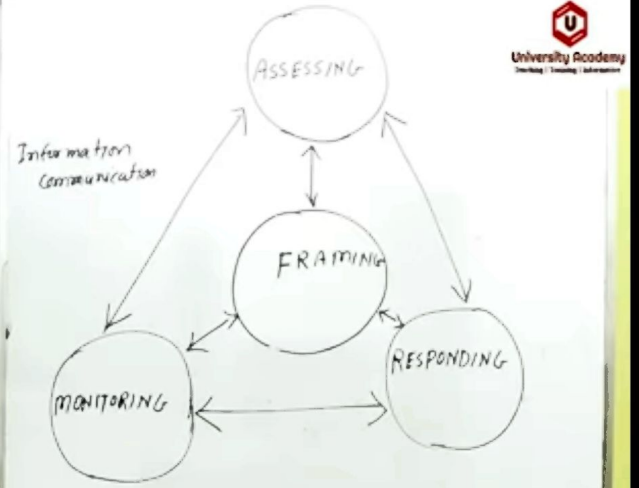
Information Security Governance & Risk Management

It involves the identification of an organisation's information assets & development, documentation & implementation policy, standard, procedure and guidlines to ensure CIA

Risk management is the identification, measurement, control, and minimization of loss associated with uncertain event or risks.

Risk Management process involves following four activities

1. Framing : Sense the threats
2. Assessing : Analyze the level of Risk
3. Monitoring : Keep eye on threats and monitor the system continuously Secure or Not
4. Responding : prevent or corrective measures, so system can be protected.

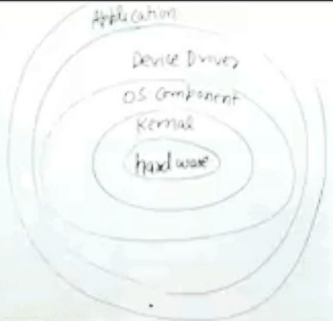


Security Architecture and Design

Security Architecture and Design describes the fundamental of hardware, operating System and software security component. How to use those component to Design, Architect, and evaluate Secure Computer System

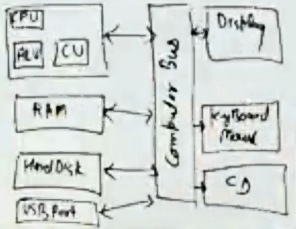
Secure Computer System Design Concept

1. Layering — Hardware, Kernal, OS, Application
2. Abstraction — hide Unnecessary detail from User
3. Security Domain: List of object allowed to access
   - Ring Model
     - Ring 0
     - Ring 1
     - Ring 2
     - Ring 3



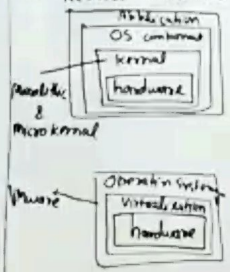
Secure hardware Architecture

1. System Unit and Motherboard
2. Computer Bus
3. North Bridge and South Bridge



Secure software Architecture

1. Kernal 2. Virtualization

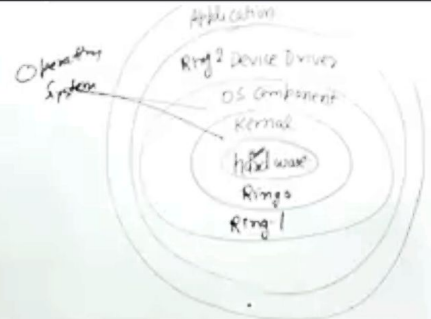


Security Architecture and Design

Security Architecture and Design describes the fundamental of hardware, operating System and software Security component. How to use those component to Design, Architect, and evaluate Secure Computer System

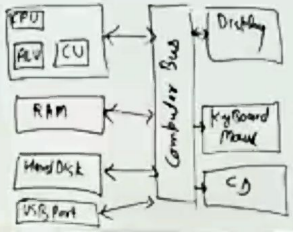
Secure Computer System Design Concept

1. Layering — Hardware, Kernel, OS, Application
2. Abstraction — hide Unnecessary detail from User
3. Security Domain: List of object allowed to access
4. Ring Model
   - Ring 0
   - Ring 1
   - Ring 2
   - Ring 3



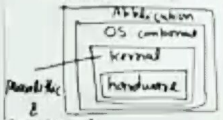
Secure hardware Architecture

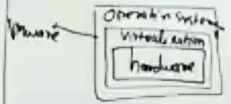
1. System Unit and motherboard
2. Computer Bus
3. North Bridge and South Bridge



Secure software Architecture

1. Kernel 2. Virtualization





...ure Computer System

System Design Concept

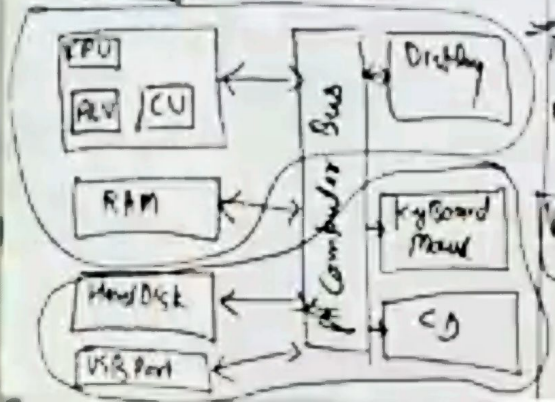
1 2 3 4
Hardware, Kernel, OS, Application

Unnecessary detail from User

List of object allowed to access

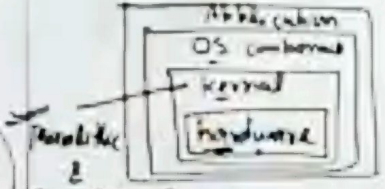
Secure hardware Architecture

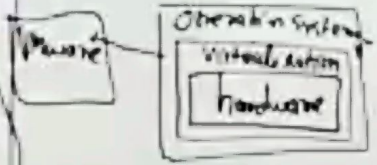
1. System Unit and motherboard
2. Computer Bus
3. North Bridge and South Bridge



Secure software Architecture

1 Kernel 2 Virtualization



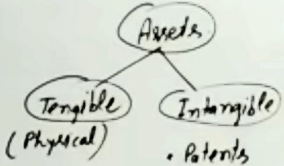


Physical Security of IT Assets

A Physical Assets is an item of Economic, Commercial or exchange Value that has a Material Existence.

The physical Assets are:

- Machinery
- Building and land
- Inventory
- Cash
- Furniture
- Vehicles
- Equipment
- Computers

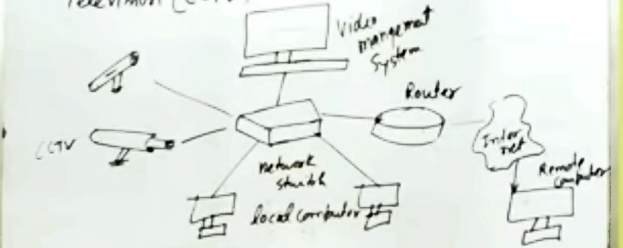


A Threats for Physical Assets

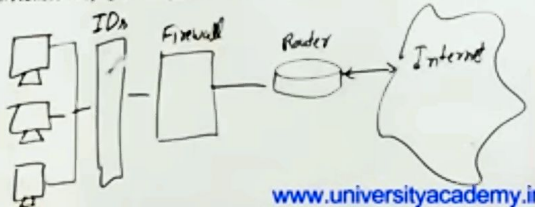
1. Physical Access exposure to human being.
2. Physical Access exposure to Natural Disasters.

To provide physical security to your we need to use following Mechanism:

1. Physical Access Control: Using locks, biometrics, Photo id, entry logs, computer terminal lock.
2. Electronic and Visual Surveillance - Close circuit Television (CCTV)



3. Intrusion Detection System



Backup Security Measures

Data Backup are taken to important data files and system from being lost due to Natural Disaster or human error and Recover in case loss of Information

To maintain proper data Backup security, an organisation should implement the following practices:

1. Assigning Responsibility, Authority and Accountability
2. Assessing Risk → Risk mgmt team Asses of data backup Risk.
3. Developing Data protection process
4. Communication the processes to concerned
5. Executing and testing the process.

University Academy
Teaching | Training | Informative

Advantage of Databackup security

1. Close personal protection
2. Crowd control
3. gaurd house personal
4. Alarm Responses
5. Surveillance and private Investigation

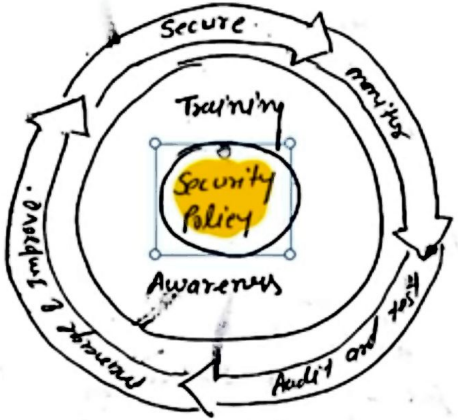
Unit - IV

SECURITY POLICIES

A security policy is a strategy for how your company will implement information security principle and technologies. An Information security policy is the documentation of organisation-level decisions on safeguarding information. A security policy is is different from will provide both high level and specific guidlines on how your company is to protect its data.

There are various forms, styles, and kind of security policies for different organisations, businesses, agencies. and Uni'

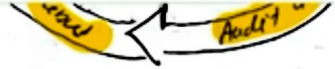
www.universityacademy.in



A security policy must accomplished three objective.

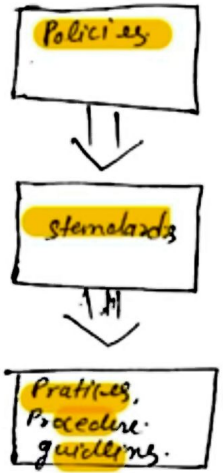
1. Confidentiality
2. Integrity
3. Availability.

Development of Security policy: A security policy is a ...



Development of Security policy: A security policy is a written document in an organisation outlining how to protect the organisation from threats, and how to handle situation when they occur.

- Planning for security:
  1. Creation and review of organisation policies, standard and practices.
  2. Creation of Architecture and security blueprint.
  3. Education and training to implement policies.



Policy are sectioned by senior manager

Standard built on sound policy and carry the lightweight of policy.

Practices, procedure and guidelines include de... steps requi... requirement of stan...

Types of Security policies.

requirement of standard.

Types of Security policies.

1. www policies. policy
ii Email Security policy
iii The Corporate policy
iv. Sample Security policy.

1. WWW Policy: The world wide web is a system for information over the Internet, the web is constructed from specially written program called web server that make information available the network. Other type program called web browsers can be u accesses information stored on Servers.

program called ... program called web browsers can be used to the network. Other ... program called web browsers can be used to access information stored on Servers.

There are following security policy should be applied on www.

1. No Offensive or harassing material available through company web site.
2. No personal commercial advertising available on company website.
3. The personal material should be minimum on website.
4. No company confidential material should be made available.
5. Users of an organisation should not be permitted to install ... run ... software.

(ii) **E-mail Security policy:** E-mail can be used for communication, transmit information, harass others, engage in illegal activities, and serve evidence against the action. E-mail is actually the electronic version of postcard and require special policy and guidelines. An organisation can include some policy for e-mail.

1. You will give same respect as verbal communications.
2. You will check spelling, grammar before send it.
3. You will not forward any chain letter.

policy and guidlines. An organisation can include some policy for e-mail.

1. You will give same respect as verbal communicating
2. You will check spelling, grammar before send it.
3. You will not forword any chain letter.
4. You will not send any spam.
5. not send any illegal document.
6. not send sensitive data
7. You will not use broadcasting except making appropriate Amanement.

you will not use broadcasting except [illegible]

Amusement.

8.

(iv) Corporate policy:

Corporate policy is the formal declaration of principle and procedure according to which a company will operate. These principle and guidelines are created by board directors, company senior management policy committee.

A corporate policy comprises:

1. Company mission statement
2. Company objectives.

A corporate :

1. Company mission statemnt
2. Company objectives.
3. Principle on the basis of which strategic decisions are made.

(iv) Sample Security policy: Lets Look the sample security policy:

1. Information security policy: Aim, Purpose, Responsibility, users.
2. Risk Assesmnt and Classification: Risk Assesmnt of Information and Personal data.

3. Protection of Information System and Assets.
4. Protection of Confidential information.
5. Risk Identification and Analysis: Threats and Risk.
6. Appendix: Sample Risk Assessment
7. Glossary.

Policy Review Process:

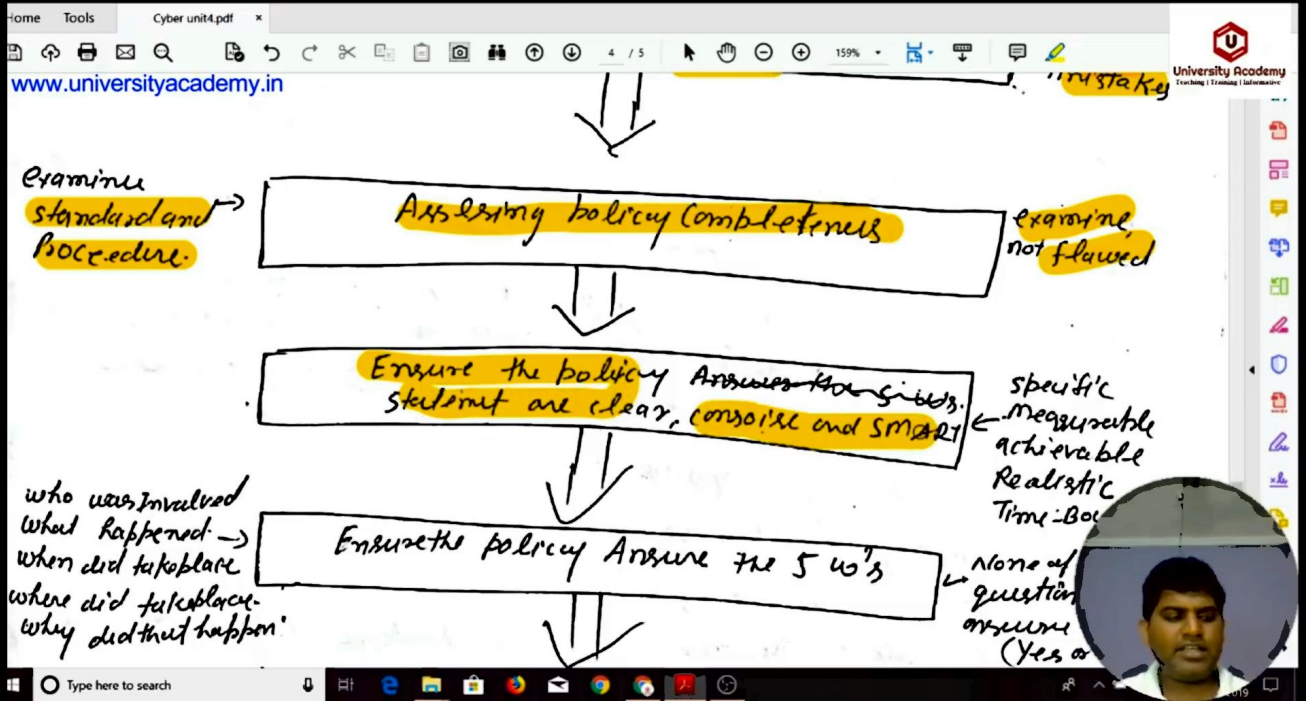
Policy Review Process:

Each policy created should be reviewed appropriately to ensure successfull policy development. there are six steps to evaluating information security policy.

own error in small % of time → Have Someone other than person who wrote the Policy. ← other Person Review for mistake

↓

examine standard and Procedure. → Assessing policy Completeness exam not fl



who was involved
what happened →
when did take place
where did take place
why did that happen

Ensure the policy Ansure the 5 w's

← None of these question can be answered by (Yes or No)

Realistic
Time-Bound.

Ensure Consistency with laws, Regulations.

laws & Regulation of Each country are different.

checking policy freshness and easy availability to organisation member

Keep the policy Update.

Publishing and Notification Requirement of the policies.

After ter policy have been written, they will not do your organisation any good if they sit on the shaf collecting dust. it should be not only documented but it also should be accessible to all users.

A common way of doing this is to publish the policy on local Intranet. this way not only the policy available to all users but your orga... updating costs and update can be

After ter policy have been written, they will not do your organisation any good if they sit on the shaf collecting dust. it should be not only documented but it also should be accessible to all users.

A common way of doing this is to publish the policy on local Intranet. this way not only are the policy available to all users but your organisation will save on printing costs. and update can be made easily on central location.

Introduction

- The evolution of technology has made a significant impact on how we do business today – for better or worse.
- Technological evolution is a theory of radical transformation of society through technological development.

- Evolving Technologies are : Mobile, Cloud, Outsourcing, SCM

Mobile security

- Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.
- There are following mobile security concerns
  - Loss of Devices
  - Securing Application
  - Data Leakage
  - Malware attacks
  - Device theft

Mobile security

- **How to Ensure Your Mobile Security and Privacy**
  - Always password-protect your phone.
  - Only download safe apps
  - Always read the terms and privacy policy
  - Turn off the Bluetooth
  - Set up remote locate/wipe
  - Back up your data
  - Update the operating system
  - Download anti-malware
  - Use public WiFi with caution

Cloud Security

- The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location.
- Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN
- Cloud Computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application.
- **Service Models**
  - Infrastructure-as–a-Service (IaaS)
  - Platform-as-a-Service (PaaS)
  - Software-as-a-Service (SaaS)

Cloud Security

- **Security** in cloud computing is a major concern. Data in cloud should be stored in encrypted form.
- Since all the data is transferred using Internet, data security is of major concern in the cloud. Here are key mechanisms for protecting data.
  - Access Control
  - Auditing
  - Authentication
  - Authorization
- Since data stored in cloud can be accessed from anywhere, a mechanism to isolate data and protect it from client's dire

Outsourcing

- Outsourcing is the business practice of hiring a party outside a company to perform services and create goods that traditionally were performed in-house by the company's own employees and staff.
- Outsourcing is a practice usually undertaken by companies as a cost-cutting measure
- **The Benefits and Risks of Outsourcing Security Services:**
  - Get access to skilled expertise. …
  - Focus on core activities. …
  - Better Risk Management. …
  - Increasing in-house efficiency. …
  - Run your business 24X7. …
  - Staffing Flexibility. …
  - Improve service and delight the customer. …
  - Cut costs and save BIG!

www.universityacademy.in
https://www.youtube.com/c/UniversityAcademy

Outsourcing Security

- **Risks associated with outsourcing security services are**
- Sensitive information that you do not want in the hands of an outsourced provider?
- Does the provider make specific commitments regarding confidentiality, integrity and availability?
- Will outsourcing introduce a single point of failure to your environment and, if so, what impact would a failure have?
- If you are storing critical data at the provider, will you keep local backups?

Supply Chain Management (SCM):

- Supply chain management (SCM) is the broad range of activities required to plan, control and execute a product's flow, from acquiring raw materials and production through distribution to the final customer, in the most streamlined and cost-effective way possible.

Supply Chain Management (SCM).

- **Typical supply-chain security activities include**
  - Credentialing of participants in the supply chain
  - Screening and validating of the contents of cargo being shipped
  - Advance notification of the contents to the destination country
  - Ensuring the security of cargo while in-transit via the use of locks and tamper-proof seals
  - Inspecting cargo on entry

University Academy

Teaching|Training|Informative

Cyber Security

Unit-V

Information Security Standards

By

Mr. Sandeep Vishwakarma

Assistant Professor

Dr. A.P.J. Abdul Kalam

Technical University,Lucknow

ISO (International Standards Organization)

- The **International Organization for Standardization** (**ISO**) is an international standard-setting body composed of representatives from various national standards organizations.
- Founded on 23 February 1947, the organization promotes worldwide proprietary, industrial and commercial standards. It is headquartered in Geneva, Switzerland and works in 164 countries.
- The International Organization for Standardization is an independent, non-governmental organization, the members of which are the standards organizations of the 164 member countries.

ISO security standard

- ISO has laid the following security standard:
  - ISO/IEC 27002:2005
  - ISO/IEC 27001:2005
  - ISO/IEC 15408:2005
  - ISO/IEC 1335

- ISO: International Organization for Standardization
- IEC: International Electrotechnical Commission

ISO/IEC 27002:2005

- ***Code of practice for information security management***
- ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.
- ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following

- security policy;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management;
- compliance.

ISO/IEC 27001:2005

- ***Information security management systems -- Requirements***
- ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations).
- ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks.
- The standard defines a cycle model known as "Plan-Do-Check-Act"
  - Plan Phase to establish the ISMS
  - Do Phase Implement the and Operate the ISMS
  - Check Phase Monitor and review the ISMS
  - Act Phase to maintain and improve the ISMS

ISO/IEC 15408:2005

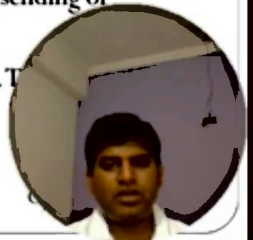
- ***Evaluation criteria for IT security : Introduction and general model***
  - Part 1: Introduction and general model (15408-1) :It defines general concepts and principles of IT security evaluation and presents a general model of evaluation.
  - Part 2: Security functional requirements (15408-2): It defines Security functional requirements, establishes a set of functional components as a standard way of expressing the functional requirements for TOEs [Targets Of Evaluation).
  - Part 3: Security assurance requirements (15408-3): It Defines Security assurance requirements, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs

ISO/IEC 1335

- ***Management of information and communications technology security***
  - Part 1: Concepts and models for information and communications technology security management
  - Part 2 of ISO/IEC 13335 provides operational guidance on ICT(Information and Communication Technology) security.
- Together these parts can be used to help identify and manage all aspects of ICT security.

Information Technology Act, 2000

- The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.
- The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 May 2000.
- The original Act contained 94 sections, divided into 13 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India
- A major amendment was made in 2008. It introduced Section 66A which penalized sending of "offensive messages".
- It also introduced provisions addressing child porn, cyber terrorism and voyeurism. T amendment was passed on 22 December 2008 without any debate in Lok Sabha.



Information Technology Act, 2000

- **Ley us have Look on the main features of this IT Act:**
  1. Preliminary
  2. Digital Signature
  3. Electronic Governance
  4. Attribution, Acknowledgement and Dispatch of Electronic Records
  5. Secure Electronic Records and Secure Digital Signatures
  6. Regulation of Certifying Authorities
  7. Digital Signature Certificates
  8. Duties of Subscribers
  9. Penalties and Adjudication
  10. The Cyber Regulations Appellate Tribunal
  11. Offences
  12. Network Service Providers Not to be Liable in Certain Cases
  13. Miscellaneous

Copyright Act

- The Copyright Act 1957 (as amended by the Copyright Amendment Act 2012) governs the subject of copyright law in India.
- The Act is applicable from 21 January 1958. The history of copyright law in India can be traced back to its colonial era under the British Empire.
- The Copyright Act 1957 was the first post-independence copyright legislation in India and the law has been amended six times since 1957.
- The most recent amendment was in the year 2012, through the Copyright (Amendment) Act 2012.

Definition of Copyright

- Copyright is a bundle of rights given by the law to the creators of literary, dramatic, musical and artistic works and the producers of cinematograph films and sound recordings.
- The rights provided under Copyright law include the rights of reproduction of the work, communication of the work to the public, adaptation of the work and translation of the work.
- The scope and duration of protection provided under copyright law varies with the nature of the protected work.
- In a 2016 copyright lawsuit, the Delhi High Court states that copyright is "not inevitable, divine, or natural right that confers on authors the absolute owne their creations

Cyber Law (IT Law) in India

- **Cyber Law** also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.
- ***According to Ministry of Electronic and Information Technology, Government of India :***

> ***Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.***

Area of Cyber Law:

- The major areas of cyber law include:
  - ***Fraud:*** Prevent identity theft, credit card theft and other financial crimes that happen online
  - ***Copyright:*** Protects the rights of individuals and companies to profit from their own creative works
  - ***Defamation:*** Protect from harm a business or someone's personal reputation
  - ***Harassment:***
  - ***Freedom of Speech***
  - ***Trade Secrets:*** Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.
  - ***Contracts and Employment Law:*** terms and conditions of using a website used cyber law

Intellectual Property India

- Intellectual property is an intangible property which applies to any product of the human intellect that has commercial value.
- Intellectual Property Rights (I P Rights) are one's legal rights in respect of the 'property' created by one's mind – such as an
  - Invention,
  - Piece of music,
  - An artistic work,
  - A name or slogan or symbol, or a design,
  - which is used in commerce, in the form of books, music, computer software, designs, technological know-how, trade symbols, etc.
- These rights are largely covered by the laws governing Patents, Trademarks, Cop Designs.

Patents

- The idea behind a patent is exclusivity of use of the invention within a particular territory. Thus, the owner of a patent has the exclusive right to stop others from making, selling, offering for sale, importing or using the patented invention in any other way.
- The inventor(s), assignee(s), legal representative(s) of deceased inventor or assignee may make the application for patent , either solely or jointly.
- In India, the patent system follows the First-to-File principle.
- A patent gives legal/commercial protection to the Applicant(s) (individual(s)/company(s)) holding it.

Patents

- **Criteria for an invention to be patentable**
  - **Novelty:** The invention has to be new and cannot be part of the "prior state of art"
  - **Inventive Step:** The invention will be judged by a person skilled in the relevant area. It should not be an obvious extension of the state-of-the-art.
  - **Industrial Applicability:** An invention must be capable of being produced or used in some kind of industry.

Trademarks

- A Trademark is a sign of serious commercial intent and protects/increases the goodwill of the owner's business
- It is seen as an evidence of ownership
- A trademark gives the owner legal recourse against illicit use
- Generally, the following can be registered as trademarks.
  - Invented words - one or more
  - A word, or combination of words, a logo, device, symbol, phrase, design, or a combination of any of these
  - Words without geographical significance and words which don't connote a personal name, surname or common abbreviation
  - A trademark which has acquired distinctiveness through use over a fairly long p time

Designs

- Creation of a novel and original outer appearance.
- The purpose of the design registration is to see that the artisan/creator/originator of the design
- First-to-File principle is applicable here
- A design should:
  - Be new and original
  - Not have been disclosed to the public
  - Not be contrary to public order or morality

Copyright

- Artistic work - 'Artistic Work' means a painting, sculpture, a drawing, an engraving or photograph
- Dramatic work - 'Dramatic Work' includes any piece for recitation, choreographic work or entertainment
- Literary Work - The term 'Literary Work' refers to any literary writings, as well as computer programs, tables, compilations and computer databases
- Musical work - 'Musical work' means a work consisting of music and includes any graphical notation of such work, but does not include any words or any action intended to be sung, spoken or performed with the music

Software License

- A software license is a document that provides legally binding guidelines for the use and distribution of software.
- Software licenses typically provide end users with the right to one or more copies of the software without violating copyrights.
- The license also defines the responsibilities of the parties entering into the license agreement and may impose restrictions on how the software can be used.
- Software licensing terms and conditions usually include fair use of the software, the limitations of liability, warranties and disclaimers and protections if the software or its use infringes on the intellectual property rights of others
- Software licenses typically are either
  - Proprietary : *Microsoft Windows, Adobe Flash Player, PS3 OS, iTunes, Adobe Photoshop, Google Earth, macOS*
  - Free: VLC player, Adobe PDF, yahoo messenger, Google Talk
  - Open source: OpenOffice, Mozilla's Firefox , MySQL , Ubuntu

Semiconductor Chip Protection Act of 1984

- A semiconductor material has an electrical conductivity value falling between that of a metal, like copper, gold, etc. and an insulator, such as glass. Its resistance decreases as its temperature increases, which is behaviour opposite to that of a metal.
- Computer chips, both for CPU and memory, are composed of semiconductor materials. Semiconductors make it possible to miniaturize electronic components, such as transistors.
- The **Semiconductor Chip Protection Act of 1984** (or **SCPA**) is an act of the US Congress that makes the layouts of integrated circuits legally protected upon registration, and hence illegal to copy without permission. It is an integrated circuit layout design protection law.
- Prior to 1984, it was not necessarily illegal to produce a competing chip with an identical layout.

Unit-III : Developing Secure Information Systems(Lecture 15-19)

1) Explain briefly the process of developing secure information system.
2) Describe in brief the application development security.
3) What do you understand by security architecture and design?
4) What are the security issue related to hardware ,data storage, and downloadable devices?
5) What are primary measures applied for the security of backup?

University Academy
Teaching | Training | Informative

Unit-IV: Security Policies (Lecture 20-25)

1) What is security policy? How do we develop a security policy?
2) Write short notes on
   a. www policy
   b. Email policy
   c. The corporate policy
3) What do you understand by Publishing and Notification Requirement of the Policies
4) What is Evolving Technology Security. Explain Outsourcing, SCM.
5) How to Ensure Your Mobile and Cloud Security and Privacy?

Unit-V: Information Security Standards (Lecture 26-30)

1) Describe the intellectual property issues (IPR).
2) Write short notes on Copyright act and the patent law.
3) Explain the semiconductor layout and design in detail.
4) Explain briefly the IT Act, 2000.
5) Briefly explain the ISO Standard.