सत्यमेव जयते

Cyber Security Awareness Programme

Internal to RCB

Introduction

Content

- Introduction
- Transition in our working styles and environment
- Cyberspace and incidents
- Basic Security concepts
- Information Security Management
- Security Frameworks
- Benefits of cyber security
- Scope
- Objective of policy
- Roles and responsibilities
- Security Categorization of Departments
- Components of Policy
- DARPG
- Securing your PC

Security Awareness

Since I am handling the documents(data=information) the responsibility lies with me…(each one of us)

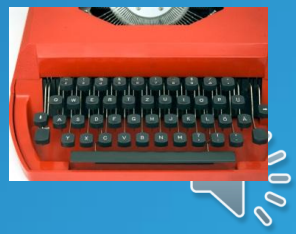
What is a Cyber Resource and Cyberspace?

What does Cyber Security mean

What is a security breach, what is an incident, how can I secure official documents when I work with computers, networks and other equipment

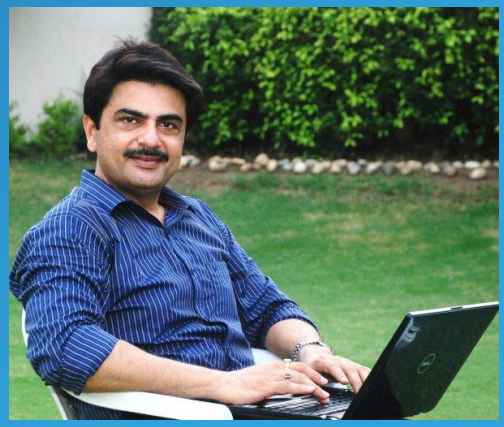
Transition in our working styles and environment

Typical Office Environment



Phones
Messages, Letters
Customer/Client/Vendor Information
Shared Files
Data security

With the advent of the newer technological devices, we need to learn newer ways of handling and securing documents…



Wireless networks, laptops, tablets, smartphones, mobile/remote working, biometrics

Daily office working generates information, which could be any of the following….

- Official letters or correspondence
- Office files
- Noting
- Personnel files
- Personnel records
- Financial records
- Department Plans
- Presentations
- Legal Documents (copy of contracts)
- Telephone and Address lists (vendors, suppliers, official contacts)

Note: Material in a computer is like material in a desk;

- With respect to both privacy and
- appropriateness

CYBERSPACE AND INCIDENTS

Cyberspace ?

- **Coined by science fiction writer William Gibson**
- ***Gibson* coined the term "*cyberspace*" in his short story "Burning Chrome" (1982) and later popularized the concept in his debut novel, *Neuromancer* (1984).**
- **It means the information spaces created by the technology of digital networked computer systems, most of which ultimately connect with the mother of all networks, the Internet.**

- Cyberspace

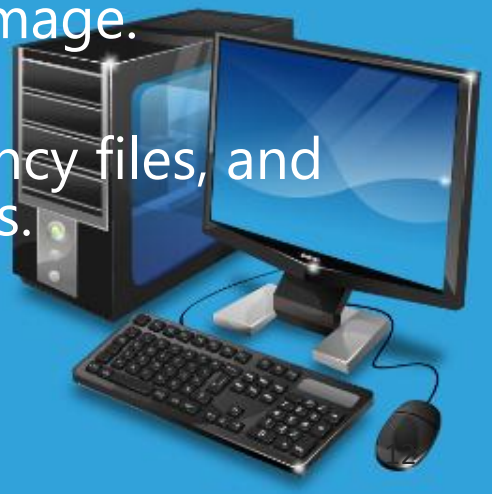
Securing data in cyberspace…

- By 1995, there was a growing consensus that cyberspace is that region that affects the
  - structure of our economies,
  - development of our communities, and
  - protection of our rights as free citizens.

- A secure cyberspace is vitally important to the nation.

- Every nation faces the real risk that adversaries will exploit vulnerabilities in the nation's critical information systems, thereby causing considerable suffering and damage.

- Online e-commerce business, government agency files, and identity records are all potential security targets.

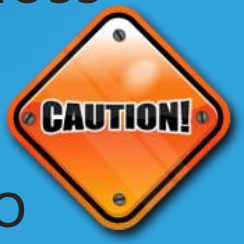


What do we all use the Internet for?

- Communication
  - e-Mails
  - Chat / Instant Messaging
  - Blogs
  - Social Networking
- Education & Research
- Current Affairs
- Online Shopping
- Online Banking
- Fun/Entertainment
  - Games
  - Movies
  - Songs

Risks, Threats and Vulnerabilities

- **Risk** is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset).
-
- A **vulnerability** is a weakness that could be used to endanger or cause harm to an informational asset

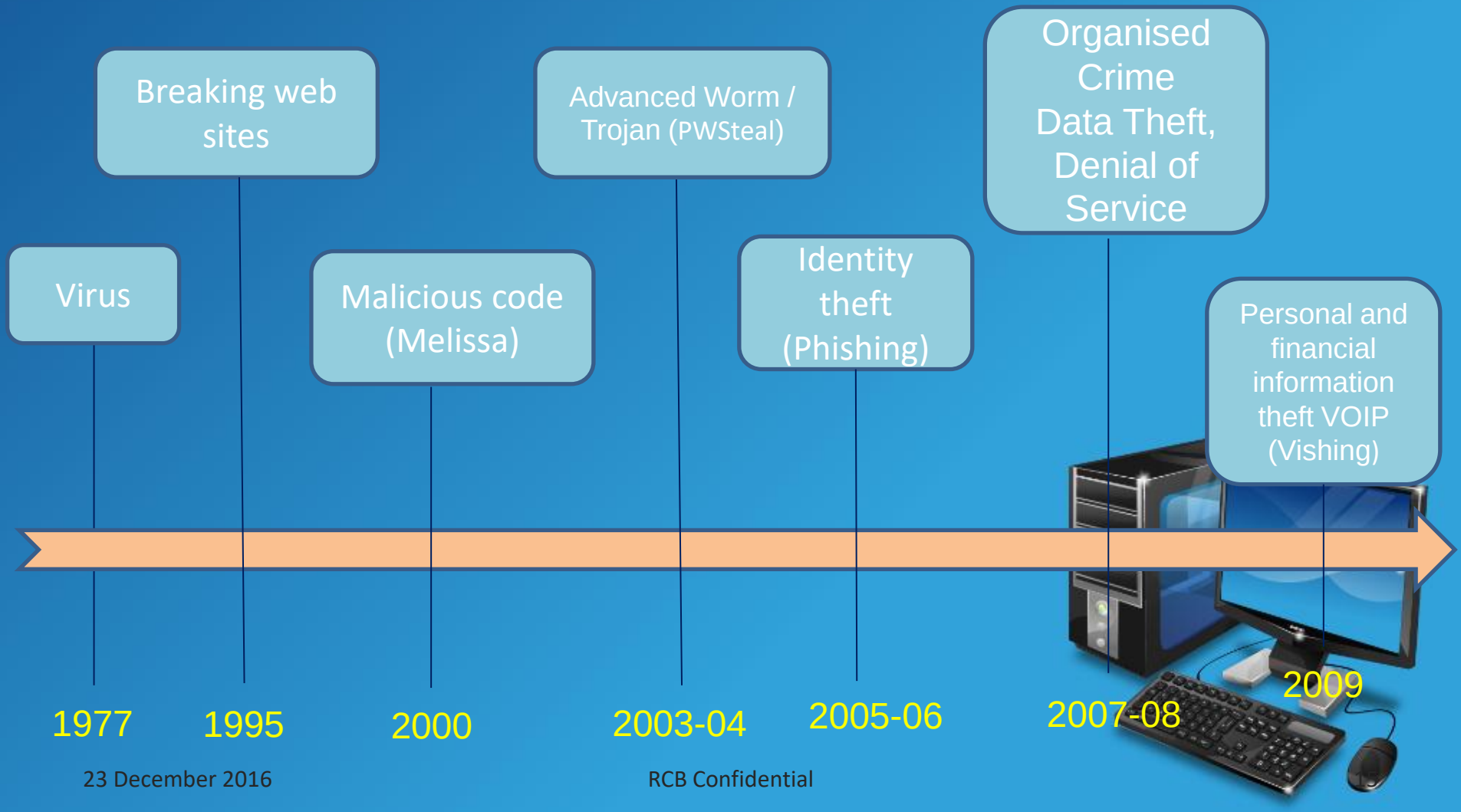


- A **threat** is anything (man made or act of nature) that has the potential to cause harm.

When a threat does use a vulnerability to inflict harm, it has an impact.

The impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property).

Cyber threats



Reports of some security incidents and their impact

- The Michelangelo worm in the 1990s, infected computers for about six years. A computer could be infected without the user even knowing - that is, until, the birthday of the famous artist on March 6, after whom the worm was named. On this date, it would engage with the operating system, overwriting computer storage devices and make them unusable. The damage it could cause in terms of lost productivity and billions in lost profits, caused panic.

- In late 2008, **McColo** a San Jose-based web hosting service provider, was shut down by the two upstream providers, Global Crossing and Hurricane Electric, because a significant amount of malware and botnets had been trafficking from the McColo servers.

- The **PlayStation Network outage** between April 17, 2011 and April 19, 2011, wherein individual pieces of personally identifiable information from each of the 77 million accounts appeared to have been stolen

- As many as 27 websites of various departments of Andhra Pradesh were hacked on Thursday, exposing the chinks in the state's cyber security.
- IANS Hyderabad, February 16, 2012

- Microsoft India store hacked by a Chinese group called Evil Shadow Team
- PTI New Delhi, February 14, 2012

Cyber attacks

- Web defacement
- Spam
- Spoofing
- Proxy Scan
- Denial of Service
- Distributed Denial of Service
- Malicious Codes
  - Virus
  - Bots
- Data Theft and Data Manipulation
  - Identity Theft
  - Financial Frauds
- Social engineering Scams

BASIC SECURITY CONCEPTS

Information Assurance

- The Five Pillars of Information Assurance model as defined by the U.S. Department of Defense (DoD)
- "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation."

Confidentiality

Integrity

Availability

Authentication

Non-Repudiation

Availability

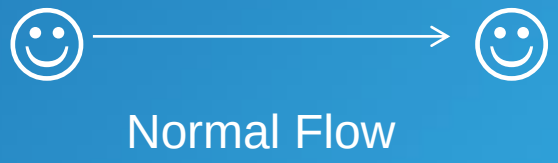
For any information system to serve its purpose, the information must be available when it is needed.

Mr. Sharma **Requirement** **Mr. Verma**

- computing systems
- security controls
- communication channels must function correctly
- preventing service disruptions due to
  - power outages,
  - hardware failures
  - system upgrades.
  - Denial of service attacks

Integrity

- In information security, integrity means that data cannot be modified without proper authorizations.
- Integrity is violated when a message is actively modified in transit.
- If some correspondence of the file is tampered with, without proper authorizations.



Confidentiality

- Confidentiality means to prevent the disclosure of information to unauthorized individuals or systems.

- Photo by: Microsoft

Confidentiality Breach

Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it.

If a laptop computer containing sensitive information about a company's employees is stolen or sold.

Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information

Authenticity

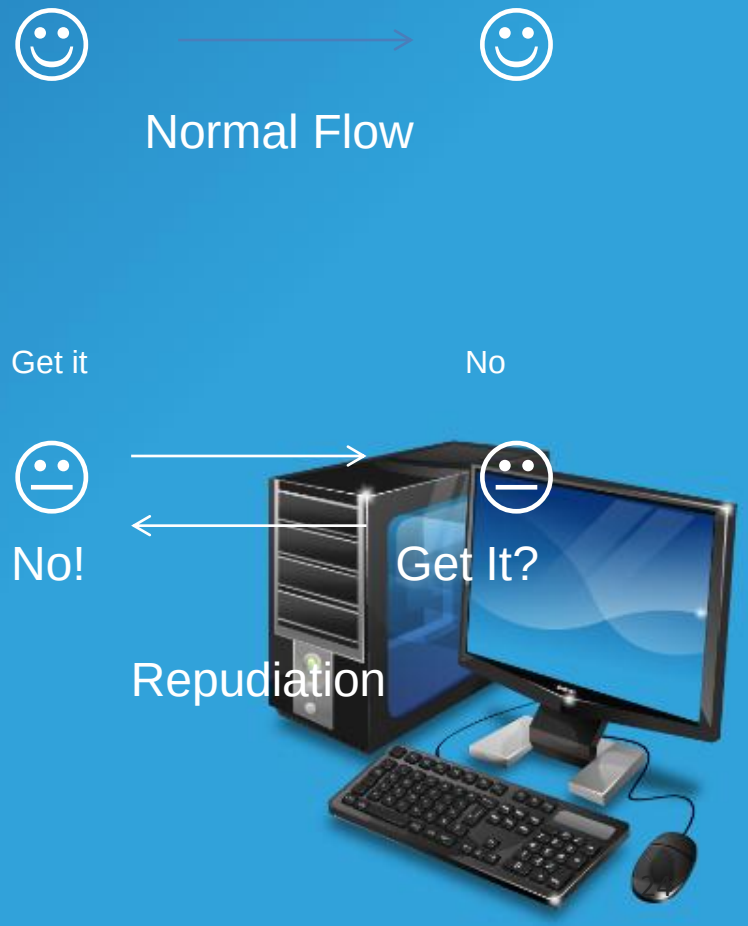
- In computing, e-Business, and information security, it is necessary to ensure that the
  - data,
  - transactions,
  - communications or
  - documents (electronic or physical)

  are genuine.

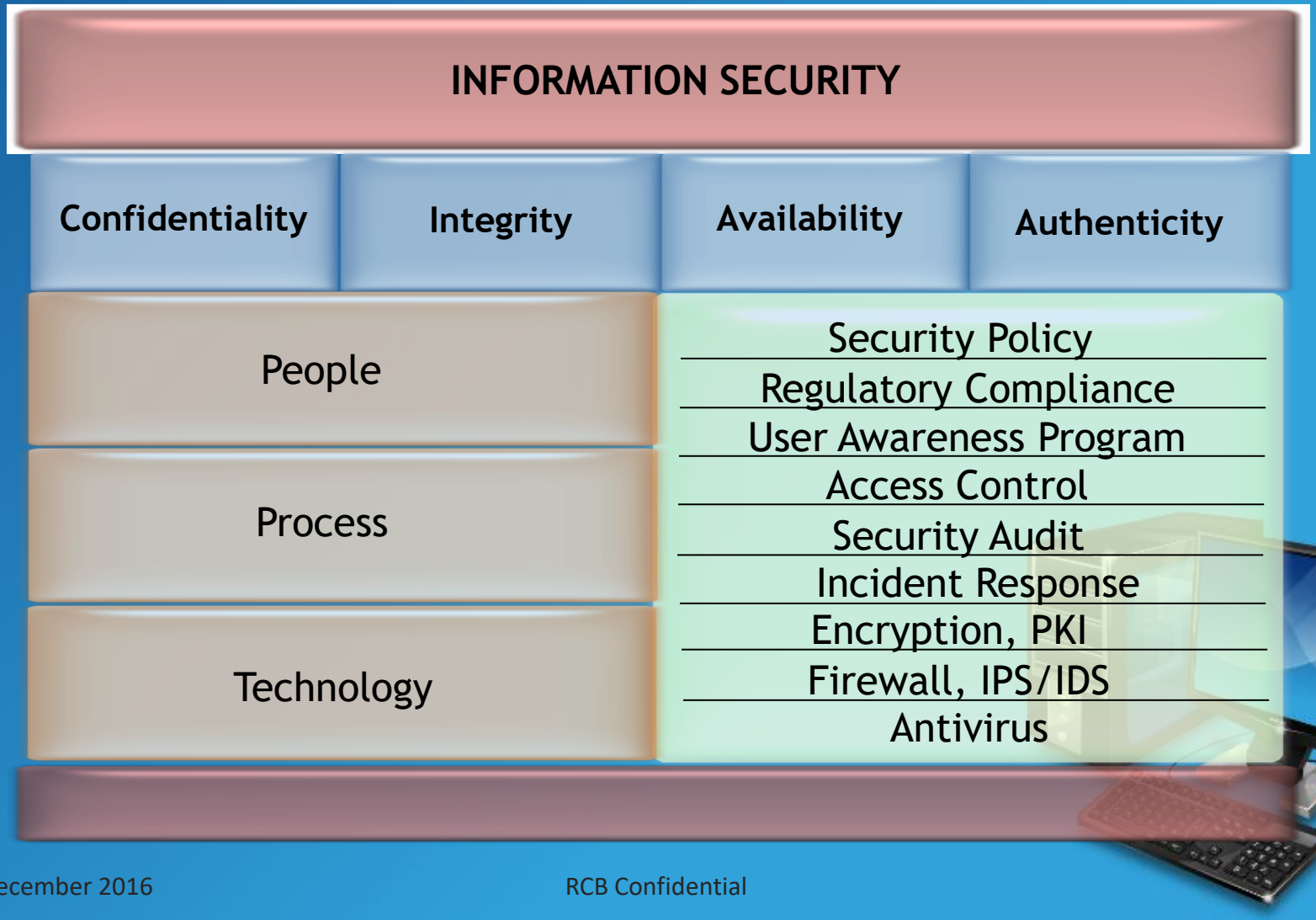
- It is also important for authenticity to validate that both parties involved are who they claim they are.

Non-repudiation

- Non-repudiation implies one's intention to fulfill their obligations to a contract.
- It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.
- Electronic commerce uses technology to establish authenticity and non-repudiation
  - digital signatures
  - public key encryption



Information Security Management involves



Security Standards

- National Institute of Standards and Technology (NIST)
  - US standards
  - Security Guidelines for federal systems
- ISO 17799
  - Internationally recognised standard
  - Applicable to both public and private sector implementations
- CERT
  - Carnegie Mellon University's Software Engineering Institute
  - They study internet security vulnerabilities, research long term changes in networked systems
  - Develop information and training to improve security.
- CERT-In
  - functioning under DIT is India's response to cyber threats and also assists members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.

Benefits of Cyber Security

- Safeguard information
- Ensure accountability for security and information
- Manage IT infrastructure
- Manage and prevent security lapses
- Standardize processes

INTRODUCTION TO THE CYBER SECURITY POLICY OF GoI

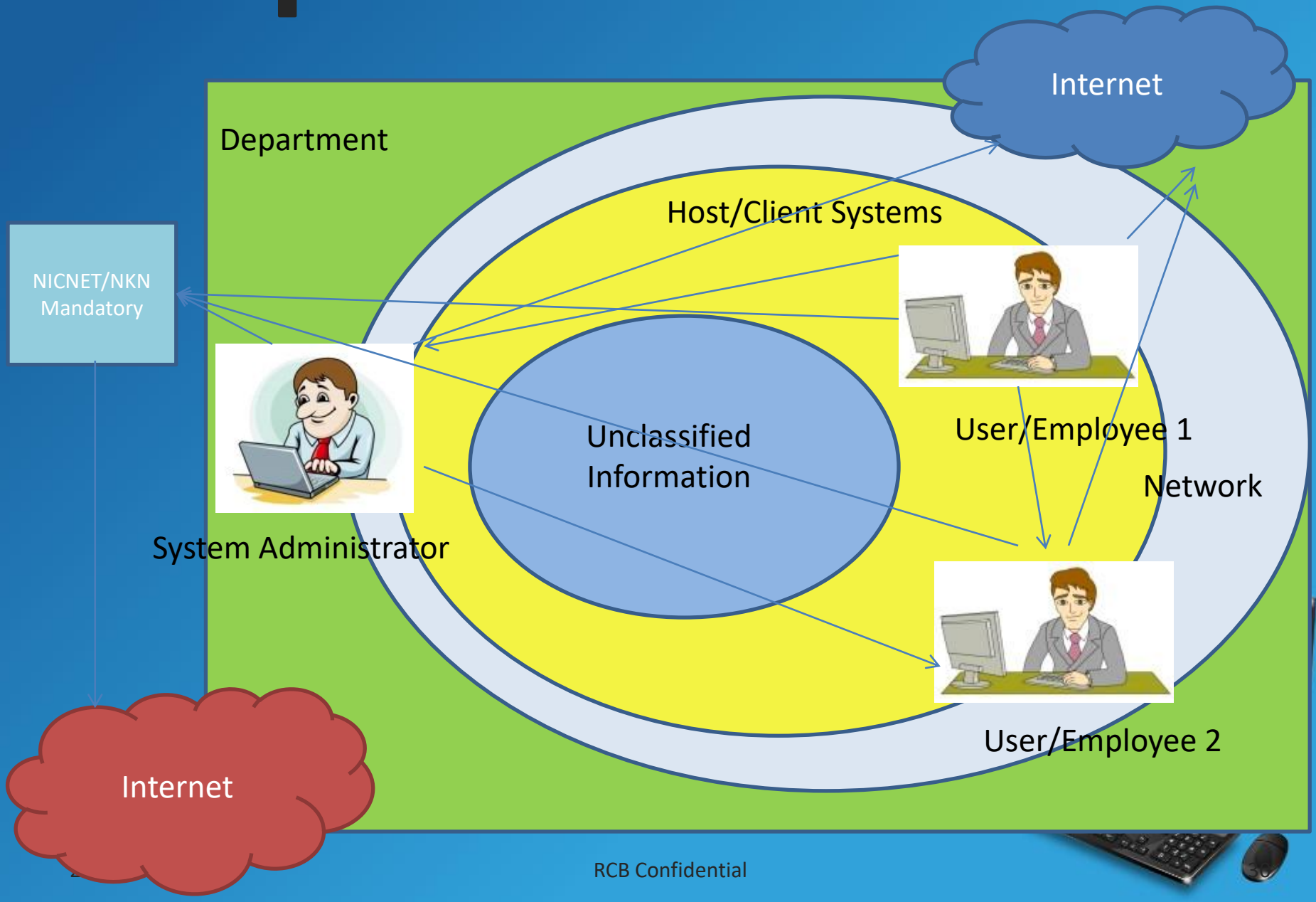
Objective

- Providing ‘secure and acceptable use of cyber resources’

Scope

- Deals with ‘unclassified’ information only
- Applicable across all Ministries/ Departments/ Subordinate Offices
- Covers the following groups:
  - Employee (‘user’)
  - System administrator
  - Network connected to the Internet
  - Department

Scope - what is covered



Scope – what is not covered

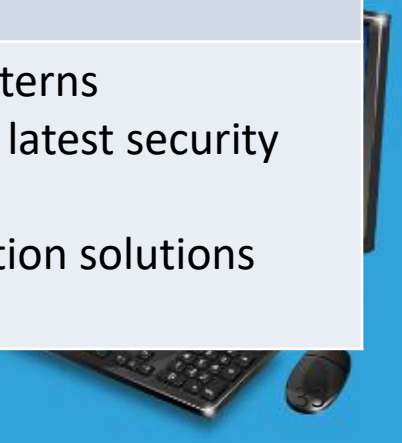
Physical security of cyber resources, Data Centres
Mail Servers, Web Servers,

Roles and Responsibilities

- National Information Security Officer (NISO)
- National Security Operations Centre Head
- NSOC Administrator
- NSOC Operator
- Chief Information Security Officer (CISO)
- Cyber Security Administrator (CSA)
- Information Security Officer (ISO)
- System Administrator (SA)
- Network Security Administrator (NSA)
- Network Administrator (NA)

Responsibilities

S.No.	Roles	Responsibility
1.	**CHIEF INFORMATION SECURITY OFFICER (CISO)**:	➢ Formulate department-level policy ➢ Disseminate policy ➢ Review and approve exceptions ➢ Ensure resolution of security incidents ➢ Interact with CERT-In and report incidents ➢ Facilitate awareness and training
2.	**CYBER SECURITY ADMINISTRATOR (CSA)**	Analyze attack patterns Keep abreast with latest security vulnerabilities Implement mitigation solutions

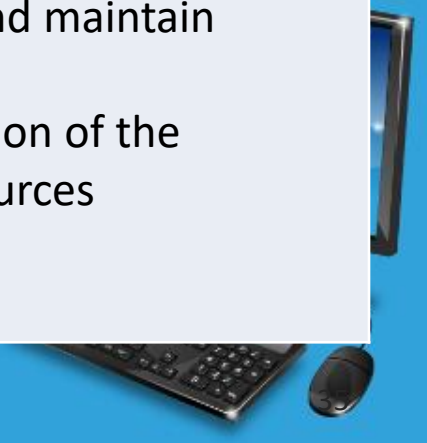


Responsibilities contd.

S.No	Roles	Responsibilities
3.	**INFORMATION SECURITY OFFICER (ISO)**	➢ Oversees implementation of security policy in Department ➢ Report security incidents to CISO ➢ Provide administrative support for resolving security incident
4.	**SYSTEM ADMINISTRATOR (SA)**	➢ Implement client-level security policies ➢ Perform client system' administration ➢ Conduct internal security compliance ➢ Report security incidents to ISO and NSA ➢ Investigate incidents and enforce policies ➢ Asset management

Responsibilities contd.

S.No.	Roles	Responsibility
5.	**NETWORK SECURITY ADMINISTRATOR (NSA)**	➢ Frames network security policy ➢ Design, implement, and maintain network security solutions ➢ Report incidents to ISO and SA ➢ Investigate incidents and ensure enforcement of policies ➢ Manage the SOC
6.	**NETWORK ADMINISTRATOR**	➢ Manage the network ➢ Monitor and tune the network ➢ Design, implement, and maintain network architecture ➢ Maintain documentation of the network security resources ➢ Manage the NOC



Security categorization of Departments

- **Category – I:**
- Security is managed by agencies like NIC
- Each Department shall have a Network Operations Centre (NOC) and a Security Operations Centre (SOC) managed by the same agency.
- **Category – II:**
- Network is managed by the Ministry/ Department itself.
- NOC/ SOC is also established and managed by the Ministry/Department.

  eg. RCB

Policy components: user level

- Employees in the Ministry/Department/Subordinate Office of the Government of India handling unclassified information
- Covers:
  - Data Backup and restoration procedure
  - Email use
  - Password Security
  - Anti Virus
  - Portable Media storage
  - Network access policy
  - Logs
  - Enforcement – misconduct under CCS conduct rules

Policy components: user level (contd.)

E-mail use

- For official communication only e-mail account provided by the Department to be used
- E-mail account password not to be shared
- Passwords used for filling up online forms/services/registration to be different from official e-mail account password
- Unauthorised use of E-mail account shall not be done
  i. Distribution of messages anonymously
  ii. Misusing other's E-mail ID
  iii. Using a false identity
  iv. Sending messages to intimidate or harass others.

Password Security - General

- User shall not share or reveal passwords.
- Password should not be recorded anywhere by the user
- Ensure that nobody is watching when password is being keyed in.
- Remember password feature shall not be used.
- Default password shall be changed.
- Passwords shall be changed at regular intervals (90 days)
- Users should not reuse last 3 passwords

Password reset

- Only the owner of the user account shall request for password reset
- When a new password is issued the password shall be changed after Firstlogon.
- If password has been suspected to have been disclosed/compromised, it shall be changed immediately and a security incident shall be reported to the System Administrator.

Password complexity

- Passwords should be unique to each user id.
- Password length shall be minimum 8 characters for user accounts
- Password shall be a combination of upper and lower case character (e.g a-z A- Z) , DIGIT (e.g. 0-9)
- and permitted special character (e.g.! @#$)
- Password shall not be based on any of the following
  - Dictionary words and its reverse
  - Combination of dictionary word
  - Names reference or abbreviation of user id user name
  - Date of birth telephone number personal details, name of the
  - Department or ministry

How to change your password

If you have a user account

1. Open User Accounts in Control Panel.

2. Click Change my password.

3. Type your current password.

4. Type a new password and Type the new password again to confirm.

You can also enter descriptive or meaningful text in Type a word or phrase to use as a password hint to help you remember your password.

5. Click Change Password.

•

Policy- acceptable use of the client systems

- User shall be responsible for the activities carried out on the client system
- Backup of important files shall be taken by the user at regular intervals
- Maintenance of faults in the client systems should be carried out under their close supervision
- User shall not leave their system unattended. They should lock out his/her system before leaving the system.
- User shall ensure that unauthorised peer to peer file sharing software is not installed.
- User shall not share hard disk or folders with anyone, by default. If necessary, only the required folders shall be shared with specific user.
- User shall allow the installation of service packs and paches

Secure Your PC

- Turn on Windows Internet Firewall

- An Internet firewall helps create a protective barrier
- between your computer and the Internet.

- Use Automatic Updates to Keep Software Up-to-date
- Install all updates as soon as they are available.

- Automatic updates provide the best Protection

- Install and Maintain Antivirus Software

- Antivirus software helps to detect and remove computer viruses before they can cause damage.
- For antivirus software to be effective, you must keep it up-to-date.

- *Don't let it expire*

- *Use Malicious Software Removal Tool regularly for scanning . Get Free PC Safety scan*

Plan for RCB

- There is a IT security Group/Committee Constituted for RCB
- A Security policy for RCB is being drafted.
- A Hand book of forms which will have to be filled will be circulated
- Anti-virus to be updated (IT)
- Exceptions to be approved (Dir)
- Incidents (suspected) to be reported to SA/IT

End of the Day?

- It is Shutdown Time

- Always Shutdown when you leave your PC
- at the end of the Day