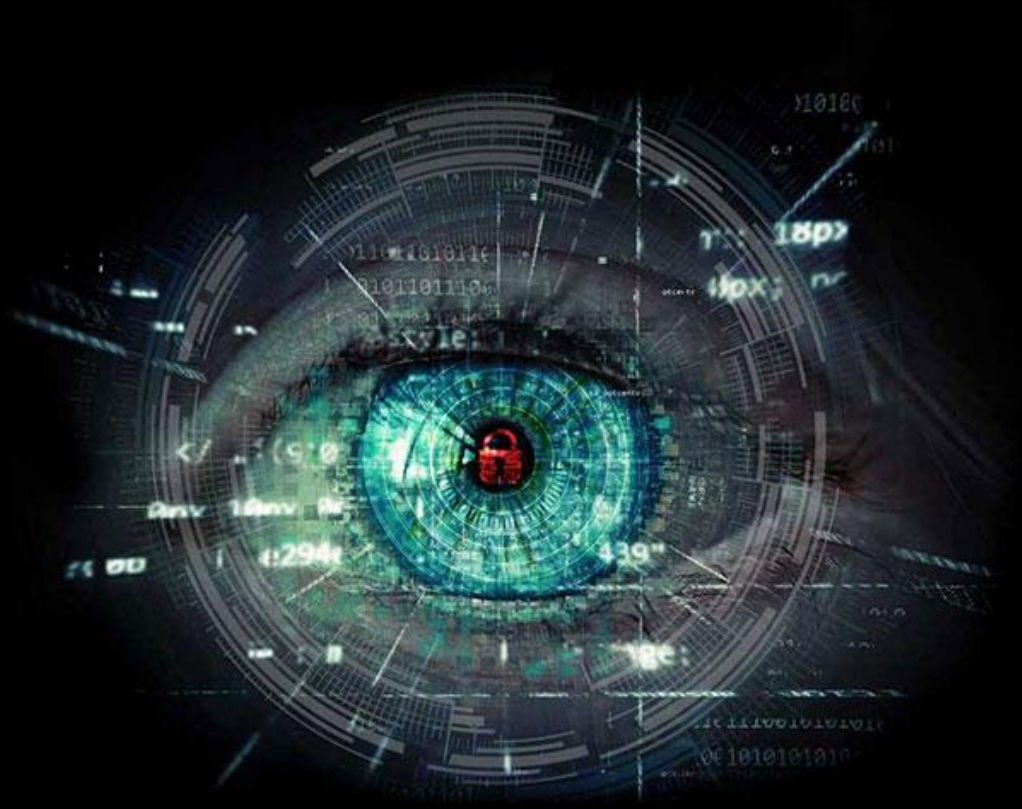
Data Security !

Group 4

Abhinav Goyal, M02
Aman Gupta, M07
Ayan Saha, M12
Deepak Sharma, M17
Kamal Chaudhary, M22

Our Focus of Today !



01 Introduction

02 Classification of Data

03 Storage of Data

04 Data security

05 Controls

06 Top Threats

07 Tools for Data Security

08 Data security Actions in India

09 Conclusion

Introduction

- Data is the raw form of information, which stored in our databases, network servers, personal computers and some other places.
- Some data or information is personal, as well as implicit for its own purpose.
- Some people or organizations can try to capture those ‘not accessible information’.

So Data Security has come into focus !

CLASSIFICATION OF DATA

PUBLIC DATA: Open to all users and no security measures are necessary.

LIMITED ACCESS DATA: Only authorized users have access to this type of data.

PRIVATE DATA: This data is open to a single user only, the owner of that particular data.

STORAGE OF DATA

Mechanical (Paper, punched card, film, gramophone record, etc.)

Magnetic Storage (Magnetic tape, floppy disk)

Optical Storage (Photographic paper, microform, optical disc)

Electrical (Semiconductor used in volatile RAM chips, etc.)

WHAT IS DATA SECURITY

- Security is the protection of information, information systems and services against disasters, mistakes and exploitation.
- Data security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled.
- Thus data security helps to ensure privacy. It also helps in protecting personal data.
- It implies protection of data from unauthorised access, modification and destruction.


D A T A
security

WHY DATA SECURITY ?

Access controls regulate the reading, copying, changing and deletion of data and programs**.**

Flow controls can prevent a service program from leaking the customer's confidential data.

Inference controls: A method of preventing data about specific individuals from being inferred from statistical information in a data base about groups of people.

Various threats to computer systems

Unaware Staff

Dissatisfied Staff

Hackers

Spy

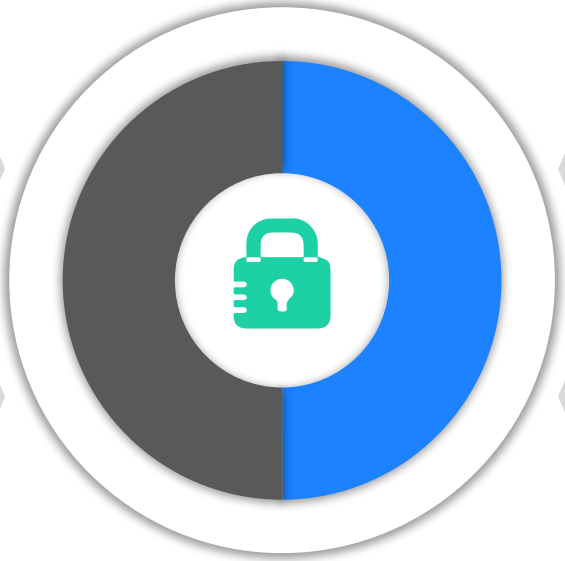
Top Threats to Data Protection

Technical Data Security Threats to Information Systems	Mitigation
Non-existent Security Architecture	Third party be brought in to consult with the IT team
Un-patched Client Side Software and Applications	Robust patch management program
“Phishing” and Targeted Attacks (“Spear Phishing”).	Install professional enterprise-level e-mail security software
Internet Web sites	Employ firewalls and antivirus
Poor Configuration Management	Specify security mechanisms and procedures
Mobile Devices	Encrypt data on all mobile devices storing sensitive information
Cloud Computing	Comply with the organization’s information system security requirements
Removable media	Disabling the “auto run” feature of the operating system
Botnets	Implement a holistic approach to data security
Zero-day Attacks	Keep abreast of the latest software patches

Non-technical Cyber Security Threats to Information Systems	Mitigation
Insider	Enforce a well-defined privilege rights management system allowing only to perform specific functions
Poor Passwords	Use a professional password-generating program as an enterprise-level solution
Physical Security	Strong physical security includes access control policies and procedures; physical barriers
Insufficient Backup and Recovery	Establish an organizational policy and specify procedures for data backup, storage, and retrieval
Improper Destruction	Ensure best practices recommended National Institute of Standards and Technology (NIST)
Social Media	Reinforce a policy forbidding access to some social media websites while using an organization’s resources and equipment
Social Engineering	Train users to increase their awareness about social engineering threats and educate them on how to avoid being manipulated

TOOLS FOR DATA SECURITY

- CRYPTOGRAPHY
- BIOMETRIC SYSTEMS
- ANTIVIRUS
- FIREWALL



- INTRUSION DETECTION DEVICES
- VIRTUAL PRIVATE NETWORK
- SSH ENCRYPTION
- SSL ENCRYPTION

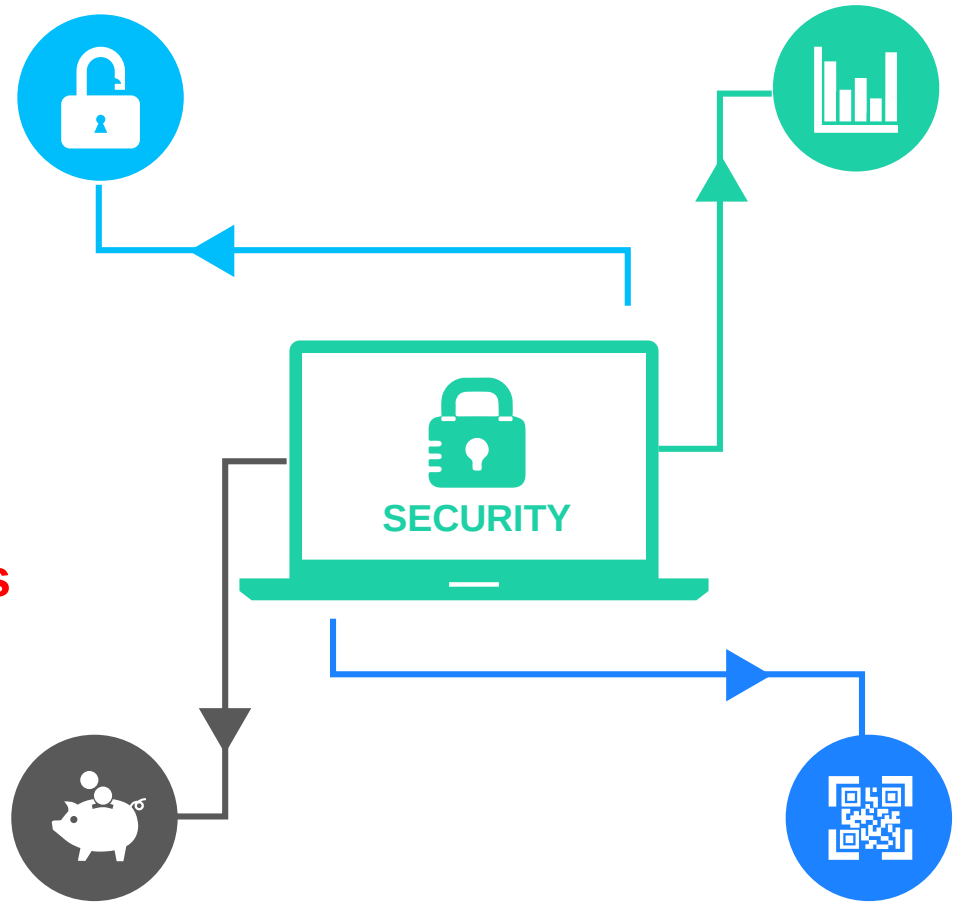
DATA SECURITY TOOLS

CRYPTOGRAPHY

Practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver.

BIOMETRIC SYSTEMS

BIOMETRICS is the practice of enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver.



Malicious code and Anti virus solutions

Anti virus is a computer program used to prevent detect and remove malware.

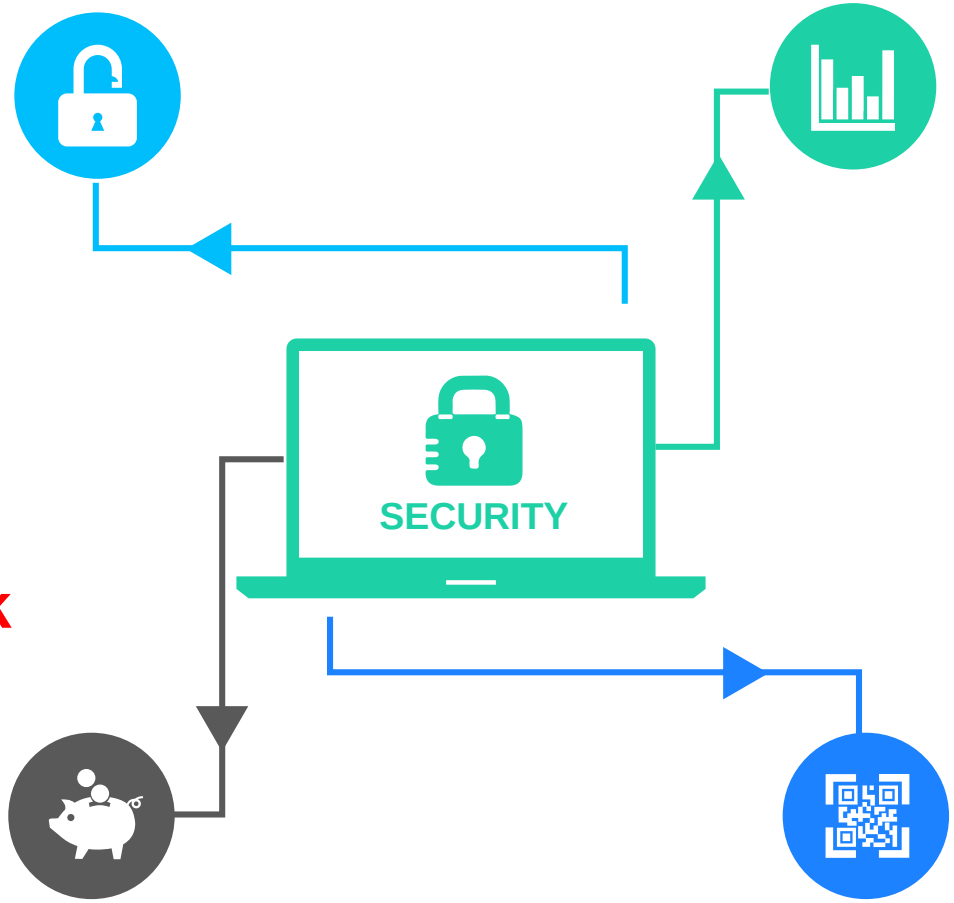
Firewall

Computer security system that controls the flow of data from one computer or network to another.

DATA SECURITY TOOLS

INTRUSION DETECTION DEVICES

A device or software application that monitors network and/or system activities or policy violations and produces reports to a management station.



SSH ENCRYPTION

Secure shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Virtual Private Network

.A network that is constructed by using public wires to connect nodes.These symptoms use encryption and other security mechanisms to ensure that only authorised users can access the network and that the data cannot be intercepted.

SSL ENCRYPTION

Secure Sockets Layer is a protocol developed by Netscape for transmitting private documents via the internet.

Data Security Actions in India

Acts for Data Security

IT Act 2000, India

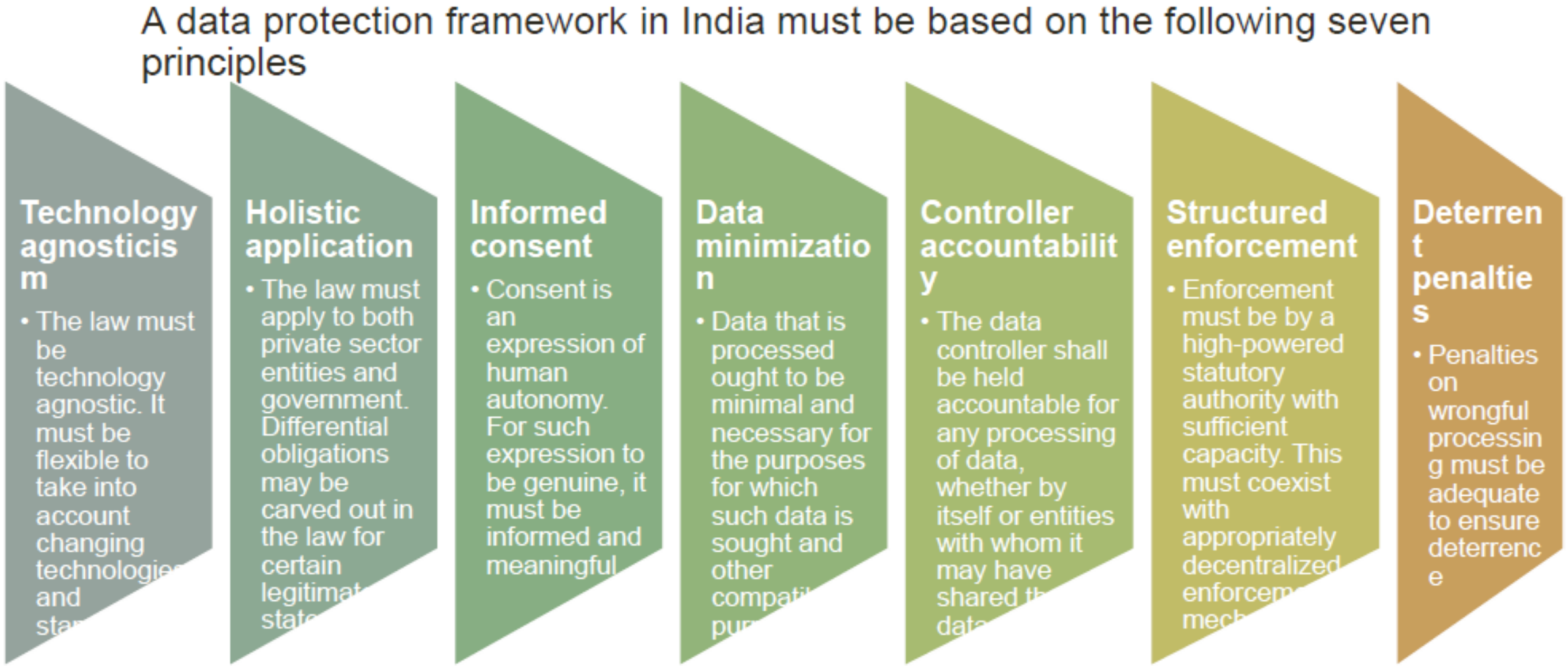
Enforcement agencies

1. NIC
2. C-DAC
3. State Cyber Crime Police station

Data Security council of India

- A section 25 not for profit company, was setup by NASSCOM
- Promote Data protection
- Develops Data Security and privacy codes & standards.
- Encourage IT/BPO industry to implement the same

KEY PRINCIPLES AROUND DATA PROTECTION IN INDIA



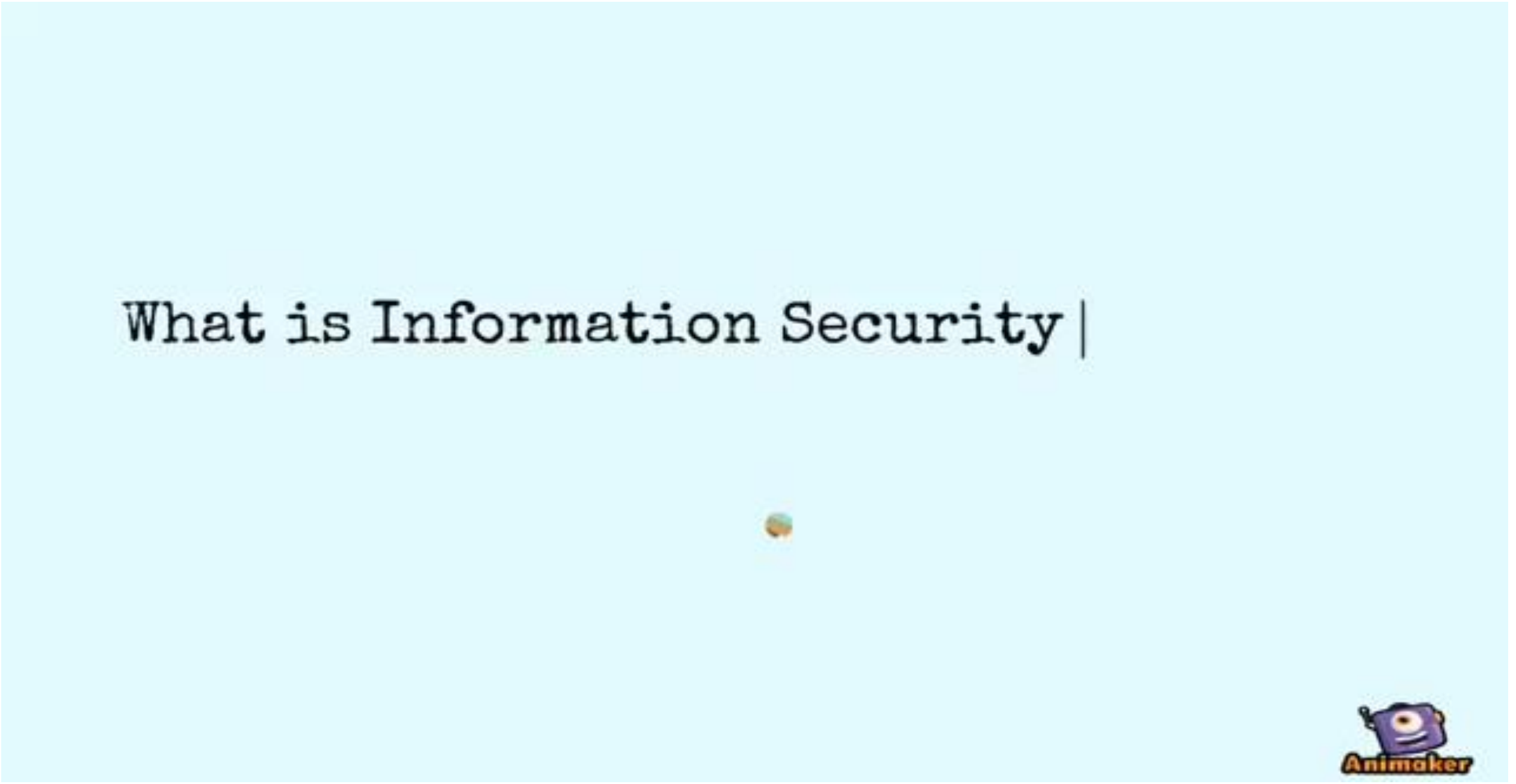
Some Security Tips

1. Encouraging employees to choose passwords that are not common
2. Require employees to change passwords every 90 days.
3. Virus protection subscription is current and update.
4. Educating employees about the security risks of e-mail attachments.
5. Assessing security patches regularly.
6. When an employee leaves a company, remove that employee's network access immediately.
7. If people opt work from home, then provide a secure, centrally managed server for remote traffic.
8. Updating Web server software regularly.
9. Do not run any unnecessary network services.

Conclusion

- Adopt latest technology for defending the various threats
- Continuously educating the workforce about data security
- Stringent data security standards
- Periodical data security audit

Data Security in a nutshell !




Thank You !!