Information Security

By:

Dr. John K. Tarus

School of Information Sciences

INF 411/CMM 213: MANAGEMENT OF ICT

Information Security

- ***Information*** is recognized as an important and valuable asset to any organization, hence needs to be protected and secured from exposure.
  - ✓ **Asset:** Anything that has value to an organization.

- **Information Security:** "protection of information and information systems against unauthorized access, use, disclosure, modification, or destruction in order to provide confidentiality, integrity, and availability". *(Source: The National Institute of Standards and Technology (NIST)).*

- N/B: ***Information security is everyone's responsibility.***

What is Information Security?

- Preservation of *Confidentiality*, *Integrity* and *Availability (CIA)* of information through security technologies.

C – Confidentiality

- Ensuring that information is accessible only to those authorized to have access i.e. preventing the disclosure of classified information to an adversary.

I – Integrity

- Safeguarding the accuracy and completeness of information.

A – Availability

- Ensuring that authorized users have access to information when required i.e. assuring that authorized users have continued and timely access to information and resources.

- The aim of information security is to protect data & information against threats through technical means and effective management.

Information Security

- In addition to C. I. A, other properties such as *authenticity*, *accountability*, *non-repudiation* and *reliability* should also be preserved.
  - ✓ *Authenticity* - ascertaining that the identity claimed by a party is indeed the identity of that party.
  - ✓ *non-repudiation* - the use of a digital signature procedure affirming both the integrity of a given message and the identity of its creator to protect against a subsequent attempt to deny authenticity.
- Information Security protects information from a wide range of *threats*.
- Information security is both a **management** and a **technological** process.

Benefits of Information Security

- Protects information against various threats
- Ensures business continuity
- Minimizes financial losses and other impacts
- Optimizes return on investments
- Creates opportunities to do business safely

Types of Information in Information Security Management System

Internal Information

- Information for internal use only within the institution and must be protected due to ethical or privacy considerations e.g. institutional policies, internal memos etc.

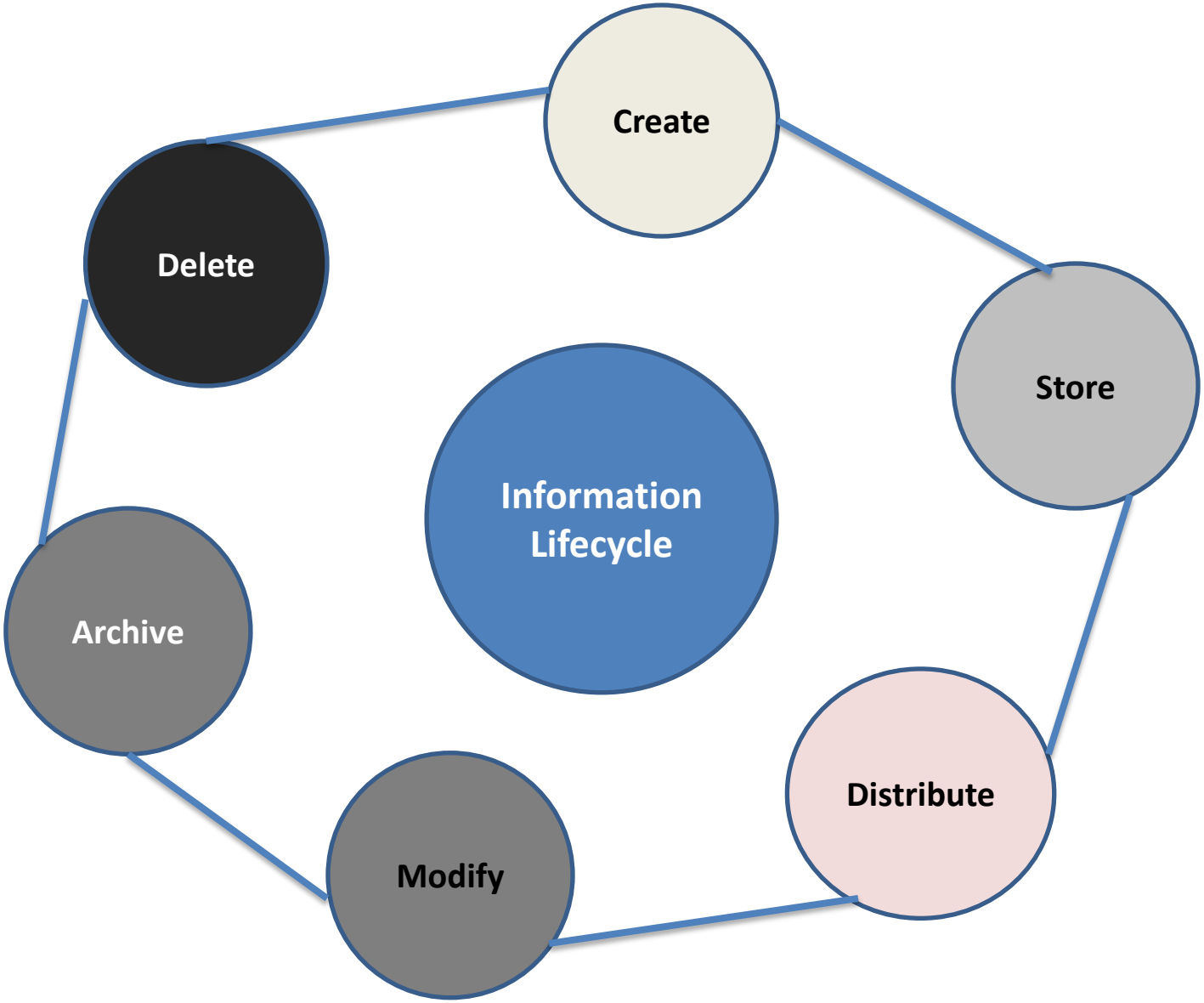
Confidential Information

- Information that is exempt from disclosure to unauthorized users i.e. information you would not wish to divulge to unauthorized users or third parties e.g. security information.

Shared/Public Information

- Information that is generally regarded as publicly available and may be shared with other parties e.g. advertising / marketing information, information in public websites etc.

Information lifecycle



Information may need protection through its entire lifecycle including deletion or disposal

Risks to Information as a Valuable Asset

Without suitable protection, information can suffer from:

- Loss of information
- Theft of information
- Unauthorized or accidental disclosure
- Unauthorized modification
- Unavailability

Identification of Threats & Vulnerabilities

Threat: Potential cause of an unwanted incident that may result in harm to a system or organization.

- ✓ High user knowledge of IT systems
- ✓ Sabotage by users
- ✓ Hackers and identity theft
- ✓ Viral attacks
- ✓ Systems & network failure
- ✓ Interception of information
- ✓ Cyber crime – *Cyber attackers attack the weakest points in a defense.*
- ✓ Natural calamities & fire

Identification of Threats & Vulnerabilities

Vulnerability: A weakness of an information asset or control which can be exploited by a threat.

- ✓ *Lapse in physical security*
- ✓ *Poor password etiquette*
- ✓ *System errors*
- ✓ *Open computer ports e.g ftp, telnet, ssh etc.*

- *A **vulnerability** in itself does not cause harm, it is merely a condition or set of conditions that may allow a threat to affect an information asset.*

Most Common Information Security Mistakes

- Passwords - *poor password management, weak passwords.*
- Lack of backups
- Lack of antivirus
- Exposing personal information on social media.
- Sharing flash disks and mobile phones with important information.
- Failure to log out *(Windows - L)* computer or e-mail.
- Physical security – *leaving doors open.*

Data and Information Security Measures

- **Use of strong passwords** - use a combination of upper and lower case letters, numbers, and symbols, and make it 8 to 12 characters long.
- **Strong firewall** - A firewall protects your network by controlling internet traffic coming into and flowing out of your network. It is a gatekeeper between your computer and the Internet.
- **Regular backups** – backups (onsite & offsite) to an external hard drive or in the cloud. Complete daily, weekly, or incremental backups periodically.
- **Antivirus protection** - They work by detecting and removing viruses, malware, and spyware.
- **Controlled access** - Limit access to critical data. Make sure that individuals can only access data and services for which they are authorized - *The principle of least privilege.*

Data and Information Security Measures

- **Intrusion-detection systems** – Install IDS to monitor system and network activity.
- **Ignore Suspicious Emails**
- **Update your programs regularly** - Updates contain vital security upgrades that help protect against known bugs and vulnerabilities.
- **Secure your laptops and smartphones** - They hold a lot of valuable data, and are at a higher risk of getting lost or stolen. Protect data in these devices using backups, encryption, password protection, and enabling of the 'remote wiping' option.
- **Educating your employees** on data and information security as well as regular cyber security awareness. *According to statistics, 70% of enterprise information loss is caused by negligence or intentional leakage by internal staff.*
- **Formulating an ICT security policy**

END

Thank You

Q & A ?

Information Security Is Everybody's Job!