INTRODUCTION TO INFORMATION SECURITY

Faculty of Information Technology, Hanoi University

Contents

I. What is information security and CIA?
II. Why is security important?
III. InfoSec today

I. WHAT IS SECURITY?

1. What assets do we need to protect?
2. How are those assets threatened?
3. What can we do to counter those threats?

I. WHAT IS SECURITY?

- Security = to ensure one's own "safety"
- Security is protecting what you or others have
- The security of not only physical assets, but non-physical asset are important
- Non-physical assets include confidential information and data; intellectual property; research data with the potential of high value realization and high investment; and the security of your customers or end users while using your systems
- Security is even more important with the recent rise in widespread use of technology such as mobile phones, the internet, tablets, and other mobile devices.

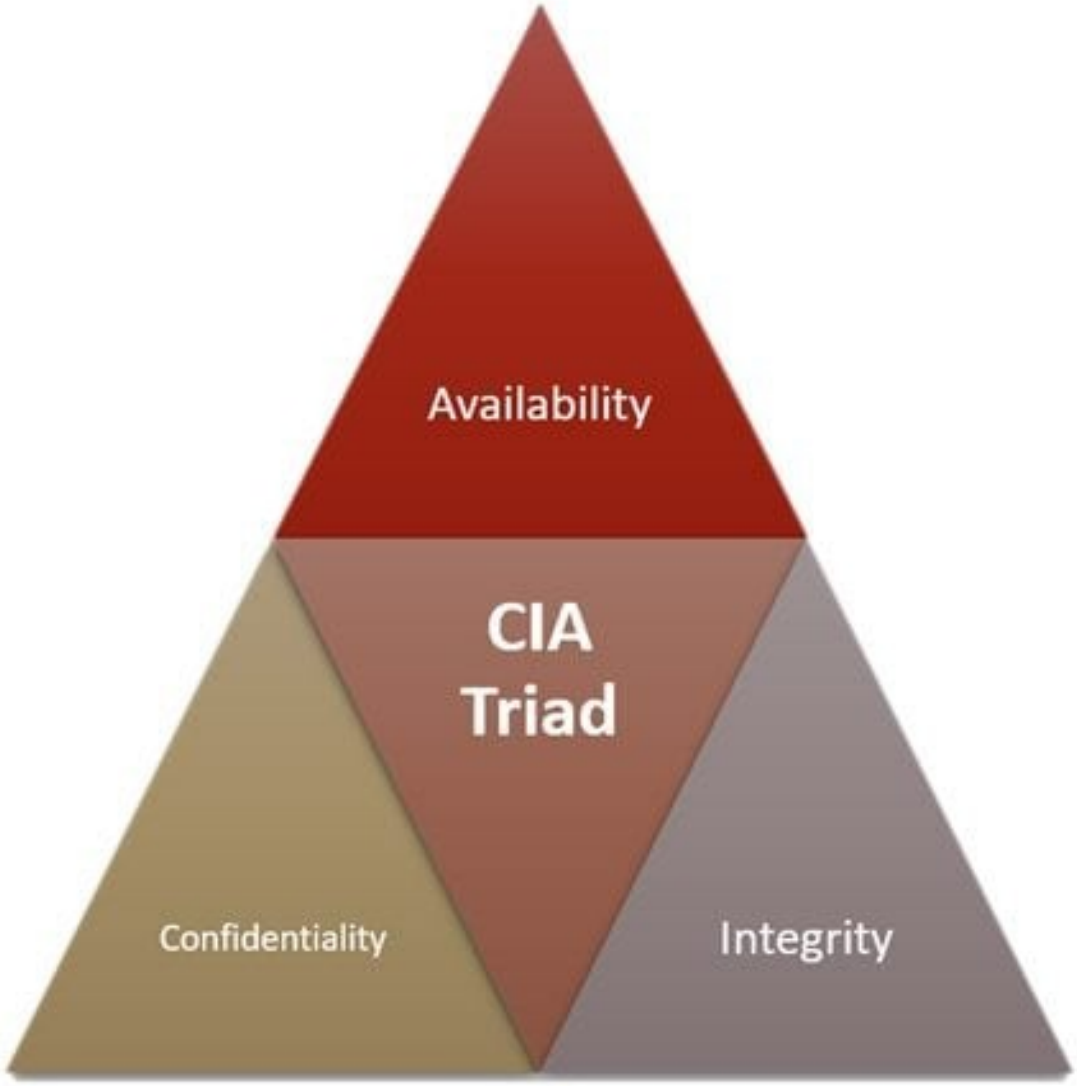
I. WHAT IS SECURITY?

- **Information security**, sometimes shortened to **InfoSec**: typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information

I. WHAT IS SECURITY?

- **Computer Security**: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

CIA TRIAD



CIA TRIAD

- **Confidentiality:** This term covers two related concepts:
  — Data confidentiality:1 Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  — Privacy**:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- **Integrity:** This term covers two related concepts:
  — Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
  — System integrity**:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

CIA Levels

- **Low**: The loss could be expected to have a limited adverse effect, result in minor damage to organizational assets; minor financial loss; or minor harm to individuals.
- **Moderate**: The loss could be expected to have a serious adverse effect, result in significant damage to organizational assets; significant financial loss; or significant harm to individuals.
- **High**: The loss could be expected to have a severe adverse effect, result in major damage to organizational assets; major financial loss; or severe harm to individuals

II. WHY IS SECURITY IMPORTANT?

- Earning is difficult, but losing is extremely easy
- Everyone wants to preserve their energy and secure their future for themselves and their children
- Every organization wants to secure its bright future.
- Computer hackers may just want to satisfy their ego or show their supremacy over the technology and may steal useful and valuable information and publish it to others
- Others may want to mine for data of value so that they can sell the same to others, who want the information to either harm others or make commercial gains from it.
- Terrorists may want the information to either destroy the strategic or military capability of a country, or to threaten the economy of a country by using the information they steal

II. WHY IS SECURITY IMPORTANT?

- 3D printers present a new possible threat by potentially being used by terrorists to create weapons
- The protection of business information of value is the primary reason for information security
- Automated Teller Machines (ATMs) being hacked
- There are many instances where information has been stolen from emails, laptops, or cell phones, identity theft, which can lead to huge losses, hacking into banking accounts and initiating transactions

II. WHY IS SECURITY IMPORTANT?

- Malicious software attacks through links or attachments in emails, through add-ins to the browser, or through the download of free applications or games
- Wireless access points set up by attackers attract many users which leads to the compromise of important information like login credentials.
- With a lot of information getting distributed easily across the globe because of Web and Cloud technologies, there are a lot of challenges to ensure that data and information of value are well protected so that they are not compromised.

INFOSEC TODAY

- There is always a race between hackers and crackers and the information security personnel
- With widespread use of Information Technology and related tools, particularly with the advent of the Internet, it has become a challenge for organizations and their employees to prevent the misuse of information.
- All forms of technology, including the Internet, credit cards or debit cards, ATMs, bank web portals, and so on, are all under attack; most times intentionally, sometimes accidentally.
- Cloud computing is the popular buzz word today and has many benefits but also presents many new risks
- The rise in the use of electronic chips in everything from automobiles to refrigerators to TVs is another cause for concern

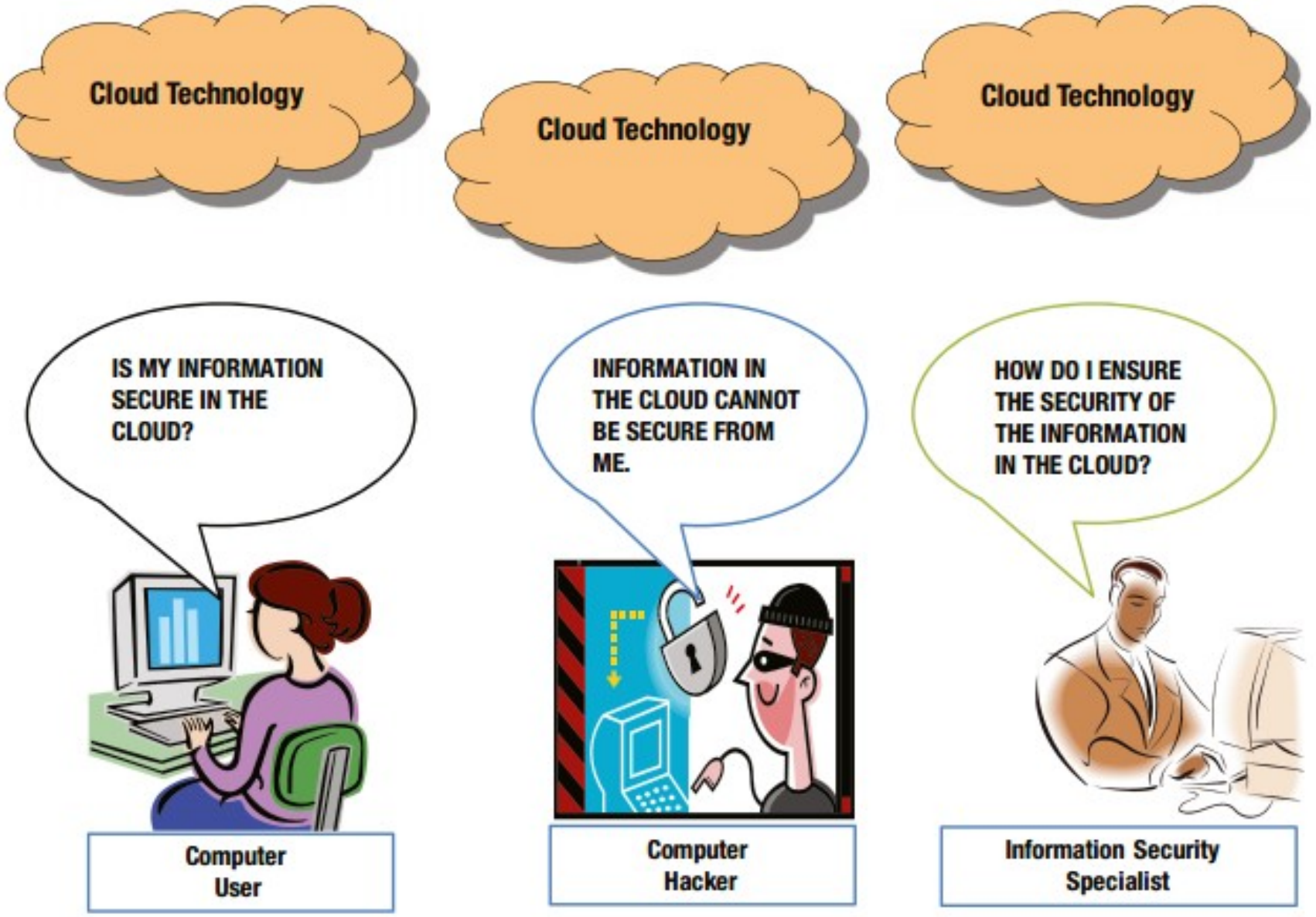


Figure 1-1. *Mistrust on "Cloud" and its security*

INFOSEC TODAY

- The Norton Report highlights the following information
- Consumers are more mobile than ever, but are leaving security behind. 63% of those surveyed own smartphones and 30% own tablets, nearly one out of two users don't take basic precautions such as using passwords, having security software, or backing up files on their mobile device.
- Cybercrime continues to be a growing global concern (US $113 billion; up from $110 billion) and the average cost per victim of cybercrime ($298; up from $197) increased this year.
- Nearly half (49%) of the respondents report using their personal devices (PCs, laptops, smartphones, tablets) for work-related activities

Q & A