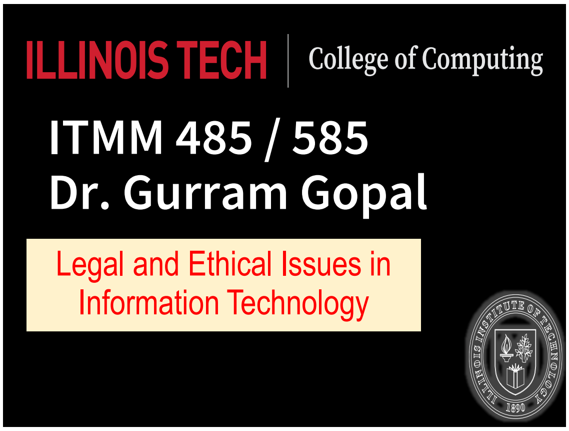


ILLINOIS TECH | College of Computing

ITMM 485 / 585
Dr. Gurram Gopal

Legal and Ethical Issues in Information Technology

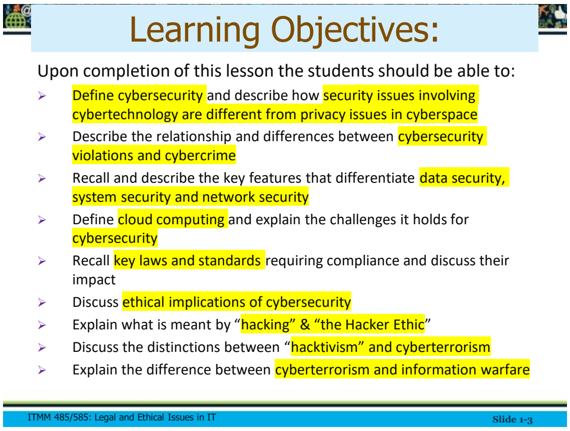
1

Ethical Concepts and Theories

ILLINOIS TECH | College of Computing

Ch6: Security and Compliance
P1: Intro to Cybersecurity

2



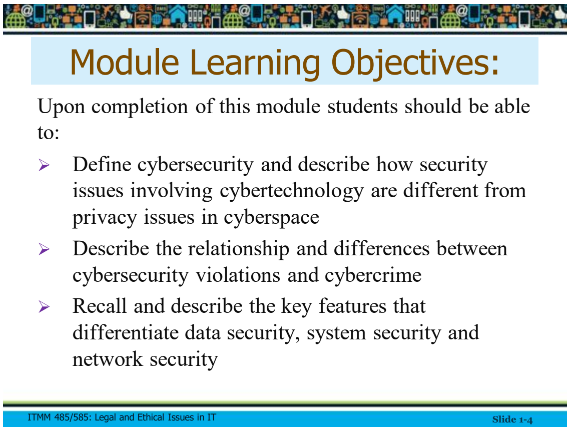
Learning Objectives:

Upon completion of this lesson the students should be able to:

- Define cybersecurity and describe how security issues involving cybertechnology are different from privacy issues in cyberspace
- Describe the relationship and differences between cybersecurity violations and cybercrime
- Recall and describe the key features that differentiate data security, system security and network security
- Define cloud computing and explain the challenges it holds for cybersecurity
- Recall key laws and standards requiring compliance and discuss their impact
- Discuss ethical implications of cybersecurity
- Explain what is meant by "hacking" & "the Hacker Ethic"
- Discuss the distinctions between "hacktivism" and cyberterrorism
- Explain the difference between cyberterrorism and information warfare

ITMM 485/585: Legal and Ethical Issues in IT Slide 1-3

3



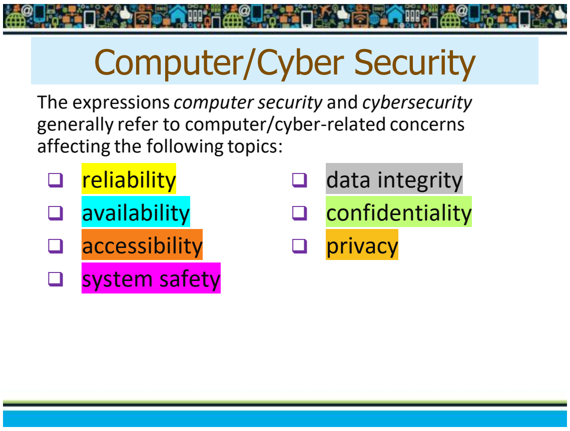
Module Learning Objectives:

Upon completion of this module students should be able to:

- Define cybersecurity and describe how security issues involving cybertechnology are different from privacy issues in cyberspace
- Describe the relationship and differences between cybersecurity violations and cybercrime
- Recall and describe the key features that differentiate data security, system security and network security

ITMM 485/585: Legal and Ethical Issues in IT Slide 1-4

4

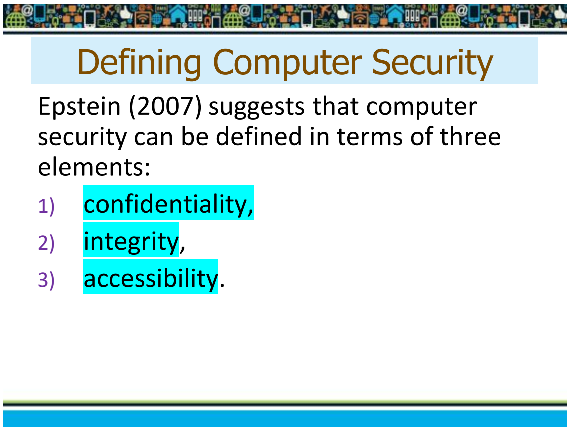


Computer/Cyber Security

The expressions *computer security* and *cybersecurity* generally refer to computer/cyber-related concerns affecting the following topics:

- ❑ reliability
- ❑ availability
- ❑ accessibility
- ❑ system safety
- ❑ data integrity
- ❑ confidentiality
- ❑ privacy

5

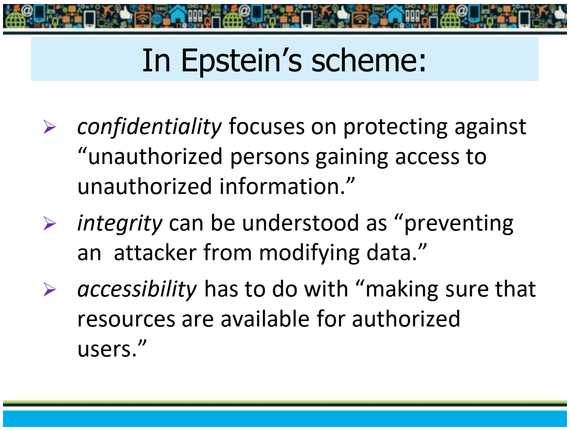


Defining Computer Security

Epstein (2007) suggests that computer security can be defined in terms of three elements:

1) confidentiality,
2) integrity,
3) accessibility.

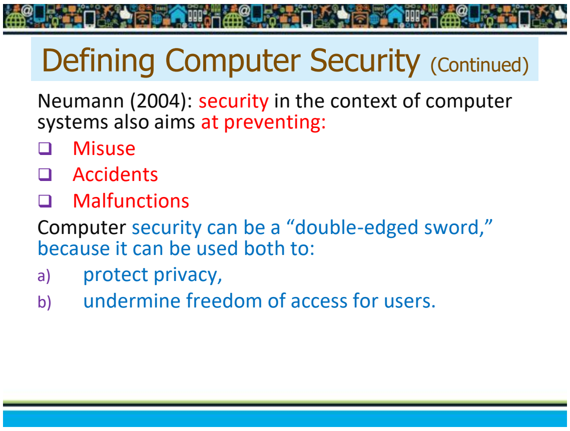
6



In Epstein’s scheme:

- *confidentiality* focuses on protecting against “unauthorized persons gaining access to unauthorized information.”
- *integrity* can be understood as “preventing an attacker from modifying data.”
- *accessibility* has to do with “making sure that resources are available for authorized users.”

7



Defining Computer Security (Continued)

Neumann (2004): security in the context of computer systems also aims at preventing:

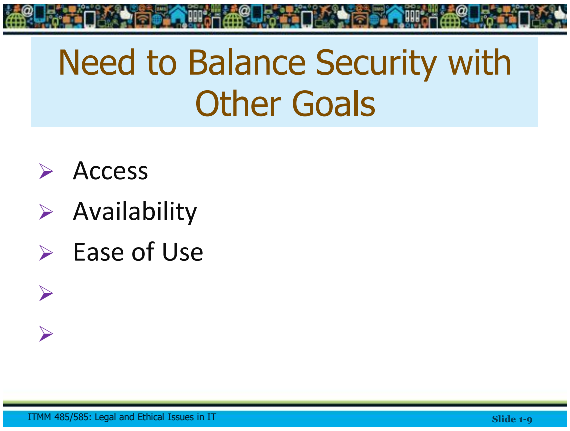
- ❑ Misuse
- ❑ Accidents
- ❑ Malfunctions

Computer security can be a “double-edged sword,” because it can be used both to:

a) protect privacy,

b) undermine freedom of access for users.

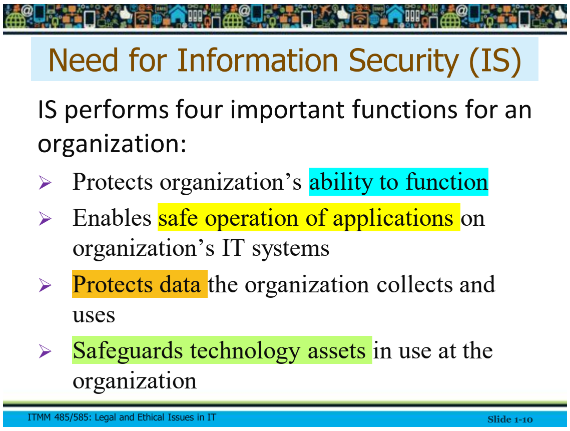
8



Need to Balance Security with Other Goals

- Access
- Availability
- Ease of Use
-
-

9

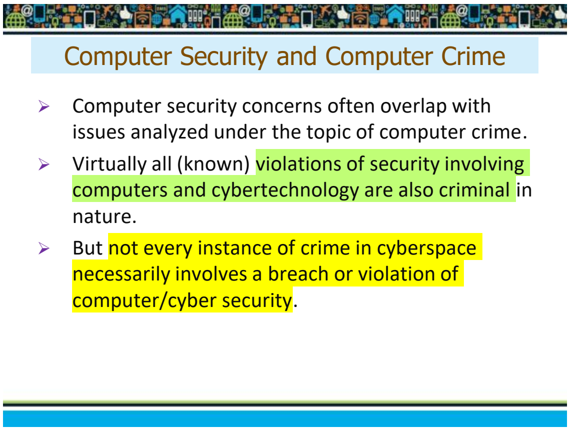


Need for Information Security (IS)

IS performs four important functions for an organization:

- Protects organization’s ability to function
- Enables safe operation of applications on organization’s IT systems
- Protects data the organization collects and uses
- Safeguards technology assets in use at the organization

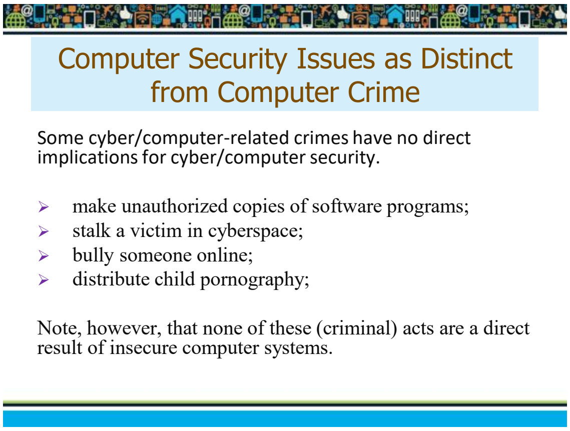
10



Computer Security and Computer Crime

- Computer security concerns often overlap with issues analyzed under the topic of computer crime.
- Virtually all (known) violations of security involving computers and cybertechnology are also criminal in nature.
- But not every instance of crime in cyberspace necessarily involves a breach or violation of computer/cyber security.

11



Computer Security Issues as Distinct from Computer Crime

Some cyber/computer-related crimes have no direct implications for cyber/computer security.

- make unauthorized copies of software programs;
- stalk a victim in cyberspace;
- bully someone online;
- distribute child pornography;

Note, however, that none of these (criminal) acts are a direct result of insecure computer systems.

12

Security as Related to Privacy (continued)

- Privacy-related concerns often arise because users are concerned about losing control over ways in which personal information about them can be accessed by organizations (especially by businesses and government agencies), who claim to have some *legitimate* need for that personal information in order to make important decisions.
- Cyber-related security concerns (unlike those of privacy) typically arise because of either:

a) fears that many individuals and organizations have that their data could be accessed by those who have no legitimate need for, or right to, such information;

b) worries that personal data or proprietary information, or both, could be retrieved and possibly altered by individuals and organizations who are not authorized to access that data.

13

Security as Related to Privacy (continued)

- Privacy and security concerns can also be viewed as two sides of a single coin, where each side of the coin also complements and completes the other.
- Note that many people wish to control information about them themselves, including how that information is accessed by others.
- Because securing personal information stored in computer databases is an important element in helping individuals to achieve and maintain their privacy, the objectives of privacy would seem compatible with (and complementary to) security.

14

Security as Related to Privacy (continued)

- But sometimes the objectives of privacy and security seem to be at odds with each other, causing a tension between these two notions.
- When cyberethics issues are examined from the perspective of security in cyberspace, the goals of protecting anonymity and individual autonomy seem less important than when cyberethics concerns are analyzed from the vantage-point of personal privacy.

15

Three Aspects of Cybersecurity: Data, System, and Network Security

Security issues involving cybertechnology span concerns having to do with three distinct kinds of (computer-related) vulnerabilities, which include:

I. unauthorized access to *data*, which either is resident in or exchanged between computer systems (i.e., *data security*);

II. attacks on *system* resources (such as computer hardware, operating system software, and application software) by malicious computer programs (i.e., *system security*);

III. attacks on computer *networks*, including the infrastructure of privately owned networks and the Internet itself (i.e., *network security*).

16

Data Security: Confidentiality, Integrity, and Availability of Information

- *Data security* is concerned with vulnerabilities pertaining to unauthorized access to data that can either:

a) reside in one or more computer storage devices,

b) be exchanged between two or more computer systems.

- Data-security issues affect the confidentiality, integrity, and availability of that information.

17

Data Security (Continued)

- Spinello (2000) describes what is required for *data security* by noting that:

> ...*proprietary or sensitive information* under one's custodial care is kept confidential and secure, that information being transmitted is not altered in form or content and *cannot be read by unauthorized parties*, and that all information being disseminated or otherwise made accessible through Web sites and on-line data repositories is *as accessible and reliable as possible*. [Italics Added]

18

System Security

- *System security* is concerned with vulnerabilities to system resources such as computer hardware, operating system software, and application software.
- It is also concerned with various kinds of viruses, worms, and related "malicious programs" that can disrupt and sometimes destroy computer systems.

19

System Security (Continued)

- Examples of malicious programs that have significantly disrupted system security are the:
- ILOVEYOU Virus (2001);
- Code Red Worm (2002);
- Blaster virus (2004);
- Conficker Worm (2009);
- Stuxnet Worm (2010);
- Flame Virus (2012).
- Heartbleed Virus (2014).

20

System Security (Continued): Viruses and Worms

- What are some of the key differences between computer viruses and worms?
- According to Skoudis (2004), a *virus* is a

  self-replicating piece of software code that "attaches itself to other programs and usually requires human action to propagate."
- Skoudis defines a *worm* as a

  self-replicating piece of code that "spreads via networks and usually doesn't require human interaction to propagate."

21

Viruses and Worms (Continued)

- Simpson (2006) points out that worms also replicate and propagate without needing a host or program to accomplish this objective.
- Review Scenario 6-1 (in the textbook) involving the Stuxnet Worm).

22

Viruses and Worms (Continued)

- Dale and Lewis (2016) also distinguish between worms and viruses, but in a slightly different way.
- They define a virus as a "malicious, self-replicating program that embeds itself into other code."
- Dale and Lewis define a worm as a "malicious stand-alone program that often targets network resources."
- However, some believe that both viruses and worms, as well as all other kinds of malicious programs are better described under the single category "malware."

23

Malware

- Miller (2015) defines *malware* as "software designed to produce, damage, or provide unauthorized access to computers or computer systems."
- Under this broad definition, all of the following would be included under the category "malware":
- viruses,
- worms,
- Trojan horses,
- logic bombs,
- (at least some forms of) "spyware".

24

Network Security

- *Network security* is concerned with securing a wide range of computer networks – i.e., from privately owned computer networks (such as LANs and WANs) to the Internet itself – against various kinds of attacks.
- The Internet's infrastructure, which includes the set of protocols that makes communication across individual (or privately owned) computer networks possible, has been the victim of several attacks.

25

Network Security (Continued)

- Attacks on computer networks have ranged from programs launched by individuals and organizations whose intentions were malicious to those (individuals and organizations) claiming that their intentions were benign.
- Some network attacks have severely disrupted activities on (segments of) the Internet.
- In some cases, these attacks have also rendered the Internet virtually inoperable.

26

Network Security (Continued)

- It is not always easy to determine whether a major computer network disruption is the result of malicious individuals or whether it is due to the failure of some aspect of the network infrastructure itself.
- For example, some suggest that a significant power outage experienced by AT&T in 1990, which, at the time, was attributed to a software glitch in the system's programming code, was the result of "malicious" individuals who caused the network to crash?
- Review Scenario 6-2 (in the textbook) involving the GhostNet Controversy, which illustrates some key issues at stake at the level network security.

27

?

28