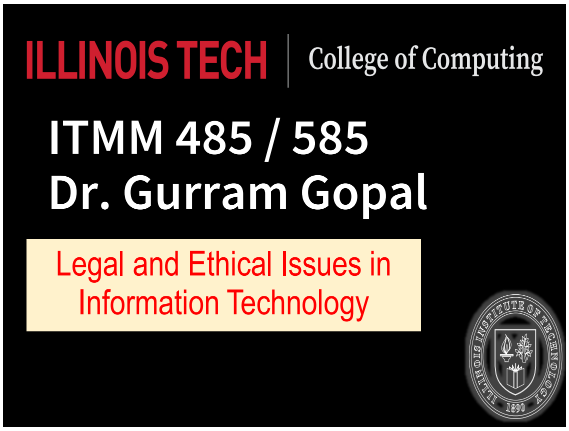


ILLINOIS TECH | College of Computing

ITMM 485 / 585
Dr. Gurram Gopal

Legal and Ethical Issues in Information Technology

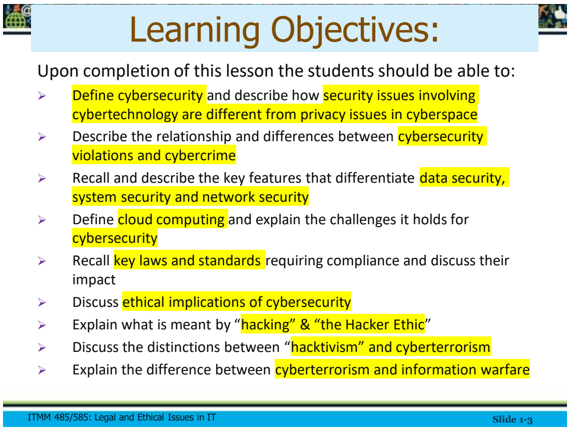
1

Ethical Concepts and Theories

ILLINOIS TECH | College of Computing

Ch6: Security and Compliance P3: Compliance, Cybersecurity Ethics, Hacking and the Hacker Ethic

2

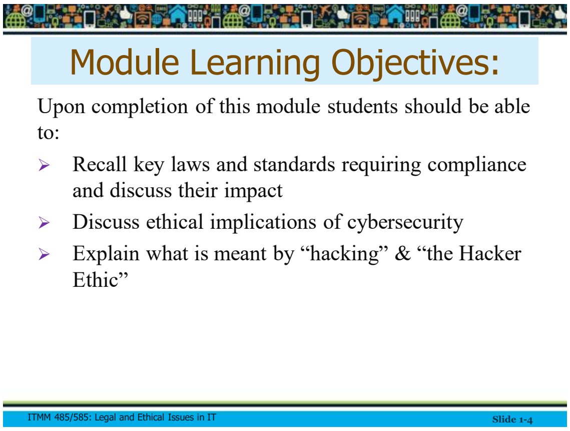


Learning Objectives:

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

3

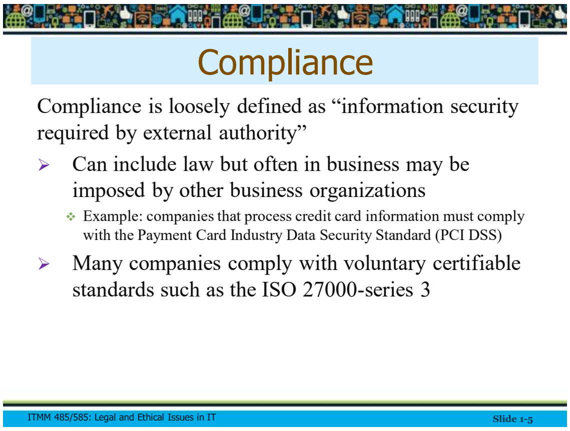


Module Learning Objectives:

Upon completion of this module students should be able to:

- 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"

4

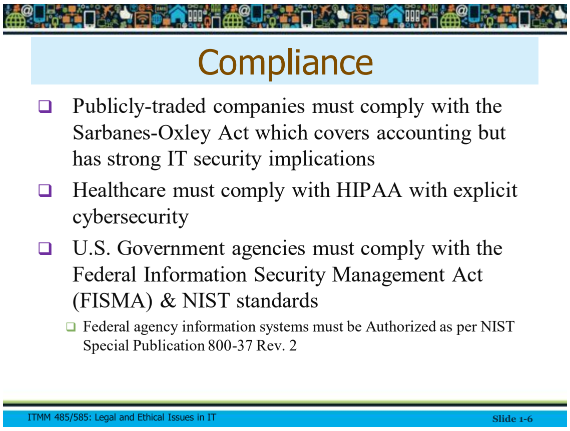


Compliance

Compliance is loosely defined as "information security required by external authority"

- Can include law but often in business may be imposed by other business organizations
  - Example: companies that process credit card information must comply with the Payment Card Industry Data Security Standard (PCI DSS)
- Many companies comply with voluntary certifiable standards such as the ISO 27000-series 3

5



Compliance

- ❑ Publicly-traded companies must comply with the Sarbanes-Oxley Act which covers accounting but has strong IT security implications
- ❑ Healthcare must comply with HIPAA with explicit cybersecurity
- ❑ U.S. Government agencies must comply with the Federal Information Security Management Act (FISMA) & NIST standards
  - ❑ Federal agency information systems must be Authorized as per NIST Special Publication 800-37 Rev. 2

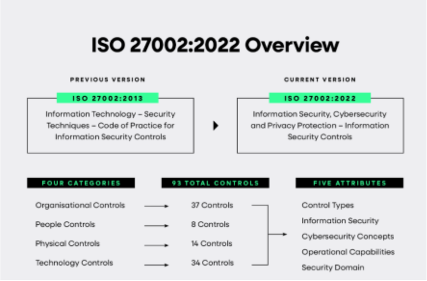
6

Compliance with State, Federal and Foreign Laws

- Examples
- 23 NYCRR 500 New York Department of Financial Services Cybersecurity Regulation
- California Privacy Rights Act (CPRA)
- European Union General Data Protection Regulation (GDPR)

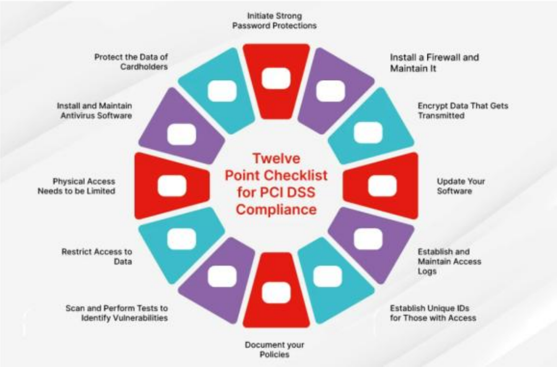
7

Accreditation and Certification



ISO 27002:2022 Overview

8



Twelve Point Checklist for PCI DSS Compliance
Initiate Strong Password Protections
Install a Firewall and Maintain It
Encrypt Data That Gets Transmitted
Update Your Software
Establish and Maintain Access Logs
Establish Unique IDs for Those with Access
Document your Policies
Scan and Perform Tests to Identify Vulnerabilities
Restrict Access to Data
Physical Access Needs to be Limited
Install and Maintain Antivirus Software
Protect the Data of Cardholders

9

Ethical Aspects of Cybersecurity

- Ethical issues affecting individual autonomy, privacy, and expectations of anonymity arise because of cybersecurity.
- To realize autonomy, as well as privacy and anonymity, users need to have some control over how personal information about them is gathered and used.
- On the one hand, secure computers can help users realize this goal.
- But secure computers can also undermine this goal, and this can raise *ethical* concerns.

10

Ethical Aspects of Cybersecurity (Continued)

- An ethical analysis of cybersecurity issues needs to consider whether an appropriate balance can be found in preserving both:

a) adequately secure computer systems;

b) autonomy and privacy for computer users.

11

Hacking and the "Hacker Ethic"

- Individuals and groups that launch malicious programs of various kinds are commonly described in the media as *hackers*.
- According to Simpson (2006), a hacker is anyone who "accesses a computer system or network without authorization from the owner."
- Simpson defines "crackers" as hackers who break into a computer system with "the intention of doing harm or destroying data."

12

Hacking and "Hacker Ethic" (Continued)

- Many computer scientists are unhappy with how the word "hacker" has come to be used in the media.
- Kaufman, Perlman, and Spencinor (2002) describe "true computer hackers" as

> individuals who play with computers for the "pure intellectual challenge" and as "master programmers, incorruptibly honest, unmotivated by money, and careful not to harm anyone."

13

Hacking and "Hacker Ethic" (Continued)

- Many people who are now identified in the media as hackers are neither brilliant nor accomplished computer experts.
- "Early computer hackers" have been described as individuals who aimed at accessing computer systems to see how they worked, and not to cause any harm to those systems.
- Were these kinds of hackers also behaving unethically?
- These individuals are sometimes described as behaving in accordance with a certain "code of ethics."

14

Hacking and the "Hacker Ethic" (Continued)

- Steven Levy (2001) describes the "Hacker Ethic" as comprising the following beliefs:

i. Access to computers should be unlimited and total.
ii. All information should be free.
iii. Mistrust Authority - Promote Decentralization.
iv. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
v. You can create art and beauty on a computer.
vi. Computers can change life for the better.

15

Hacking Activities

- Some hacking activities can be viewed as examples of three of the principles included in Levy's "Hacker Ethic":

1) information should be (totally) free;
2) hackers provide society with a useful and important service;
3) activities in cyberspace are virtual in nature; so they do not cause real harm to people in the real (physical) world.

16

"Information Wants to Be Free"

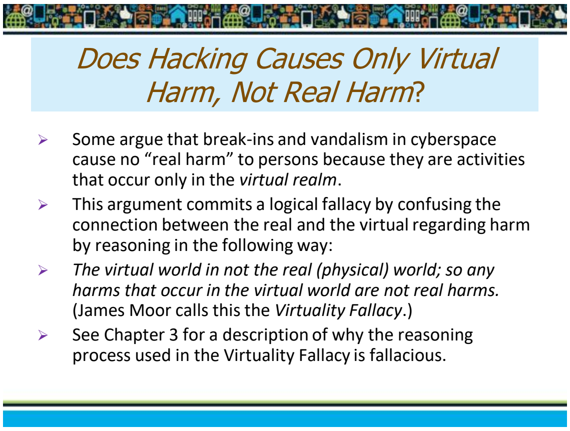
- Should all information be totally free?
- The view that information should be free is regarded by some critics (for example, Spaf- ford 2004) as naïve, idealistic, or romantic.
- Spafford notes that if information were free:
- privacy would not be possible because we would not be able to control how information about us was collected and used.
- it would not be possible to ensure integrity and accuracy of that information.

17

Do Hackers Really Provide an Important Service?

- Spafford also provides counterexamples to this version of the "hacker argument."
- He asks whether we would permit someone to start a fire in a crowded shopping mall in order to expose the fact that the mall's sprinkler system was not adequate.
- Alternatively, would you be willing to thank a burglar who successfully broke into your house?
- For example, would you thank that burglar for showing that your home security system was inadequate?

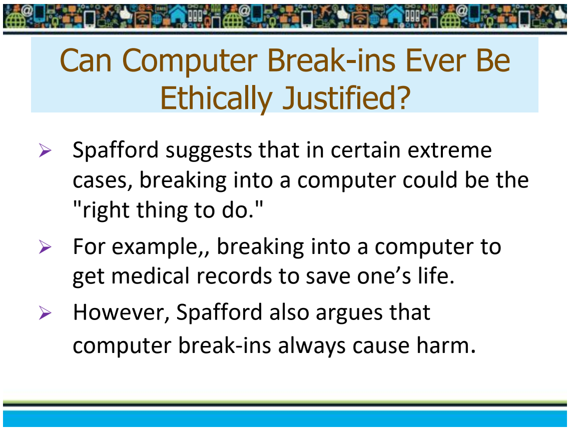
18



Does Hacking Causes Only Virtual Harm, Not Real Harm?

- Some argue that break-ins and vandalism in cyberspace cause no “real harm” to persons because they are activities that occur only in the *virtual realm*.
- This argument commits a logical fallacy by confusing the connection between the real and the virtual regarding harm by reasoning in the following way:
- *The virtual world in not the real (physical) world; so any harms that occur in the virtual world are not real harms.* (James Moor calls this the *Virtuality Fallacy*.)
- See Chapter 3 for a description of why the reasoning process used in the Virtuality Fallacy is fallacious.

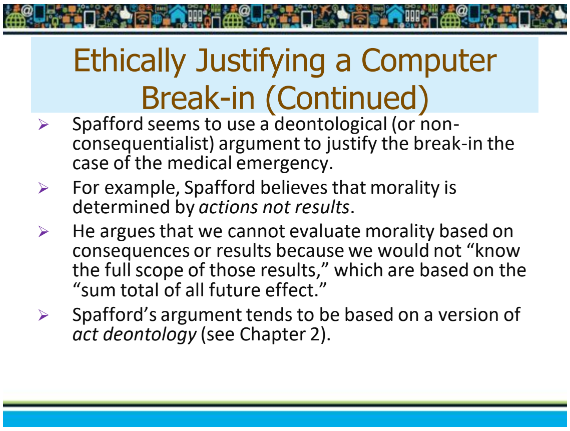
19



Can Computer Break-ins Ever Be Ethically Justified?

- Spafford suggests that in certain extreme cases, breaking into a computer could be the "right thing to do."
- For example,, breaking into a computer to get medical records to save one’s life.
- However, Spafford also argues that computer break-ins always cause harm.

20



Ethically Justifying a Computer Break-in (Continued)

- Spafford seems to use a deontological (or non-consequentialist) argument to justify the break-in the case of the medical emergency.
- For example, Spafford believes that morality is determined by *actions not results*.
- He argues that we cannot evaluate morality based on consequences or results because we would not “know the full scope of those results,” which are based on the “sum total of all future effect.”
- Spafford’s argument tends to be based on a version of *act deontology* (see Chapter 2).

21

ITMM 485/585: Legal and Ethical Issues in IT

Slide 1-22

22