ILLINOIS TECH | College of Computing

ITMM 485 / 585
Dr. Gurram Gopal

Legal and Ethical Issues in Information Technology

1

ILLINOIS TECH | College of Computing

Ch6: Security and Compliance P2: Cloud Computing Security and Risk Management

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:

- Define cloud computing and explain the challenges it holds for cybersecurity
- Describe the role of risk management in information security

4

"Cloud Computing" and Security

- What is *Cloud Computing*?
- The National Institute of Standards and Technology (NIST) officially defines cloud computing as

  …a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services).

5

Cloud Computing (Continued)

Popular examples of cloud-computing applications include:

- photo storing services, such as Google's Photos
- web-based email services, such as Gmail
- file storage services, such as Dropbox
- Streaming Services, like Netflix and Spotify

6

Cloud Computing (Continued0

The NIST definition of cloud computing identifies four distinct "deployment models" and three kinds of "service models."

Deployment models include

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

Service models include

- Software as a Service (or SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

7

Securing User Data Residing in the Cloud

- Cavoukian (2008) argues that for cloud computing to be fully realized, users will have to be confident that their personal information is protected and that their data (in general) is both secure and accessible.
- Currently, however, users have at least four different kinds of worries or "concerns" along these lines.
- One concern has to do with how users can control their data stored in the cloud – e.g., at present, users have very little "control over or direct knowledge about how their information is transmitted, processed, or stored" (Privacy Rights Clearinghouse).

8

Securing User Data Residing in the Cloud..

- A second concern involves the integrity of the data – for example, if the host company goes out of business, what happens to the users' data?
- A third kind of concern affects questions about access to the data – i.e., can the host deny a user access to his/her own data?
- A fourth concern has to do with who actually "owns" the data that is stored in the cloud (Privacy Rights Clearing House).

9

Securing User Data Residing in the Cloud (Continued)

- Talbot (2011) notes that many businesses worry about turning over their data to third parties.
- He identifies three main kinds of concerns that these businesses have, which involve:

1) accidental loss of data,
2) fear of hacking attacks,
3) theft by "rogue employees of cloud providers."

- Until these concerns are resolved, Talbot suggests that users will be skeptical about placing their trust in cloud-computing services to protect their data.

10

Assessing *Risk* in the Context of Cloud Computing

- What is meant by *risk analysis* in the context of cyber- security in general and cloud computing in particular?
- Bruce Schneier (2004), who argues that security is an "ongoing process," believes that a key element in that process involves an understanding of the concept of risk.
- However, it is still not clear who is responsible for assessing and managing it in computing/IT-security contexts?
- One reason why it is becoming even more difficult to determine who is responsible for doing this may have to do with a factor that Pieters and van Cleeff (2009) call the "de-perimeterization" of the security landscape.

11

Risk (Continnued)

- Pieters and van Cleeff point out that because the information security landscape has become increasingly "de-perimeterized," IT systems now "span the boundaries of multiple parties" and they "cross the security perimeters."
- They also note that de-perimeterization-related concerns lead to "uncertain risk" for IT security, because of the lack of clear boundaries defining the security landscape with no secure "digital fence" or perimeter safeguarding the users' data.
- So both ordinary users and businesses may be required to assume some level of *uncertain risk* with regard to their data and system resources that reside in the cloud.

12

Zero Trust

- "never trust, always verify"
- Eliminates implicit trust and continuously validates every stage of a digital interaction
- Devices are not be trusted by default, even if connected to a managed corporate network
- Requires all users, in or outside of the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture

- Raina, Kapil (2021) "Zero Trust Security Explained: Principles of the Zero Trust Model" https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/
- "What is a Zero Trust Architecture" (2021) Palo Alto Networks https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
- Zero trust security model (2022) Wikipedia https://en.wikipedia.org/wiki/Zero_trust_security_model

13

Cybersecurity Risk Management

Well-developed risk management program has three formal processes:

- Risk identification, assessment, and analysis
- Risk appetite definition
- Risk control

Each manager in the organization should focus on reducing risk

- In this instance, risk to information assets, but they are also concerned with financial risk and risk to personnel (aka safety)

14

Cybersecurity Risk Management

Risk Management involves discovering and understanding answers to some key questions with regard to the risk associated with an organization's information assets:

- Where and what is the risk (risk identification)?
- How severe is the current level of risk (risk analysis & assessment)?
- Is the current level of risk acceptable (risk evaluation)?
- What do I need to do to bring the risk to an acceptable level (risk treatment)?
- (Process applies to anyrisks managed, not just cybersecurity risk)

15

Cybersecurity Risk Management Framework

https://www.linkedin.com/pulse/uncovering-must-dos-your-nist-risk-management-framework-dewayne-hart/

16

?

17