JAKARTA INTERNATIONAL UNIVERSITY

JIU

# Management Information System

GLORIA PRATIWI WAANG, SE., MBA | Email: gloria@jiu.ac

## 9. Risk, Ethics, and Trust

# Learning Objectives

By the end of this session, students should be able to:

- Identify Vulnerabilities: Spot IT risks, ethical dilemmas, and trust breakdowns in case studies. and distinguish between intentional threats (malware) and human error.
- Evaluate Business Impact: Quantify financial, legal, and reputational damages from MIS failures, and explain compliance needs for corporate governance (SOX, GDPR, HIPAA).
- Apply MIS Frameworks: Use Laudon’s Five Moral Dimensions to assess digital firm ethics., and apply Bidgoli's Three Security Controls (Technical, Operational, Managerial).
- Design Internal Controls: Mix accounting with IT to design General and Application Controls and draft disaster recovery plans that balance risk mitigation with cost.
- Build Digital Trust: Evaluate corporate policies on data privacy and employee monitoring and connect robust digital trust to customer loyalty and competitive advantage.

# Part 1: The Anatomy of Digital Risks

## Real-world Scenarios and the Fragility of Systems

# Case Study:
# The Invisible Thief

Imagine a global retail giant. A single unpatched server allows a hacker to sit silently in the network for 6 months.

**Result:** 150 million credit card records sold on the dark web. The CFO faces a $2 billion cleanup bill.

*Is this a technical failure or a management failure?*

Source: https://elements-resized.envatousercontent.com/elements-video-cover-images/f155cca6-ddb4-40aa-85d3-d5981cdb55ab/video_preview/video_preview_0000.jpg?w=500&cf_fit=cover&q=85&format=auto&s=1ef682c42d95b72ae10e2ce55e9da269a850f4f570bbd89020cc6f328bfbabea

# Case Study:
# Algorithmic Injustice

A bank implements an AI for loan approvals. It's efficient, but later discovered to systematically deny loans to specific zip codes.

- **Ethical Dilemma:** Efficiency vs. Fairness.
- **Accountability:** Who is responsible? The coder? The manager? The machine?

Source: https://images.squarespace-cdn.com/content/v1/62ec2bc76a27db7b37a2b32f/2f9ca28f-8de6-44d4-a7e3-a8fecdf528e3/is-ai-becoming-self-aware.jpg

# The Trusted Accountant

A senior accountant uses "Super-User" access to bypass internal controls and embezzle $500,000 over three years by creating ghost vendors.

**The Breach of Trust:** The system worked exactly as programmed. The flaw was in the **governance** and **segregation of duties**.

## *Class Discussion*

**“Are we too reliant on Information Systems? If your company's database disappeared today, could you still do business tomorrow?”**

# Phase 2: Why it Matters

## Analyzing the Multi-Dimensional Impact

# The Cost of System Failure

**$4.45M**

Average Cost of a Data Breach (2023)

Source: https://www.digitalnewsasia.com/sites/default/files/images/digital%20economy/Hacker%20Stealing%20Money.jpg

# Compliance: The Carrot and the Stick

## GDPR

Fines up to 4% of global annual turnover for privacy violations.

## SOX Act

Ensures accuracy of financial statements through strict internal controls.

## CCPA

California's landmark privacy act protecting consumer data rights.

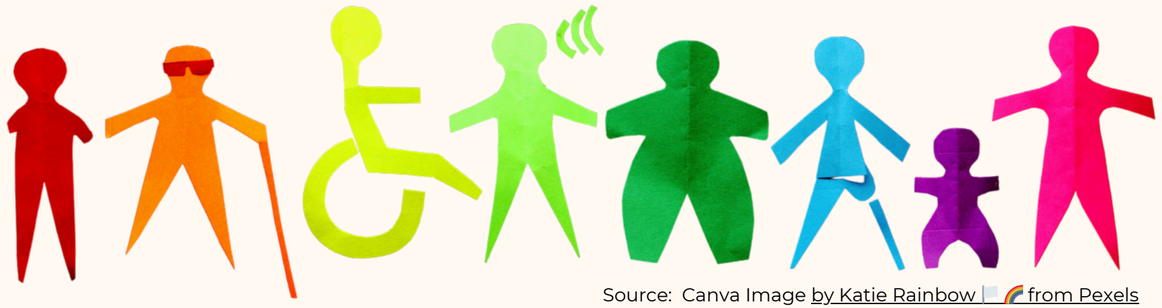
# The Digital Handshake

Trust is the foundation of the digital economy.
Once lost, it takes years to rebuild.

# The Information Society

**MIS trends have created social tensions:**

- The Digital Divide: Disparity between those with access and those without.
- Profiling & NORA: Ability to combine data from disparate sources to create a "digital twin."
- Mental Health: The "Always-On" culture and technostress.



Source: Canva Image by Katie Rainbow from Pexels

## Critical Tought

“"In the age of Big Data,
is privacy a right, a privilege, or an illusion?"”

# Phase 3: The Theory

## Frameworks for Moral Decision-Making

# Five Moral Dimensions

Source: Canva Image Şinasi Müldür from Pexels

**Information Rights:**
What do we own?

**Property Rights:**
Intellectual Property.

**Accountability & Control:**
Who is liable?

**System Quality:**
Standards of data.

**Quality of Life:**
Social impact.

# Classic Ethical Benchmarks

## Golden Rule

Do unto others as you would have them do unto you.

## Categorical Imperative

If an action is not right for everyone to take, it is not right for anyone (Kant).

## Rule of Change

If an action cannot be taken repeatedly, it is not right to take at all (Descartes).

# Utility and Risk

## Utilitarian Principle

Take the action that achieves the higher or greater value for all.

## Risk Aversion Principle

Take the action that produces the least harm or the least potential cost.

# The "No Free Lunch" Rule

"Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise."

**Fundamental for Intellectual Property and Software Piracy issues.**

# How to Analyze a Dilemma

- **Identify the Facts:** Who did what to whom?
- **Define the Conflict:** Higher-order values involved.
- **Identify Stakeholders:** Groups with a vested interest.
- **Identify Options:** Realistic actions you can take.
- **Consequences:** Potential outcomes of those options.

Source: Canva Image

# Professional Ethics

**ACM & AIS Codes:**

- Contribute to society and human well-being.
- Avoid harm to others.
- Be honest and trustworthy.
- Respect the privacy of others.

"The profession of MIS is not just about moving bits; it's about managing the truth."

Source: Canva Image by Sebastian Moldoveanu's Images

# Part 4: Risk Theory

## Threats, Vulnerabilities, and Internal Controls

# Risk Management Basics

**Risk:** The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

**Risk = Probability of Event × Impact of Event**

# The CIA Triad (Bidgoli)

- **Confidentiality:** Only authorized users can access data.
- **Integrity:** Accuracy and reliability of information.
- **Availability:** Systems are accessible when needed.

# Categories of Threats

## Technical

Software bugs, hardware failure, power outages.

## Human

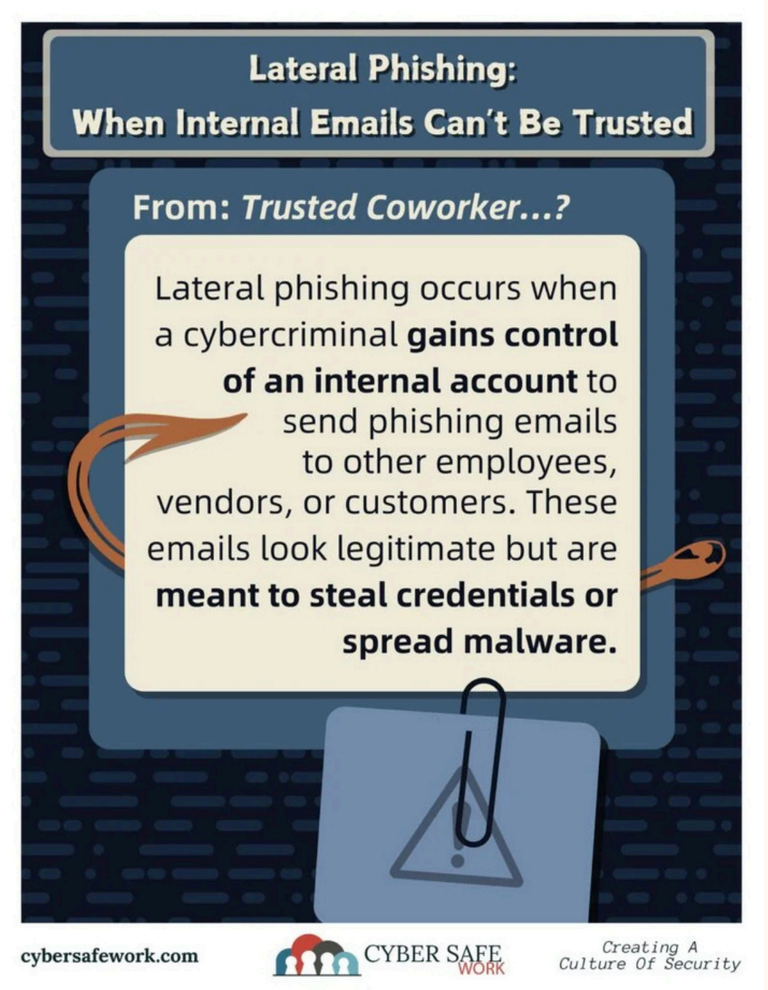
Social engineering, insider fraud, poor passwords.

## Natural

Floods, fires, earthquakes (Force Majeure).

# Cybercrime 101

- **Phishing:** Deceptive emails to steal credentials.
- **Ransomware:** Encrypting data for payment.
- **Spyware:** Monitoring user activity.




Source: https://coursevector.com/wp-content/uploads/202503-Lateral-Phishing-791x1024.jpg

# Part 5: Protecting Assets

## Security Tools and Defensive Strategies

# Network Defense

## Firewalls

Hardware or software that filters traffic based on security rules.

## VPN

Secure "tunnel" for remote workers to access internal systems safely.

# Cryptography

Transforming readable data into scrambled **"ciphertext."**

| Type | Mechanism | Use Case |
| --- | --- | --- |
| Symmetric | One key for both | Internal DBs |
| Asymmetric | Public/Private key pair | Internet Banking |

# Access Control

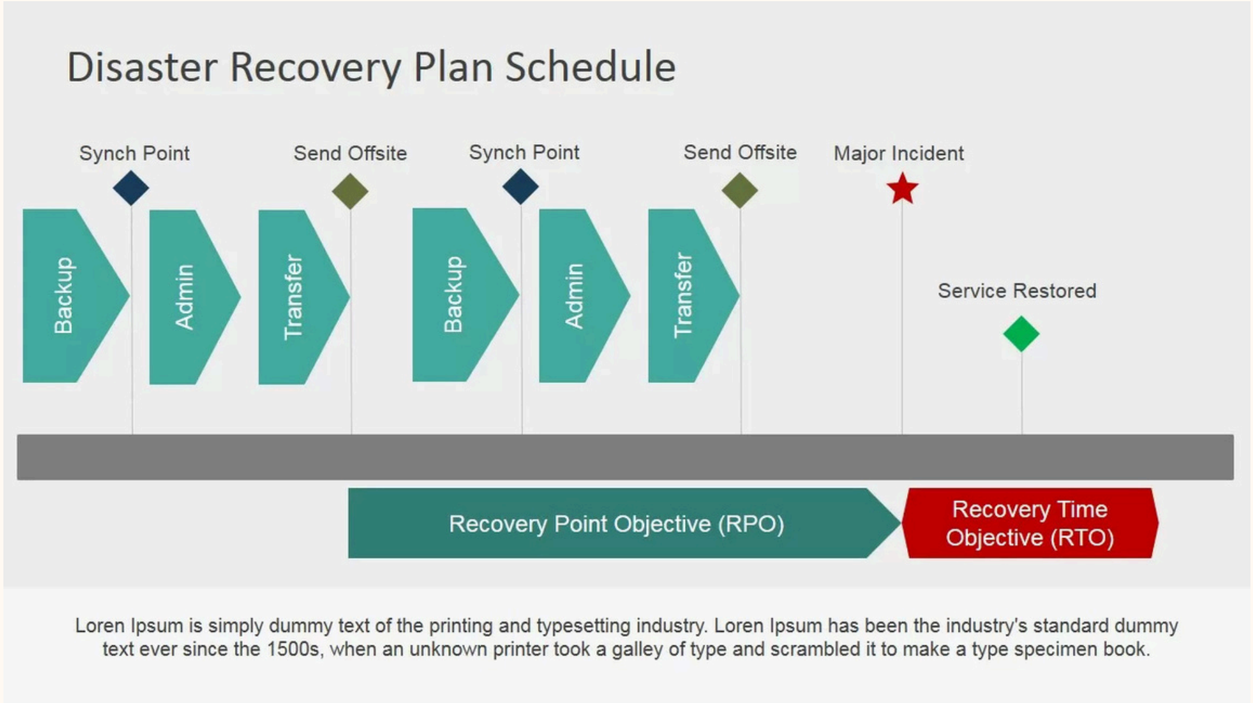

Source: https://elements-resized.envatousercontent.com/elements-video-cover-images/fc04a57b-6d74-44d2-a46b-7bc67418dde6/video_preview/video_preview_0000.jpg?w=500&cf_fit=cover&q=85&format=auto&s=4393faee1eb313f65c9fc01766c09e8876553235cdf08e8c998c8afe994e9570

**Multi-Factor Authentication (MFA):**

- Something you KNOW (Password).
- Something you HAVE (Phone/Token).
- Something you ARE (Fingerprint/Face).

# Planning for the Worst

- **Disaster Recovery Plan (DRP):** Technical steps to restore systems.
- **Business Continuity Plan (BCP):** How the “entire business” operates during the outage.




Source: https://slidemodel.com/wp-content/uploads/6990-01-disaster-recovery-powerpoint-template-11.jpg

# The Role of the Auditor

Internal and external auditors verify that security policies are followed.

- Testing user permissions.
- Verifying backup integrity.
- Checking the physical security of server rooms.

# Part 6: Building Trust

## The Future of Digital Integrity

# What Makes a System Trustworthy?

**Transparency**
Users know what is being collected.

**Predictability**
The system behaves as expected.

**Benevolence**
The intent of the system is to help, not exploit.

Source: https://media.istockphoto.com/id/2213683294/vector/abstract-man-and-ai-robot-engaging-in-a-handshake-partnership-concept.jpg?s=612x612&w=0&k=20&c=OeFJmmAdNqEmSKsAJkNrdb5mzgF_kE3BqWZoWbCon2Q=

# N O R A

## Non-Obvious Relationship Awareness

The ability to connect records across diverse systems
(phone bills, criminal records, flight data) to find "hidden" threats.

**The ultimate test of Privacy vs. Security.**

# The AI Frontier

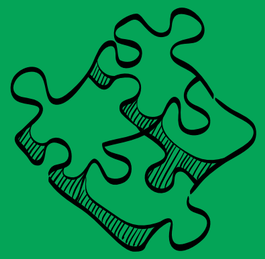
Trusting black-box algorithms:

**Explainability:**
Can the AI tell us
**why** it made a decision?

**Bias Mitigation:**
Constantly auditing data for historical prejudice.

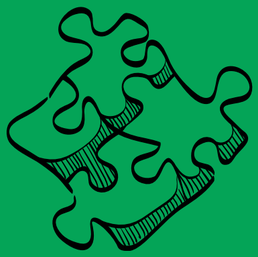
# Conclusion

- As we move toward autonomous systems, the human element becomes **more** important, not less.
- **Final Takeaway:** Technology provides the power, but Ethics provides the direction. Trust is the currency of the information age.


# Thankyou!




# Referense


- Management Information System, Hossein Bidgoli. Cengage. 10th Edition. 2020
- Management Information System: Managing the Digital Firm. Kenneth C. Laudon & Jane P. Laudon. Pearson. 16th Edition. 2020.