Contemporary Issues in Finance - Lecture 9

Lesson Title: Cybersecurity and Data Privacy in Finance

Instructor: Dr. Mary Githinji

Course Overview

- Digital transformation of finance and rising cyber risks
- Focus: Cybersecurity, data privacy, regulations, ethics, and innovation
- Integrates real-world cases and best practices

Goal: Build capacity to manage cyber and data risks responsibly

Learning Objectives

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

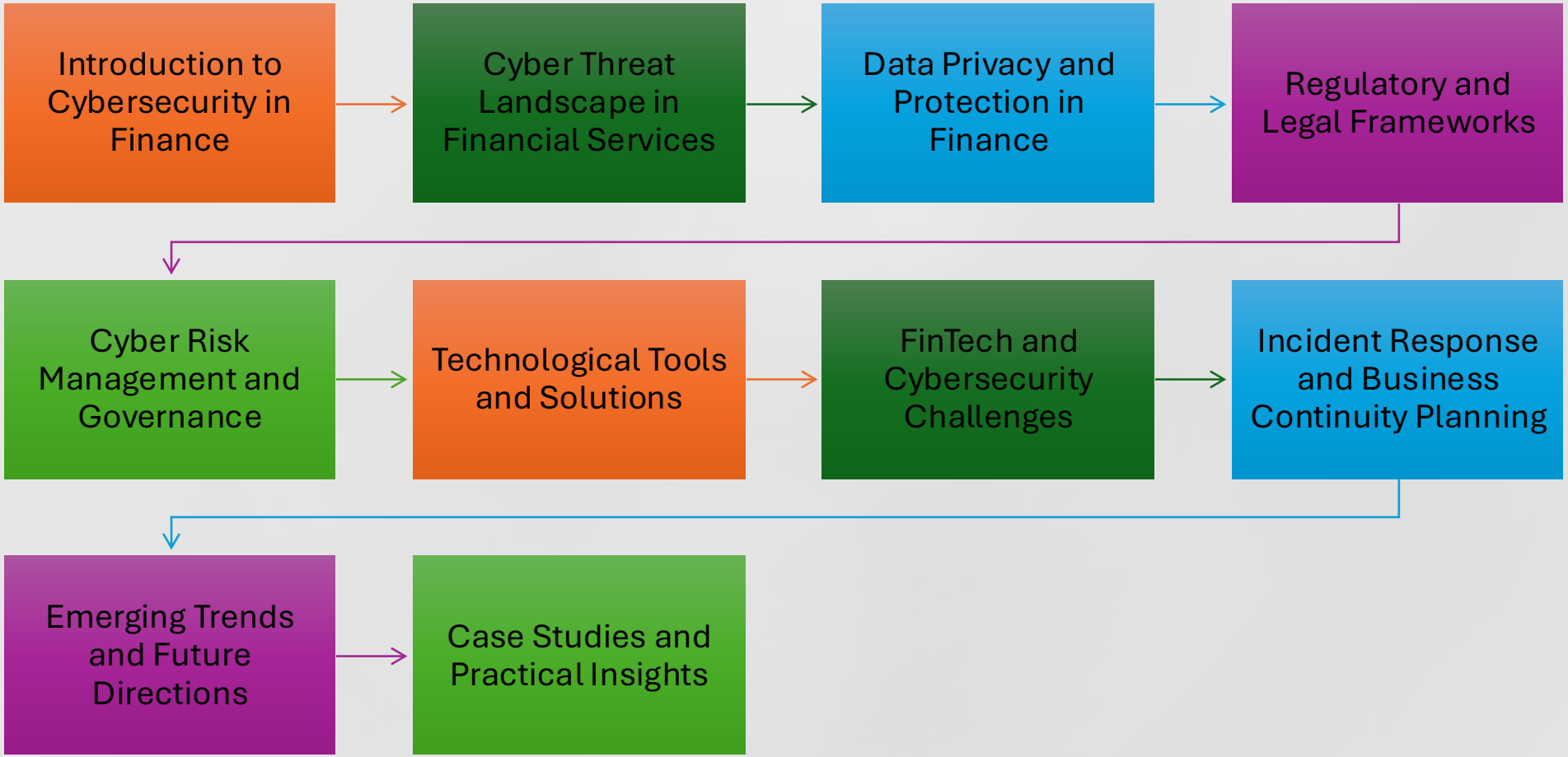
- Understand the importance of cybersecurity in finance
- Identify key types of cyber threats
- Discuss major global data privacy regulations
- Analyze risk management and governance frameworks
- Evaluate ethical issues and emerging technologies

Learning Outcomes

After this session, Learners will be able to:

- Explain core cybersecurity and data privacy concepts
- Critically assess vulnerabilities in financial systems
- Apply risk management principles
- Evaluate new technologies' impact on security and privacy
- Recommend policy and governance measures

Outline

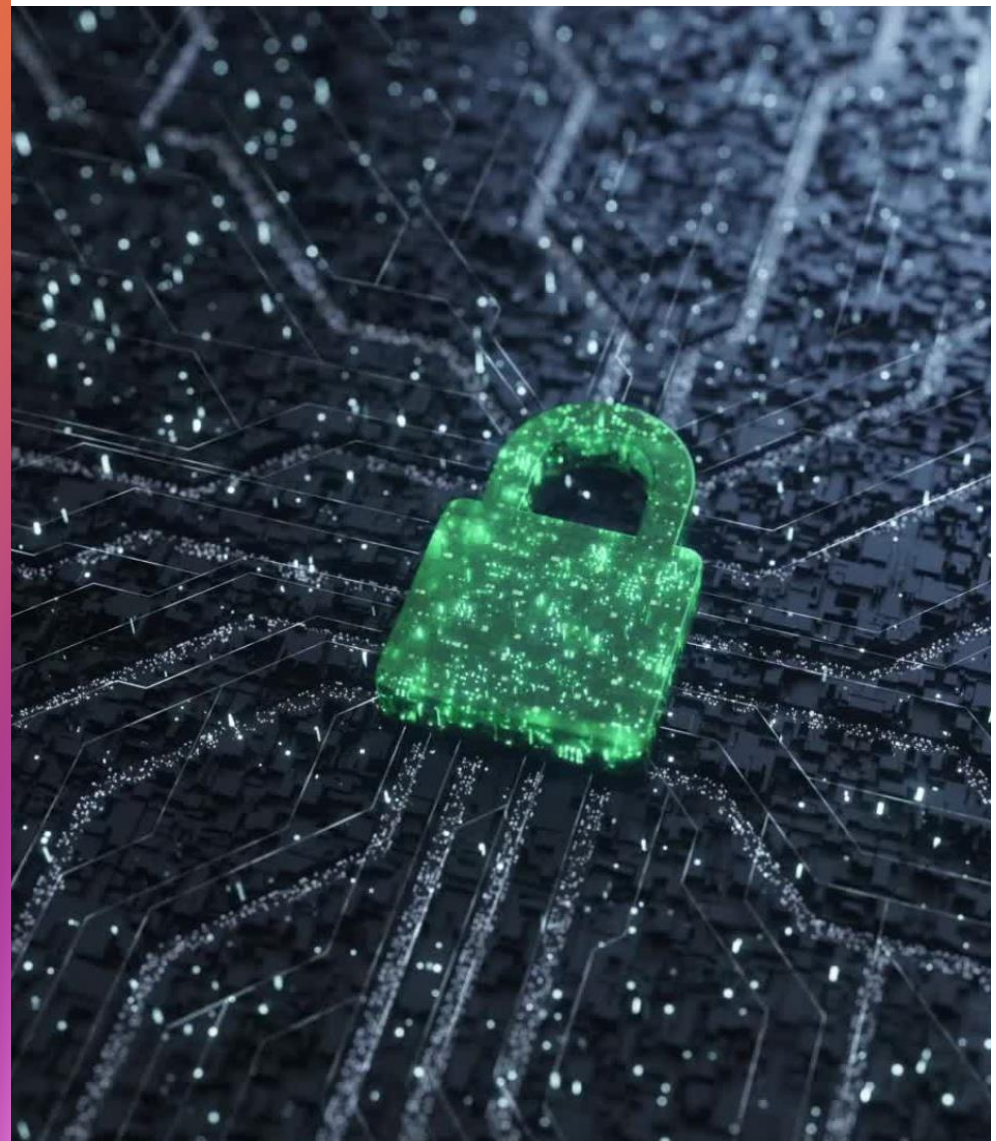

Introduction to Cybersecurity in Finance
Cyber Threat Landscape in Financial Services
Data Privacy and Protection in Finance
Regulatory and Legal Frameworks
Cyber Risk Management and Governance
Technological Tools and Solutions
FinTech and Cybersecurity Challenges
Incident Response and Business Continuity Planning
Emerging Trends and Future Directions
Case Studies and Practical Insights

Introduction

- Finance is a top target for cybercrime
- Digital transformation to increased exposure
- Trust and stability depend on secure systems
- Data privacy leads to ethical and legal responsibility

Question

What threats do you think affect the financial industry?



The Cyber Threat Landscape

Common threats include:

- Phishing and Social Engineering
- Ransomware Attacks
- Data Breaches
- Insider Threats
- DDoS Attacks (System Overload)

Phishing and Social Engineering

- Fraudulent emails, texts, or calls trick users into revealing credentials or financial data.
- Often use fake websites or brand impersonation.
- Most common attack vector for financial institutions.

Mitigation:
Awareness training, multi-factor authentication, and email filtering systems.

Ransomware Attacks

- Malicious software encrypts data, demanding ransom for release.
- Disrupts banking operations and payment systems.
- May result in data loss, reputational damage, or regulatory penalties.

Mitigation:
Regular backups, patch management, incident response planning, and staff awareness.

Data Breaches

- Unauthorized access and exposure of confidential financial data.
- Can lead to identity theft, regulatory fines, and customer distrust.
- Often caused by weak passwords, insider misuse, or unpatched systems.

Mitigation:
Encryption, network monitoring, strong access controls, and compliance audits.

Insider Threats

- Employees or contractors misuse access privileges to steal or leak sensitive data.
- Motivations include financial gain, coercion, or negligence.
- Often more difficult to detect than external attacks.

Mitigation:
Background checks, access restrictions, monitoring, and a culture of accountability.

DDoS Attacks (System Overload)

Distributed Denial of Service floods financial servers with traffic.

Causes system downtime and disrupts online banking services.

Can be used as a distraction for other attacks.

Mitigation:
Traffic filtering, load balancing, firewalls, and backup servers.

Data Privacy in Finance

Personal financial data is high-value target

Core principles:

- Confidentiality – Protecting access
- Integrity – Preventing manipulation
- Availability – Ensuring system uptime

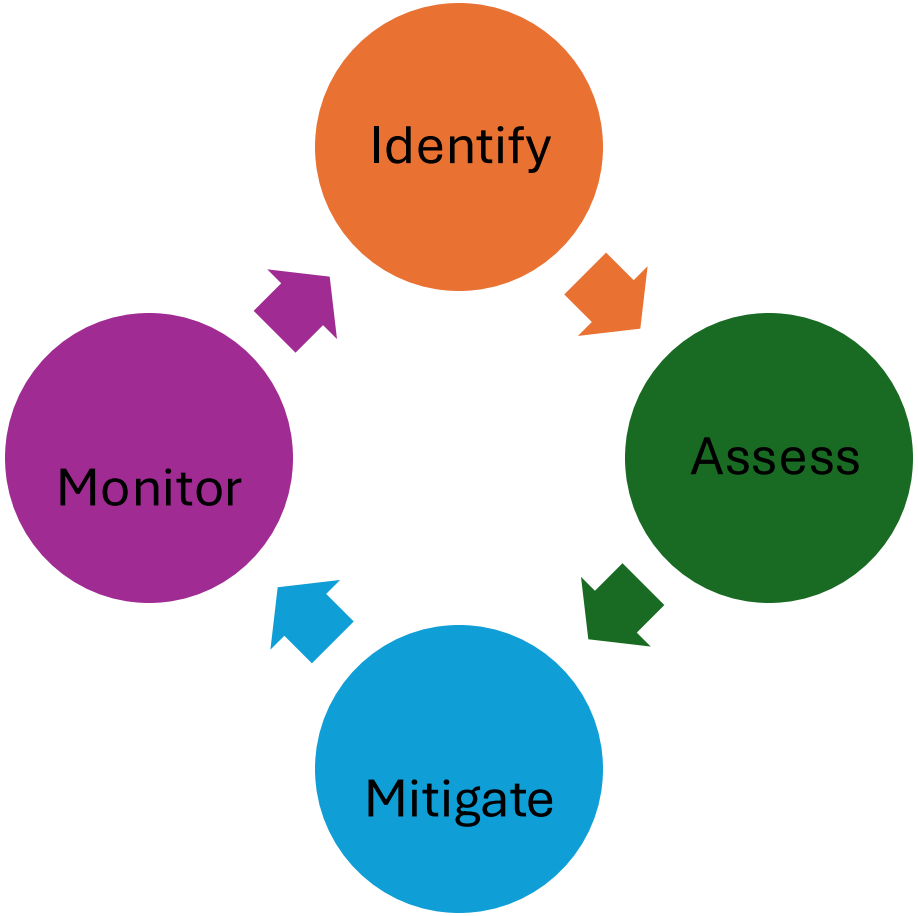
GDPR (EU) – CONSENT, DATA MINIMIZATION, RIGHT TO BE FORGOTTEN

PCI DSS – PAYMENT DATA PROTECTION

BASEL COMMITTEE – OPERATIONAL RESILIENCE

KENYA DATA PROTECTION ACT (2019) – LOCAL COMPLIANCE EXAMPLE

Cyber Risk Management



Cyber Risk Management

Key elements:

- Risk registers
- Incident response plans
- Board oversight
- Regular audits and testing

Governance and Institutional Roles

- CISO (Chief Information Security Officer)
- Data Protection Officer (DPO)
- Board Cyber Committees
- Cross-department collaboration

Technology and Tools

- Firewalls and Intrusion Detection Systems
- Multi-Factor Authentication (MFA)
- Encryption and Tokenization
- AI and ML for threat detection
- Blockchain for secure transactions

FinTech and New Risks

Digital banking and mobile wallets

Cloud computing vulnerabilities

Third-party service risks

Cryptocurrency and DeFi threats

Ethical Dimensions

Responsible data use and consent

Balancing personalization vs privacy

Avoiding algorithmic bias

Transparency and accountability

Incident Response

Incident Response

Key actions:

- Notify regulators and affected customers
- Preserve digital evidence
- Strengthen post-incident controls

Business Continuity Planning

Backup systems and redundancy

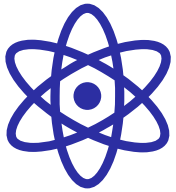
Crisis communication protocols

Recovery time objectives (RTOs)

Cyber insurance

Emerging Trends

RegTech: Compliance automation



Quantum computing and cryptography

Global cyber cooperation

ESG link: cybersecurity as part of “G” (governance)

Case Studies

Equifax Breach – Data exposure and loss of trust

Capital One (2019) – Cloud misconfiguration

Kenya’s NCBA Mobile Banking Attacks (2023) – Local lessons

Discussion Prompt

- Can financial innovation and privacy coexist?
- Are privacy laws slowing innovation?
- Should consumers trade data for convenience?

Conclusion

- Cybersecurity and privacy are pillars of financial trust
- Governance, ethics, and technology must align
- Continuous vigilance and adaptation are essential

References

- Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements.
- European Union. (2018). *General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)*. Official Journal of the European Union.
- Kshetri, N. (2016). *Cybersecurity and business: The role of regulation and technology*. *Computer*, 49(8), 84–88.
- Republic of Kenya. (2019). *Data Protection Act, No. 24 of 2019*. Kenya Gazette Supplement No. 181 (Acts No. 24).
- World Economic Forum. (2022). *Global cybersecurity outlook 2022*.

(PowerPoint Generated using Microsoft 365 and all images are free Microsoft images)

Thank You