

Cybersecurity Concepts (Introduction to Security)

Prepared by Dr. Sumaya Alkubaisi

FNT625
Cybersecurity Concepts

Lecture 1



Lecture

1

Learning Goals

By the end of this lecture, you will be able to:

- Define cybersecurity and explain why it is important.
- Understand the CIA triad (Confidentiality, Integrity, Availability) with real-world examples.
- Recognize major cyber threats.
- Explain core security measures for individuals and organizations.
- Discuss emerging trends and issues in cybersecurity.

Lecture

1

What is Cybersecurity?

Protecting computers, networks, and data from attacks.

Goal: keep information

- Safe
- accurate
- available.

Example: keeping bank accounts safe, protecting online payments, and ensuring transactions run smoothly.

Lecture

1

What is Cybersecurity?

Cybersecurity can be grouped into three interconnected dimensions:

Human – users, administrators, policies, and awareness.

Hardware – physical devices, servers, and network equipment.

Software – operating systems, applications, and security programs.

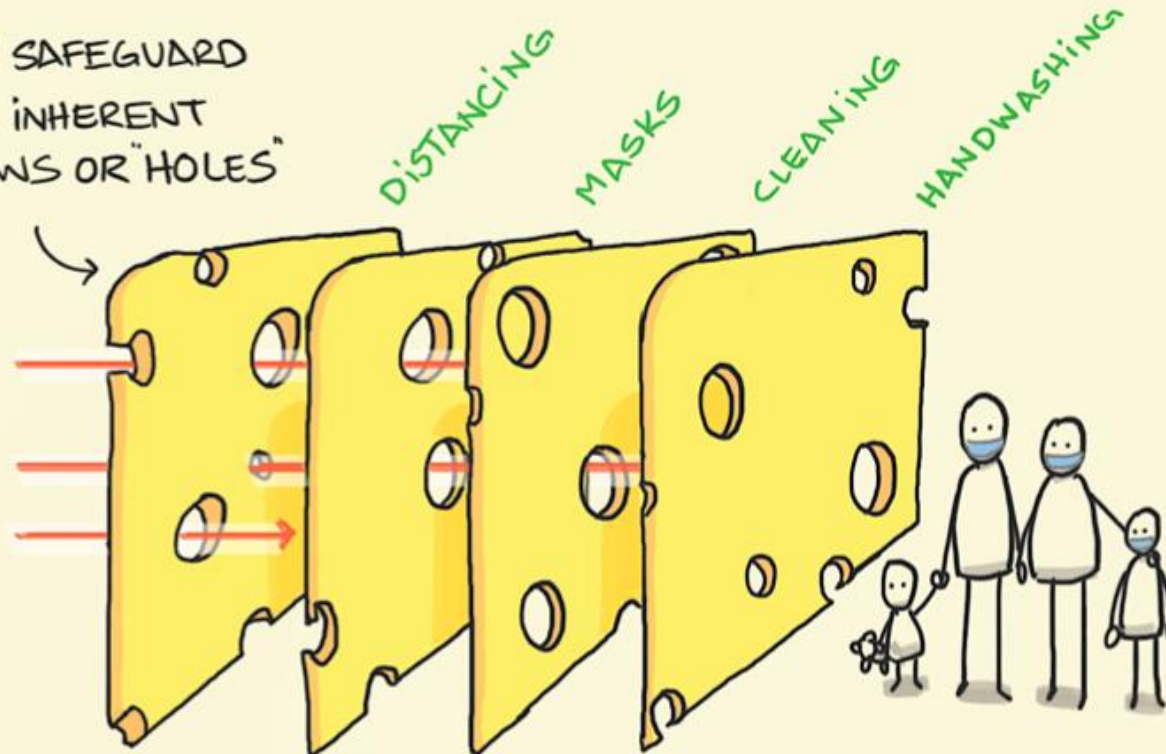
Cybersecurity is more than just these parts in isolation.

Think of it as a digital immune system: layered like an onion or stacked like slices of Swiss cheese — each layer has gaps, but when combined, they form a resilient defense.

THE SWISS CHEESE MODEL

FOR UNDERSTANDING ACCIDENTS AND IMPROVING SAFETY

ANY SAFEGUARD
HAS INHERENT
FLAWS OR "HOLES"



PROBLEMS OCCUR WHEN MULTIPLE "HOLES" LINE UP

MODEL: J REASON

sketchplanations

Lecture

1

Why Cybersecurity Matters?

Cybersecurity is crucial because it protects individuals and organizations from the severe consequences of cyberattacks.

These consequences include:

- **Financial Loss** – Stolen bank details, fraudulent transactions, or ransomware attacks can drain personal accounts or cost businesses millions.
Example: A ransomware gang locks a fintech company's database and demands Bitcoin payment to restore access.
- **Loss of Reputation** – Once a breach becomes public, customers may lose trust in the organization, leading to customer churn and long-term revenue decline.
Example: A digital wallet provider suffers a data leak, causing users to abandon the platform.

Lecture

1

Why Cybersecurity Matters? (Continue...)

Increased Costs – Cyberattacks force organizations to spend heavily on recovery, new security measures, and sometimes fines for non-compliance.

Example: After a data breach, a bank must pay for forensic investigations, customer credit monitoring, and upgraded security tools.

Risk of Repeat Attacks – Hackers often target the same company again once they find weaknesses.

Example: A fintech app breached via poor API security is attacked multiple times until the vulnerability is properly fixed.

- **Financial data is a prime target** – hackers aim for money and personal data.
- **Customer trust** – users only trust secure financial services.
- **Compliance** – laws like PSD2 enforce strong security in payments.
- **Business continuity** – banks and fintech apps must operate 24/7.

Example: Strong authentication in online payments



Chapter

01

Why Cybersecurity in Fintech?

Definition: Compliance in cybersecurity means following laws, regulations, and industry standards that protect data and ensure safe financial operations.

Lecture

1

Key Terminologies

- **Cybercrime:** Any criminal activity carried out using the internet or digital networks. Includes fraud, identity theft, ransomware, and hacking.

Example: Hackers launch a phishing campaign targeting online banking users to steal login credentials and transfer funds illegally.

- **Computer-related crime:** Any crime in which a computer plays a role, even if it is not the main target (A computer can be the tool, the target, or the storage of evidence).

Example: Money laundering using cryptocurrency wallets — the crime is financial, but the computer systems facilitate transactions and store digital evidence.

Lecture

1

Key Terminologies

- **Digital Forensics:** The scientific process of collecting, preserving, analyzing, and presenting digital evidence for legal purposes.
 - Ensures that data from computers, networks, or mobile devices can be used in court.
 - Phases: Identification → Preservation → Analysis → Presentation

Example: After a mobile banking app breach, forensic investigators recover logs from compromised servers to trace the attacker's IP address and prove fraud.

Lecture

1

CIA Triad (Core Principles)

The CIA Triad is the foundation of security

Confidentiality → Safe data (keeping financial/customer data private).

Integrity → Accurate data (making sure financial records aren't changed or tampered).

Availability → Available data (banking services and systems always accessible).

Lecture

1

Common Cyber Threats

- **Phishing**

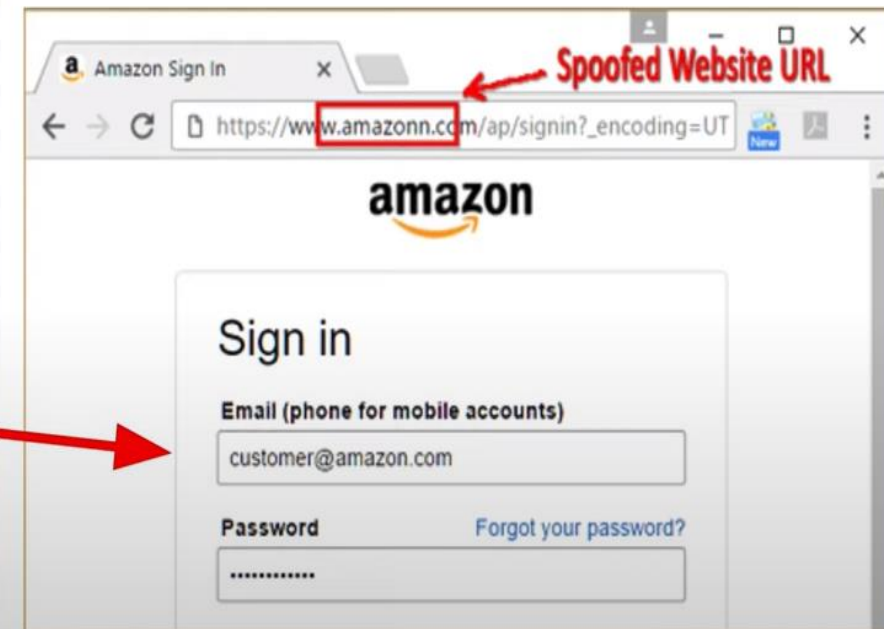
Definition: A social engineering attack where attackers trick users into revealing sensitive data (e.g., passwords, bank details).

Now often AI-powered, with very realistic fake emails or even deepfake voices (stealing login or card info).

Example:

Fake email pretending to be from a bank asking for login details.

Phishing email



Lecture

1

Common Cyber Threats

- **Malware**

Malicious software designed to disrupt, steal, or damage data.

Types:

Viruses – Malicious programs that attach themselves to files or software and spread when those files are shared.

Worms – Self-replicating malware that spreads automatically across networks without user action.

Ransomware – Malware that locks or encrypts data and demands payment for its release.

Trojans – Malicious software disguised as legitimate programs to trick users into installing it.

Example: Ransomware encrypts a bank's systems and demands payment to unlock them.

Lecture

1

Common Cyber Threats

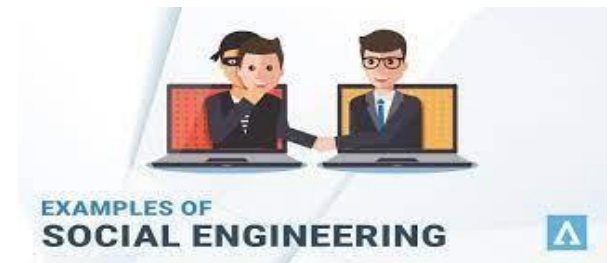
- **Insider Threats**

Security risks originating from employees or trusted users misusing their access.

Example:

A bank employee leaking credit card data to criminals.

An employee shares sensitive company data with a friend, who then passes it on to a rival company.



Lecture

1

Common Cyber Threats

- **DDoS (Distributed Denial of Service):** An attack that floods a system with requests, making it unavailable.

Example: Botnet Attacks

A botnet is a network of compromised computers or devices (“bots” or “zombies”) that are remotely controlled by a hacker (the “botmaster”).

The attacker uses these infected machines together to launch large-scale attacks such as Distributed Denial of Service (DDoS), spam campaigns, or credential-stuffing. Botnets are dangerous because they are hard to trace, spread quickly, and combine the power of thousands of devices.

Botnet Example: A botnet floods the login page of a mobile banking app with millions of fake login requests. This overwhelms the servers, causing the app to crash and preventing real customers from accessing their accounts.

Lecture

1

Common Cyber Threats

- **MITM (Man-in-the-Middle) Attacks**

- A cyberattack where the attacker secretly intercepts or modifies communication between two parties, allowing them to eavesdrop, steal credentials, or inject malicious content.
- These attacks are very dangerous because they happen silently; users often do not realize that their data is at risk.
- To prevent them, you should use secure networks, make sure websites start with HTTPS, and avoid entering sensitive information on public networks without a VPN."

Example:

-A hacker sets up a fake Wi-Fi hotspot in a café to steal mobile banking login details.

Lecture

1

Case Study: SWIFT Hack (2016)

- Attackers stole \$81M from Bangladesh Bank, by abusing weak security in the global banking message.
- Method: Exploited weak authentication in SWIFT banking messages.
- Lesson: Even trusted infrastructures require strong monitoring.

Lecture

1

Case Study: Capital One (2019)

- A hacker accessed 100M customer applications.
- Cause: Cloud misconfiguration (a cloud setup mistake) in Amazon Web Services (AWS).
- Lesson: Cloud security controls are critical in fintech.

Lecture

1

Protecting Against Cyber Threats

- Strong passwords & multi-factor authentication (prevents unauthorized access).
- Employee awareness training (reduces phishing success).
- Regular updates & patches (fix vulnerabilities).
- Data backups (protection from ransomware).
- Access controls (limit insider misuse).
- Monitoring & incident response (quick detection and action).

Lecture

1

Protecting Against Cyber Threats (Individuals)

Strong Passwords & MFA: Use long, unique passwords + extra verification (e.g., SMS, authenticator app).

Example: A user logs in to an app with a password + fingerprint.

Regular Updates & Patches: Keep personal devices and apps up-to-date to close vulnerabilities.

Example: Installing iOS/Android updates to prevent malware infections.

Personal Data Backups: Back up files to cloud or external drives to recover from ransomware or device loss.

Example: Backing up mobile banking transaction receipts to a secure cloud.

Awareness Training (Self-Education): Recognizing phishing emails, fake websites, and scam links.

Example: Deleting a suspicious SMS claiming to be from a bank.

Lecture

1

Protecting Against Cyber Threats (Organizations)

Access Controls: Limit employee access to only what they need (least privilege).

Example: A teller can view accounts but cannot approve wire transfers.

Monitoring & Incident Response: Detect and respond to cyberattacks quickly using logs, SIEM tool, and incident teams.

Example: Detecting abnormal login attempts and locking affected accounts.

Enterprise Backups & Disaster Recovery: Organization-wide backups and tested recovery plans.

Example: A fintech company restores services after a ransomware attack using backups.

Regular Communication & Reporting: Encourage staff to report suspicious activity without fear.

Example: An employee reporting a lost company laptop immediately.

Testing Defenses: Evaluate readiness using phishing simulations and penetration testing.

Example: A fintech hires ethical hackers to test mobile payment systems.

Lecture

1

How Cybersecurity Works (Core Mechanisms)

Cybersecurity is not a single tool, but a continuous cycle of protection., it involves four main mechanisms/Lifecycle:

Identify → Protect → Detect → Respond

Lecture

1

How Cybersecurity Works (Core Mechanisms)

1. Identify Risks

"Know what you must protect"

- Conduct risk assessments to find vulnerabilities across people, processes, and technology.
- Classify assets (data, servers, applications) based on their importance.

Example: A bank maps out risks for mobile payment systems, including weak API security.

Lecture

1

How Cybersecurity Works (Core Mechanisms)

2. Protect Against Risks

“Put defenses in place”

- Implement safeguards like two-factor authentication, encryption, firewalls, and secure coding practices.
- Ensure employees receive cybersecurity training.

Example: A fintech company deploys MFA for all online transactions.

Lecture

1

How Cybersecurity Works (Core Mechanisms)

3. Detect Incidents

“Spot attacks early”

-Attacks are often hidden — detection requires intrusion detection systems (IDS), log monitoring, and anomaly detection with AI tools.

Example: A fraud detection system spots unusual login attempts from different countries within seconds.

Lecture

1

How Cybersecurity Works (Core Mechanisms)

4. Respond & Recover

“Limit damage and bounce back stronger”

-Once detected, incidents require immediate response: isolating affected systems, patching vulnerabilities, and restoring backups.

-Response also includes reputation management — rebuilding customer trust.

Example: After a phishing breach, a digital wallet provider not only resets compromised accounts but also launches a customer reassurance campaign.

Lecture

1

How Cybersecurity Works (Core Mechanisms)

Example of Cybersecurity Lifecycle :

A mobile banking app goes through this cycle:

1. Identifies risks in its API,
2. Protects with encryption + MFA,
3. Detects suspicious login attempts via anomaly detection,
4. Responds by locking accounts and alerting customers.

Lecture

1

Security Domains in Fintech

- **Network Security** → Protect data moving between devices.
- **Application Security** → Build secure apps and prevent bugs.
- **Data Security** → Encrypt and mask sensitive information.
- **Cloud Security** → Shared responsibility between provider and fintech.
- **Compliance** → Following laws and security standards.

In the following, examples of security in cloud and data protection standards/regulations:

Lecture

1

Cloud Security

- Cloud security means keeping data and applications safe when they are stored and run on the internet (instead of only on your computer). Services like AWS, Microsoft Azure, and Google Cloud are examples of cloud platforms.

Because companies often use the cloud for apps and payments, they must protect against:

- Hackers trying to break in,
- Mistakes in cloud settings (misconfigurations),
- Unauthorized access to sensitive customer data.

Example:

A mobile banking app stores customer information on Amazon AWS. The bank uses encryption to keep data private and access controls to make sure only authorized employees can see it.

Cloud Security

Shared Responsibility Model:

- Cloud providers secure the underlying infrastructure (datacenters, networks, hardware).
- Customers are responsible for securing their own data, account settings, user access, and service configurations.
- Many incidents occur when companies mistakenly assume the provider handles everything.

Cloud Misconfiguration Examples

- Misconfiguration happens when cloud services (AWS, Azure, GCP) are set up incorrectly, leaving data exposed.
- Common mistakes include leaving databases publicly accessible or failing to enforce strong authentication.

Example: Capital One breach (2019) where AWS firewall rules allowed unauthorized access to customer data.

Lecture

1

PCI-DSS (Payment Card Industry Data Security Standard)

- PCI-DSS is a global security standard created by major credit card companies (Visa, Mastercard, American Express, Discover, JCB).
- It sets rules and requirements for how organizations must store, process, and transmit credit card data securely.

Why it matters

- Prevents credit card fraud and data breaches.
- Builds trust between businesses and customers.
- Non-compliance can lead to fines or losing the ability to process card payments.

Key requirements

- Encrypt cardholder data — so even if stolen, it's useless.
- Use firewalls and secure systems to block attacks.
- Control access — only authorized people can see sensitive data.
- Monitor networks for suspicious activity.
- Regular testing of security systems.

Lecture

1

GDPR (General Data Protection Regulation)

- A European law that protects people's personal data and privacy.

Why it matters:

- Companies must handle your data responsibly and notify you if it's exposed.

Example:

If a bank suffers a data breach, it must tell customers within 72 hours.

Lecture

1

Emerging Trends & Ethical Issues

AI in Cybersecurity

- Using artificial intelligence (AI) to help computers find and stop cyberattacks.
- AI can scan huge amounts of data and notice patterns that look suspicious (like fraud or hacking).

Example:

A credit card company uses AI to spot unusual spending (e.g., \$5000 spent in a country the customer never visited) and blocks the transaction.

Lecture

1

Emerging Trends & Ethical Issues

Adversarial AI

- Tricks or attacks designed to fool AI systems.
- Hackers change data slightly so that AI makes the wrong decision.

Example:

Criminals slightly change the way they make fraudulent transactions so that the bank's AI fraud detector doesn't recognize them as suspicious.

Lecture

1

Emerging Trends & Ethical Issues

Zero Trust Security

- A security model that means “never trust anyone automatically, always check.”
- Every person, device, or app must prove who they are every time they try to connect.

Example:

Even employees inside a bank must log in with multi-factor authentication each time they access customer data.

Lecture

1

Emerging Trends & Ethical Issues

Quantum-Safe Cryptography

Encryption methods designed to resist attacks from quantum computers. Normal encryption (like RSA) could be broken by future quantum computers, so new methods are being developed.

Example:

A global bank starts testing quantum-safe algorithms to protect international payment systems.

Lecture

1

Emerging Trends & Ethical Issues

Cyber Resilience

- The ability of a company to keep working even during or after a cyberattack.
- Focuses on preparation, backup systems, and recovery plans.

Example:

If a fintech payment app is hit by ransomware, it switches to backup servers and continues serving customers while recovering.

Lecture

1

Emerging Trends & Ethical Issues

Ethical Hacking

Authorized hacking by security experts (often called “white hats”) to find weaknesses. They attack the system in a safe way to help fix problems before real criminals exploit them.

Example:

A digital wallet company hires ethical hackers to test its mobile app and patch security flaws.

Lecture

1

Emerging Trends & Ethical Issues

Privacy vs Transparency

- The balance between protecting personal data (privacy) and giving regulators enough access to prevent fraud (transparency).
- Too much privacy can hide crime, but too much transparency can hurt customer trust.

Example:

Banks must share suspicious transaction data with regulators (AML rules) but still protect customers' personal details under GDPR.

Lecture

1

Emerging Trends & Ethical Issues

Privacy vs Transparency

- The balance between protecting personal data (privacy) and giving regulators enough access to prevent fraud (transparency).
- Too much privacy can hide crime, but too much transparency can hurt customer trust.

Example:

Banks must share suspicious transaction data with regulators (AML rules) but still protect customers' personal details under GDPR.

Lecture

1

Emerging Trends & Ethical Issues

Privacy vs Transparency

- Regulator: is an official authority or government body that makes and enforces rules in a specific industry.

In cybersecurity/fintech: Regulators create rules to make sure banks, fintech companies, and payment providers protect customer data and prevent fraud.

- AML = Anti-Money Laundering – laws and practices that stop criminals from hiding illegal money by passing it through banks or fintech platforms.

Criminals try to “clean” stolen or illegal money by moving it through financial systems to make it look legal. AML rules require companies to check transactions for suspicious activity.

Emerging Trends & Ethical Issues

Privacy vs Transparency

- Regulator: is an official authority or government body that makes and enforces rules in a specific industry.

In cybersecurity/fintech: Regulators create rules to make sure banks, fintech companies, and payment providers protect customer data and prevent fraud.

- AML = Anti-Money Laundering – laws and practices that stop criminals from hiding illegal money by passing it through banks or fintech platforms.

Criminals try to “clean” stolen or illegal money by moving it through financial systems to make it look legal. AML rules require companies to check transactions for suspicious activity.

Lecture

1

Applying what we learned

Simulation: Bank Fraud Case

Scenario: You are a bank employee in the cybersecurity team notices unusual activity:

- A customer usually makes small daily transactions.
- Suddenly, there's a transfer request of \$50,000 to an overseas account at 2 AM.

Task: Is this fraud or legitimate? What steps would you take?

Lecture

1

Simulation: Bank Fraud Case (Solution)

Answer:

This is most likely fraud due to the unusual pattern.

Steps to take:

- Compare with past customer behavior.
- Temporarily flag or hold the transaction.
- Contact the customer for verification.
- Document the incident and escalate if needed.
- Strengthen monitoring on the account.

So, the most likely case is that this is a fraud attempt, because the sudden and significant change in financial behavior is a strong risk indicator. However, we cannot make a final judgment until we verify with the customer.

Lecture

1

Recap

In this lecture, we learned:

- Cybersecurity protects individuals and organizations from financial loss, reputational damage, and repeat attacks.
- The **CIA triad** (Confidentiality, Integrity, Availability) forms the foundation of secure systems.
- Major **cyber threats** include phishing, malware, ransomware, botnets, DDoS, insider threats.
- Protection requires both **individual measures** and **organizational measures**.
- **Regulators** enforce compliance frameworks like PCI-DSS, GDPR to secure the fintech sector.
- Core technologies such as **cryptography, cloud security, and digital forensics** safeguard data and enable investigations.
- New challenges are emerging: such as **AI (defensive and adversarial), zero trust, and quantum-safe cryptography**.

References

- Stallings, W. (2014). Foundations of Security: Principles and Practice. Pearson.
- Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.
- Gupta, R. (2022). Cybersecurity Tools. CRC Press.
- Britz, M. T. (2013). Computer Forensics and Cyber Crime: An Introduction. Pearson.
- PCI Security Standards Council (2022). Payment Card Industry Data Security Standard (PCI DSS) v4.0.
- European Commission (2018). General Data Protection Regulation (GDPR).
- NIST (2023). Cybersecurity Framework 2.0.