Database Security and Forensics

Chapter 1: Information Security and Technologies

Mr Laïdi FOUGHALI

l.foughali@univ-skikda.dz

(Site ⇒ al-moualime.com)

University of Skikda — Computer Science Department

1st Year Master in Information Security (IS)

Academic Year 2025-2026

Version v1.0 — 2026-02-10 à 08:36:38

Outline

1. Introduction
2. Threats
3. Malware
4. Defense
5. Conclusion

Overview

Chapter Objective

Master database security through three complementary axes

Axis 1: CIA Pillars

- **Confidentiality**: access reserved to authorized entities (encryption, authentication)
- **Integrity**: accurate and consistent data, controlled modifications
- **Availability**: reliable 24/7 access, fault tolerance

Axis 2: Threats

- **External attacks**: pirates, hackers, cyberterrorism
- **Internal attacks**: 50%
- **Malware**: viruses, ransomware, Trojans
- **Social engineering**: 90% (phishing)

Axis 3: Protection Solutions

- **Multi-layer defense**: network (firewall, IDS/IPS Intrusion Detection/Prevention Systems) + OS Operating System (patches, antivirus) + DBMS Database Management System (access controls, audit)
- **4-step cycle**: *Prevention* → *Detection* → *Response* → *Recovery*
- **Continuous improvement**: 24/7 vigilance and adaptation to new threats

GDPR — General Data Protection Regulation

Definition

GDPR is a European regulation in force since May 2018 that mandates the protection of personal data of European citizens.

The five fundamental rights

1. **Explicit consent**: clear agreement before any data collection
2. **Right to be forgotten**: deletion upon request
3. **Portability**: data retrieval (CSV Comma-Separated Values, JSON JavaScript Object Notation)
4. **Transparency**: explanation of data usage
5. **Notification**: 72h maximum to report a breach

Protected data

Name, email, IP Internet Protocol address, cookies, GPS Geolocation, SSN Social Security Number

Penalties

20M€ or **4% global revenue**
Ex: Google 50M€ (2019)

HIPAA — Health Insurance Portability and Accountability Act

Definition

HIPAA (1996) requires healthcare entities to protect **PHI** Protected Health Information, any identifiable medical information about a patient.

The five requirements

1. **Confidentiality**: limited access to authorized personnel
2. **Integrity**: no modification without trace
3. **Availability**: guaranteed emergency access
4. **Audit trail**: complete traceability of access
5. **Encryption**: encrypted data (transit and storage)

PHI

Medical records, lab results, prescriptions

Penalties

Civil: **1.5M$/year**
Criminal: **250k$** + **10 years** prison

The IT security paradox

Undeniable progress

Cybersecurity investments have tripled. Training is mandatory in universities. Standards (GDPR, ISO International Organization for Standardization 27001) are widely adopted.

Yet: DB security remains neglected

- Critical shortage: 10 job openings for 1 available expert (2024)
- 80% of sensitive data concentrated in DBs Databases (IBM 2024)
- DBs are hackers' first target (Verizon 2024)

Explanation of the paradox

We invest in perimeter security (firewall, antivirus) but neglect the vault itself. Yet databases contain the real treasures: credit cards, medical records, industrial secrets.

Key cybersecurity figures

Alarming findings (Verizon 2024)

- **55%** of breaches = INTERNAL threat (employees)
- **4.45 M$** (≈ 4.1 M€) = average cost per breach (IBM 2024)
- **277 days** = average detection time (9 months)
- **90%** of attacks = phishing
- **95%** of incidents = human error

Impact on the company

- GDPR fines: up to 20M€ or 4% global revenue
- Customer loss: -30% on average
- Class action lawsuits possible

Key takeaway

9 months detection = time to copy millions of files undisturbed.

The four pillars of a secure environment

The security cycle

1. **PREVENTION**: block attacks with firewall, strong passwords, encryption
2. **DETECTION**: spot intrusions via alerts and activity logs
3. **RESPONSE**: limit damage by isolating DB and blocking hacker access
4. **RECOVERY**: restore via backups and reconstruction

Fundamental principle

Security is not a product you buy once, it's a CONTINUOUS PROCESS

Practical applications

PREVENTION: Multi-factor authentication, firewalls, security training
DETECTION: Real-time monitoring systems, intrusion alerts
RESPONSE: Incident procedures, isolation systems
RECOVERY: Regular backups, disaster recovery plans (DRP Disaster Recovery Plan)

The CIA Triad — The three fundamental pillars

Understanding the CIA Triad

The CIA Triad is the reference model in information security. Every security decision must consider these three pillars simultaneously.

The three pillars

C = CONFIDENTIALITY: Only authorized people can access data

- Technical means: Encryption, authentication, access control
- Organizational: Strict security policies, training

I = INTEGRITY: Data is accurate, complete, and unaltered

- Technical means: Digital signatures, checksums, hashing
- Organizational: Change validation procedures

A = AVAILABILITY: Data accessible when needed (24/7)

- Technical means: Redundancy, backups, replication
- Organizational: Disaster recovery plan (DRP)

Practical CIA Example — Medical Database

Scenario: Hospital patient database

CONFIDENTIALITY:

- Only doctors treating the patient can see the file
- Medical data encrypted (AES-256 Advanced Encryption Standard)
- Strong authentication required (username + password + fingerprint)

INTEGRITY:

- Each modification logged with: who/when/what
- Impossible to delete medical history (immutable)
- Automatic checksums detect corrupted data

AVAILABILITY:

- Database must be accessible 24/7 (emergency room)
- Automatic replication on backup servers
- If main server fails → automatic switch to backup

Concrete impact

CIA violation in a hospital = lives at risk

Confidentiality — Only the right people access

Definition

Confidentiality ensures that data is accessible ONLY to authorized.

Five confidentiality techniques

1. **Access Control**: Define who can access what
   - RBAC Role-Based Access Control: Access by role (doctor, nurse, admin)
   - DAC Discretionary Access Control: Owner decides who accesses
   - MAC Mandatory Access Control: System enforces rules
2. **Encryption**: Make data unreadable without key
   - Symmetric: AES (same key to encrypt/decrypt)
   - Asymmetric: RSA (public/private key pair)
3. **Authentication**: Verify identity
   - Something you know (password)
   - Something you have (badge, token)
   - Something you are (fingerprint, face)

Confidentiality — Techniques (continued)

Five confidentiality techniques (continued)

4. **Data Masking**: Hide sensitive data
   - Production: 5500 1234 5678 9012 (full number)
   - Development: 5500 **** **** 9012 (masked number)
5. **Network Segmentation**: Isolate sensitive systems
   - Separate network for financial DB
   - Firewall blocks unauthorized access

Common violation examples

- Password on sticky note on screen
- Unencrypted database backup on USB stick
- Single shared password for all employees
- Confidential document left on printer

Integrity — Accurate and unaltered data

Definition

Integrity ensures that data remains accurate, complete, and protected against unauthorized or accidental modification throughout its lifecycle.

Two types of integrity

1. **Physical integrity**: Protect against material failures
   - RAID Redundant Array of Independent Disks: Disk redundancy (RAID 1, 5, 6, 10)
   - ECC Error-Correcting Code memory: Automatically detects/corrects bit errors
   - Checksums: Detect file corruption
2. **Logical integrity**: Protect against erroneous or malicious modifications
   - DB constraints: NOT NULL, UNIQUE, FOREIGN KEY
   - ACID Atomicity, Consistency, Isolation, Durability transactions: Guarantee data consistency
   - Digital signatures: Prove data hasn't been modified
   - Versioning: Keep modification history

Integrity — Audit and detection

Integrity protection mechanisms

Complete audit trail:

- Log EVERY database modification
- Record: WHO (user) + WHAT (action) + WHEN (date/time) + WHERE (IP)
- Impossible to delete logs (immutable)

Hash functions (checksums):

- Generate unique digital fingerprint of a file
- If file modified → fingerprint changes
- Used for: file verification, passwords, blockchain

Digital signatures:

- Proof that document hasn't been altered
- Uses asymmetric cryptography (public/private keys)
- Used for: contracts, emails, software

Concrete example

Availability — Access 24/7 without interruption

Definition

Availability guarantees that data and systems are accessible when legitimate users need them, without excessive delays or failures.

Measuring availability

Expressed as percentage uptime per year:

- 99% = 3.65 days downtime/year ($\approx$ 87.6 hours)
- 99.9% (three 9s) = 8.76 hours downtime/year
- 99.99% (four 9s) = 52.6 minutes downtime/year
- 99.999% (five 9s) = 5.26 minutes downtime/year
- 99.9999% (six 9s) = 31.5 seconds downtime/year

Example: Amazon requires 99.99% (52 min/year) for AWS

Cost reality

Each additional 9 costs exponentially more. Going from 99.9% to 99.99% can cost 10$\times$ more.

High Availability: Fundamental concepts (1/10)

Definition

High Availability (HA) is the ability of a system to remain operational despite failures, ensuring continuous service.

Key HA principles

1. **Redundancy**: No single point of failure
   - Example: 2 identical servers, if one fails → the other takes over
2. **Failover**: Automatic switch to backup system
   - Automatic detection of main server failure
   - Switch to backup in seconds (transparent to users)
3. **Load Balancing**: Distribute workload
   - Requests distributed across multiple servers
   - If one overloaded → others take over

Typical architecture

Production server + Backup server + Load balancer + Monitoring

High Availability: Key metrics (2/10)

RTO and RPO — The two critical metrics

RTO (Recovery Time Objective):

- Maximum tolerable downtime
- Question: "How long can we be down?"
- Example: RTO = 4 hours → Must restore service in less than 4h

RPO (Recovery Point Objective):

- Maximum tolerable data loss
- Question: "How much data can we lose?"
- Example: RPO = 1 hour → Backups every hour maximum

Practical example

E-commerce: RTO = 15 min, RPO = 0 (no loss) → Needs real-time replication + instant failover
Internal reporting: RTO = 24h, RPO = 12h → Daily backup sufficient

High Availability: Cluster types (3/10)

What is a cluster?

Group of interconnected servers appearing as single system. If one server fails, others take over automatically.

Two cluster types

Active-Passive (cold standby):

- One server works (active), other waits on standby (passive)
- If active fails → passive activates
- Advantage: Simple
- Disadvantage: Passive server unused (wasted resources)

Active-Active (hot standby):

- All servers work simultaneously
- Load distributed between servers
- If one fails → others absorb its load
- Advantage: Better resource usage
- Disadvantage: More complex to configure

High Availability: Failover mechanisms (4/10)

Failover steps

1. **Detection**: Monitor system detects main server failure
2. **Decision**: Determines that switch is necessary
3. **Activation**: Backup server takes over
4. **Redirection**: Traffic redirected to backup server
5. **Notification**: Admins alerted of incident

Typical timings

Detection: 5-30 seconds (heartbeat monitoring)
Switch: 10-60 seconds (depending on complexity)
Total: Generally < 2 minutes for standard failover

Critical point

Failover must be tested regularly! Untested failover = major risk.

High Availability: Redundancy and replication (5/10)

RAID Redundant Array of Independent Disks

- **RAID 1**: Data mirroring
- **RAID 5**: Simple parity, tolerates 1 disk failure
- **RAID 6**: Double parity, tolerates 2 disk failures
- **RAID 10**: Performance and security

Data replication

- **Synchronous**: Real-time update, guaranteed consistency
- **Asynchronous**: Slight delay, better performance
- Architectures: **master-slave** or **multi-master**

High Availability: Power and backups (6/10)

Power supply

- UPS Uninterruptible Power Supply for short outages
- Diesel generators for extended autonomy
- **Dual power feeds**: Two independent power sources (e.g., main grid + backup generator)

Backups

- **Full**: Backup of all data
- **Incremental**: Since last backup
- **Differential**: Since last full backup

3-2-1 rule and testing

3 copies of data, 2 different media, 1 off-site copy and regular testing (at least quarterly)

Understanding RAID reliability: Intuition (7/10)

Basic intuition

Reliability measures the probability that a system works without failure. For a single disk with reliability $R_d = 0{,}95$, this means:

- 95% chance of working correctly for 1 year
- 5% risk of failure

How to combine multiple disks?

RAID 0 (striping): Data spread across 2 disks

- If ONE SINGLE disk fails $\rightarrow$ ALL data is lost
- Risks **multiply**: $R_{\text{RAID0}} = R_d \times R_d = R_d^2$
- Less reliable than a single disk!

RAID 1 (mirroring): Data duplicated on 2 disks

- BOTH disks must fail to lose data
- System survives as long as at least 1 disk works
- Much more reliable than a single disk!

Extreme RAID reliability: Formulas (8/10)

Definition

A system's **reliability** is the probability it functions correctly during a given time interval. For RAID, it depends on:

- disk reliability R_d
- RAID type
- number of disks

Extremes: RAID 0 vs RAID 1

- **RAID 0** (striping, 2 disks): $R_{\text{RAID0}} = R_d^2$
  $\rightarrow$ total loss if one disk fails
- **RAID 1** (mirroring, 2 disks): $R_{\text{RAID1}} = 1 - (1 - R_d)^2$
  $\rightarrow$ tolerates 1 failure

Remarks

RAID 0 $\rightarrow$ maximum performance, minimum reliability
RAID 1 $\rightarrow$ maximum security, doubled cost

Exercise: RAID 0 and RAID 1 reliability (9/10)

Problem statement

We have two identical hard drives, each with annual reliability

$$R_d = 0{,}95.$$

Calculate the system's overall reliability in the following cases:

1. RAID 0 architecture
2. RAID 1 architecture

Formulas used

$$R_{\text{RAID 0}} = R_d^2 \qquad R_{\text{RAID 1}} = 1 - (1 - R_d)^2$$

Educational objective

Highlight the opposition between the two architectures:

- RAID 0: High performance but low fault tolerance
- RAID 1: Redundancy and high reliability

Backup sites (10/10)

Comparison of backup sites

Type	Activation	Data	Usage / Cost
HOT	immediate (min)	real-time sync	critical, no downtime tolerated
WARM	few hours	regular sync	important, small delay acceptable
COLD	48-72 h	not pre-loaded	tolerates 1-3 day unavailability, economical

Choosing site type

Depends on:

- **RTO** Recovery Time Objective: Maximum acceptable delay to restore service
- **RPO** Recovery Point Objective: Maximum acceptable data loss

Balance and trade-offs of the C.I.A. Triangle

Natural tensions between pillars

Confidentiality vs Availability: Strengthening security can slow access.

- MFA Multi-Factor Authentication lengthens login time
- CPU-intensive encryption can delay data processing

Integrity vs Performance: More controls and constraints slow the system.

- Database constraints on INSERT/UPDATE
- ACID transactions add notable overhead

Availability vs Cost: Improving availability requires more resources.

- Redundancy at minimum doubles hardware
- Going from 99.9% to 99.99% availability can cost 10 times more

Finding the right balance

Optimal balance depends on business needs, acceptable risk level, and budget constraints.

Threat overview

Who attacks us and why?

Two main categories of threats target databases:

1. **External threats** (45%): Attackers outside the organization
2. **Internal threats** (55%): Employees, administrators, ex-employees

The security paradox

55% of breaches come from inside
Yet 80% of security budgets are spent against external threats!

The four attack vectors

1. Social engineering (90% of attacks): Deceiving humans
2. Web vulnerabilities: Flaws in websites/applications
3. Malware: Viruses, worms, Trojans, ransomware
4. Deceptive applications: Fake sites impersonating real ones

EXTERNAL threats — Who are they?

The four external attacker profiles

1. **Ethical hackers** (white hats): Legal professionals who find flaws to fix them
   - Pay: 500-2000€/day
   - Work with written authorization
2. **Script Kiddies** (amateur pirates): Teenagers (13-19) using free tools
   - Dangerous by their number: 100× more numerous than pros
   - Don't understand what they're doing
3. **Cybercriminals** (black hats): Motivated by money
   - Ransomware, data theft, extortion
   - 2023 impact: 6000 billion USD
4. **State-sponsored espionage**: Groups backed by governments
   - Unlimited budgets
   - Target state secrets and intellectual property

Mafiaboy case (2000) — When a teen paralyzes the Internet

The Script Kiddie who made history

The attacker: Michael Calce, 15-year-old Canadian
Alias: "Mafiaboy" (his online nickname)
The attack:

- Paralyzes Yahoo, Amazon, CNN, eBay with downloaded free tools
- DDoS (*Distributed Denial of Service*) flooding attack
- Impact: 1.7 billion USD losses in a few hours

The consequences:

- Sentence: 8 months juvenile detention
- Today: Recognized cybersecurity consultant

The lesson to learn

A teenager with simple tools can paralyze
the biggest Internet sites in a few hours

WannaCry case (2017) — The digital pandemic

The malware

Name: WannaCry (from English "Want to Cry")
Type: Worm + Ransomware combined
Flaw: SMB v1 (*Server Message Block version 1*)

The spread

- 230,000 PCs, 150 countries
- In only 4 days
- "EternalBlue" exploit stolen from NSA (*National Security Agency*)
- Automatic (no click needed)

The victims

- NHS (*National Health Service*) UK: Surgeries cancelled
- Renault: Factories stopped
- FedEx, Telefónica
- Ambulances rerouted

The miraculous stop

A researcher accidentally discovers a "kill switch" in the code
Solution: Register a domain name for $10 → Spread stopped!

The lesson

Apply updates on time — Microsoft released the patch 2 months before!

INTERNAL threats — The unknown danger

The scary number

55% of breaches come from INSIDE the organization

Why are they so dangerous?

Employees have three advantages over external hackers:

1. **Legitimate access**: They already have credentials, passwords and permissions. No need to hack to get in.
2. **Internal knowledge**: They know exactly where sensitive data is stored (servers, databases, folders)
3. **Implicit trust**: Security systems are configured to trust them. We monitor strangers, not colleagues.

The four insider threat profiles

44% Negligent: Click on phishing email, password "123456", lost USB key
23% Malicious: Data theft, sabotage, espionage for competitor
20% Compromised admins: Hacker gains admin access via phishing
13% Ex-employees: Employee left 6 months ago still has active account

Capital One (2019) — When negligence costs dearly

The context

Profile: Cloud engineer, negligent (not malicious)
The company: Capital One, major American bank

The fatal error

Misconfigures firewall on Amazon AWS (*Amazon Web Services*) cloud server

- Server meant to be private → accidentally exposed on public Internet
- External hacker (Paige Thompson) discovers the flaw
- She downloads 100 million customer files in hours

The consequences

For the company:

- 80 million $ GDPR fine
- Stock crashes -6% in one day
- **Ongoing** class action lawsuits

For the engineer: Fired, but not criminally prosecuted
For the hacker: 5 years prison (computer intrusion)

Edward Snowden (2013) — The most famous insider

The profile

Name: Edward Snowden
Position: NSA National Security Agency system administrator (authorized access to everything)
Motivation: Reveal mass surveillance programs he deemed illegal

The leak

- Downloads 1.7 million top-secret documents
- Gives documents to journalists (Guardian, Washington Post)
- Revelations: PRISM program (Google, Facebook, Apple surveillance)

The consequences

For Snowden:

- Refugee in Russia since 2013
- Wanted by USA (espionage charges)
- Considered hero by some, traitor by others

For NSA: Total scandal, loss of public trust, reforms forced

What is malware?

Definition

Malware = **Mal**icious soft**ware** (malicious software)
Any program designed to damage, spy, or take control of a computer or network

The scary numbers

600,000 new malware created EVERY DAY
2.3 billion active malware in 2024 (AV-TEST)
92% delivered via email (phishing)

The five main families

1. **Virus**: Attaches to files, needs click to activate
2. **Worm**: Self-propagates via network, no human action needed
3. **Trojan**: Disguised as legitimate software
4. **Ransomware**: Encrypts files + demands ransom payment
5. **Botnet**: Network of zombie computers under hacker control

Virus — Attaches to files

How it works

A virus attaches itself to an existing file (Word document, PDF, .exe)
It activates ONLY when the user opens the infected file
Then it spreads by infecting other files on the system

Characteristics

Propagation: Requires human action (click, open file)
Speed: Relatively slow (depends on user actions)
Damage: Varies (from annoying ads to complete data destruction)
Historical example: Melissa (1999)

- Spreads via Word documents
- Sends itself to first 50 Outlook contacts
- Impact: 80 million $ damage

Why still dangerous?

Users still click on malicious attachments (90% of attacks)

Worm — Self-propagates automatically

How it works

A worm is a self-replicating program that spreads via networks
Does NOT need human action to propagate (100% automatic)
Exploits security flaws in operating systems or applications

Characteristics

Propagation: Automatic via network (no click needed)
Speed: Extremely fast (can infect millions of machines in hours)
Damage: Network saturation, system slowdown, opens backdoors
Historical example: Code Red (2001)

- Exploits Microsoft IIS web server flaw
- 359,000 servers infected in 14 hours
- Launched DDoS attack against White House website
- Cost: 2.6 billion $

Why extremely dangerous?

No human action needed → propagates while you sleep

Trojan — The deception master

How it works

A Trojan disguises itself as legitimate software
User voluntarily downloads and installs it (thinking it's useful)
Once installed, the Trojan opens a secret door for the hacker

Characteristics

Disguise: Fake game, PDF, update, antivirus
Propagation: User must install it themselves
Damage: Spying, data theft, remote control, backdoor installation
Typical example: Fake Flash Player update

- User sees "Update Flash Player to watch video"
- Downloads and installs fake software
- Trojan installs, gives hacker complete access

Why so effective?

Exploits user trust — we voluntarily install our enemy

Ransomware — Digital kidnapping

How it works

1. Infects the system (email, fake site, USB)
2. Encrypts ALL user files (photos, documents, databases)
3. Displays ransom message: "Pay $5000 in Bitcoin to get key"
4. Sets deadline (72h) with increasing amount threat

Alarming statistics

Cost 2023: 20 billion $ globally
Average ransom: 200,000 $ per company
Payment rate: 47% of victims pay (but only 65% get files back)
Detection time: 21 days average → too late

Real example: Colonial Pipeline (2021)

- 45% of USA East Coast fuel supply stopped
- Ransom paid: 4.4 million $
- 6 days complete shutdown → fuel shortage panic

Botnet — Zombie army

How it works

Botnet = BOT NETwork (robot network)
Network of infected computers (zombies) controlled remotely by hacker
Infected computers work normally, but obey hacker's secret commands

Main uses

1. **DDoS attacks**: All zombies attack same site simultaneously
   - 100,000 zombies send requests → server crashes
2. **Spam sending**: 85% of spam comes from botnets
3. **Bitcoin mining**: Uses your electricity/CPU to mine cryptocurrency
4. **Credential theft**: Steals passwords, credit cards

Famous example: Mirai (2016)

- 600,000 infected IoT $_{\text{Internet of Things}}$ devices (cameras, routers)
- DDoS attack: 1.2 Tbps (terabits per second)
- Knocked down Twitter, Netflix, Reddit, CNN for hours

Comparing the five malware families

Comparison table

Type	Propagation	Damage	Example
Virus	User click	Variable	Melissa (1999) - $80M
Worm	Auto network	Network saturation	Code Red (2001) - $2.6B
Trojan	User install	Spying, theft	Fake Flash Player
Ransomware	Various	Encryption + ransom	WannaCry (2017) - $4B
Botnet	Various	DDoS, spam	Mirai (2016) - 600k devices

Key point

90% of infections start with a PHISHING EMAIL
→ Employee awareness = first defense

The security cycle — Continuous process

Fundamental principle

Security is NOT a product you buy once.
It's a **CONTINUOUS PROCESS** that never stops.
Metaphor: Like car maintenance (oil change, service, tires)

The four cycle phases

Phase 1 — ASSESSMENT: Where are our flaws? (audit, pentest)
Phase 2 — DESIGN: How to protect? (architecture, tools)
Phase 3 — DEPLOYMENT: Implementation (installation, training)
Phase 4 — MANAGEMENT: 24/7 monitoring, fixes, updates
$\rightarrow$ Return to Phase 1 after 6-24 months (new threats emerge)

Common mistake

Do 1-2-3 then stop = Rapid obsolescence and undetected flaws

Defense in depth — The three layers (1/2)

Basic principle

Never depend on ONE SINGLE protection.
Layer multiple independent defenses.
Medieval castle analogy: Moat + walls + gates + guards + keep

Layer 1 — NETWORK (perimeter)

- Firewall: Filters incoming/outgoing traffic
- IDS/IPS (*Intrusion Detection/Prevention Systems*): Detects and blocks attacks
- Segmentation: Separate production, development, guests

Layer 2 — SYSTEM (servers, computers)

- Regular security updates (patches)
- Next-generation antivirus
- Disable unnecessary services

Defense in depth — The three layers (2/2)

Layer 3 — DATABASE (the data itself)

- Strict access control (who can see what)
- Encryption of sensitive data
- Complete audit (logging all actions)

Key principle: multi-layer defense

If one layer fails, others continue protecting.
Example: Even if hacker breaks through firewall (layer 1), they must still bypass system protections (layer 2) and database protections (layer 3).

Metaphor

A fortress doesn't rely on a single wall —
each obstacle slows and discourages the attacker.

Defense example — SQL Injection attack

Scenario: Hacker attempts SQL Injection

Layer 1 — Network: WAF (*Web Application Firewall*) detects suspicious pattern → Blocks 70% of basic attempts
Layer 2 — System: Web server validates user inputs → Blocks another 20% of attempts that passed layer 1
Layer 3 — Database: Parameterized queries prevent injection → Treats everything as DATA, never as CODE
Layer 3 bis: Even if injection succeeds, RBAC (*Role-Based Access Control*) limits damage → Web account can ONLY read, not modify or delete
Layer 3 ter: Audit logs EVERYTHING → Alert triggered, forensic analysis possible
Layer 3 quater: Data encrypted → Even if stolen, unreadable without key

Result

Attacker must breach 6 barriers → Very low success probability

Essential chapter messages

The three numbers to remember

55% of breaches = INTERNAL (employees)
90% of attacks = PHISHING (human manipulation)
600,000 new malware created EVERY DAY

The five malware families

Virus: Attaches to files, needs click
Worm: Self-propagates via network
Trojan: Disguised as legitimate software
Ransomware: Encrypts files + demands payment
Botnet: Network of zombie computers under control

The two defense principles

1. **Continuous cycle**: Assessment → Design → Deployment → Management → Repeat
2. **Multi-layer defense**: Network + System + Database

The final message — Humans at the center

The uncomfortable truth

95% of security incidents
involve HUMAN ERROR
at some point in the attack chain

Security is a human process

Technology alone is not enough. We need:

- **Train** all employees regularly
- **Raise awareness** about phishing and password dangers
- **Create a culture** of security in the organization
- **Understand** that everyone is responsible for security

Priority reminder

Databases contain the most precious assets:
Customer data | Industrial secrets | Medical information | Financial data
Their protection must be THE ABSOLUTE PRIORITY