GESTIÓN DE RIESGOS I

Ciclo 2025 - 1
SI904V (ST215V) - Seguridad de Sistemas
Jesús Huapaya Ciriaco, MBA

Content

Title: "Risk Management in Cybersecurity: Know Yourself, Know Your Enemy"

Subtitle: "Asset Identification, Threat Assessment & Risk Ownership"

Sources:

NIST Cybersecurity Framework

ISO 27005 Risk Assessment

YouTube Video: Risk Analysis - Know Your Threat Tolerance

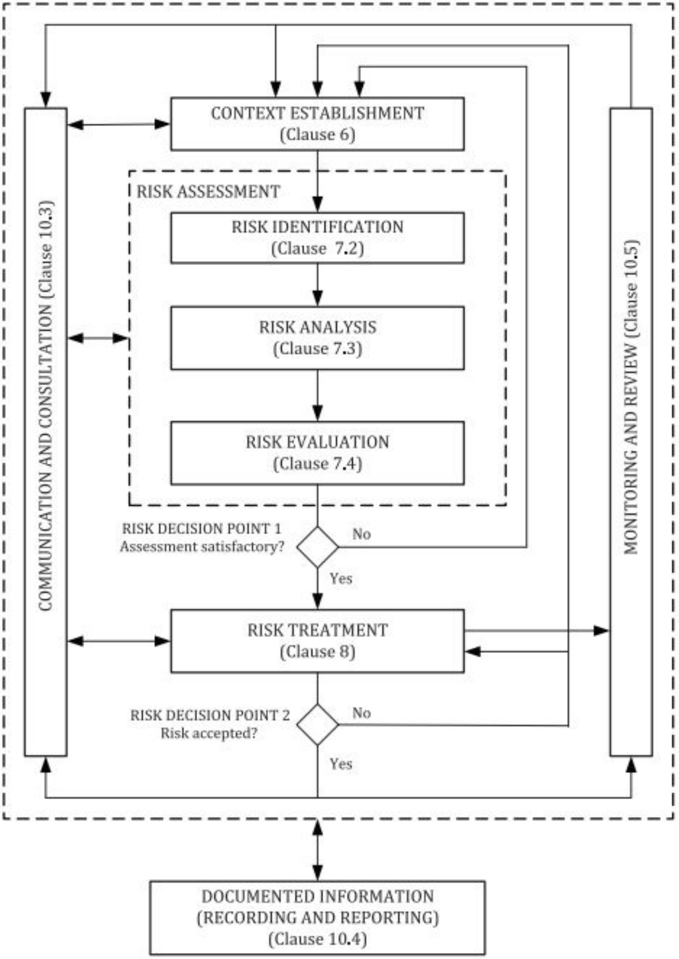


Figure 1 — Information security risk management process

Know Your Organization (Self-Assessment)

Inventory of assets (data, systems, people).

Business criticality analysis.

Sources:

[NISTIR 7693, Specification for Asset Identification 1.1]

[Information Technology Sector (CISA)]

YouTube Video: ITAM - What Is It? Introduction to IT Asset Management

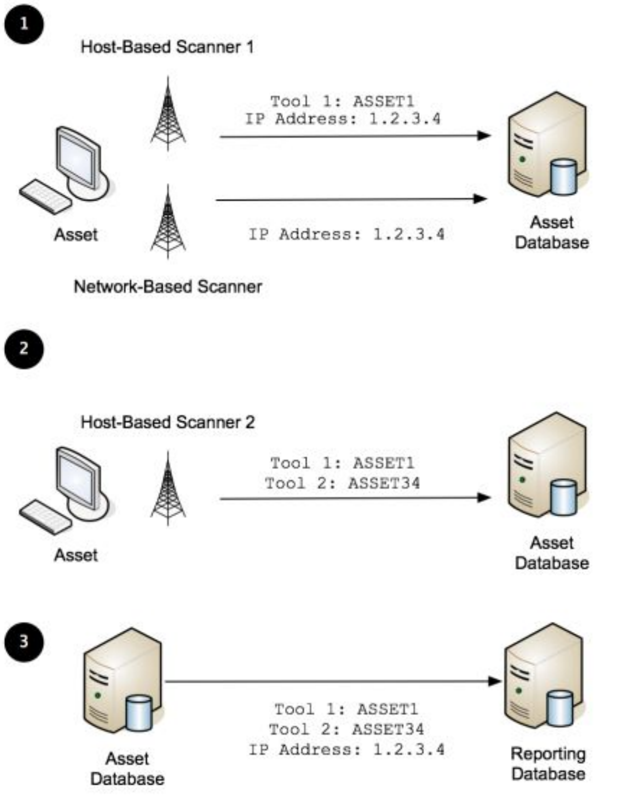


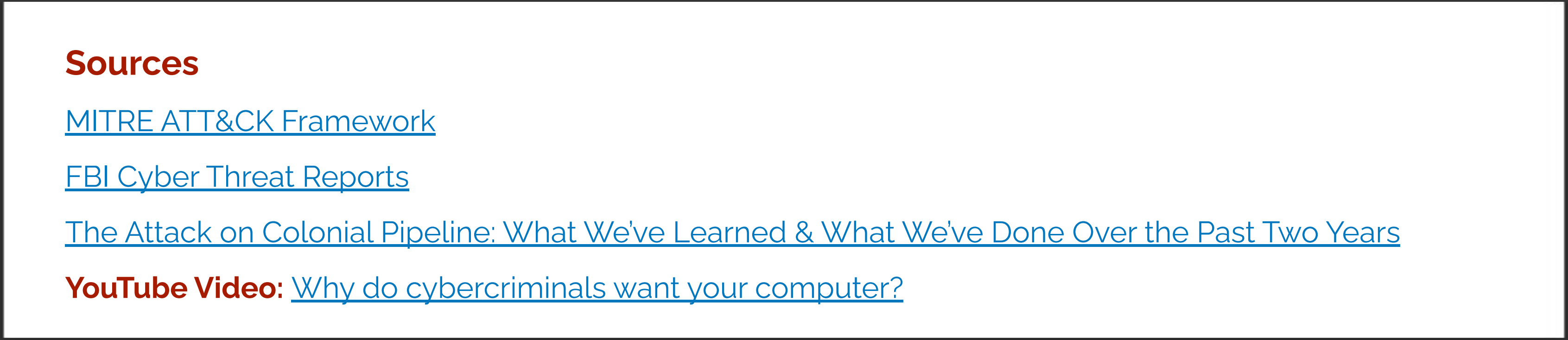
Figure 5-1: Sample Correlation Workflow

Know Your Enemy (Threat Actors)

Types: Hacktivists, nation-states, insiders.

Motivations: Financial, espionage, disruption.

Example: Colonial Pipeline ransomware attack.



Sources

MITRE ATT&CK Framework

FBI Cyber Threat Reports

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years

YouTube Video: Why do cybercriminals want your computer?

Risk Management Responsibility

Shared responsibility model (IT, leadership, employees).

Roles: CISO, risk owners, auditors.

Example: Uber's CSO fired for breach cover-up.

Sources

Cybersecurity is Everyone's Job

Federal Trade Commission Gives Final Approval to Settlement with Uber

The Role of the CISO and the Digital Security Landscape (ISACA)

YouTube Video: IT Security Tutorial - Understanding Cyber Security RISKS

Risk Management Process

1. Identify assets/threats.
2. Assess risks.
3. Mitigate/monitor.

- Example: NIST RMF applied in healthcare.

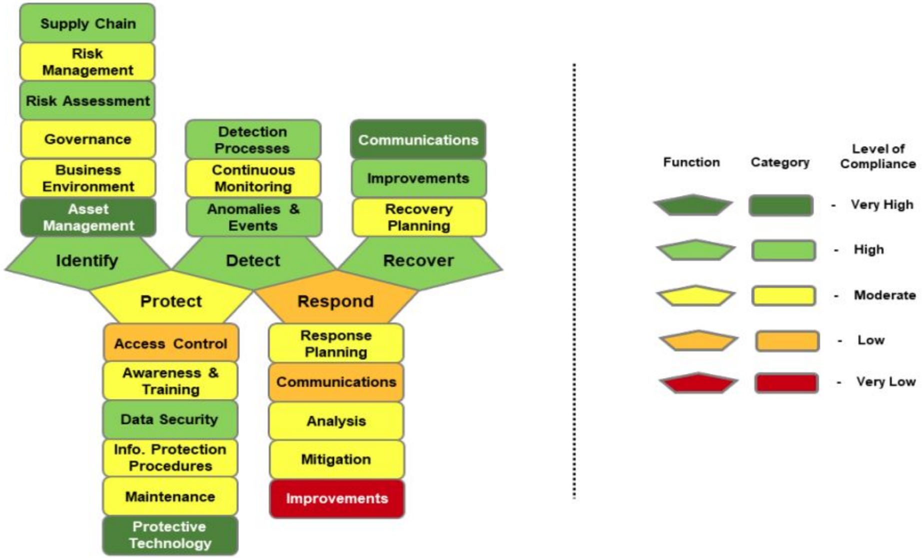
Sources:

[NIST RMF Steps](#)

[Healthcare RMF Case (HHS)](#)

YouTube Video: [Definitive Guide to RMF (Actionable plan for FISMA Compliance)](#)

Figure 5. Example NIST Cybersecurity Framework Scorecard



Threat Identification

Methods: Threat intelligence, pentesting, logs.

Tools: SIEM, vulnerability scanners.

Example: SolarWinds supply chain attack.

Sources:

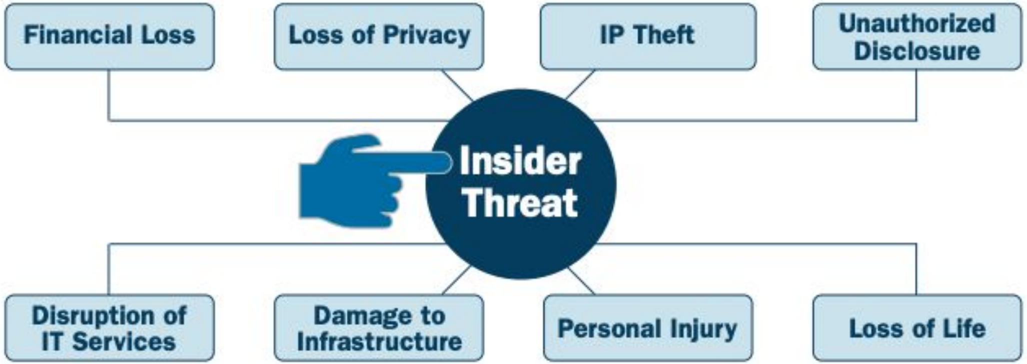
Insider Threat Mitigation Guide (CISA)

OWASP Threat Modeling

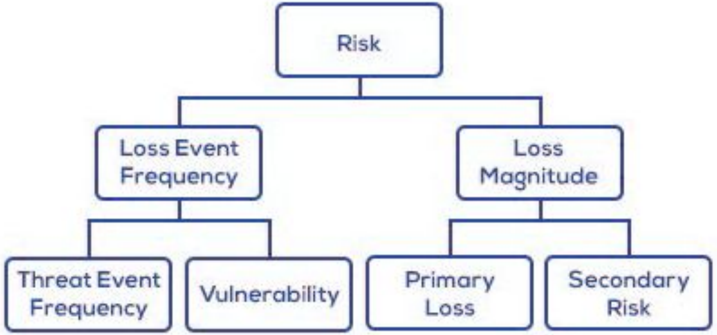
SolarWinds Analysis (Microsoft)

YouTube Video: Cybersecurity Threat Hunting Explained

Figure 3. Potential Consequences of an Insider Incident



Asset Identification & Valuation



Criteria: Financial value, legal impact, reputation.

Methods: Interviews, automated discovery.

Example: Maersk's $300M NotPetya loss.

Sources:
How to Protect Your High Value Assets
Maersk says June cyberattack could cost it up to $300 million
What Is a Cyber Value-at-Risk Model?

YouTube Video: RiskLens Introduction Video

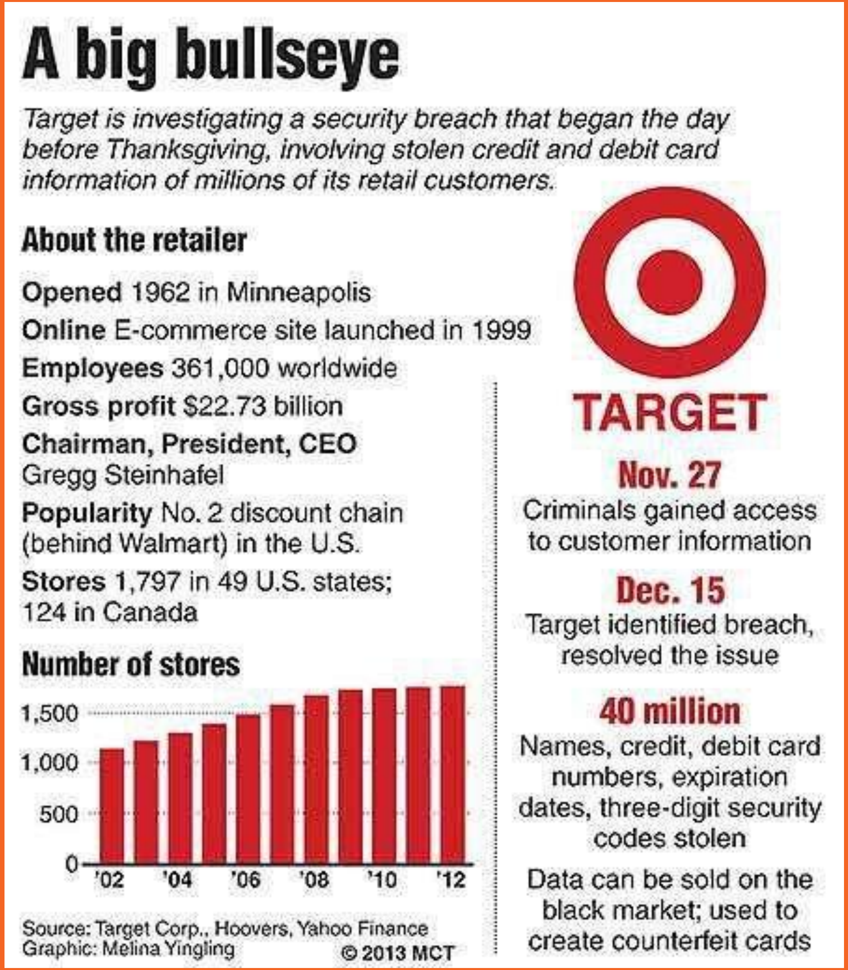
Case Study – Target Data Breach (2013)

Missed risk: Third-party HVAC vendor access.

Impact: 40M credit cards stolen, CEO fired.

Lesson: Include vendors in risk assessments.

Sources:
[Target Hackers Broke in Via HVAC Company](#)
[PCI DSS – 5 Most Commonly Observed Control Failures](#)
[What is Third Party Risk Management (TPRM)? A Comprehensive Guide](#)
YouTube Video: [CBS National News Interviews Keith Squires on Target Breach](#)



A big bullseye

Target is investigating a security breach that began the day before Thanksgiving, involving stolen credit and debit card information of millions of its retail customers.

About the retailer

Opened 1962 in Minneapolis
Online E-commerce site launched in 1999
Employees 361,000 worldwide
Gross profit $22.73 billion
Chairman, President, CEO Gregg Steinhafel
Popularity No. 2 discount chain (behind Walmart) in the U.S.
Stores 1,797 in 49 U.S. states; 124 in Canada

Number of stores

Nov. 27
Criminals gained access to customer information

Dec. 15
Target identified breach, resolved the issue

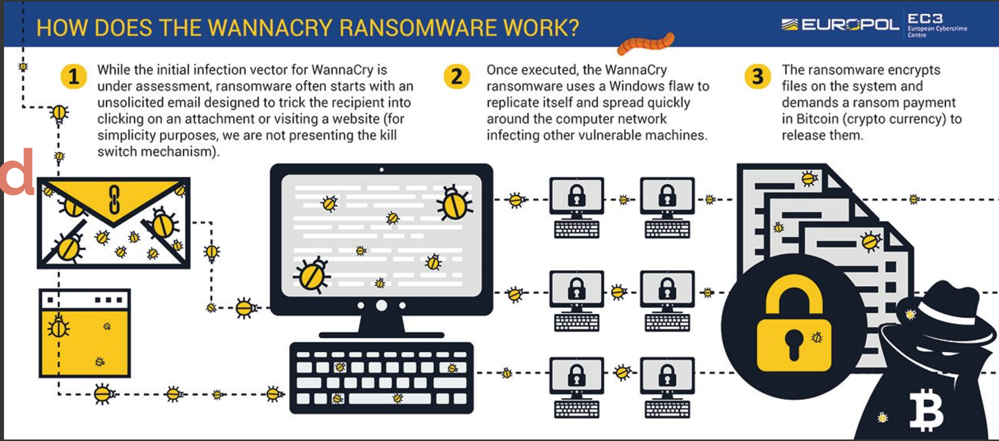
40 million
Names, credit, debit card numbers, expiration dates, three-digit security codes stolen

Data can be sold on the black market; used to create counterfeit cards

Source: Target Corp., Hoovers, Yahoo Finance
Graphic: Melina Yingling
© 2013 MCT

Case Study – WannaCry & Patch Management

Unmitigated risk: Unpatched Windows systems.
Impact: 200K+ systems infected, NHS paralyzed.
Lesson: Prioritize vulnerability management.



HOW DOES THE WANNACRY RANSOMWARE WORK?

1. While the initial infection vector for WannaCry is under assessment, ransomware often starts with an unsolicited email designed to trick the recipient into clicking on an attachment or visiting a website (for simplicity purposes, we are not presenting the kill switch mechanism).
2. Once executed, the WannaCry ransomware uses a Windows flaw to replicate itself and spread quickly around the computer network infecting other vulnerable machines.
3. The ransomware encrypts files on the system and demands a ransom payment in Bitcoin (crypto currency) to release them.

Sources

NHS England business continuity management toolkit case study: WannaCry attack

Ransomware: 'WannaCry' guidance for home users and small businesses

#StopRansomware Guide

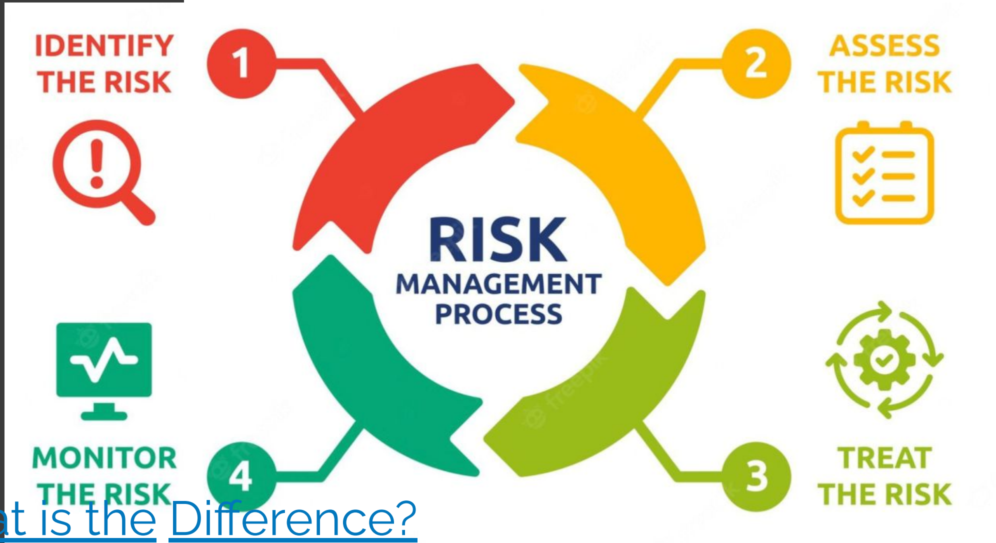
YouTube Video: Cyber Attack: Ransomware causing chaos globally - BBC News

Mitigation Strategies

Avoid, Transfer, Accept, Mitigate.

Example: Cyber insurance (transfer).

Sources:
Managing Information Security Risk
Cyber Insurance Guide (FTC)
Risk Appetite vs. Risk Tolerance: What is the Difference?
Applying Risk Appetite and Risk Tolerance in the Age of AI
YouTube Video: How Would Cyber Insurance Companies Cover Catastrophic Hacks? | WSJ Tech News Briefing



Case Study – Case Study – Zoom Security Risks (2020)

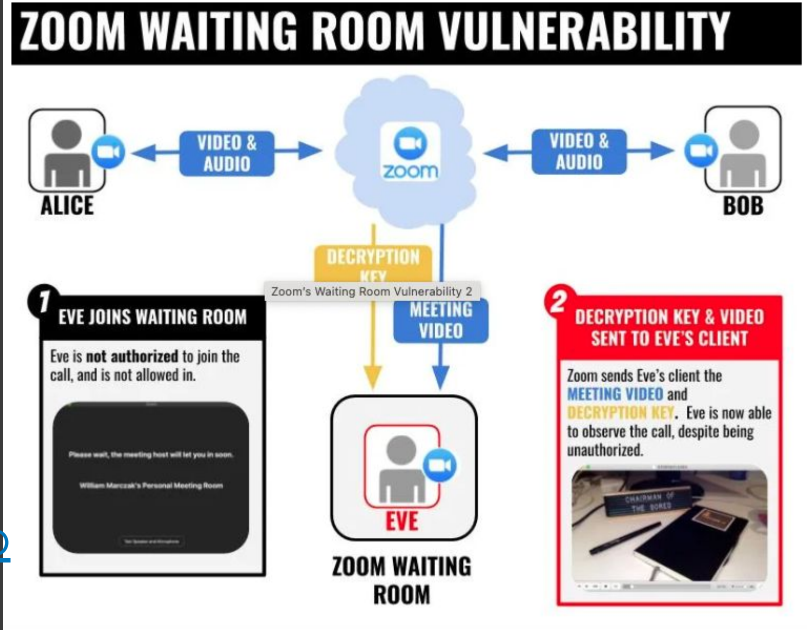
Unforeseen risks: Pandemic-driven scaling exposed vulnerabilities.

Response: 90-day security overhaul.

Lesson: Dynamic risk reassessment.

Sources:
Zoom Privacy Issues: Everything You Need to Know

YouTube Video: Guidance for Securing Video Conferencing


ZOOM WAITING ROOM VULNERABILITY
ALICE
VIDEO & AUDIO
zoom
VIDEO & AUDIO
BOB
DECRYPTION KEY
Zoom's Waiting Room Vulnerability 2
MEETING VIDEO
1
EVE JOINS WAITING ROOM
Please wait, the meeting host will let you in soon.
William Marczak's Personal Meeting Room
EVE
ZOOM WAITING ROOM
2
DECRYPTION KEY & VIDEO SENT TO EVE'S CLIENT
CHAIRMAN OF THE BORED

Eve is **not authorized** to join the call, and is not allowed in.

Zoom sends Eve's client the MEETING VIDEO and DECRYPTION KEY. Eve is now able to observe the call, despite being unauthorized.

Figure 2: EVE uses her Zoom client to attempt to join the meeting of ALICE and BOB. Despite not being authorized by ALICE or BOB, Zoom sends EVE the meeting video and decryption key for the meeting.

Case 1: Cambridge Analytica & Data Privacy Violations (2018)

What happened: Harvested 87M Facebook profiles without consent for political targeting

Legal consequences: $5B FTC fine (largest in Facebook's history)

Ethical issues: Consent, data misuse, and democratic integrity

Sources:

FTC Settlement Document

YouTube Video: What is the Cambridge Analytica scandal?

Case 2: Uber Data Breach Cover-up (2016)

What happened: Paid hackers $100k to hide breach of 57M user records

Legal fallout: $148M settlement across US states

Professional ethics: CSO fired for concealment

Sources:

What can the Uber breach teach us about information security?

YouTube Video: Uber Paid Hackers $100K To Delete Data And Stay Quiet | CNBC

Case 3: Sony Pictures Hack (2014)

What happened: North Korean hackers leaked emails and unreleased films

Legal issues: First cyberattack declared act of terrorism by US

Intellectual property implications: Pirated films cost millions

Sources:

The Sony Pictures Breach: A Deep Dive into a Landmark Cyber Attack

YouTube Video: The Perfect Weapon (2020): Sony Hack (Clip) | HBO

Case 4: Microsoft vs. US Government (2013-2018)

Legal battle: Refusal to hand over emails stored in Irish data center

Outcome: CLOUD Act resolution (clarifying cross-border data access)

Privacy vs. law enforcement debate

Sources:

United States vs Microsoft

YouTube Video: Defending the cloud: Microsoft argues landmark data storage case

Case 5: Google Right to Be Forgotten (2014-Present)

EU ruling: Individuals can request removal of personal search results

Implementation challenges: Over 5 million URLs processed

Balance between privacy and free speech

Sources:

Google wins landmark right to be forgotten case

YouTube Video: Privacy Law and the right to be forgotten: Three Minute Lectures