LA NECESIDAD DE SEGURIDAD DE LA INFORMACIÓN

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

Content

Title: "The Need for Information Security: Business First, Technology Second"

Subtitle: "Quality Tools, Threat Categories, and Attack Descriptions"

Sources:

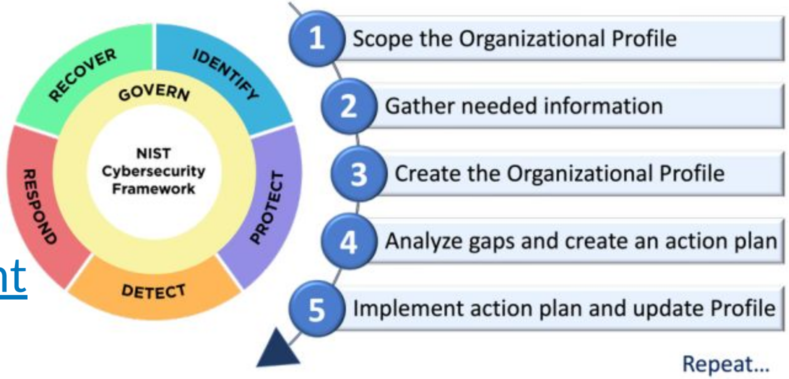

RECOVER
IDENTIFY
GOVERN
NIST Cybersecurity Framework
RESPOND
PROTECT
DETECT
1 Scope the Organizational Profile
2 Gather needed information
3 Create the Organizational Profile
4 Analyze gaps and create an action plan
5 Implement action plan and update Profile
Repeat...

Fig. 3. Steps for creating and using a CSF Organizational Profile

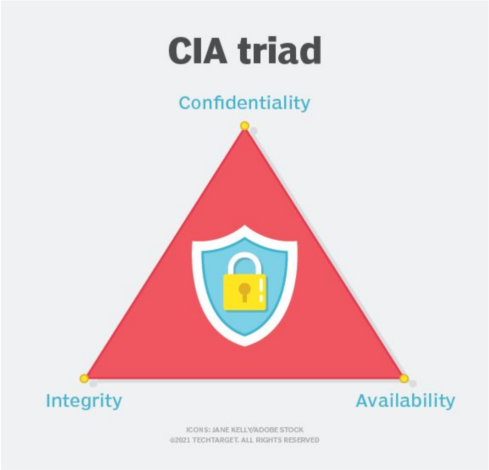
NIST Cybersecurity Framework

ISO 27001: Information Security Management

SANS Institute: Security Awareness

YouTube Video: Data Security : Protect your critical data (or else) - IBM

The Need for Information Security


CIA triad
Confidentiality
Integrity
Availability
ICONS: JANE KELLY/ADOBE STOCK
©2021 TECHTARGET. ALL RIGHTS RESERVED

Why security is critical (data breaches, compliance, reputation).

CIA Triad (Confidentiality, Integrity, Availability).

Aligning security with business goals.

Sources:

[CIA Triad Explained (TechTarget)]

[The Essentiality of Cybersecurity for Small Businesses: Applying Zero Trust Principles]

[Cost of Data Breaches (IBM Ponemon)]

YouTube Video: [Verizon CEO reveals how to keep your data secure as breaches surge - Fox Business]

Quality Tools for Problem-Solving

PDCA (Plan-Do-Check-Act), Fishbone Diagrams, Pareto Charts.

How these tools apply to security incident resolution.

Sources

Is PDCA the Right Tool for Leaders in 2022? - NIST

Root Cause Analysis (ASQ)

Pareto Principle in Security - Continuous Penetration Testing and the Rise of the Offensive SOC (SANS)

YouTube Video: Ishikawa Vs 5 Why I Root Cause Analysis: Understanding the Difference and Relationship

The 7-Step Quality Improvement Method

1. Define the problem
2. Measure current performance
3. Analyze root causes
4. Develop solutions
5. Implement changes
6. Verify results
7. Standardize improvements.

Sources

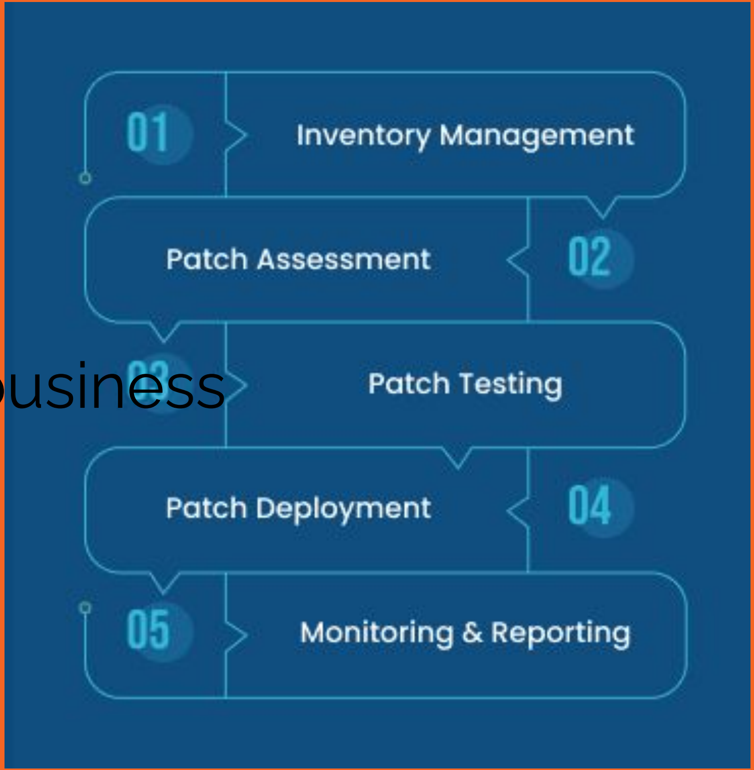
The 7 steps of problem solving

Measurement Guide for Information Security - Identifying and Selecting Measures - NIST

Measurement Guide for Information Security - Developing an Information Security Measurement Program - NIST

YouTube Video: 7 Step Problem Solving

Business Needs Before Technology



- Example: Equifax ignored patch management for business "efficiency."
- How to align security budgets with business risks.

Sources:
[Equifax Case Study (US Senate Report)]
[How do you ensure continuous alignment in your cybersecurity budget? - Gartner]
[How to Demonstrate The ROI of Investing in Cybersecurity]
YouTube Video: [Understanding RSA Business-Driven Security]

Threats – CSI/FBI Survey Highlights

Top threats: Insider attacks, ransomware, cloud vulnerabilities.

Stats from the latest CSI/FBI Computer Crime Report.

Sources:

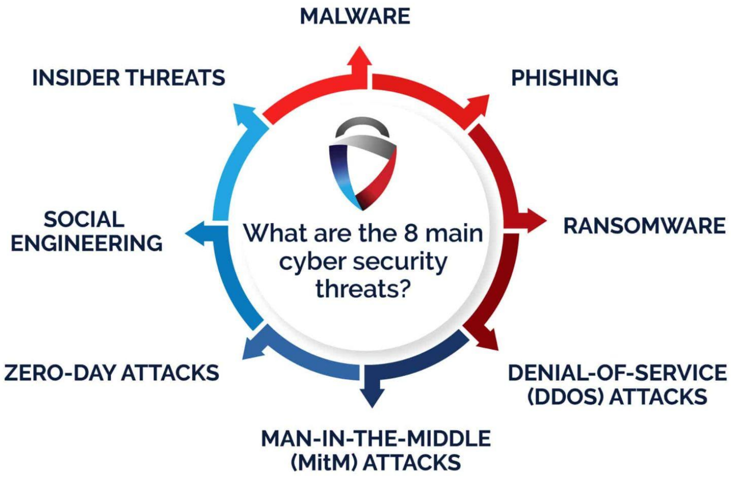
Internet Crime Report 2023 - FBI

Verizon DBIR 2024

#StopRansomware: RansomHub Ransomware (CISA)

YouTube Video: FBI receives 840k+ cybercrime complaints

Top Cyber Security Threats
Malware Attacks
Phishing Scams
Denial-of-Service Attacks
Ransomware Attacks
Insider Threats


MALWARE
PHISHING
RANSOMWARE
DENIAL-OF-SERVICE (DDOS) ATTACKS
MAN-IN-THE-MIDDLE (MitM) ATTACKS
ZERO-DAY ATTACKS
SOCIAL ENGINEERING
INSIDER THREATS
What are the 8 main cyber security threats?

Threat Categories

Human Error (e.g., phishing).

Malicious Actors (hackers, insiders).

System Failures (outages, misconfigurations).

Sources:
[NIST Threat Taxonomy]
[OWASP Top 10]
[ENISA Threat Landscape]
YouTube Video: [10 Most Common Cybersecurity Threats | Types of Cyber Attacks]

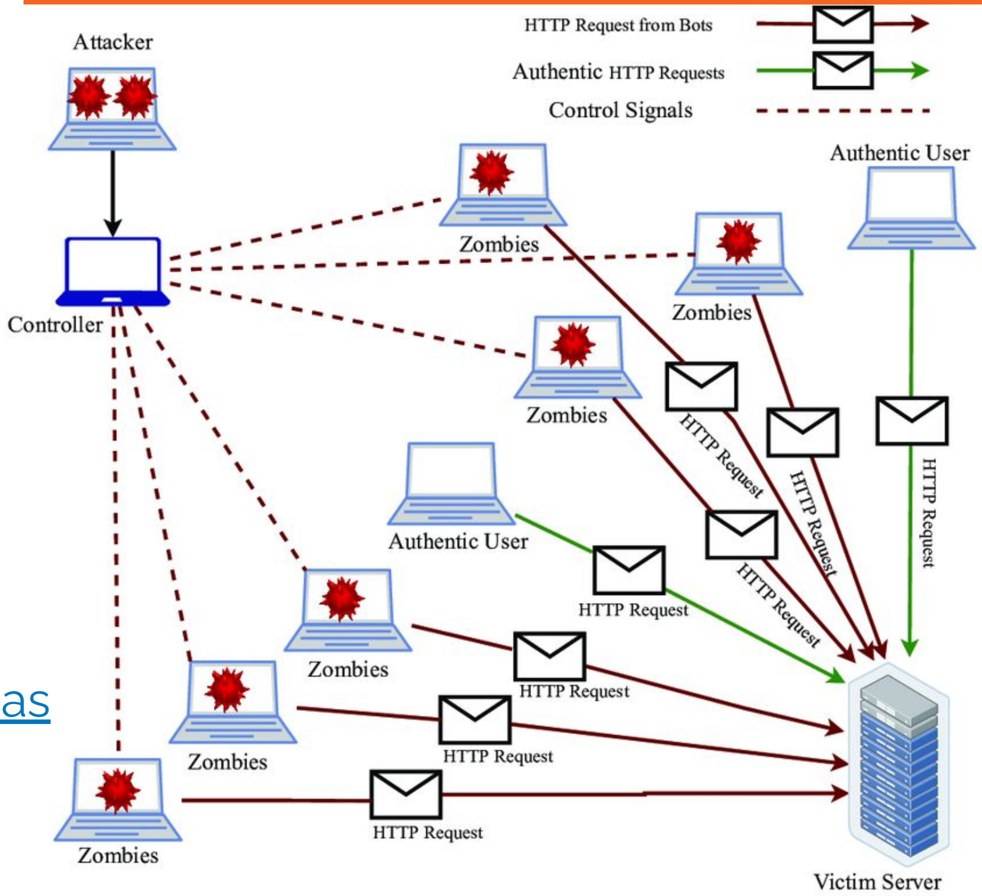
Attacks – Descriptions & Examples

Phishing (e.g., 2020 Twitter Bitcoin scam).

DDoS (e.g., 2016 Dyn attack).

Zero-Day Exploits (e.g., SolarWinds).

Sources:
[Twitter Hack Analysis (Krebs)]
[Ataques DDoS. Recomendaciones y buenas prácticas]
[What is a zero-day exploit?]
YouTube Video: [The SolarWinds Hack Explained | Cybersecurity Advice]



Case Study:
Ransomware in Healthcar

2021 Irish Health Service ransomware attack.

How lack of backups and training led to $600M in damages.

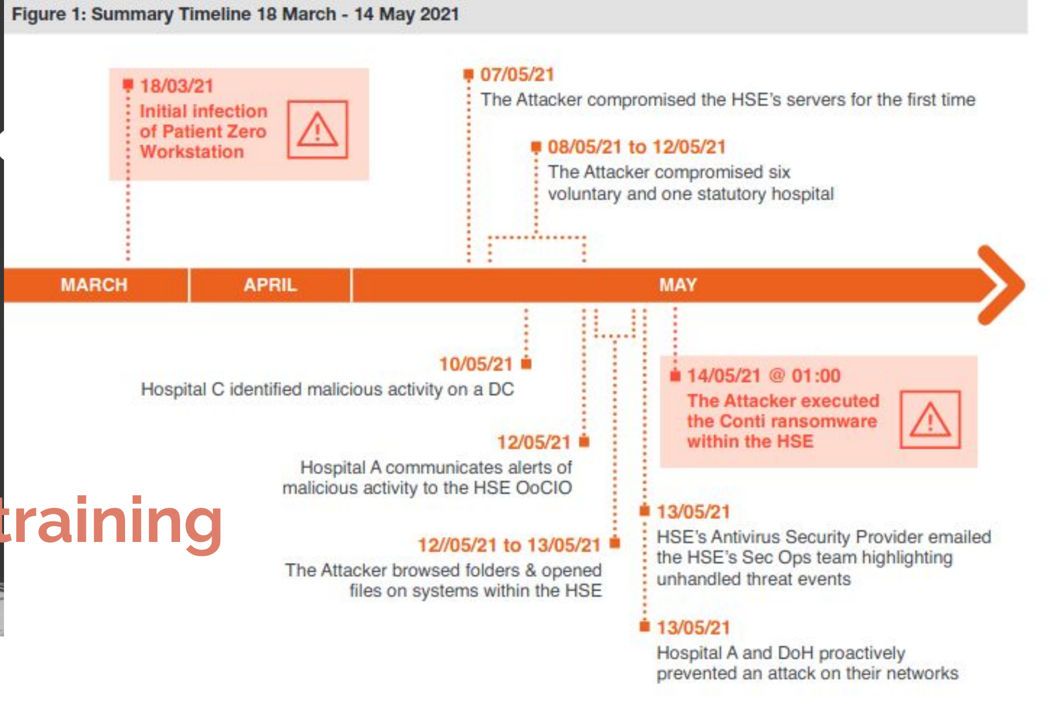


Figure 1: Summary Timeline 18 March - 14 May 2021

MARCH
APRIL
MAY
18/03/21
Initial infection of Patient Zero Workstation
07/05/21
The Attacker compromised the HSE's servers for the first time
08/05/21 to 12/05/21
The Attacker compromised six voluntary and one statutory hospital
10/05/21
Hospital C identified malicious activity on a DC
12/05/21
Hospital A communicates alerts of malicious activity to the HSE OoCIO
12//05/21 to 13/05/21
The Attacker browsed folders & opened files on systems within the HSE
14/05/21 @ 01:00
The Attacker executed the Conti ransomware within the HSE
13/05/21
HSE's Antivirus Security Provider emailed the HSE's Sec Ops team highlighting unhandled threat events
13/05/21
Hospital A and DoH proactively prevented an attack on their networks

Sources

[Conti cyber attack on the HSE]

[14 lessons CISOs learned in 2022]

[Enhancing Cyber Resilience: Insights from the CISA Healthcare and Public Health Sector Risk and Vulnerability Assessment]

YouTube Video: [Explainer: What ransomware is and how it has affected the HSE]

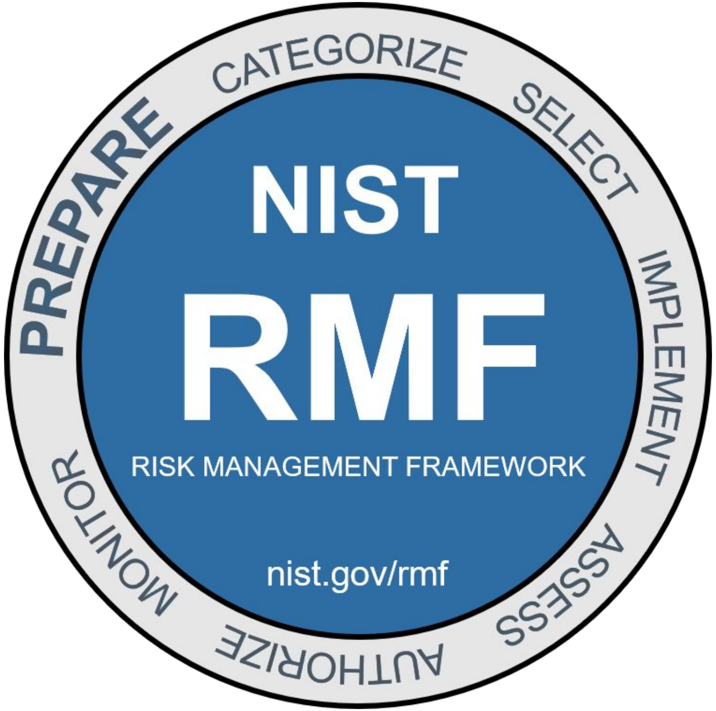
Key Takeaways

Security starts with business needs.

Use quality tools for systematic improvements.

Prioritize threats based on risk.

Sources:
NIST Risk Management
ISO 27005 Risk Assessment
SANS Cybersecurity Leadership Curriculum
YouTube Video: Cybersecurity in the age of AI | Adi Irani | TEDxDESC Youth



Case 1: Equifax Data Breach (2017)

Overview: Hackers exploited a vulnerability in Apache Struts, exposing 147 million records.

Impact: Financial losses, reputational damage, and regulatory fines.

Lessons: Importance of patch management and vulnerability scanning.

Sources:

Equifax Breach Analysis - Krebs on Security

YouTube Video: FTC investigating Equifax breach - CBS News

Case 2: WannaCry Ransomware Attack (2017)

Overview: Ransomware exploited a Windows SMB vulnerability, affecting 200,000+ systems globally.

Impact: Disrupted healthcare systems (e.g., NHS) and caused billions in damages.

Lessons: Importance of regular updates and backups.

Sources:

WannaCry Analysis - Symantec

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

Case 3: SolarWinds Supply Chain Attacl (2020)

Overview: Hackers compromised SolarWinds' Orion software, affecting 18,000+ organizations.

Impact: Espionage on US government agencies and private companies.

Lessons: Importance of securing the software supply chain.

Sources:

SolarWinds Attack - FireEye

YouTube Video: The SolarWinds Hack And The Future Of Cyber Espionage - CNBC

Case 4: Target Data Breach (2013)

Overview: Hackers stole 40 million credit card records via a third-party HVAC vendor.

Impact: $18.5 million settlement and reputational damage.

Lessons: Importance of third-party risk management.

Sources:

Target Breach Report - Krebs on Security

YouTube Video: The Today Show talks about the new report regarding the Target breach

Case 5: NotPetya Cyberattack (2017)

Overview: Malware disguised as ransomware caused widespread destruction, targeting Ukraine initially.

Impact: Global losses exceeding $10 billion, affecting companies like Maersk and Merck.

Lessons: Importance of network segmentation and incident response planning.

Sources:

NotPetya Analysis - Wired

YouTube Video: What lessons can we learn from devastating NotPetya cyberattack?

Case 6: Colonial Pipeline Ransomware Attack (2021)

Overview: DarkSide ransomware group attacked the largest fuel pipeline in the US.

Impact: Fuel shortages, $4.4 million ransom paid, and national security concerns.

Lessons: Importance of critical infrastructure protection and ransomware preparedness.

Sources:

Colonial Pipeline ransomware attack

YouTube Video: Why this security expert calls the Colonial Pipeline attack 'our worst nightmare'