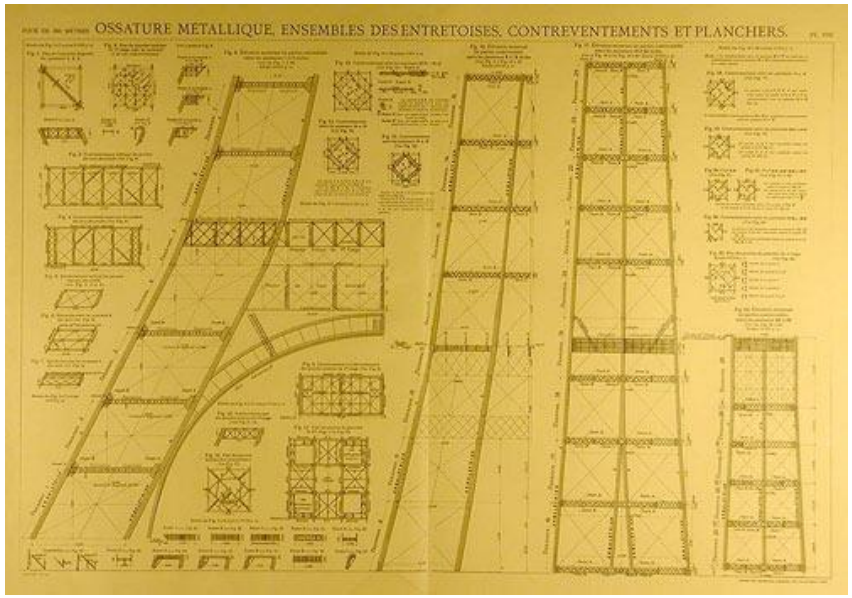
UNIT 1. INTRODUCTION TO SECURITY ENGINEERING

- The framework of security engineering.
- The lifecycle of security
- Principles of design for secure systems
- Threats Vulnerabilities
- Security measures

  (according to its form of action and according to its nature)

Motivation: definition of the problem

How do we go from requirements to secure systems?



General comment about the tower made by the engineers:
A thousand-foot safe tower is technically impossible! *(1889)*

- Security was not an afterthought!

Security are non functional requirements

... because security makes systems not functional?

Security can make the systems more sophisticated, but it can not make them non-functional!

SAFETY

Relative quality that expresses the balance between risk (threat, vulnerability and impact) and the measures that have been taken to avoid it

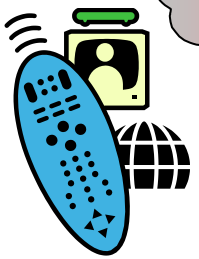
Objectives of security engineering

- Provide engineering solutions for the protection of investments in assets
- Protect assets
- Prevent undesirable events
- Prevent and mitigate undesirable consequences
- Disaster recovery
- Facilitate Operations
- Meet requirements which are mandatory by law

Objectives of security engineering

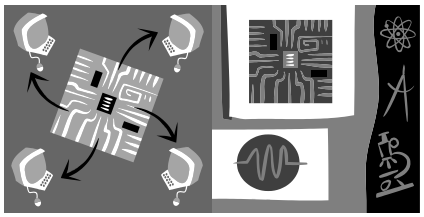
- Security engineering tries to:
  - Establish a balanced set of security needs
  - Transform security needs into security guides
  - Establish confidence in the correctness and effectiveness of security mechanisms
  - Judging the operational impact due to residual security vulnerabilities that are tolerable
  - Integrate all aspects into a combined understanding of the trust of a system

Defense problem



Resources

Emerging technologies



Assets

Threats

Emerging Threats Design
Including Technologies

Weapons,
Guards,
Games
Technologies

...a complex, dynamic problem ...
Where resources shall be assigned?

SECURITY ENGINEERING

Discipline whose aim is the **design, construction and maintenance** of secure systems against mistakes and deliberate and accidental threats, based on **available resources** and following **legal regulations** and **technical standards**

SECURITY ENGINEERING

- Safety is a chain, as secure as its weakest link
- Security is a process not a product

Bruce Schneier. *Secrets and Lies*

SECURITY MANAGEMENT

Planning, organizing and managing the lifecycle of a company security measures

Lo mejor para la seguridad informática: reiniciarlo todo

Por JOHN MARKOFF

MENLO PARK, California — Mucha gente cita el siguiente aforismo de Albert Einstein: "Todo debería hacerse tan simple como se pueda, pero no más simple". Sin embargo, pocos han tenido la oportunidad de debatir ese concepto personalmente con el sabio durante el desayuno.

Uno de ellos es Peter G. Neumann, un informático de 80 años que actualmente trabaja en SRI International, un vanguardista laboratorio de investigación en ingeniería de Menlo Park.

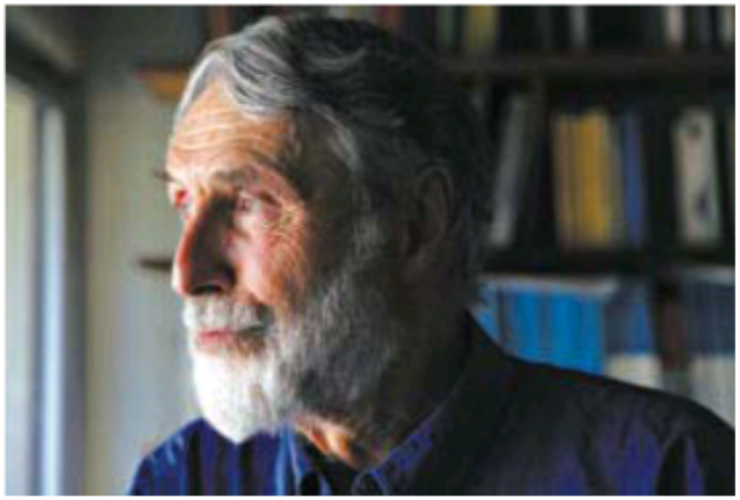
El 8 de noviembre de 1952, cuando era estudiante de matemáticas aplicadas en la Universidad de Harvard, Neumann desayunó durante dos horas con Einstein. Lo que se llevó fue una filosofía muy arraigada del diseño que ha sido su principio rector en materia de ordenadores y seguridad informática.

A lo largo de muchos años, Neumann ha reiterado incesantemente que el mundo de la informática tiende a repetir los errores del pasado. Como destacado especialista en seguridad informática predijo que los fallos que han acompañado a la atropellada explosión de los sectores de los ordenadores e Internet tendrían consecuencias desastrosas. "Su contribución más importante ha sido insistir en que los problemas de seguridad y fiabilidad obedecen a que se trata de sistemas", asegura Steven M. Bellovin, director de tecnología de la Federal Trade Commission. "Es decir, que el problema no se produce por un fallo, sino por cómo interactúan muchas piezas diferentes".

Según Bellovin, fue Neumann quien le hizo ver que las averías de los sistemas complejos son complejas y que la sofisticación cada vez mayor de los equipos y programas modernos ha hecho que sea prácticamente imposible identificar los fallos y las vulnerabilidades de los sistemas informáticos y garantizar su seguridad.

La consecuencia es una epidemia de programas dañinos y una inquietud cada vez mayor ante una ciberguerra que podría constituir una amenaza para la seguridad internacional.

Neumann lidera una iniciativa para replantear por completo la creación de ordenadores y redes seguras en un proyecto financiado por el organismo del Pentágono para los proyectos de investigación avanzada para Defensa, o Darpa, en colaboración con Robert N. Watson, investigador de seguridad informática en el Laboratorio de Informática de la Universidad de Cambridge. "La mayoría de los responsables no quieren ni oír



JIM WILSON/THE NEW YORK TIMES

Peter G. Neumann sostiene desde hace años que la informática solo puede ser segura si vuelve a replantearse desde cero.

hablar de complejidad", se queja Neumann. "Solo les interesan las soluciones rápidas y sucias".

Hoy en día, la seguridad informática es un sector multimillonario, aunque de competencia dudosa. Neumann sostiene que la única solución viable y completa para la crisis de este sector es estudiar la investigación del último medio siglo, elegir las mejores ideas y construir algo nuevo desde cero.

Richard A. Clarke, antiguo zar del antiterrorismo estadounidense, coincide en que la iniciativa Clean Slate de Neumann es esencial. "Sin duda, la remodelación supondría un gasto enorme", señala, "pero empecemos y veamos si funciona mejor, y que entonces decida el mercado".

El programa de Neumann incluye dos iniciativas relacionadas: Crash, por Clean-Slate Design of Resilient Adaptive Secure Hosts, y MRC, por Mission-Oriented Resilient Clouds. La idea es replantearse por completo la informática, desde las placas de silicona a las que van adheridos los circuitos hasta los programas utilizados por los usuarios, así como los servicios que almacenan información privada y personal en centros de datos.

Para combatir la uniformidad de los programas, los diseñadores están adoptando diversos planteamientos que convierten los recursos de los sistemas informáticos en objetos móviles. El proyecto Clean Slate está creando programas que cambian constantemente de forma para esquivar posibles atacantes.

El hecho de que Internet permita que casi cualquier ordenador del mundo conecte directamente con otro posibilita que un atacante que identifique una sola vulnerabilidad ponga en peligro casi de inmediato a gran cantidad de sistemas.

Pero Neumann observa que los organismos biológicos poseen múltiples estructuras inmunes: no solo existen barreras iniciales, sino también un segundo sistema que consiste en centinelas como los linfocitos, que pueden detectar y eliminar a intrusos, y luego recordarles que ofrezcan protección en el futuro.

Uno de los diseños que está aplicando el equipo de Neumann es conocido como arquitectura etiquetada. En la práctica, cada dato del sistema experimental debe incluir un código encriptado en el cual confíe dicho sistema. Si los datos o documentos programáticos no están ordenados, el ordenador no los procesa.

Para Neumann, un motivo de gran frustración es ver que algunos problemas que fueron resueltos hace cuatro décadas siguen asolando el mundo de la informática.

La conversación de Neumann con Einstein supuso el comienzo de un romance de por vida con la belleza y los peligros de la complejidad, algo a lo que apuntaba el físico. "¿Qué opina de Johannes Brahms?", le preguntó, a lo que Einstein repuso: "Creo que Brahms se esforzaba mucho en ser complicado".

http://www.csl.sri.com/users/neumann/

El País, 15 de noviembre de 2012

COMPUTER SYSTEMS. Causes of insecurity

- Complexity
  - Multiple functions
  - Usability
- Interdependence
  - Mobile links
- Unexpected behavior
- Unpredictable mistakes

SAFETY. DRAWBACKS

Δ Safety $\Rightarrow$

Δ Cost

∇ Performance

∇ Usability

ASSET PROTECTION

- *Hardware*
- *Software*
- Data

WHAT IS IT NECESARY TO PROTECT ?: Assets

Data

⇓

Confidentiality

+

Integrity

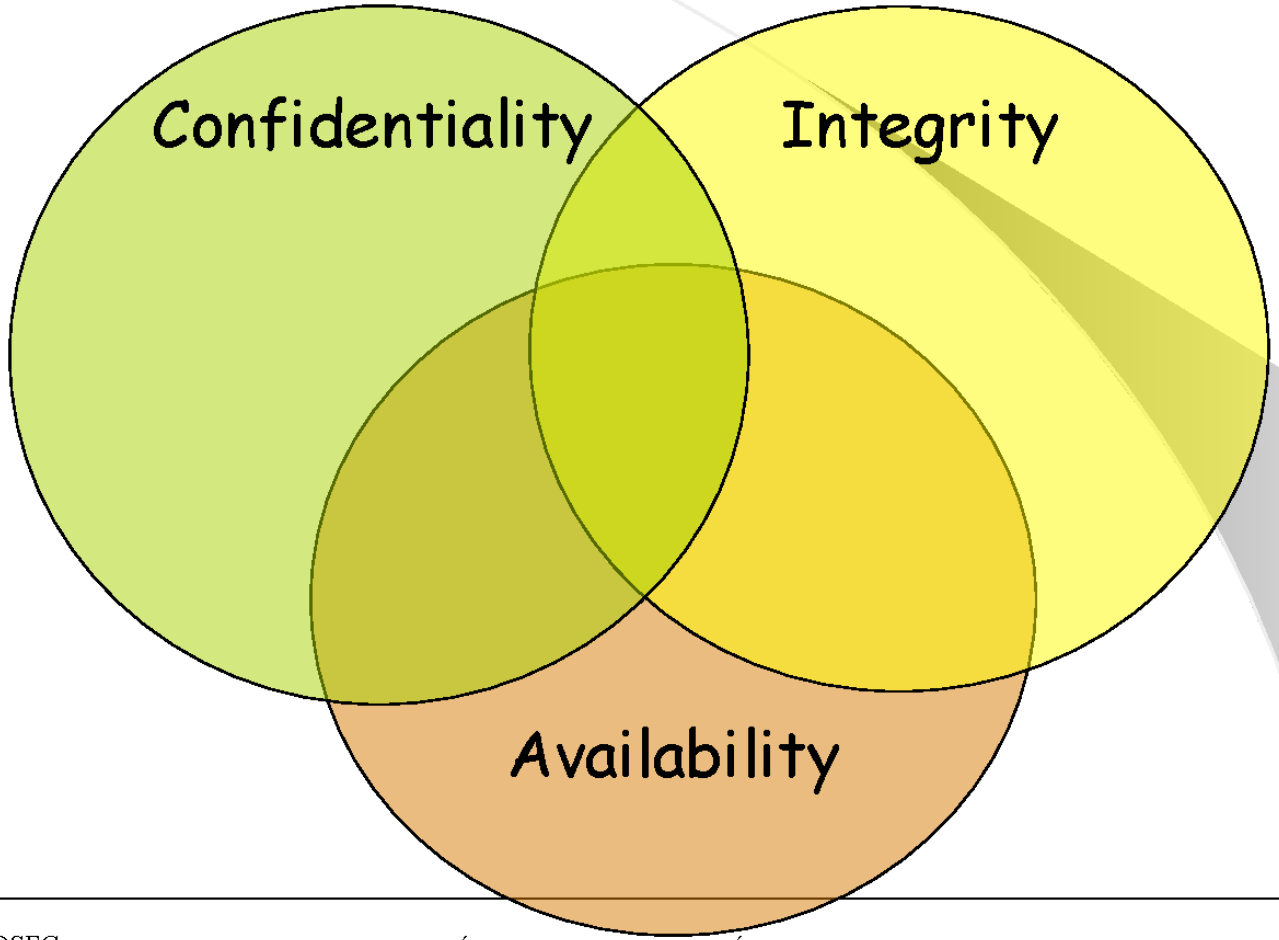
+

Availability

⇓

Safety Goals

SAFETY DIMENSIONS



DATA SECURITY (INFORMATION)

Data protection against accidental or intentional revelations to unauthorized users, against inappropriate modifications or against destruction.

Information Security

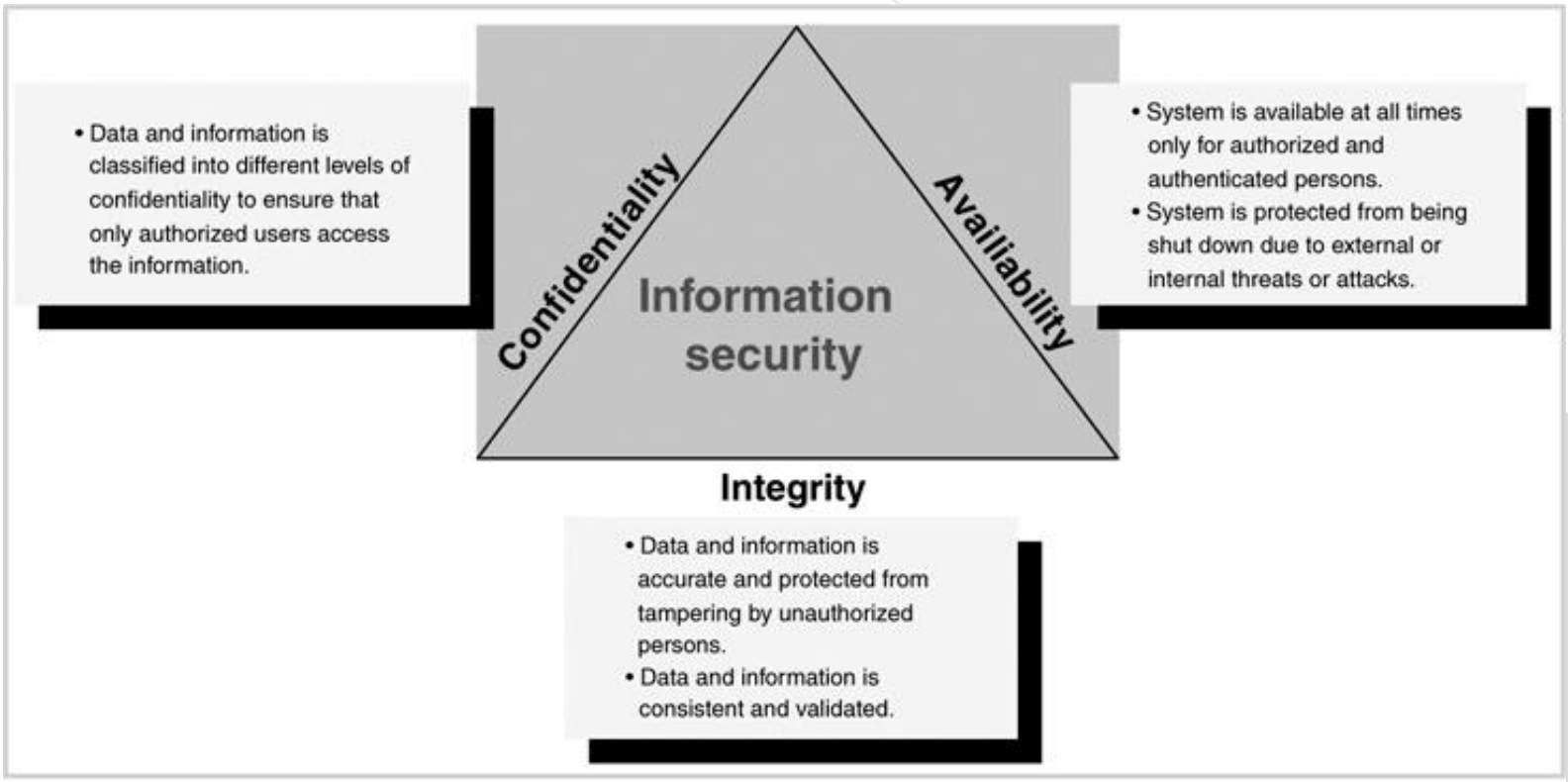


FIGURE 1-5 Information security C.I.A triangle

But….

- What does confidentiality mean?
- What does integrity mean?
- What does availability mean?

Confidentiality

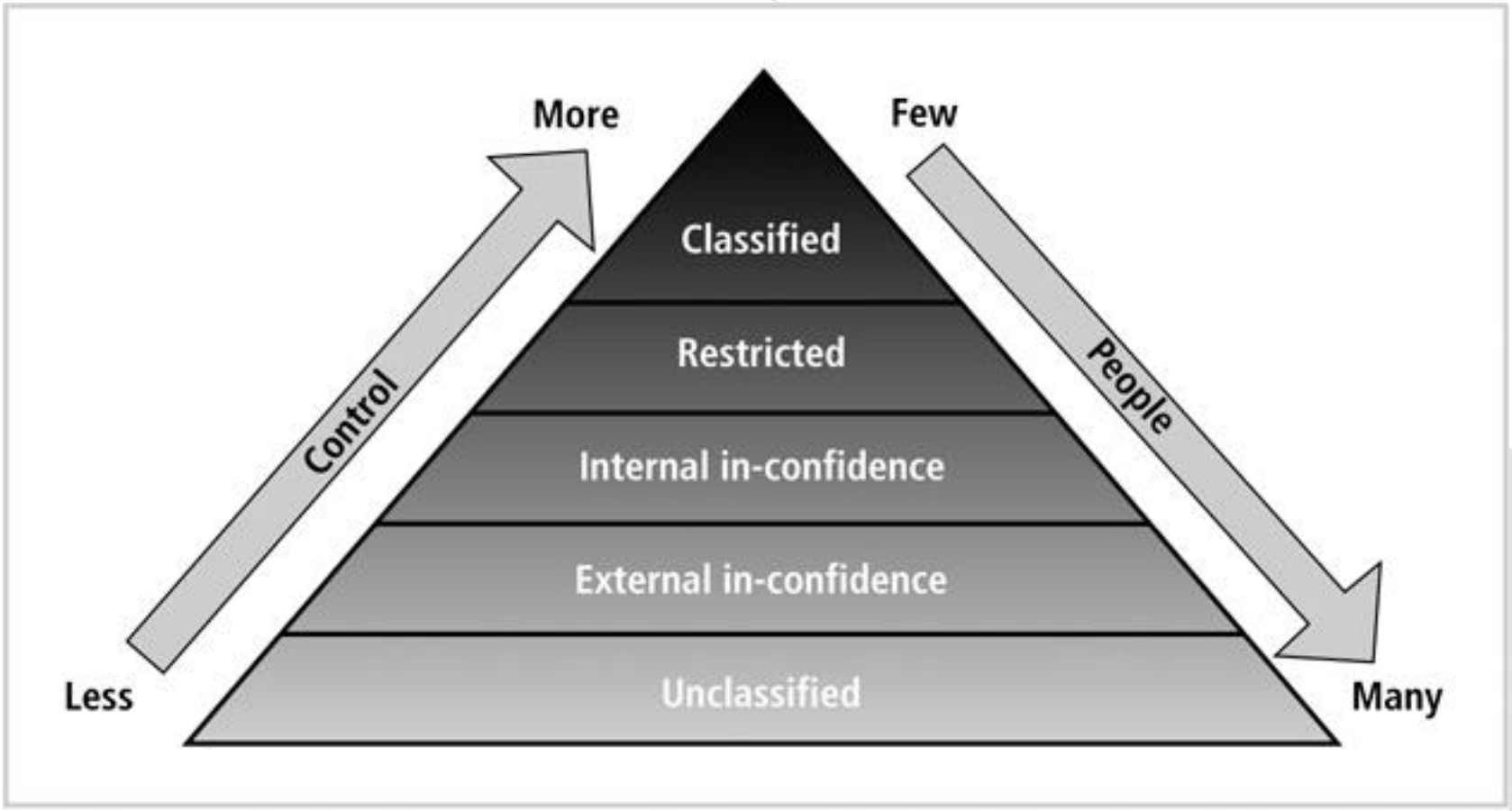


FIGURE 1-6 Confidentiality classification

Integrity

TABLE 1-2 Degradation of data integrity

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Invalid data	Indicates that not all the entered and stored data is valid without exception; checks and validation processes (known as database constraints) that prevent invalid data are missing.	■ User enters invalid data mistakenly or intentionally. ■ Application code does not validate inputted data.
Redundant data	Occurs when the same data is recorded and stored in several places; this can lead to data inconsistency and data anomalies.	■ Faulty data design that does not conform to the data normalization process. (**Normalization** is a database design process used to reduce and prevent data anomalies and inconsistencies.)
Inconsistent data	Occurs when redundant data, which resides in several places, is not identical.	■ Faulty database design that does not conform to the data normalization process.
Data anomalies	Exists when there is redundant data caused by unnormalized data design; in this case, data anomalies occur when one occurrence of the repeated data is changed and the other occurrences are not.	■ Faulty data design that does not conform to the data normalization process.

Integrity

TABLE 1-2 Degradation of data integrity (continued)

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Data read inconsistency	Indicates that a user does not always read the last committed data, and data changes that are made by the user are visible to others before changes are committed.	▪ DBMS does not support or has weak implementation of the read consistency feature.
Data nonconcurrency	Means that multiple users can access and read data at the same time but they lose read consistency.	▪ DBMS does not support or has weak implementation of the read consistency feature.

Availability

- The property that a system or resource is accessible and usable before the demand of another system or authorized entity (according to the performance specifications of the system)
  - Turning off a computer provides confidentiality and integrity but hurts availability ...
  - Denial of service attacks are direct assaults on availability

2015 WORRIES. Plattforms

- Web 2.0: Blogs; social networks, …
- Smartphones (Androids)
- Critical infraestructures (APT)
- BYOD (*Bring your own devices*)
- *Cloud computing*
- Windows XP attacks
- *Internet of Things* (IoT)
- …

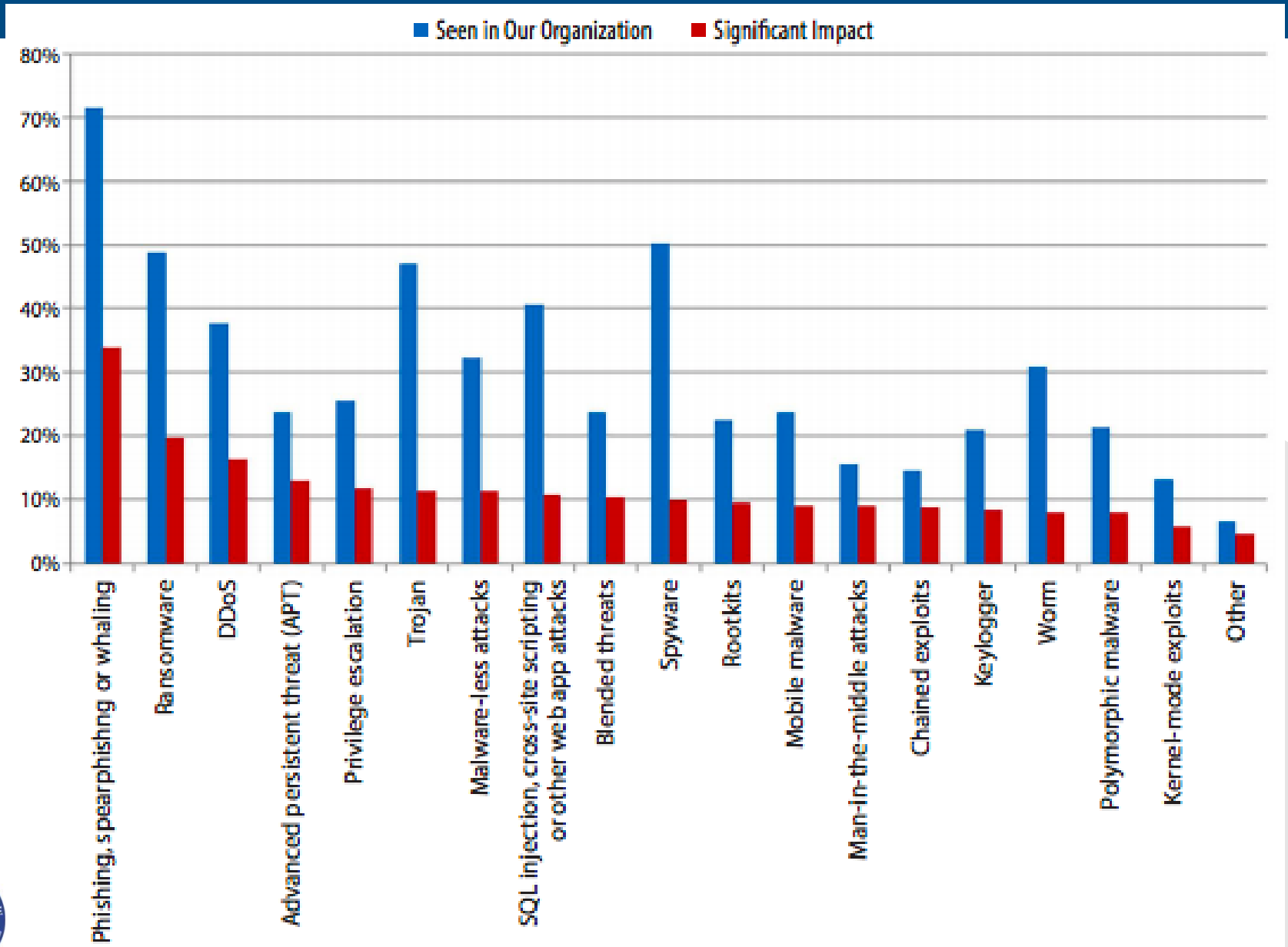
2015 WORRIES. Attacks

- One factor authetication
- *Spear phising*
- *Man in the middle* attacks
- *Botnet*
- Downloads from malicious websites
- *Spam*
- *…*

MAIN ATTACKS 2014

- SSL: Heartbleed/Bash/Poodle
- Intimate photos : Celebgate
- J P Morgan Chase: 76 M familiar data/7 M companies
- CyberVor (Russian mafia): $1{,}2\times10^8$ credentials
- Home Depot: 56×10^6 credit / debit cards
- Sony Picture (North Corea)

ATTACKS 2017



2015 PERSPECTIVES . New defenses

- Big Data
- Unified Security Platforms
- Information sharing
- Cyber Intelligence
- …

PREVIOUS CONCEPTS (Cripto & IT Security)

- Asset
- Threat (Attack)
- Vulnerability
- Risk
- Safety Measures (Services)
  - Mechanisms

2014 PERSPECTIVES

ComputerWeekly.com

Cybercrime costs business £265bn a year, report reveals

Cyber crime costs businesses across the globe an estimated £265bn a year, wiping out up to 20% of all the value created by the internet, a study has revealed.

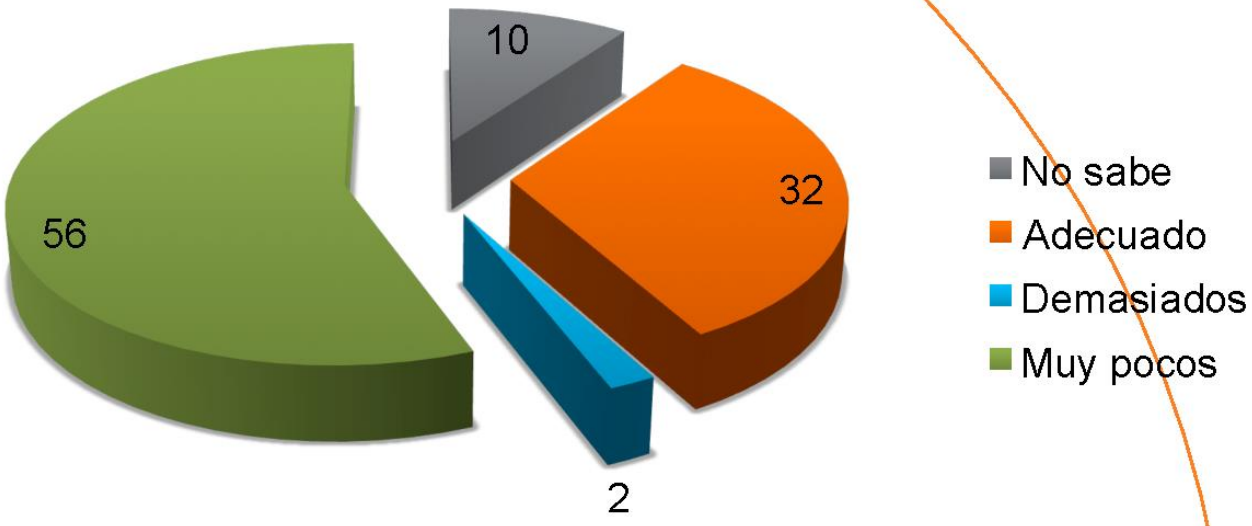
The biggest cost comes from damage to company performance and to national economies, according to a report by the Center for Strategic and International Studies(CSIS) and McAfee, part of Intel Security.

Cyber crime damages trade, competitiveness, innovation and global economic growth, affecting about 150,000 jobs in the European Union.

In the UK, 93% of large corporations and 87% of small businesses reported a cyber breach in the past year, with breaches costing large businesses up to £1.4m and small businesses more than £60,000.

Information Professionals

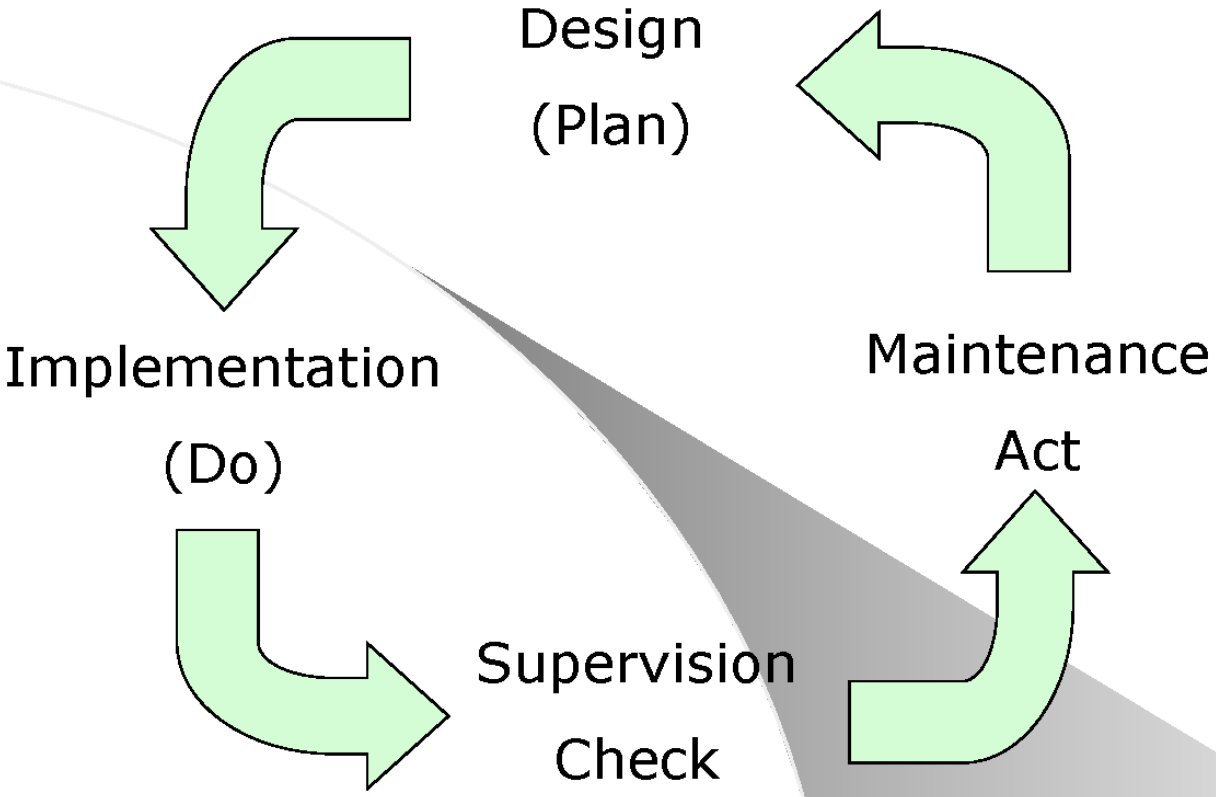
Does your organization have an adequate number of ICT security professionals?



THE LIFE CYCLE OF SECURITY

Set of activities that lead to design, implement, maintain and monitor (review) certain security measures

THE LIFE CYCLE OF SECURITY

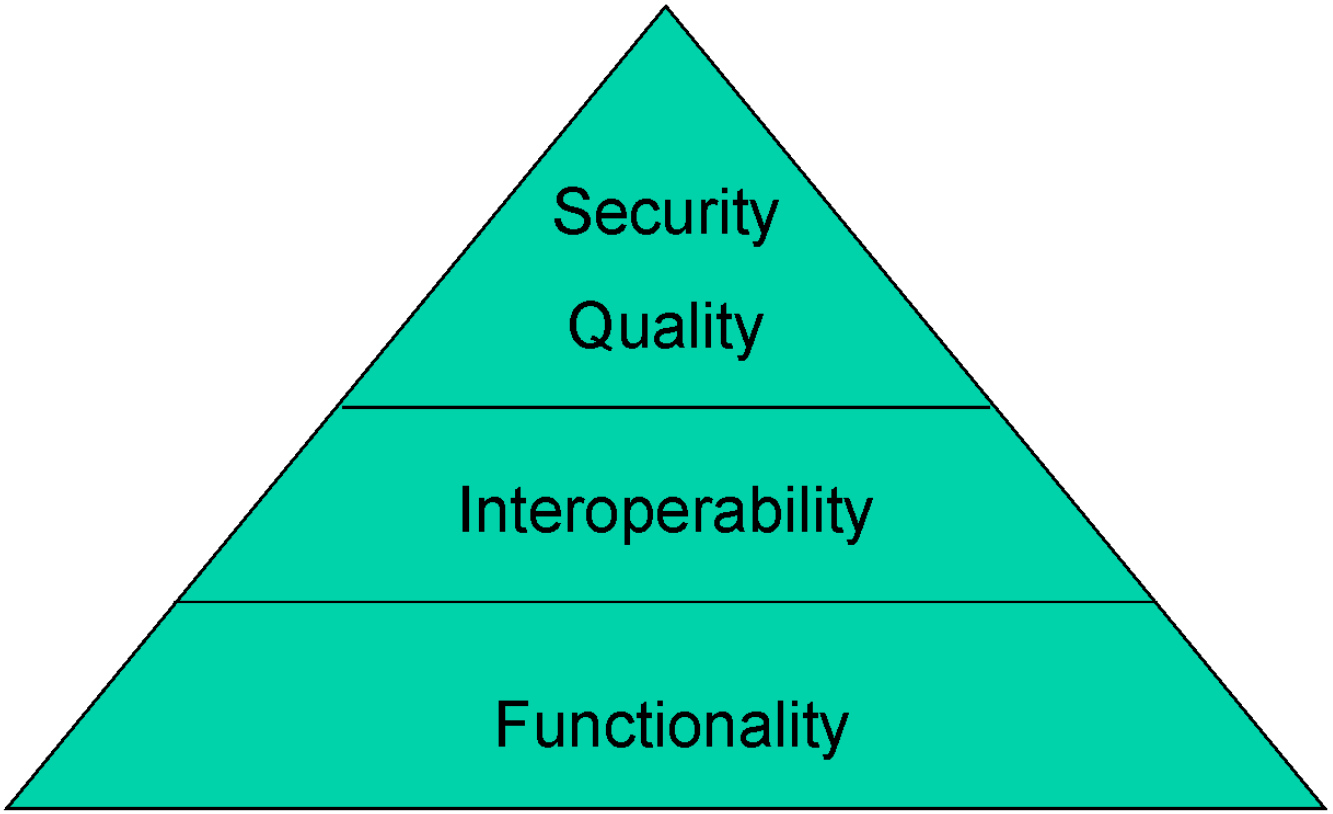


CHAPTER 1. Programme

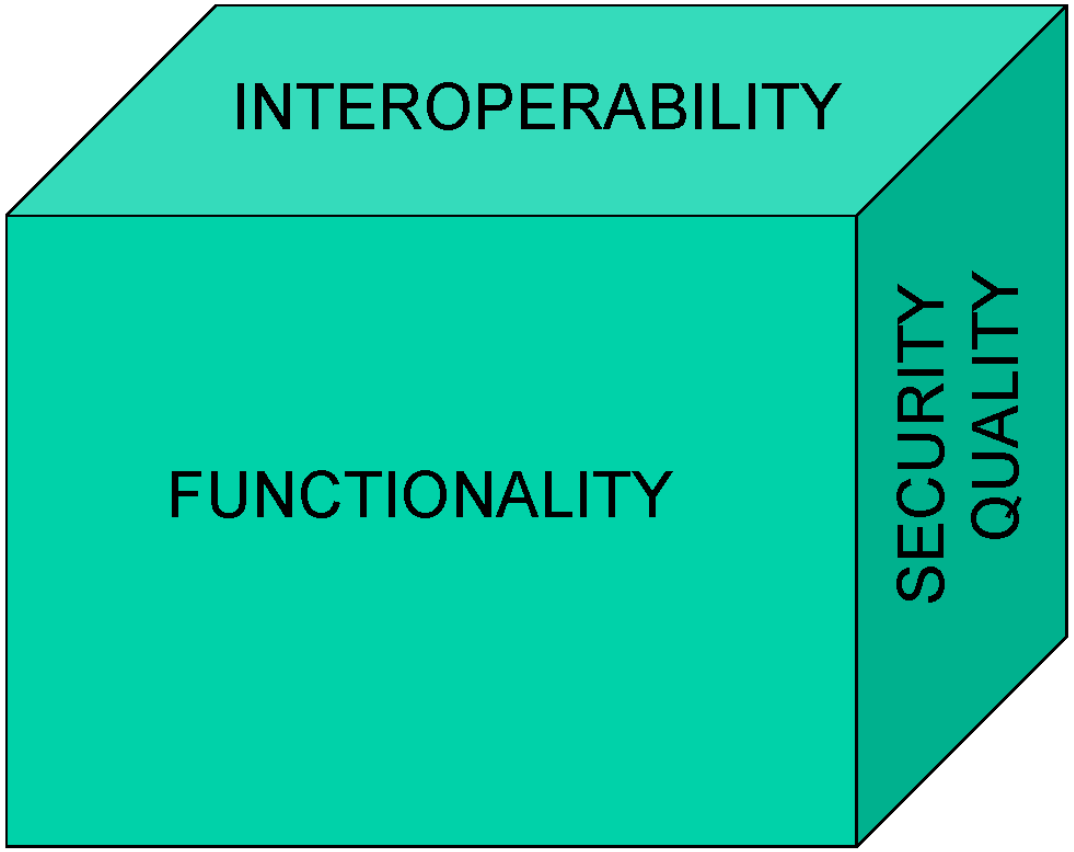
UNIT1. INTRODUCTION TO SECURITY ENGINEERING

- Security Engineering Framework. The life cycle of security
- Principles about design of secure systems

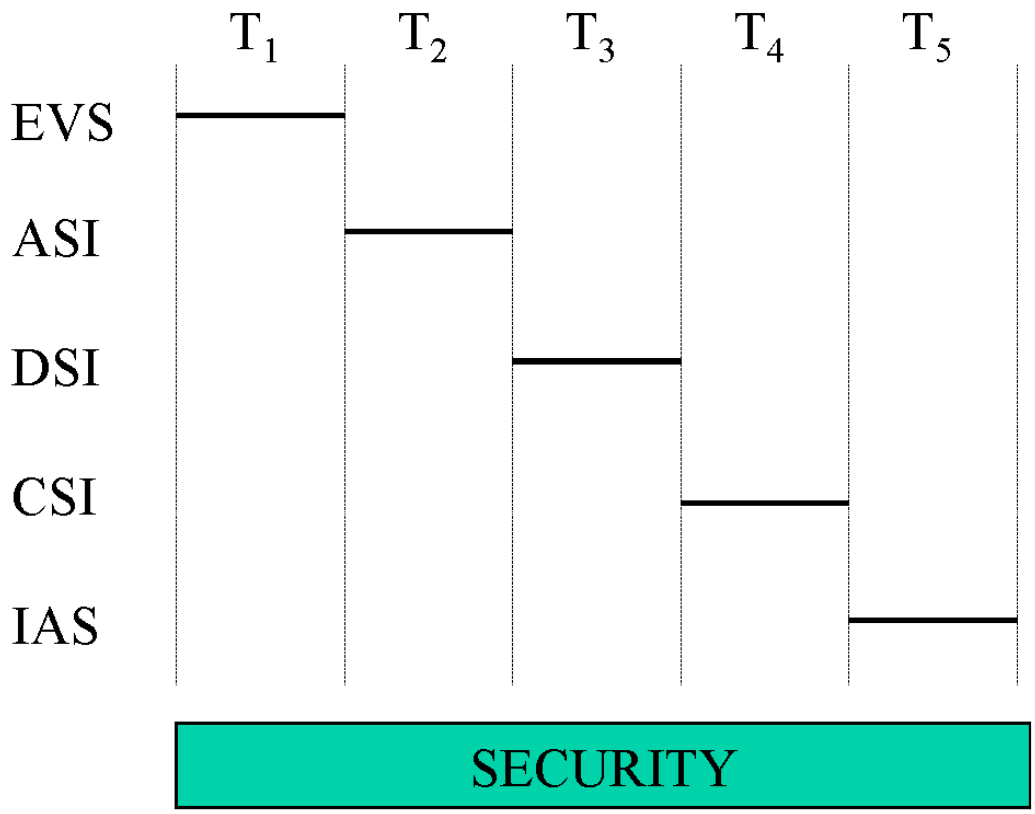
PRODUCT DEVELOPMENT. Classical



PRODUCT DEVELOPMENT. Ideal



PRODUCT DEVELOPMENT: Metric



EVS: Information System Feasibility Study
ASI: Information System Analysis
DSI: Information system Design
CSI: Information system Construction
IAS: Information system Implementation Acceptance

www.seg.inf.uc3m.es

CHAPTER 1. Programme

UNIT1. INTRODUCTION TO SECURITY ENGINEERING

- Security Engineering Framework. The life cycle of security
- Principles about design of secure systems

DESIGN PRINCIPLES. Secure systems

1. Economy of mechanisms.
   Simplicity over complexity

DESIGN PRINCIPLES. Secure systems

1. Economy of mechanisms.
2. Default security

   Everything that is not allowed is forbidden (against everything that is not forbidden is allowed)

DESIGN PRINCIPLES. Secure systems

1. Economy of mechanisms.
2. Default security
3. Full mediation

   All accesses must be filtered by the security mechanisms

DESIGN PRINCIPLES. Secure systems

1. Economy of mechanisms.
2. Default security
3. Full mediation
4. Open design

Transparent security against dark security

DESIGN PRINCIPLES. Secure systems

1. Economy of mechanisms.
2. Default security
3. Full mediation
4. Open design
5. Segregation of duties

   i.e., security administrator against system Administrator

DESIGN PRINCIPLES. Secure systems

6. Minimun privileg

Access to essential resources in order to perform the tasks

DESIGN PRINCIPLES. Secure systems

6. Minimum privileg
7. Minimum common mechanisms
8. User acceptability

Intuitive and easy to use interfaces.

DESIGN PRINCIPLES. Secure systems

6. Minimum privileg
7. Minimum common mechanisms
8. User acceptability
9. Working Factor

Cost breakdown of security mechanisms. Compared to the expected benefits. Principle of proportionality

DESIGN PRINCIPLES. Secure systems

6. Minimum privileg
7. Minimum common mechanisms
8. User acceptability
9. Working Factor
10. Event log

Periodic analysis of logs

CHAPTER 1. Programme

UNIT1. INTRODUCTION TO SECURITY ENGINEERING

- Security Engineering Framework. The life cycle of security
- Principles about design of secure systems
- Threats. Vulnerabilities. Attacks

PREVIOUS CONCEPTS (Cripto & IT Security)

- Asset
  - An IT system component or funcionality prone to be attacked deliberately or accidentally with consequences for the organization

PREVIOUS CONCEPTS (Cripto & IT Security)

- Threat
  - A potential for violation(accidental or malicious) of system security
  - Any operation that puts at risk the security goals

PREVIOUS CONCEPTS (Cripto & IT Security)

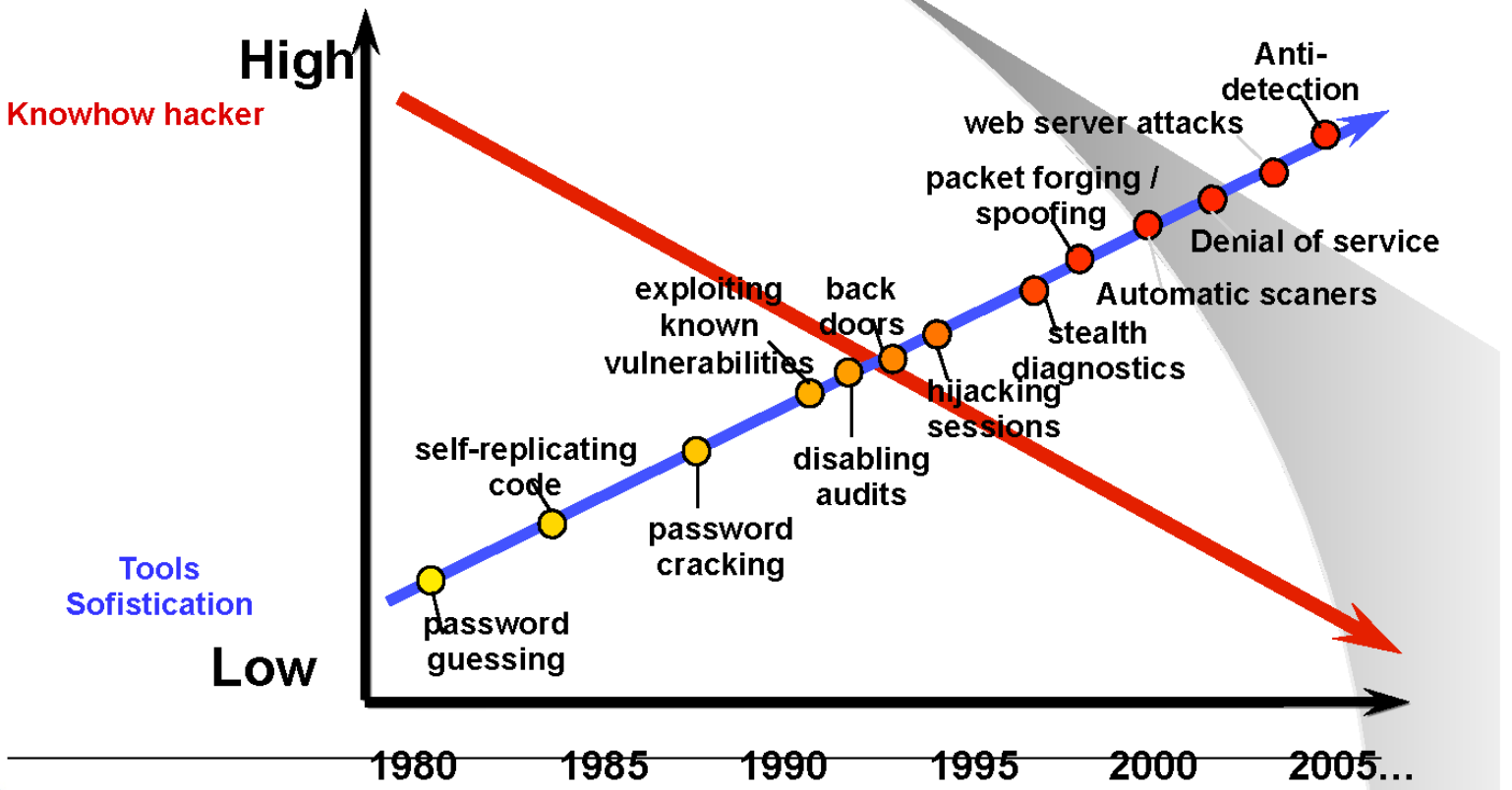
Vulnerability

- A flaw or weakness in a system's design, implementation, or operation and manage ment that could be exploited to violate the system's security policy
- A weakness in a computing system (or protection system) that can result in harm to the system or its operations
- Vulnerabilities produced during system development
- Vulnerabilities produced during system operation
- Vulnerabilities produced during maintenance

PREVIOUS CONCEPTS (Cripto & IT Security)

- Attack
  - A deliberate attempt to evade security services and violate the security policy of a system
- Clasification
  - Sophisticated tools
  - Automated tools
  - Social engineering (Phishing)

PREVIOUS CONCEPTS (Cripto & IT Security)



PREVIOUS CONCEPTS (Cripto & IT Security)

- Security measures (Services)
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
  - Intend to counter security attacks.
  - Make use of one or more security mechanisms to provide the service.

PREVIOUS CONCEPTS (Cripto & IT Security)

- Security measures (Mechanisms)
  - Phisic or logic implementation of a security service
  - Types
    - Encrypt
    - Digital signature
    - Access control
    - Authentication functions
    - Flow control
    - Traffic padding
    - Trusted Third Parties

THREATS: The human factor

- Employees (and computer users)
  - Negligent
  - Careless

NEGLIGENT EMPLOYEES. Software update[1]

Intrusions explode fixed vulnerabilities

1. Source CERT

VULNERABILITIES. Software update[1]

Over 90% of software security incidents are caused by attackers exploiting known software defects.

70% of security defects were design defects (analysis of 45 e-business applications)

Experienced software engineers inject, on average, one defect every nine lines of code.

Cada 10^6 line of code systems typically contains 10^3 -1,5 10^3 defects when shipped

THREATS: Human factor

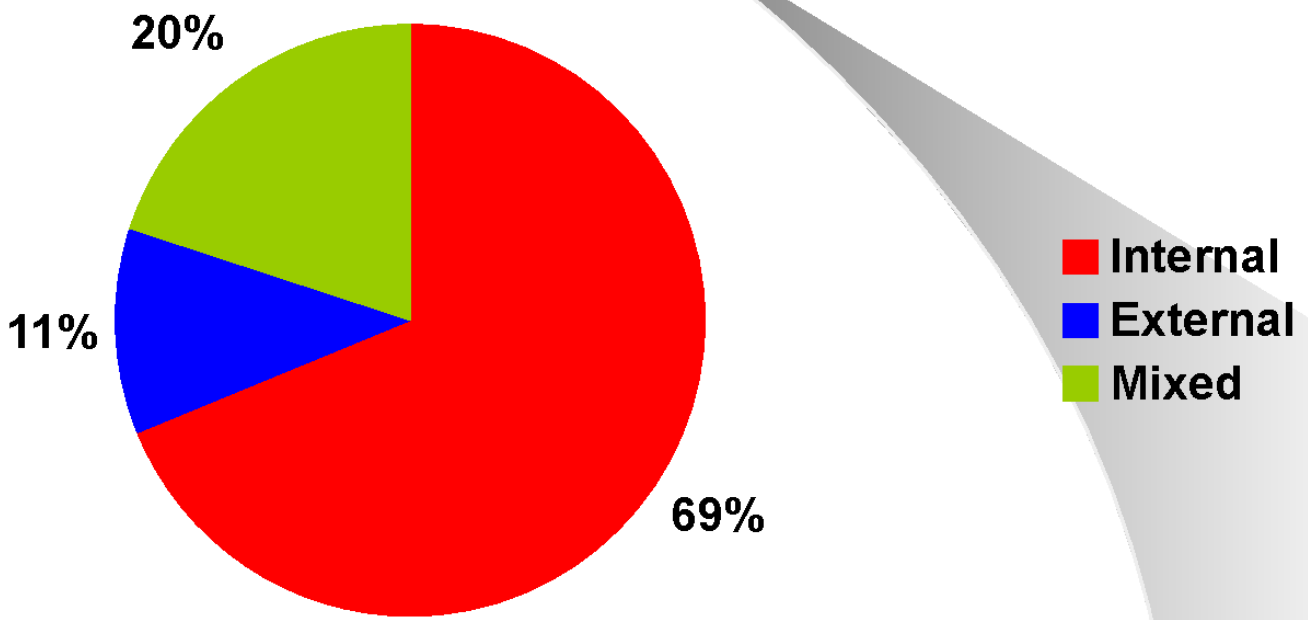
Hacks	2007	2008
Employees/Ex Employees	89%	50%
Hackers	41%	28%
Unknown	*	42%
Partners/customers/other	48%	31%
Terrorism/foreign governments	6%	4%

- * Not allowed

More than one answer was allowed

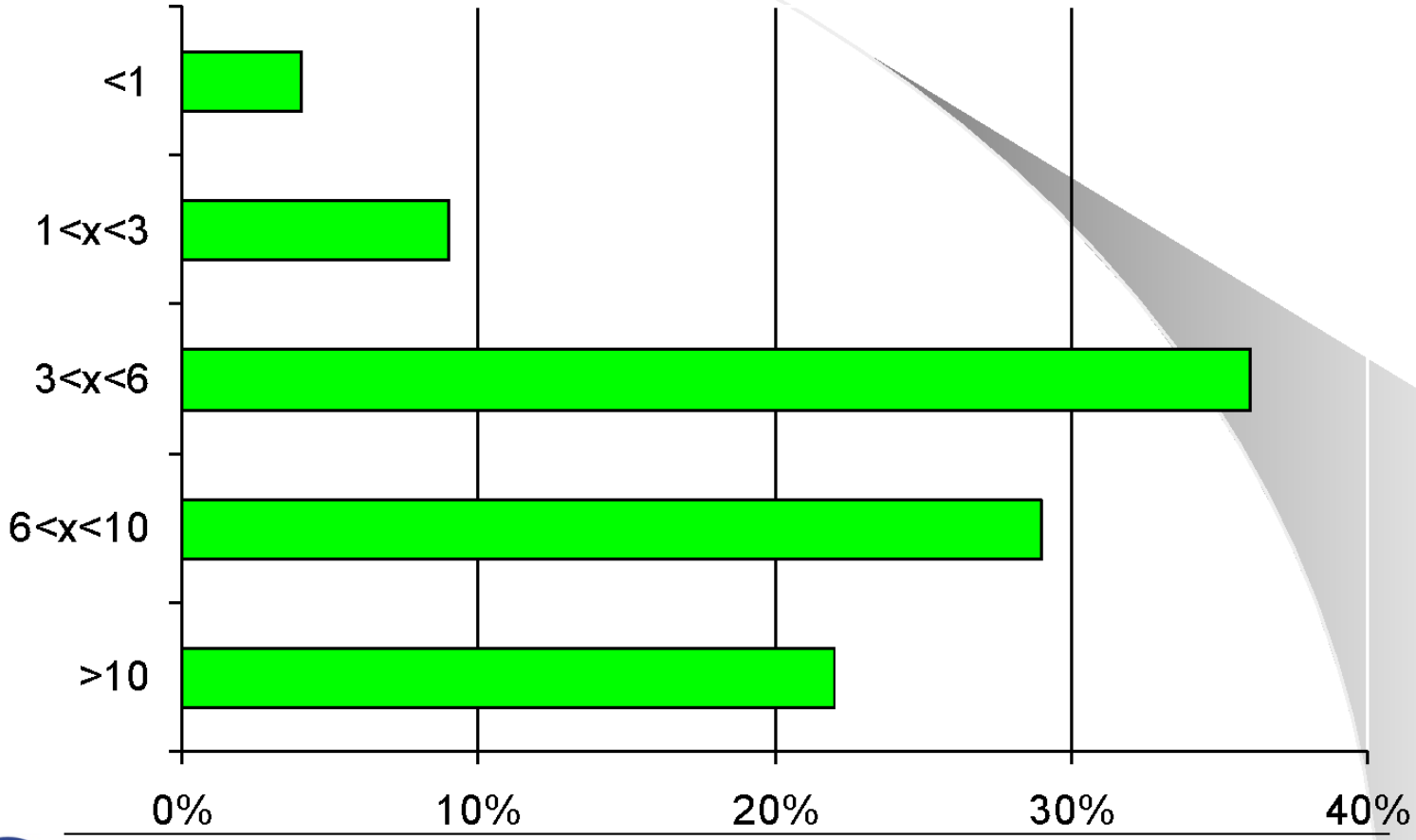
1. 5º Global State of I.S. PwC. 2008

RELATIONSHIP WITH THE COMPANY[1]



1. Perfil defraudador. 2007. KPMG

YEARS IN THE COMPANY[1]



1. Perfil defraudador. 2007. KPMG

Many cyber vulnerabilities exist because of a **lack of cybersecurity awareness** on the part of computer users, systems administrators, technology developers, auditors, chief information officers and corporate boards. Such awareness-based vulnerabilities present **serious risks to critical infrastructures**[1]

1. National Strategy to Secure Cyberspace.Casa Blanca 2003

HUMAN FACTOR: Motivation

- Personal satisfaction (self-esteem)
  - No effects
  - Vandalism
- Benefit (economic)
- critical or militar Infraestructure lock down (ciberterrorism)

VULNERABILITIES . "Patches"

Hispasec - una-al-día 24/01/2015
Todos los días una noticia de seguridad www.hispasec.com

Síguenos en Twitter: http://twitter.com/unaaldia
Noticia en formato HTML:
http://unaaldia.hispasec.com/2015/01/google-publica-chrome-40-y-corrige-62.html
---
Google publica Chrome 40 y corrige 62 vulnerabilidades

Google anuncia una nueva versión de su navegador Google Chrome 40. Se publica la versión 40.0.2214.91 para las plataformas Windows, Mac y Linux, que junto con nuevas funcionalidades y mejoras, además viene a corregir 62 nuevas vulnerabilidades.

La actualización incluye la corrección de 62 nuevas vulnerabilidades. Como es habitual, Google solo proporciona información sobre los problemas solucionados reportados por investigadores externos o las consideradas de particular interés. En esta ocasión, aunque se han solucionado 62 vulnerabilidades, solo se facilita información de 26 de ellas (17 de gravedad alta y las 9 restantes de importancia media

VULNERABILITIES . "Patches"

Hispasec - una-al-día 20/01/2015
Todos los días una noticia de seguridad www.hispasec.com
Síguenos en Twitter: http://twitter.com/unaaldia
Noticia en formato HTML:
http://unaaldia.hispasec.com/2015/01/oracle-corrige-169-vulnerabilidades-en.html

---

Oracle corrige 169 vulnerabilidades en su actualización de seguridad de enero

---

Siguiendo su ritmo de publicación trimestral de actualizaciones, Oracle publica su boletín de seguridad de enero. Contiene parches para 169 vulnerabilidades diferentes en una larga lista de productos pertenecientes a diferentes familias, que van desde el popular gestor de base de datos Oracle Database hasta Solaris, Java o MySQL.

2013 -2017 OWASP TOP 10

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

VULNERABILITIES.

- CVE (Common vulnerabilities and exposures)
- CWE (Common weakness enumeration)
- CAPEC (Common Attack Pattern Enumeration and Classification)
- ITU-T Recomendación X.1520 (04/2011)

VULNERABILITIES. Databases.

- National Vulnerability DB
- Open source vulnerability DB
- Security Focus
- IBM X-Force vulnerability DB

COMPANIES DOING BUSINESS WITH *BUGS*

- Zero Day Initiative (Tipping Point. 3Com)
- iDefense (Veri Sign)
- iSight Partners
- …

PART 1. Silabus

UNIT1. INTRODUCTION TO SECURITY ENGINEERING

- Security Engineering Frame work. The life cycle of security
- Design principles for secure systems
- Threats. Vulnerabilities.
- Security measures. According to their mode of action and their type

SECURITY MEASURES according to way of action

- Prevention
  - Minimize probability of attack
- Detection
  - Minimize propagation of attack
- Correction
  - Minimize damage of attack
- Recovery
  - Minimize consequences of attack

Security Measures

- Legal and normative
- Administrative y organizational
- Physical
- Technical

SECURITY MEASURES: Government organizat

- Indformation clasification
- Responsabilities
- Security function
- Training and awareness
- ....

SECURITY MEASURES Physical

- fire detection
- systems against flood
- Continuity equipment
- Access control (entities, human…)

SECURITY MEASURES Technical

- Identification and authentication
- Access control
- Confidentiality
- Integrity
- Non repudiation
- Audit

SECURITY MECHANISMS

- Authentication
- Access control
- Encryption
- Hash functions
- Digital signature
- Audit log

Principle of proportionality

The security measures and their application must be proportional to the nature of the data, the risks to which they are exposed and the information systems that treat them, and the state of the technology.

World Economic Forum. Global risks 2016

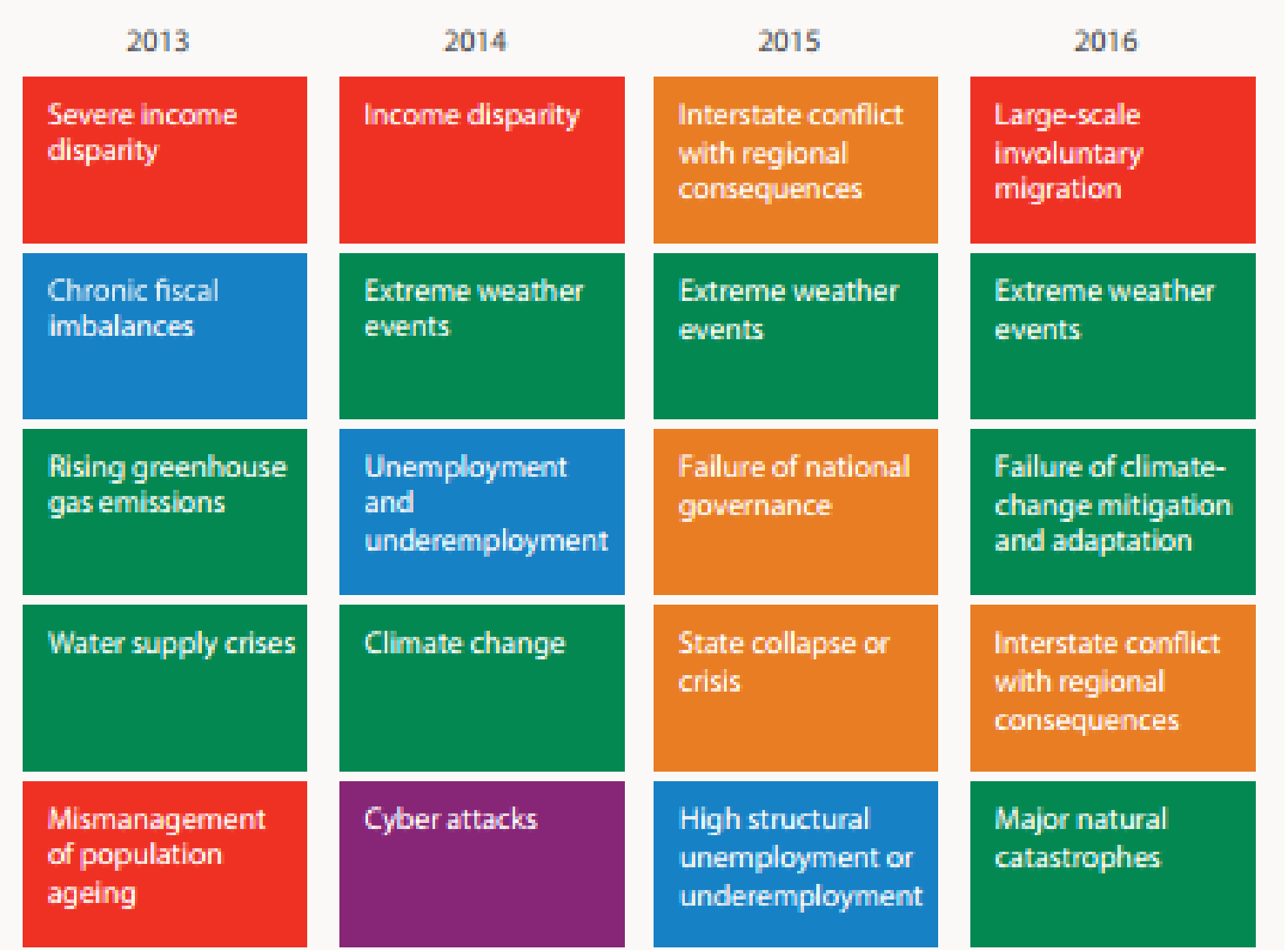
World Economic Forum. Global risks 2016 (types)

- Asset bubble in a major economy
- Deflation in a major economy
- Failure of a major financial mechanism or institution
- Failure/shortfall of critical infrastructure
- Fiscal crises in key economies
- High structural unemployment or underemployment
- Illicit trade (e.g. illicit financial flow, tax evasion, human trafficking, organized crime, etc.)
- Severe energy price shock (increase or decrease)
- Unmanageable inflation
- Extreme weather events (e.g. floods, storms, etc.)
- Failure of climate-change mitigation and adaptation
- Major biodiversity loss and ecosystem collapse (land or ocean)
- Major natural catastrophes (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms)
- Man-made environmental catastrophes (e.g. oil spill, radioactive contamination, etc.)
- Failure of national governance (e.g. failure of rule of law, corruption, political deadlock, etc.)
- Interstate conflict with regional consequences
- Large-scale terrorist attacks
- State collapse or crisis (e.g. civil conflict, military coup, failed states, etc.)
- Weapons of mass destruction
- Failure of urban planning
- Food crises
- Large-scale involuntary migration
- Profound social instability
- Rapid and massive spread of infectious diseases
- Water crises
- Adverse consequences of technological advances
- Breakdown of critical information infrastructure and networks
- Large-scale cyberattacks
- Massive incident of data fraud/theft

WEF. Global risk 16 (impact)

2013	2014	2015	2016
Major systemic financial failure	Fiscal crises	Water crises	Failure of climate-change mitigation and adaptation
Water supply crises	Climate change	Rapid and massive spread of infectious diseases	Weapons of mass destruction
Chronic fiscal imbalances	Water crises	Weapons of mass destruction	Water crises
Diffusion of weapons of mass destruction	Unemployment and underemployment	Interstate conflict with regional consequences	Large-scale involuntary migration
Failure of climate-change mitigation and adaptation	Critical information infrastructure breakdown	Failure of climate-change mitigation and adaptation	Severe energy price shock

WEF. Global risk (probability)



ATTACK MAPS

AKAMAI. Ataques DDoS

https://www.stateoftheinternet.com/trends-visualizations-security-real-time-global-ddos-attack-sources-types-and-targets.html

FIREEYE

https://www.fireeye.com/cyber-map/threat-map.html

FORTINET

http://threatmap.fortiguard.com/

ATTACK MAPS

TrendMicro Global Botnet Threat Activity Map

http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-botnet-map/index.html

Google Digital Attack Map

http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16712&view=map

SEGU-INFO BLOC

http://blog.segu-info.com.ar/2015/09/mapas-de-ataque-en-internet.html