

Principles and fundamentals of security
methodologies of information systems - Introduction

M2SSIC-Metz

Pascal Steichen

Contents

1	Presentation	4
2	Why this cours ?	4
3	Introduction	6
4	Security principles and definitions	6
4.1	CIA triad	7
4.2	Parkerian Hexad	8
4.3	7 ISO principles	10
4.4	"Traditional" 4-steps model	11
4.5	Piscitello's "Pentagon of Trust"	11
5	Risk, risk assessment, security policy, ISMS	11
5.1	Risk assessment	12
5.2	Security policy	12
5.3	ISMS	13
6	Detailed vocabulary (ISO/IEC 27000)	13
7	Where it all started - an example case	15
8	(Information) security and politics	16
8.1	USA's approach to information security	16
8.2	Europe is not sleeping either	22
9	Meanwhile in the other parts of the (security) world ...	29
10	OECD	34
11	Case study: National IS strategy - Luxembourg	35

1 Presentation

Pascal Steichen

Ministère de l'Economie et du Commerce extérieur (<http://www.eco.public.lu>)

- CASES (Cyberworld Awareness and Security Enhancement Structure) - <http://www.cases.lu/>
- CIRCL (Computer Incident Response Centre Luxembourg) - <http://www.circl.lu/>
- ENISA (European Network and Information Security Agency) - <http://www.enisa.europa.eu/>
- CLUSSIL (CLUb de la Sécurité des Systèmes d'Information du Luxembourg) - <http://www.clussil.lu/>
- ANSIL (Association de Normalisation pour la Société de l'Information du Luxembourg) - <http://www.ansil.eu/>
- hack.lu

Presentation

- Who are you?
 - your studies before M2SSIC ?
 - why M2SSIC ?
 - what job are you aiming for ?
 - what does an (C)ISO (RSSI) do?
 - anything to add...

2 Why this cours ?

- The complexity involved in controlling the security of information systems (IS) is not only technology-based but mainly related to the management of the IS within organizations.
- The importance of technology is well understood and widely recognized, both the challenges posed by new technologies and architectures (distributed, open or mobile), as well as the technological complexity of deployment of specific solutions (such as PKI).

Why this course ?

- The management dimension shall not be underestimated however.
- e.g. PKI: recent lessons learned showed that, public key infrastructure, even if technologically fine, couldn't be deployed due to a misunderstanding of the organizational impacts related to their integration into the business processes as financial aspects associated to prohibitive costs of installing and maintenance.

Why this course ?

- The **cost/return on investment ratio** is difficult to determine and many more factors than only technological aspects are involved. This is the core concept of this course.
- It is often not straightforward to decide between a "simple" password solution versus a public key certificate mechanism.
- PKI is of course much more secure, but one shall as well include the (added) **value** of the service to secure and its organization and financial impacts.
- Methods to tackle these questions have been well identified by the security community. They are known as **risk assessment/management**.

Why this course ?

- Objectives:
 - acquire the basics of information security and its tools
 - understand information security in the organization
 - get an overview of the main methodologies available
 - understand the concepts of standardisation, certification and accreditation
 - master risk assessment methodologies
 - master essential standards
- Modules:
 - Principles and fundamentals of security methodologies of information systems
 - Advanced security methodologies of information systems

3 Introduction

Communication networks and information systems are essential factors in the development of the economy and society. Secure networks are increasingly becoming as indispensable as electricity or water supply to make the Digital Economy function.

Therefore, the security of communication networks and information systems is of escalating concern for society. This stems from the complexity of information systems, accidents, mistakes and attacks to the physical infrastructures which deliver critical services to the citizens.

The growing number of security breaches has already generated substantial financial damage and has undermined user confidence. At the same time, the Information Society is becoming indispensable in all areas of life. Individuals, international institutions, public administrations and businesses have deployed security technologies, security management procedures, information campaigns and research projects, to enhance network and information security. The technical complexity of networks and information systems, the variety of interconnected products and services, and the huge number of private and public players that bear their own responsibility, is risking to undermine the smooth functioning of international markets. The modernised Information Society and its business, based upon a Digital Economy is thus, potentially, jeopardized.

4 Security principles and definitions

(information) system "whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information" - wikipedia

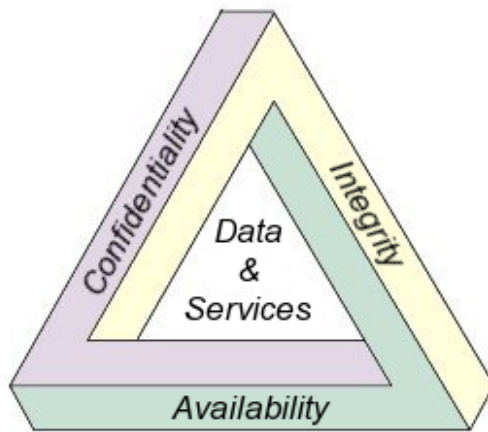
(information) security "means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction" - wikipedia

- several models:
 - CIA triad
 - Parker's six atomic elements (or Parkerian hexad)
 - 7 ISO principles
 - Traditional 4-steps model (or the 4-As)
 - Piscitello's "*Pentagon of Trust*"

4.1 CIA triad

Since the early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering. Persons desiring secure communications have used wax seals and other sealing devices since the early days of writing to signify the authenticity of documents, prevent tampering, and ensure confidentiality of correspondence.

For over twenty years we know use confidentiality, integrity and availability (known as the CIA Triad) as the core principles of information security.



44 U.S.C § 3542 (b)(1) (2006):

The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide

1. integrity

which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

2. confidentiality

which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3. availability

which means ensuring timely and reliable access to and use of information.

4.2 Parkerian Hexad

Donn B. Parker adds **three additional** atomic, non-overlapping attributes of information to the three classic security attributes of the CIA triad, (confidentiality, integrity, availability). The Parkerian Hexad attributes are the following:

- **Confidentiality** refers to limits on who can get what kind of information. For example, executives concerned about protecting their enterprise's strategic plans from competitors; individuals are concerned about unauthorized access to their financial records.
- **Possession or Control** Suppose a thief were to steal a sealed envelope containing a bank debit card and (foolishly) its personal identification number. Even if the thief did not open that envelope, the victim of the theft would legitimately be concerned that (s)he could do so at any time without the control of the owner. That situation illustrates a loss of control or possession of information but does not involve the breach of confidentiality.
- **Integrity** refers to being correct or consistent with the intended state of information. Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity. For example, data stored on disk are expected to be stable – they are not supposed to be changed at random by problems with the disk controllers. Similarly, application programs are supposed to record information correctly and not introduce deviations from the intended values.
- **Authenticity** refers to correct labeling or attribution of information. For example, if a criminal forges e-mail headers to make it look as if an innocent person is sending threatening e-mail messages, there has been no breach of confidentiality (the thief uses his or her own e-mail account), possession (no information has been taken out of the control of the victim), or integrity (the e-mail messages are exactly as intended by the criminal). What is breached is authenticity: the e-mail is incorrectly attributed to someone else. Similarly, misusing a

field in a database to store information that is incorrectly labeled is a breach of authenticity; e.g., storing a merchant's tax code in a field labeled as the merchant's ZIP code would violate the authenticity of the information.

- **Availability** means having timely access to information. For example, a disk crash or denial-of service attacks both cause a breach of availability. Any delay that exceeds the expected service levels for a system can be described as a breach of availability.
- **Utility** means usefulness. For example, suppose someone encrypted data on disk to prevent unauthorized access or undetected modifications – and then lost the decryption key: that would be a breach of utility. The data would be confidential, controlled, integral, authentic, and available – they just wouldn't be useful in that form. Similarly, conversion of salary data from one currency into an inappropriate currency would be a breach of utility, as would the storage of data in a format inappropriate for a specific computer architecture; e.g., EBCDIC instead of ASCII or 9-track magnetic tape instead of DVD-ROM. A tabular representation of data substituted for a graph could be described as a breach of utility if the substitution made it more difficult to interpret the data. Utility is often confused with availability because breaches such as those described in these examples may also require time to work around the change in data format or presentation. However, the concept of usefulness is distinct from that of availability.



4.3 7 ISO principles

The ISO (International Standardisation Organisation) defines **security** as follows:

“All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability.” (ISO/IEC 13335-1)

The terms *defining, achieving and maintaining*, show us that security is a process.

Further we have the now famous *security principles*:

- Confidentiality
(the property that information is not made available or disclosed to unauthorized individuals, entities, or processes)
- Integrity
(the property of safeguarding the accuracy and completeness of assets)
- Availability
(the property of being accessible and usable upon demand by an authorized entity)
- Non-repudiation
(the ability to prove an action or event has taken place, so that this event or action cannot be repudiated later)
- Accountability
(the property that ensures that the actions of an entity may be traced uniquely to the entity)
- Authenticity
(the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information)
- Reliability
(the property of consistent intended behaviour and results)

4.4 "Traditional" 4-steps model

In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine (i.e. they have not been forged or fabricated). As such we have to add a fourth step (principle) to our security concepts, known as "authenticity":

- Authentication (confidentiality) (who are you, are you allowed to use/read)
- Authorization (integrity) (what are you allowed to do, modify)
- Availability (is the data accessible)
- Authenticity (is the data intact)

4.5 Piscitello's "Pentagon of Trust"

Dave Piscitello made a fascinating observation. Commenting on the traditional four-steps security model (see above), he said:

Traditional models do not include asserting the trustworthiness of the endpoint device from which a (remote) user will authenticate and subsequently access data. Network admission and endpoint control are needed to determine that the device is free of malware (esp. key loggers) before you even accept a keystroke from a user. So let's prepend "**admissibility**" (**the state or quality of being admissible or allowable**) to the list, and come up with the Pentagon of Trust.

5 Risk, risk assessment, security policy, ISMS

- why this need for CIA ? => every information system is subject to risks

risk equation: Risk = Vulnerability * Threat * Impact

- Example:
 - *vulnerability*: the anti-virus software is not up to date

- *threat*: a cyber-criminal develops a virus that hides in an attachment of an advertising e-mail
- *impact*: an employee opens the attachment, the server gets infected and all data is lost

5.1 Risk assessment

- Before being able to identify (assess) risks, one has to identify the assets to protect, especially the critical ones

Asset: anything that has value to the organization, there are many types of assets, including:

- (a) information
- (b) software assets
- (c) physical assets
- (d) people, and their qualifications, skills, and experience
- (e) intangibles, such as reputation and image.

5.2 Security policy

- Security is not a state, but a process
- Protecting information systems needs daily care:
 - a security policy provides a high-level description of various controls (or areas of controls) an organisation will use to protect information (e.g. authentication, physical security, business continuity...)
 - with the aim to mitigate risks by reducing vulnerabilities
- ISO/IEC 27002 gives best practices in this area

Security policy

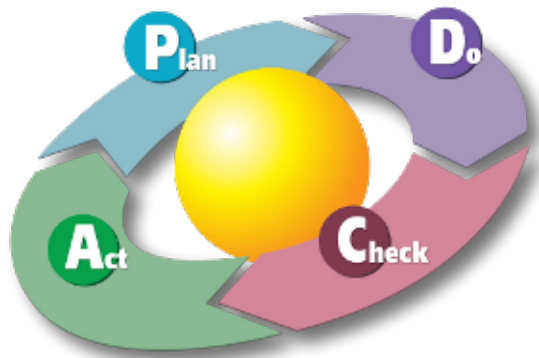
- An information security policy defines (business) rules and procedures for managing and protecting assets.
- It identifies
 - security objectives to achieve
 - and measures to implement.

- A written policy document is also a formal declaration of the management's intent to security.

5.3 ISMS

ISMS - Information Security Management System

- defines a PDCA model for an continuous business process improvement cycle (aka Deming cycle)



PLAN Establish the objectives and processes necessary to deliver results in accordance with the expected output. By making the expected output the focus, it differs from other techniques in that the completeness and accuracy of the specification is also part of the improvement.

DO Implement the new processes. Often on a small scale if possible.

CHECK Measure the new processes and compare the results against the expected results to ascertain any differences.

ACT Analyze the differences to determine their cause. Each will be part of either one or more of the P-D-C-A steps. Determine where to apply changes that will include improvement. When a pass through these four steps does not result in the need to improve, refine the scope to which PDCA is applied until there is a plan that involves improvement.

6 Detailed vocabulary (ISO/IEC 27000)

ISMS that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

Risk combination of the probability of an event and its consequence. NOTE: The term "risk" is generally used only when there is at least the possibility of negative consequences

Attack attempt that results in breaching the security policy by destroying, exposing, altering, disabling or gaining unauthorized access to assets

Threat a potential source of an incident that may result in adverse changes to an asset, a group of assets or an organization

Vulnerability weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat

Impact: adverse change to the level of business objectives achieved

Risk management coordinated activities to direct and control an organization with regard to risk

Risk assessment overall process of risk analysis and risk evaluation

Risk analysis systematic use of information to identify sources and to estimate the risk

Risk criteria terms of reference by which the significance of risk is assessed

Risk treatment process of selection and implementation of options to modify risk. NOTE: Risk treatment options can include avoiding, reducing, transferring or retaining risk.

Risk avoidance decision not to be involved in, or to withdraw from, a risk situation

Risk reduction action taken to lessen the probability, negative consequences, or both, associated with a risk

Risk transfer re-assignment with another party the burden of loss for a risk

Risk retention acceptance of the burden of loss, or benefit of gain, from a particular risk

Risk acceptance decision to accept a risk

Residual risk risk remaining after risk treatment

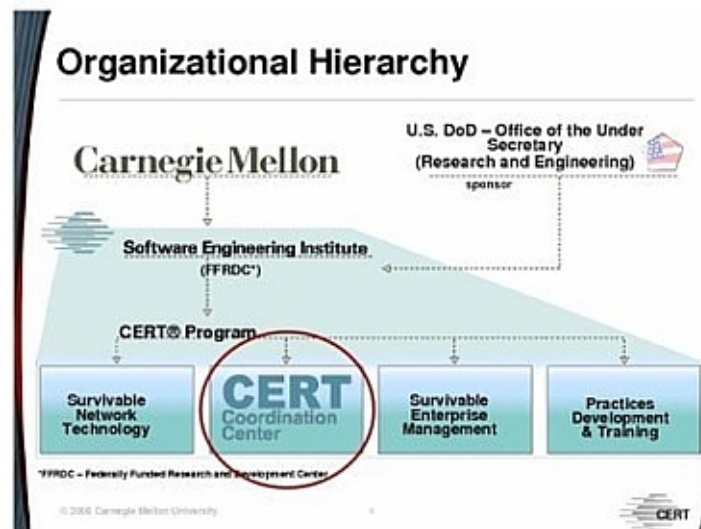
Control means of managing risk, including policies, procedures, guidelines, practice or organizational structures, which can be of administrative, technical, management, or legal nature. NOTE: Safeguard and countermeasure are also used as a synonym for control.

Information security policy A policy approved by the management that demonstrates support for, and commitment to information security.

7 Where it all started - an example case

- Back in 1968 the DoD (Department of Defense)/DARPA (Defense Advanced Research Project Agency) starts ARPANET.
- 1972: about 40 machines were connected through the ARPANET.
- 1980: more and more non-military usage of ARPANET. The network grows on a daily basis and is rebaptised "Interconnection Network", "INTERNET" in short.
- No later than 1986 the first VIRUS emerges: BRAIN.
It was a boot sector virus propagating via floppy disks. BRAIN, as you might imagine, didn't propagate on a large scale and as such didn't really do much harm.
- 1988 (2nd November 1988): Robert T. Morris (then student at Cornell university) developed the first WORM, his now famous "Internet Worm" or "Morris Worm". It infected (and most of the time crashed) more than 10% of all machines, causing millions of dollars of losses.

The "Morris Worm" demonstrated the growing network's susceptibility to attack and 2 weeks later (on 17th November 1988) the CERT/CC, a major center for internet security problems, was established at the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) operated by Carnegie Mellon University.



8 (Information) security and politics

- Nowadays information security has become part of our daily lives. Think, for instance about, the huge world wide e-mail traffic (with critical and confidential informations), or the more and more upcoming social engineering attack techniques.
- Let's analyse how politics deals with it...

8.1 USA's approach to information security

- Some prominent examples of USA's approach to NIS:
 - Video **Privacy** Protection Act (VPPA)
The VPPA was a US law passed in 1988 as Public Law 100-618. It was created to prevent what it refers to as "wrongful disclosure of video tape rental or sale records." Congress passed the VPPA after Robert Bork's video rental history was published during his Supreme Court nomination. It makes any "video tape service provider" that discloses rental information outside the ordinary course of business liable for up to \$2500 in actual damages.
 - **Health** Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 and its Security Rule establish requirements for safeguards to protect the *confidentiality, integrity, and availability* of electronic protected health information. HIPAA applies to virtually all health-care organizations - including all health care providers, health plans, public health authorities, healthcare clearinghouses, and self-ensured employers - as well as life insurers, information systems vendors, various service organizations, and universities.

The Administrative Simplification section of HIPAA resulted in several rules, including the Security Rule. The final Security Rule was published on February 20, 2003 and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual.

HIPAA requires covered entities to:

- * Ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) the covered entity creates, receives, maintains, or transmits
- * Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI
- * Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule
- * Ensure compliance by their workforce.

HIPAA calls for severe civil and criminal penalties for noncompliance, including: fines of up to \$25K for multiple violations of the same standard in a calendar year; fines of up to \$250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.

- **Gramm-Leach Bliley Act (GLBA)**

The **Financial Services** Modernization Act of 1999, more commonly known for its authors, Gramm-Leach-Bliley, includes provisions to protect consumers' personal financial information held by financial institutions. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule under section 501(b), requiring financial institutions under FTC jurisdiction to secure customer records and information. The three main objectives of GLBA 501(b) are to:

- Ensure the security and *confidentiality* of customer records and information
- Protect against any anticipated threats or hazards to the security or *integrity* of such records
- Protect against *unauthorized access* or use of such records or information which could result in substantial harm or inconvenience to any customer.

The Federal Financial Institutions Examination Council (FFIEC), comprised of examiners from many different regulatory bodies tasked with GLBA enforcement, has created an Information Security Handbook and an exhaustive set of tests to assess compliance with the Safeguards Rule, including over 20 specifically related to intrusion prevention and detection. The security process recommended by the FFIEC comprises five key areas:

1. Information security risk assessment
2. Information security strategy
3. Implement security controls
4. Security testing
5. Monitoring and updating

- Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002, outlines requirements to secure Federal information. Each **Federal Agency**, including contractors or other organizations who work with the agency, must develop, document, and implement an agency-wide information security program. Detailed guidance and recommendations are provided by the National Institute for Standards and Technology (NIST) encompassing all aspects of information security.

FISMA sections 3544 and 3505 require the following:

1. Compliance for every IT system - Required *identification* of all systems in use and that access federal information, and validation of their compliance. To help aid agencies in obtaining this, the National Institute of Standards and Technology (NIST) has released a series of guidelines, checklists, and templates that detail acceptable configurations for systems.
2. *Risk Assessment* - The agency must have an agency-wide information security program that includes controls and checks to ensure effectiveness, including reporting on existing risks and responses.

3. *Incident response* - The NIST Controls document outlines specific steps to follow and functions to perform depending on the level of threat posed by the environment.
4. *Intrusion detection* - Requires reporting on cyber security, risks and responses.
5. *Boundary protection* - Systems and applications should be protected from unauthorized access, both from outside the agency and its contractors, and from within.
6. *Compliance Reporting* - Requires detailed reporting on FISMA compliance status.

- Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act of 2002 was designed to reform the reporting, governance and disclosure of public company financial statements (heavily influence by the ENRON and Worldcom cases). Sarbanes-Oxley (SOX) mandates that public companies demonstrate due diligence in the disclosure of financial information and maintain internal controls and procedures for the communication, storage and protection of that data.

While not explicitly mentioned in the legislation, IT security is a central requirement of Sarbanes-Oxley compliance. SOX requires companies to assess any risk associated with information technology or the internal process that may impact the accurate and timely reporting of financial information. Specifically, SOX requirements include:

- Section 302: Establishes the responsibilities of the CEO and CFO for establishing and maintaining internal controls.
- Section 404: Requires management to assess the effectiveness of internal controls, obtain external validation of those controls, and provide assurances that financial/accounting processes are protected from unauthorized usage.
- Section 409: Requires real-time disclosures of material events.

Faced with the penalties for non-compliance hefty fines and possible jail time companies need a comprehensive, enterprise security system that will address these compliance issues: information security, vulnerability management, threat detection and response, policy management, and monitoring.

- Patriot Act

The Act mostly incorporates the provisions of the earlier anti-terrorism USA Act (H.R. 2975 and S. 1510). The Senate passed the USA Act on October 11, 2001. The House passed it on October 12, 2001. The primary differences between the USA Act and the USA PATRIOT Act are:

- The inclusion of the Financial Anti-Terrorism Act (H.R. 3004), which expands money laundering abatement to international terrorism.
- Immunity against prosecution for the providers of wiretaps in accordance with the Foreign Intelligence Surveillance Act of 1978.
- Request for a report on integrating automated fingerprint identification for ports of entry into the United States.
- Start of a foreign student monitoring program.
- Request for machine readable passports.
- Prevention of consulate shopping.
- Expansion of the Biological Weapons Statute.
- Clearer definition of "Electronic Surveillance"
- Miscellaneous benefits for victims of the September 11 attack and extra penalties for those who illegally file for such benefits.

Much criticism against the 2001 Act had been directed at the provisions for Sneak-and-Peek searches - a term coined by the FBI. Critics argued that Provision 213 authorizes "surreptitious search warrants and seizures upon a showing of reasonable necessity and eliminates the requirement of Rule 41 of the Federal Rules of Criminal Procedure that immediate notification of seized items be provided."

In special cases covered by FISA (amended by the USA PATRIOT Act), the warrants may come from the Foreign Intelligence Surveillance Court (FISC) instead of a common Federal or State Court. FISC warrants are not public record and therefore are not required to be released. Other warrants must be released, especially to the person under investigation.

A second complaint against Sneak-and-Peek searches is that the owner of the property (or person identified in business/library records) does not have to be told about the search. There is a special clause that allows the Director of the FBI to request phone records for a person without ever notifying the person. For all other searches, the person must be notified, but not necessarily before the search. The judge providing the warrant may allow a delay in notification when there is risk of:

- endangering the life or physical safety of an individual;
- flight from prosecution;
- destruction of or tampering with evidence;
- intimidation of potential witnesses; or
- otherwise seriously jeopardizing an investigation or unduly delaying a trial.

The delays are on average 7 days, but have been as long as 90 days. Section 213, which federal agencies report they have used 155 times since 2001, does not expire later this year like other USA PATRIOT Act provisions.

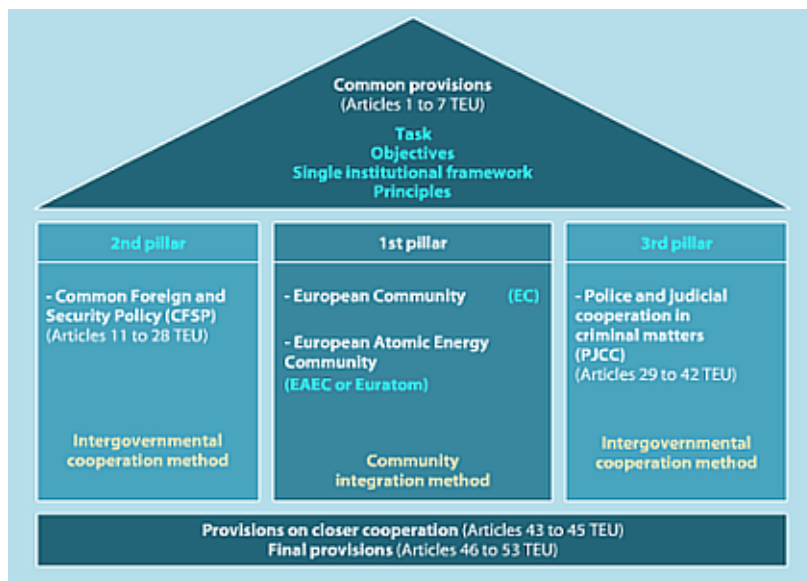
The American Civil Liberties Union argues that the term "serious jeopardy" is too broad "and must be narrowly curtailed."

However, "sneak and peek" searches have been in use for a long time in criminal cases. Title II of the USA PATRIOT Act was intended to bring the monitoring of foreign powers and the agents of foreign powers into line with such criminal legislation. The main difference between criminal and FISA delayed notification on search warrants is that FISA warrants use a different legal standard when approving such orders (they use reasonable cause, not probable cause).

Perhaps the most controversial section of the original Act was Section 215, dealing with a very narrow, implied right of federal investigators to access library and bookstore records. Section 215 allows FBI agents to obtain a warrant in camera (in secret) from the United States Foreign Intelligence Surveillance Court for library or bookstore records of anyone connected to an investigation of international terrorism or spying. On its face, the section does not even refer to "libraries," but rather to business records and other tangible items in general. Civil libertarians and librarians in particular, argue that this provision violates patrons' human rights and it has now come to be called the "library provision." The Justice Department defends Section 215 by saying that because it requires an order to be issued by a FISA Court judge, it provides better protection for libraries.

On August 26, 2005, The New York Times reported that according to the ACLU, the FBI is demanding library records from a Connecticut institution as part of an intelligence investigation. This would be the first confirmed instance in which the Federal Bureau of Investigation has sought library records, federal officials and the ACLU said. Interestingly, though, the government did not seek the records under section 215, but instead used "National Security Letters," which are the FISA equivalent of grand jury subpoenas and do not require a court order and thus are easier to use than section 215.

- 2004: ENISA is established
- 2005: the i2010 initiative - a security strategy is announced
- 2005: Framework against attacks (2005/222/JHA - pillar 3)
- 2006: Data retention directive (2006/24/EC)
- 2006: COM(2006) 251 is adopted



The three pillars

1. The first or 'Community' pillar concerns economic, social and environmental policies.
2. The second or 'Common Foreign and Security Policy' (CFSP) pillar concerns foreign policy and military matters.
3. The third or 'Police and Judicial Co-operation in Criminal Matters' (PJCC) pillar concerns co-operation in the fight against crime. This pillar was originally named 'Justice and Home Affairs'.

European Union		
First pillar	Second pillar	Third pillar
European Communities (EC)	Common Foreign and Security Policy (CFSP)	Police and Judicial Co-operation in Criminal Matters (PJCC)
<ul style="list-style-type: none"> • Customs Union and Single market • Common Agricultural Policy • Common Fisheries Policy • EU competition law • Economic and monetary union • EU-Citizenship • Education and Culture • Trans-European Networks • Consumer protection • Healthcare • Research (e.g. Sixth Framework Programme) • Environmental law • Social policy • Asylum policy • Schengen treaty • Immigration policy 	<p>Foreign policy:</p> <ul style="list-style-type: none"> • Human rights • Democracy • Foreign aid <p>Security policy:</p> <ul style="list-style-type: none"> • European Security and Defense Policy • EU battle groups • European Rapid Reaction Force • Peacekeeping 	<ul style="list-style-type: none"> • Drug trafficking and weapons smuggling • Terrorism • Trafficking in human beings • Organized crime • Bribery and fraud

e-signature directive

The electronic signature directive (1999/93/EC) establishes a harmonized *electronic* signature similar to the handwritten signature.

Some of the key elements:

- electronic signature - ES
- advanced electronic signature - AES
- qualified electronic signature - QES
- secure signature creation device - SSCD

Lisbon strategy (eEurope action plan)

The European Council, held in Lisbon on 23/24 March 2000, set the ambitious objective for Europe to become the most competitive and dynamic economy in the world. It recognised an urgent need for Europe to quickly exploit the opportunities of the new economy and in particular the Internet.

To achieve this, the European Commission drew

”...a comprehensive eEurope Action Plan ... using an open method of co-ordination based on the benchmarking of national initiatives...”

The eEurope 2002 action plan had a very tough deadline (only 2 years to achieve the ambitious goal) and was clustered on 3 main themes:

1. A cheaper, faster, secure Internet
 - Cheaper and faster Internet access
 - Faster Internet for researchers and students
 - **Secure networks and smart cards**
2. Investing in people and skills
 - European youth into the digital age
 - Working in the knowledge-based economy
 - Participation for all in the knowledge-based economy
3. Stimulate the use of the Internet
 - Accelerating e-commerce
 - Government online: electronic access to public services
 - Health online
 - European digital content for global networks
 - Intelligent transport systems

In 2002 the goal set in 2000 was unfortunately not achieved and the commission decided to continue the effort with the eEurope 2005 action plan:

By 2005, Europe should have:

- modern online public services
 - e-government
 - e-learning services
 - e-health services
- a dynamic e-business environment

- and, as an enabler for these
 - widespread availability of broadband access at competitive prices
 - a **secure information infrastructure**

Finally in 2005 the i2010 initiative emerged:

- create an open and competitive single market for information society and media services within the EU.

To support technological convergence with "policy convergence", the Commission proposes:

- an efficient spectrum management policy in Europe (2005);
 - a modernisation of the rules on audiovisual media services (end 2005);
 - an updating of the regulatory framework for electronic communications (2006);
 - **a strategy for a secure information society (2006)**;
 - and a comprehensive approach for effective and interoperable digital rights management (2006/2007).
- increase EU investment in research on information and communication technologies (ICT) by 80%.

Europe lags behind in ICT research, investing only EUR 80 per head as compared to EUR 350 in Japan and EUR 400 in the US. i2010 identifies steps to put more into ICT research and get more out of it, e.g. by trans-European demonstrator projects to test out promising research results and by integrating small and medium sized enterprises better in EU research projects.)

- promote an inclusive European information society.

To close the gap between the information society "haves and have nots", the Commission proposes:

- an Action Plan on e-Government for citizen-centred services (2006);
- three "quality of life" ICT flagship initiatives (technologies for an ageing society, intelligent vehicles that are smarter, safer and cleaner, and digital libraries making multimedia and multilingual European culture available to all (2007);
- and actions to overcome the geographic and social "digital divide", culminating in a European Initiative on e-Inclusion (2008).

ENISA

The Agency's activities consist of giving advice and recommendations, data analysis, as well as supporting awareness raising and cooperation by the EU bodies and Member States. Building on national and Community efforts, the Agency is to become a *Centre of Excellence* in this field. ENISA uses its expertise to stimulate cooperation between actions from the public and private sectors.

Among other things, the Agency provides assistance to the Commission and Member States in their dialogue with industry to address security-related problems in the hardware and software products. The Agency also follows the development of standards, promotes risk assessment activities by the Member States and interoperable risk management routines and produces studies on these issues within public and private sector organisations.

ENISA's tasks

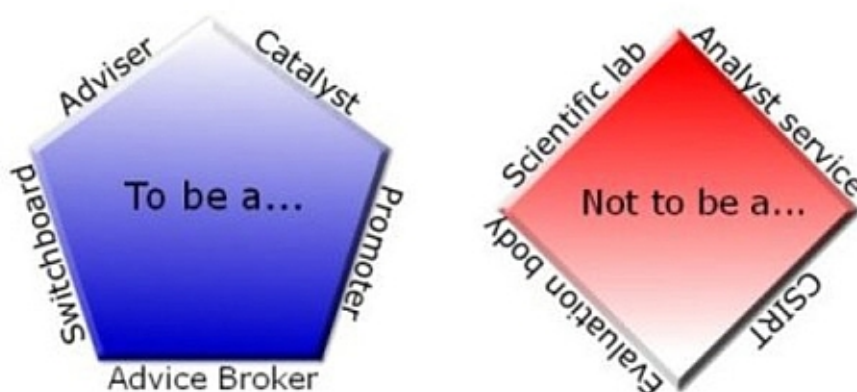
To **enhance** the **capability** of the Commission, other EU bodies and the Member States to prevent, address and to respond to NIS problems

To provide **assistance** and deliver **advice** to the Commission and the MS on issues related to NIS falling within its competencies as set out in this Regulation

To **develop** a high level of **expertise** and use this expertise to **stimulate** broad **cooperation** between actors from the public and private sectors

To **assist** the Commission, where called upon, in the **technical preparatory work** for updating and developing Community legislation in the field of NIS.

ENISA scope of activity



French government

The French Network and Information Security Agency - Agence Nationale de la Sécurité des Systèmes d'Information (created July 7th, 2009)

The French White Paper on Defence and National Security, published on June 17th, 2008, has identified cyber attacks as one of the main threats to the national territory. Indeed, society's growing dependence on information and communication technologies has made prevention and reaction to cyber attacks a major priority in the organisation of national security. This necessity has been underlined by several reports, notably those written by Deputy Pierre LASBORDES and by Senator Roger ROMANI.

In order to strengthen France's capabilities to face the challenges posed by information system security, the White Paper on Defence and National Security has planned the creation of a French Network and Information Security Agency (FNISA or ANSSI in French, standing for "Agence Nationale de la Sécurité des Systèmes d'Information"), in a similar way to France's main partner nations. This new agency is placed under the authority of the Prime Minister and is attached to the Secretary General for National Defence.

One year after the publication of the French White Paper, the ANSSI is now established by a decree issued in the Journal Officiel de la République Française of July 8th, 2009 — the creation process being under way since January 1st, 2009. The agency replaces the present Central Directorate for

Information System Security (DCSSI), and is assigned wider missions and resources.

The creation of the French Network and Information Security Agency is a milestone in the process of improving France's capability to protect its sensitive information systems.

- The core missions of the new agency are :
 - To detect and early react to cyber attacks, thanks to the creation of a strong operational center for cyber defence, working round-the-clock and being in charge of the continuous surveillance of sensitive Governmental networks, as well as the implementation of appropriate defence mechanisms ;
 - To prevent threats by supporting the development of trusted products and services for Governmental entities and economic actors ;
 - To provide reliable advice and support to Governmental entities and operators of Critical Infrastructure ;
 - To keep companies and the general public informed about information security threats and the related means of protection through an active communication policy.

9 Meanwhile in the other parts of the (security) world ...

The information security scene is not only lead by the politic's initiatives and actions, there are other actors, that are often more thoroughly involved and play a crucial and fundamental role: standardisation bodies, industry, research, ...

The standardisation bodies

- ISO/IEC (2700x)
- ITU (X.500)
- NIST (800 series)
- CEN/CENELEC/ETSI (e-sign standards)
- IEEE (802.11)

- IETF (Internet)
- OASIS (XML based standards)
- ...

Industry

”Lead” by the anti-virus producers, like Symantec, McAfee, ... as well as the firewall builders: Checkpoint, ...

Self-regulation is key: the banking sector has some good examples of own standards/regulations:

- Payment Card Industry Data Security Standard (PCI-DSS):
”Use network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.”

In response to acquirers, merchants, and service providers’ feedback regarding the need for stronger information security and a single approach to safeguarding sensitive data for all payment card brands, Visa and MasterCard collaborated and released common industry security requirements in January of 2005. These requirements are known as the Payment Card Industry (PCI) Data Security Standard. Globally accepted across the payment industry, PCI ensures that compliance with the following specific, mandated, card scheme programs are met:

- American Express Data Security Operating Policy (DSOP)
- Discover Information Security and Compliance (DISC)
- MasterCard Site Data Protection (SDP) Security Certification
- Visa Account Information Security (AIS)
- Visa Cardholder Information Security Program (CISP)

The purpose of PCI is to protect cardholder information, reduce debit and credit card fraud, and identify security issues that could lead to the compromise of cardholder information by imposing strict security standards on how cardholder data is handled and stored.

PCI requires that those businesses that process, store, or transmit cardholder account and/or transaction information adhere to its requirements. This includes all members, merchants, retailers, and payment service providers. Failure to comply with PCI and any subsequent

breach of card data within a merchant's site may result in substantial fines (up to \$500,000) and, potentially, the inability to accept card payments.

The PCI requirements apply to all "system components" which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including internal and external (web) applications.

- Basel II Capital Accord Compliance:

"...the Federal Reserve is committed to ensuring that the Basel II framework delivers a strong and risk-sensitive base of capital... we will remain vigilant in monitoring Basel II's impact on an ongoing basis."

Basel II, is also called "The New Accord" or the International Convergence of Capital Measurements and Capital Standards - Revised Framework. It is the second Basel Accord and represents recommendations from the Basel Committee on Banking Supervision (BCBS). It was created to promote greater consistency in the ways banks and banking regulators approach risk management across national borders.

The Basel Committee on Banking Supervision provides a forum for regular cooperation on banking supervisory matters. Over recent years, it has developed increasingly into a standard-setting body on all aspects of banking supervision, including the Basel II Accord.

BCBS's members come from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, United Kingdom, and United States. Countries are represented by their central bank and also by the authority with formal responsibility for the prudential supervision of banking business where this is not the central bank.

BCBS encourages contacts and cooperation between its members and other banking supervisory authorities. It circulates to supervisors throughout the world both published and unpublished papers providing guidance on banking supervisory matters. The Committee's Secretariat is provided by the Bank for International Settlements in Basel. The Secretariat is mainly staffed by professional supervisors on temporary

assignment from member institutions. The Bank for International Settlements is not a member of BCBS.

Within its three "pillars" of thought:

1. Minimum Capital Requirements;
2. Supervisory Review; and
3. Market Discipline

It addresses several key security requirements.

– Internal data

According to Basel II, the tracking of internal loss event data is an essential prerequisite to the development and functioning of a credible operational risk measurement system. Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes, and risk management procedures. Therefore, a bank must have documented procedures for assessing the on-going relevance of historical loss data, including those situations in which judgment overrides, scaling, or other adjustments may be used, to what extent they may be used and who is authorized to make such decisions. (Paragraphs 670 and 671)

A bank must develop specific criteria for assigning loss data arising from an event in a centralized function (e.g. an information technology department) or an activity that spans more than one business line, as well as from related events over time. (Paragraph 673)

– Disclosure

The Committee (BCBC) believes that providing disclosures that are based on this common framework is an effective means of informing the market about a bank's exposure to those risks and provides a consistent and understandable disclosure framework that enhances comparability. (Paragraph 810)

– Proprietary and confidential information

Proprietary information encompasses information (for example on products or systems), that if shared with competitors would render a bank's investment in these products/systems less valuable, and hence would undermine its competitive position. Information about customers is often confidential, in that it is provided under the terms of a legal agreement or counterparty relationship. This has an impact on what banks should reveal in terms of information about their customer base, as well as details

on their internal arrangements, for instance methodologies used, parameter estimates, data, etc. Banks should have a formal disclosure policy approved by the board of directors that addresses the bank's approach for determining what disclosures it will make and the internal controls over the disclosure process. In addition, banks should implement a process for assessing the appropriateness of their disclosures, including validation and frequency of them. (Paragraph 819)

Universities

- MIT
- Berkeley
- Carnegie Mellon
- KUL
- RWTH
- ...

(research) institutes

- SANS (SysAdmin, Audit, Network, Security) Institute
- ISSA (Information Systems Security Association)
- CSI (Computer Security Institute)

Certifying entities

- (ISC)2 (International Information Systems Security Certification Consortium)
- GIAC (Global Information Assurance Certification)
- ISECOM (Institute for Security and Open Methodologies)
- ISO/IEC certification bodies (LSTI, SNCH...)

Associations

- APWG (Anti-Phishing Working Group)
- ASC (Anti-Spyware Coalition)
- CAUCE (Coalition Against Unsolicited Commercial Email)
- ISACA (Information Systems Audit and Control Association)
- CLUSIx (CLUSIF, CLUSSIL...)

CSIRT community

- CERT-CC
- FIRST
- CERTA
- CIRCL
- CERT.RU
- ...

Last but not least ...

... there are the hackers!

10 OECD

In 2002 the OECD (Organisation for Economic Co-operation and Development) published a very interesting document on information security:

Guidelines for the Security of Information Systems and Networks: *Towards a Culture of Security*

It establishes 9 principles to be followed by all concerned entities with information security:

1. Awareness

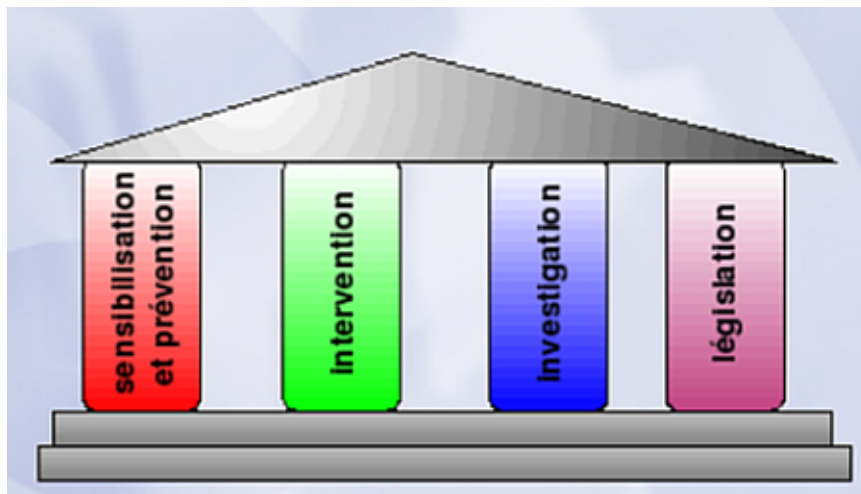
2. Responsibility
3. Response
4. Ethics
5. Democracy
6. Risk assessment
7. Security design and implementation
8. Security management
9. Reassessment

11 Case study: National IS strategy - Luxembourg

Goals:

- Promote e-services (e-commerce, e-government,...)
- Build a "culture of security"
 - Establish trust and confidence
 - Make aware of responsibilities
 - Reduce digital divide
- Enhance security of (critical) infrastructures

The strategy is based on four pillars:



1. Awareness and prevention
2. Intervention, incident handling
3. Investigation and repression
4. Legislation and standardisation

12 Bibliographic references

- Anonyme, 2001, Sécurité Optimale, Paris, Campus Press
- Blanchard P., 1995, Pirates de l'Informatique, Paris, Addison Wesley
- Bosworth S., Kabay M.E., 2002, Computer Security Handbook, New York, Wiley
- Carter D. L., 1992, Computer Crime Categories : How Techno-Criminals Operate, FBI Law Enforcement Bulletin
- Chatelain Y., Roche L., Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet, 2003, Paris, Maxima
- Donald L. P., Sécurité des Systèmes d'Information, Campus Press, 2000
- Dufresne D., Latrive F., 2000, Pirates et Flics du Net, Paris, Seuil
- Guisnel J., 1995, Guerres dans le Cyberspace, Paris, La Découverte
- Himanem P., 2001, L'Ethique Hacker et l'Esprit de l'ère de l'information, Paris, Exils

- Le Doran S., Rosé P., 1998, Cyber MAFIAS, Paris, Denoël
- Léopold E., Lhoste E., 1999, La Sécurité Informatique, Paris, Presses Universitaires de France
- Mé L., Deswarte Y., 2006, Sécurité des systèmes d'information, Paris, HERMES
- Levy S., 1984, Hackers : Heroes of the Computer Revolution, New York, Delta
- Linlaud D., 2004, Sécurité de l'information, Paris, AFNOR
- Longeon R., Archimbaud J-L., 1999, Guide de la Sécurité des systèmes d'information, Paris, CNRS
- Mitnick K., 2005, L'art de l'Intrusion, Paris, Campus Press
- Mounier P., 2002, Les maîtres du réseau, Paris, La Découverte
- Pansier F.J., Jez E., 1999, La Criminalité sur l'Internet, Paris, Presses Universitaires de France
- Peltier T.R., 2001, Information Security Risk Analysis, Etats-Unis, Auerbach
- Pipkin D., 2000, Sécurité des systèmes d'information, Paris, Campus Press
- Russel R., 2001, Stratégie Anti-Hackers, Paris, Eyrolles
- Service Centrale de la Sécurité des Systèmes d'Information (S.C.S.S.I.), 1994, La menace et les attaques informatiques, Issy-les-Moulineaux
- Franchin F., Monnet R., Le business de la cybercriminalité, Paris, Hermes Science
- Avoine G., Junod P., Oechslin P., Sécurité Informatique, Paris, Vuibert
- [CIA triad](#)
- [44 U.S.C § 3542 \(b\)\(1\) \(2006\)](#)
- [Admissibility, Authentication, Authorization, Availability, Authenticity model](#)
- [Parkerian Hexad](#)
- [ISO/IEC 13335-1](#)
- www.cert.org

- Official press release of its creation
- NSA
 - NSA surveillance octopus
- VPPA
- HIPPA
- GLBA
- FISMA
- SOX
- Patriot Act
- DMCA - Digital Millennium Copyright Act
- Gateway to the European Union
- eEurope and i2010
- ENISA
- The three pillars of the EU
- PCI
- Basel II
- Thèse "Les mondes de la cyberdélinquance et images sociales du pirate informatique"
- OECD
- Luxembourg's National NIS Strategy
- FNISA - ANSSI