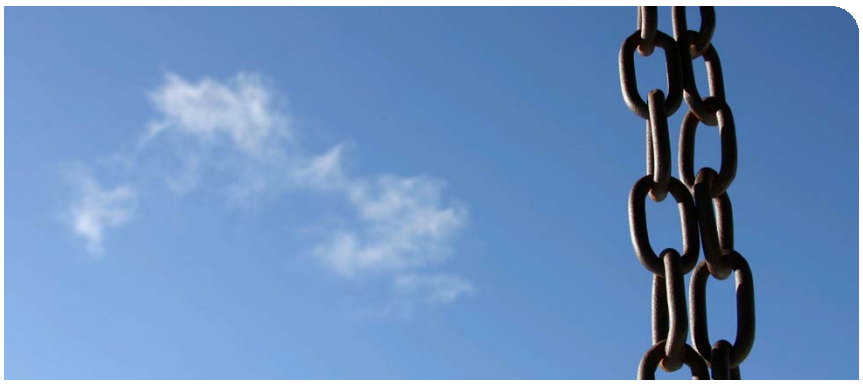
UNIL | Université de Lausanne



From risk management to information security policies and practices:
a multi perspective framework for ICT security effectiveness

Professor Solange Ghernaouti-Hélie

Member of the High Level Experts Group - Global Cybersecurity Agenda - ITU

Faculty of Business and Economics, University of Lausanne

| le savoir vivant |

ITU-T, April14th 2008
Geneva

Agenda

- ICT security context
- Security threats and cyber crime
- Cyber crime, types of offenses and challenges for
  - Citizen
  - Organization
  - State
- Why ICT security solutions can fall?
- Risk and security management
- ICT security effectiveness & conditions of success
- Global cybersecurity framework
- Capacity building and international cooperation for global cybersecurity
- Perspectives
- Global Cybersecurity Agenda (ITU – SG)

What is ICT security?

- Information and communication technologies security is an answer to the risks associated to the use of information and communication technologies (ICT) in every day activities

A wide range of issues

- Cybersecurity refers to information security issues for government, organization, individuals dealing with ICT technologies, in particular with Internet technologies

- ICT security - Information security – Cybersecurity deal with a range of issues as:
  - states' sovereignty,
  - national security,
  - protection of critical infrastructures,
  - security of material and immaterial values,
  - protection of personal data, …

Of which security are we talking about?

- Different perspectives of ICT security:
  - Could be related to fight against :
    - industrial and economic espionage
    - international terrorism or economic crime
    - manipulation of illicit contents or unauthorized use of resources
  - Could be related to:
    - computer surveillance and monitoring
    - tyrannical control & surveillance
    - the need to struggle for the respect of fundamental human rights
  - ...

Socio economic and political issues

- The question of cybersecurity can only be approached by insisting on the strategic dimension of ICT infrastructure and services for states sovereignty, organization competitiveness and safety of people

Who need ICT security?

- Each actor dealing with information and communication device, tool or service, for professional and/or private issues
  - Governmental institutions
  - Big and small organisations
  - Individuals
    - The security answer should satisfy particular protection and defence levels requirements, in regards of the actor's need

The human dimension

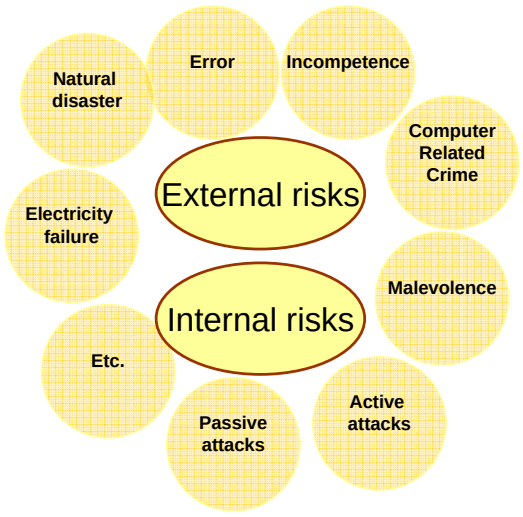
- Because human are the weak link of the security chain and because human is the final "consumer" of ICT service and infrastructures, any security solution should also take into consideration social needs
  - Need for an end-user centric security model

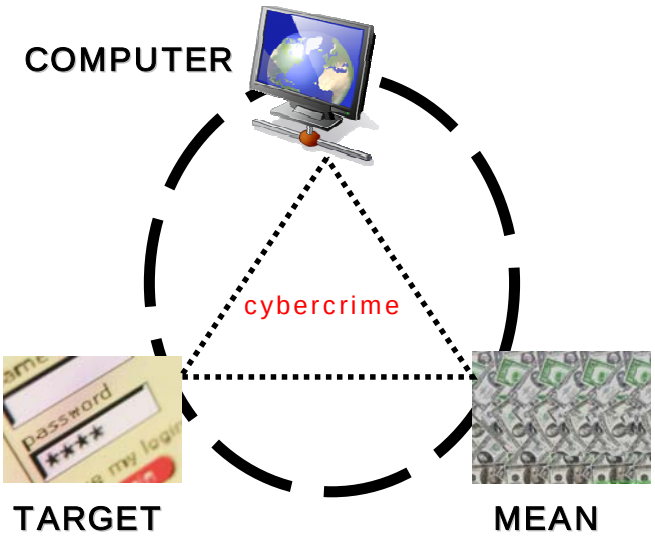
Cybersecurity is not only fighting against cybercrime

- Cybersecurity includes topics related to cybercrime issues and to potential ICT or security misuse

- Cybersecurity also concerns:
  - Producing secure, transparent and third controlling products
    - » Technologies should be less vulnerable
  - The development of a reliable and safe behaviour in regard of the use of ICT

Security threats and impacts





Cybercrime & and computer related crime:

technological crime
high – technology crime
computer and internet related crime
computer assisted crime
computer focused crime
digital crime
electronic crime
...

Computer crime:

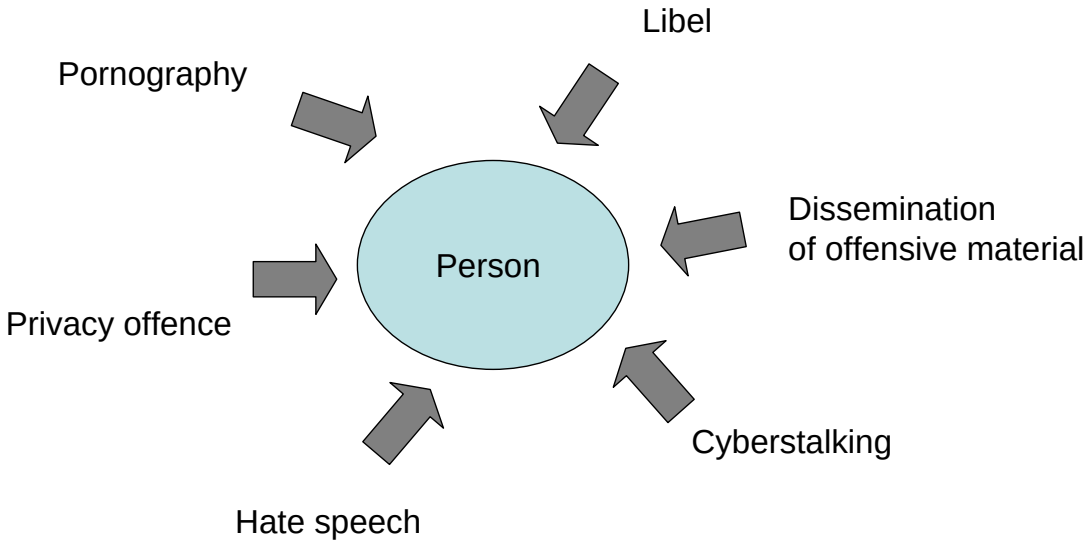
Crime where the computer system can be either:
- The object or the target of the crime (true computer crime)
- The means of committing the crime (computer related crime)
- Or both

In 1983, OECD defined computer-related crime as any illegal, unethical, or unauthorized behavior involving the transmission or automatic processing of data

Cybercrime - types of offences from The Organized crime situation report 2005 Council of Europe

- Offences against confidentiality, integrity and availability of information and communication infrastructures
- Computer related traditional crimes
- Content-related offences
- Offences related to infringement of copyright and related rights
  - Source: www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/8_Organised_crime/Documents/Report2005E.pdf

CyberCrime against persons



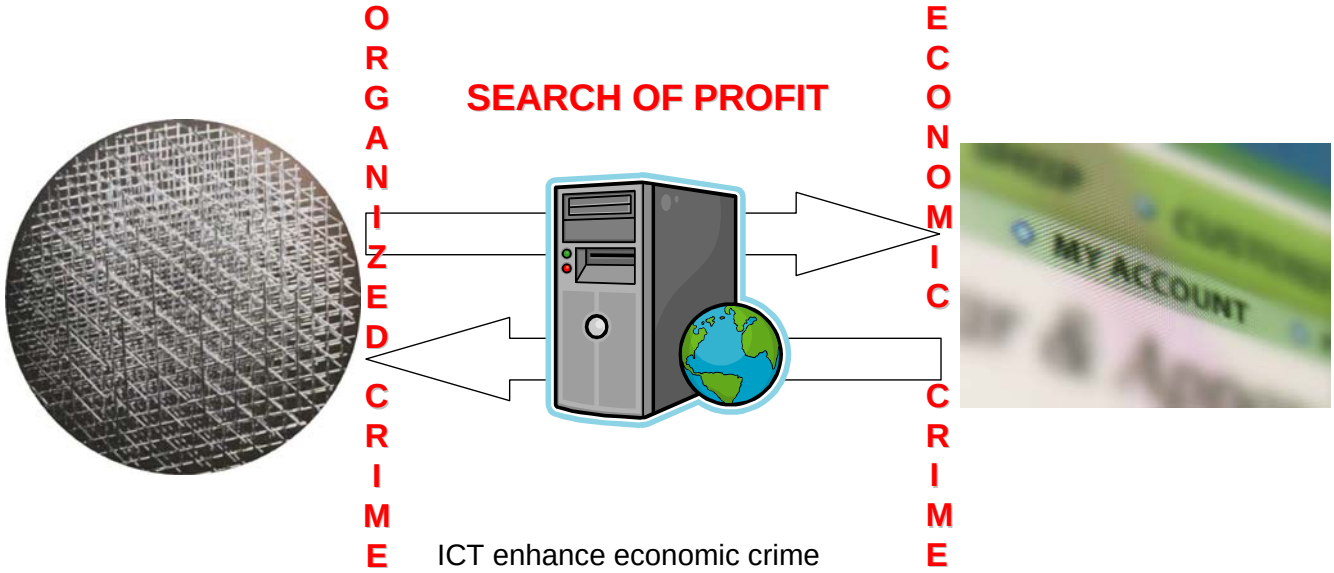
Challenges for citizen (i)

- Beyond security and surveillance
  - Privacy issues
  - Needs to privacy and security are not yet well identified and satisfied for individuals and also for enterprises
  - Technologies don't preserve, in native mode, user's privacy
    - Privacy in the cyberspace looks like a luxury!
    - Most users give preference to ICT services (GPS, mobile phone, service personalization, commercial services, security services ...) than to privacy protection
  - Illegal monitoring, illegal data obtaining and identity thief are a major concern for the end-user

Challenges for citizen (ii)

- Service availability
- Service & cost effectiveness
- Personal data protection
- Confidence into immaterial actors and resources
- Children protection
- Effective privacy and security solutions will contribute to obtain confidence into information and communication technologies

Economic cybercrime and Crime against assets



ICT enhance economic crime
And are a performance tool for organized crime and terrorism

Typology of crime against assets

- Theft of resource, service, data
- Fraud and swindle
- Blackmail and cyberextortion
- Unauthorized or illicit systems access (Spam, virus, etc.)
- Piracy and fraudulent acquisition of intellectual property
- Surveillance, espionnage, and information manipulation
- Money laundering

Challenges for organization

- Competitiveness and durability
  - Risks assessment, evaluation & mitigation
  - ICT security governance
    - Security policy and procedures
    - Security assurance
  - Legal conformity
    - Data protection laws, specific regulations, …
  - Security implementation
    - Identity management, authorization mgt,
    - Wireless security
    - Intrusion detection
    - Telephony security
- Business continuity
  - Crisis management & disaster recovery
- Keep security simple, effective, up to date:
  - Material and immaterial assets (resources and processes) protection
  - Image and reputation protection
  - Cost effectiveness

Cybercrime against institutions and state

- Information manipulation surveillance, espionage
- Hacking governmental website
- Hacking critical infrastructures
- Cyber threats against States
- Information warfare
- Environmental risk
- ...

Challenges for state

- State sovereignty
  - National security
  - Information warfare
  - Protection of critical infrastructures
- State reputation
  - Avoiding digital paradise
  - Citizen confidence
- Economic development
- Citizen protection
  - Social Control & surveillance
- E-government efficiency
- Fight against cybercrime

Multiple domains of ICT security

- At the crossroads of technological, legal, sociological, economical, and political fields, ICT security is interdisciplinary by nature
- ITC security must:
  - Reflect, depending on the country, the vision, culture and civilization of a nation
  - Meet the specific security needs of the local context in which it is introduced

Local & Global ICT security policy

- Security is strongly linked to local culture, ethic, politic, law, as to say to specific national environment
  - In a interconnected global information society, cybersecurity should answer the challenge to be locally significant and efficient for a particular national context and interoperable and compatible at the international level
  - Cybersecurity cannot be considered beyond its field of application and socio-cultural environment

Everlasting evolution of IT security

- While evolving from the technical field to the management field, ICT security concept gave way to technological and informational risk management
  - Cf. the adoption of international standards concerning security and security management (ISO 17799 and ISO 27000 standards families)

ICT Security management is not enough

- Security management cannot overcome failures due to design problem or criminal misuses of ICT infrastructures
  - The whole issue of ICT security management is:
    - Organizing protection and defence of values
    - By taking into account
      - the intrinsic vulnerability of information technologies
      - the criminal threat in institutions' strategies

Legal dimension of ICT security is becoming significant

- ICT security technologies and management do not make it possible to completely avoid incidents:
  - "Zero risk" doesn't exist
  - Responsibility issues become central with regard to information security
- This contributed to moving out the border lines of management security towards legislation
  - Thorough knowledge of new technology-related laws becomes a necessity, and the law must be borne in mind when installing security solutions.
    - Legislation becomes an endogenous factor when considering security

From management to legal considerations

- ICT security is not just a cultural problem that has a technology dimension.
- An adapted legal framework and laws that are applicable to the digital world must be operational at the national level and internationally compatible
  - An enforceable legal framework should exist and criminal laws should be updated to adequately cover extensive use of data processing and telecommunications
    - Nowadays there seems to still be a general lack of coordination and harmonization of legal frameworks at the international level
  - Security requirements should not make the Internet and information technologies an excessively controlled territory, because misuse which may undermine basic human rights then becomes an issue

From legal considerations to justice system

- Justice system representatives, the police force, investigators and lawyers must be trained to deal with acquisition, preservation, analysis and interpretation of digital evidence

Why ICT security solutions can fall?
A « tool » perspective

- Most of actors think about tools only, not about tools, process and management
- Tools can have security breaches and can be bypassed…
- Tools offer a static and specific answer to a dynamic and complex global problem

Why ICT security solutions can fall?
A « legal » perspective

- Most often, legal provisions have been specified without fully integrate the user's point of view and the technological, managerial or economic security related issues
- There is no clarified share of responsibility and it is easier to shift the security responsibility to the end-user

Why ICT security solutions can fall?
A « market » perspective

- International security standards or recommendations exist but are not implemented
- ICT products design and distribution do not put sufficient importance into security
- Users must rely on products and mechanisms they cannot master
  - Security is done by obscurity
- No one wants to support the security cost!

Who is responsible for ICT security ?

- In a context of pervasive computing and ICT dependency each actor, at his level, is responsible for ICT security
- It is everyone's responsibility to promote a safe and reliable cyberspace environment in the context of information society
  - A minimum level of security for information and communication technologies must be provided at an affordable cost
    - Security must not become an exclusion factor!

A systemic approach & framework

- A systemic approach concerns all actors of the information society:
  - all kind of end users (including children)
  - technologies, services or contents providers and professionals,
  - policy makers
  - organization's owners, shareholders, managers
  - justice and police professionals as judge, prosecutors, law enforcement people, …
- A systemic security framework should include:
  - political, social, economical and technical dimensions of cybersecurity

A global approach

- Global imply the necessity to think cybersecurity in terms of:
  - Efficient ICT use
  - Know how sharing
  - Collaboration
  - Cooperation
  - Global cyberculture

Global Cybersecurity framework

Global Cybersecurity framework for … policy makers

- Measures to understand:
  - Links between social and economic development
  - ICT related threats and risks for states, organizations and citizens
  - Needs for protection at national, regional and international levels
  - The role of all relevant stakeholders and their relationships
  - General measures to be taken to obtain a satisfying level of ICT security and protection assets (including privacy issues)
  - How to build a global cybersecurity culture based on well recognized international standards and recommendations
- In order to
  - ➢ be able to define national cybersecurity strategies and policies

Global Cybersecurity framework for … justice and police professionals

- Measures to understand:
  - Legal requirements at national and international levels
  - Laws are not enough to unmask cyber criminals

➢ In order to:

- Define a legal framework enforceable at national level and compatible at the international level
- Develop measures to fight against cybercrime and to collaborate at international level

From digital traces to criminal identification: a difficult and complex process
Computer investigation & Digital evidence

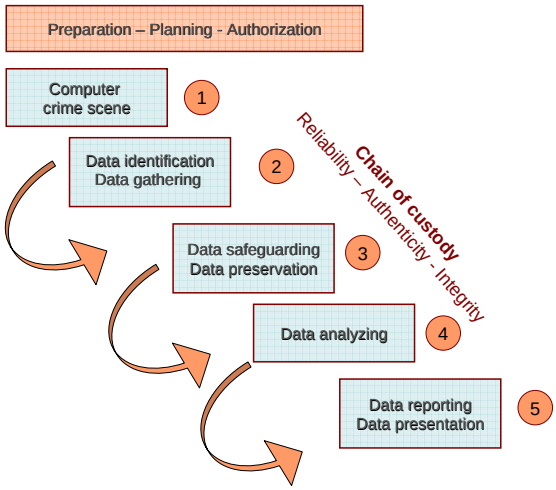
- How to identify the relevant data?
- How to trace them?
- How to store them?
- What are the judicial rules of evidence?
- How to recover files that have been deleted?
- How to prove the origin of a message?
- How to establish the identity of a person on the basis of only a digital trace?
- How to establish the conclusiveness of digital evidence in establishing the truth before a court (concept of digital evidence),
- Etc.

Collecting evidence

- Collecting evidence during a computer investigation face several technical problems that requires formalized procedures and specific technological tools

Searching for evidence & chain of custody

- Chain of custody: To be effective and relevant as a proof element for a legal proceedings and to pursue a criminal, digital evidences and its collect, have to be of high quality



Computer Crime Investigation Methodology

Global Cybersecurity framework for … executive managers

- Measures to understand basic principles in ICT security management
  - Assessments of vulnerabilities and threats
  - Security mission, management practices and conditions of success
  - How to identify valuable assets and related risks?
  - How to define security policy?
  - How to manage security in complex and dynamic environments?

➢ In order to be able to
- ➢ Produce effective security process and master ICT related risks and security costs
- ➢ Collaborate with legal, law enforcement and technical professionals
- ➢ Create appropriate organizational structures and procedures

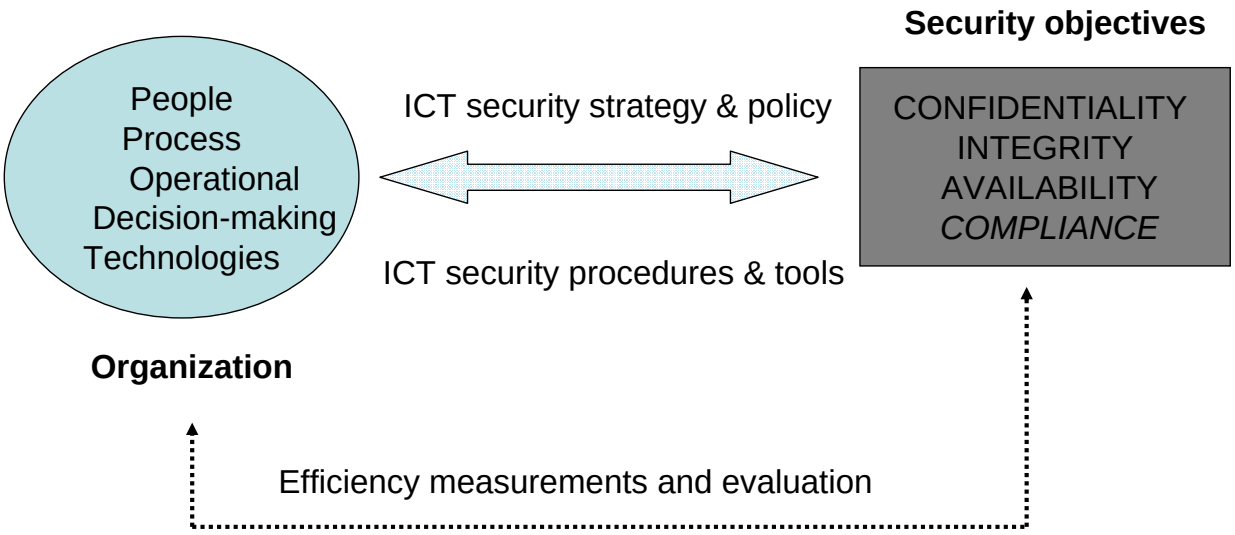
Information Risk Management

- Informational Risk Management is becoming integrated into the overall organization Risk Management program

Information Security Management System

- Need to measure effectiveness and efficiency of the Information Security Management System
  - Need for efficient measurement and metric framework for decision making optimization

Information Security Management System



Global Cybersecurity framework for … information and communication technologies professionals

- Measures to understand:
  - Societal and organizational issues and values
  - ICT related risks
  - Master ICT and security technologies in digital environments

➢ In order to:

- ➢ Define, design, produce, implement efficient security tools and measures of protection and reaction
  - ➢ Cost effective
  - ➢ User friendly (ease of use)
  - ➢ Transparent
  - ➢ Auditable
  - ➢ Third Party Controllable
- ➢ Reduce the volume of data collected without user's consent
- ➢ Prevent the no authorized use of data or resources
- ➢ Decrease the number of vulnerabilities in digital environments

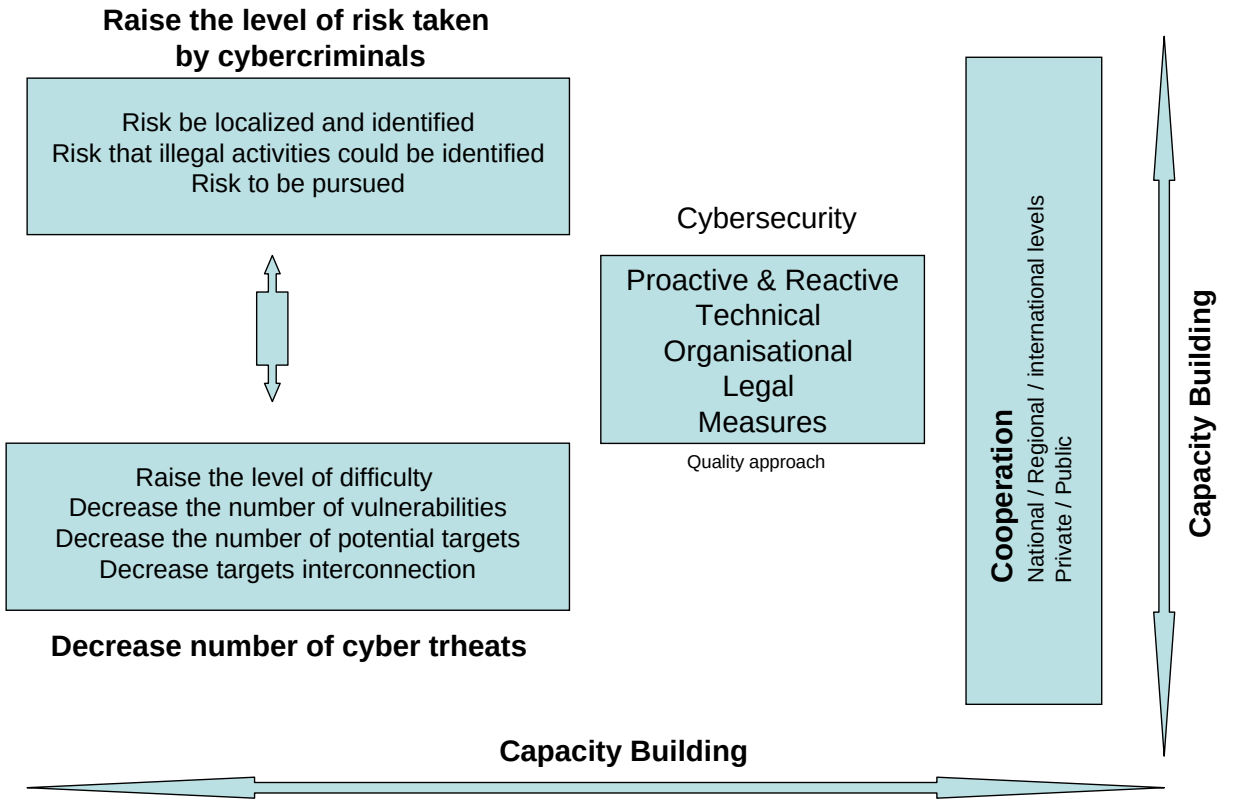
Global Cybersecurity framework for … end-users and citizens

- Measures to understand:
  - Threats for the end-user (virus, spam, identity usurpation, data protection, privacy issues…) and their impacts
- End-user should apprehend how to:
  - Adopt a security behaviour for ICT
  - Know how to use security solutions & use them
  - Do not expose personal data
  - Limit frauds
  - Avoid criminal contact and proximity
  - Prevent ICT addiction

➢ In order to
  - ➢ Raise awareness and efficient behaviour
  - ➢ Find right compromise between privacy and security needs
  - ➢ Master digital identities
  - ➢ develop and maintain confidence trough cyberspace

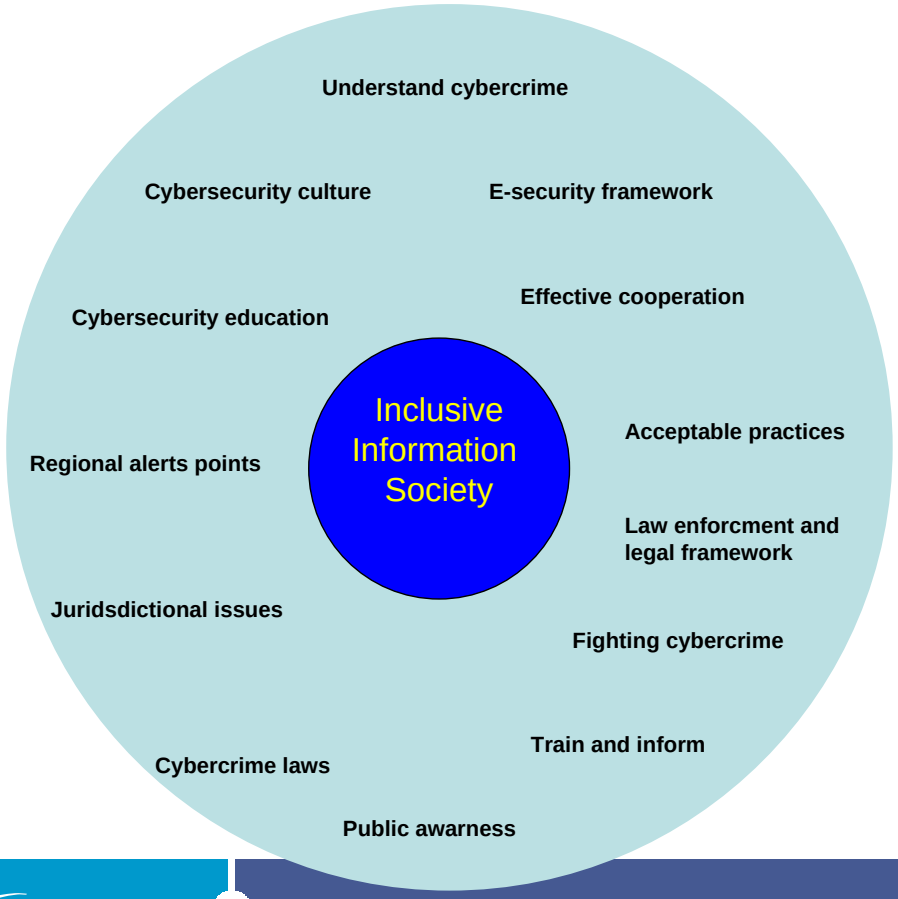
Capacity building for global cybersecurity

- Understanding of the role of cybersecurity's actors
  - Including their motivation, their correlation, their tools, mode of action, …
  - The actors can be classified into :
    - The protector (private and/or public institutions)
    - The one to be protected (the individual (citizen), the organisation and the State)
    - The criminal (professional or not)
- Understanding of the four generic relevant security functions of any security actions
  - Pro-active measures
    - Intelligence gathering
    - Preventive actions
    - Repressive actions
  - Reactive measures
    - Crisis management and recovery actions



For an inclusive information society

- An inclusive society would avoid pitfall as digital paradise or digital security exclusion
- The individual should be at the heart of the ICT security question, to help realize a conscious and inclusive information society



ICT security for developing countries

- Digital divide should not be double by a security divide
  - ICT security constitutes a driving force for the economic development of regions and must be carried out simultaneously with ICT infrastructure
  - Security needs should be answered at the same time than ICT development
- If developing countries become digital paradises or the weak link of the international security chain, that will effect the overall and global cybersecurity level

Main points to sustain ICT security effectiveness

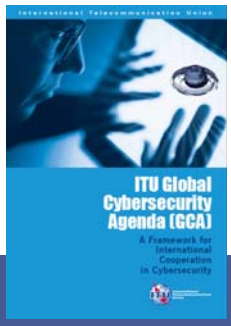
- Understand ICT Risk
- Develop public awareness
- Promote a cyber security culture
- Train and inform
- Establish private and public partnership
- Develop acceptable practices for IT protection and reaction
- Propose a unified e-security framework
- Create effective cybercrime laws
- Create regional alert points
- Manage jurisdictional issues
- Fight cybercrime
- Redefine law enforcement and legal
- Establish effective cooperation and promote cooperation and coordination
- Force information technology and content providers to improve the security of their products and services

Perspective

- There is no real technical obstacle to further global cyber security development
  - The scope of deployment of effective local and international security services is very complex
  - Technical, managerial and organizational related costs are not minor
  - Business, financial and organizational models are to be found to support effective deployment of security

ITU – SG
Global Cybersecurity Agenda initiative

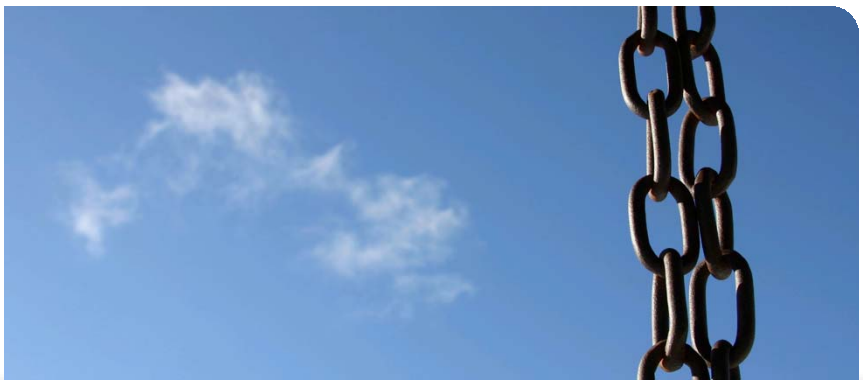
- **An international framework for Cybersecurity:**
  - **ITU's Global Cybersecurity Agenda**
    - The Global Cybersecurity Agenda website http://www.itu.int/cybersecurity/gca/
    - Questions, concerning the Global Cybersecurity Agenda
    - Please contact ITU at: **gca@itu.int**
  - "Adoption of international approaches, standards, regulations, best practices … applicable at national, regional, levels and compatible at the international level will contribute to build a global response for a safe and global information society"



The trust challenge

- Security and trust are relative notions but they are critical factors of success and business enablers for developing the information society
  - The underlying problem is to be found at the level of security and confidence offered and guaranteed through access, services as well as by information and communication technologies providers
- *"Who controls infrastructures, access, use, service, content and security?"*

UNIL | Université de Lausanne



Thank you for your attention

sgh@unil.ch
www.hec.unil.ch/sgh/

| le savoir vivant |