Increase trust and confidence in information and communication technologies by a multidisciplinary approach

Professeur Solange Ghernaouti-Hélie [1]

Ecole des HEC de l'Université de Lausanne - Suisse

La confiance accordée aux technologies de l'information et de communication est un facteur essentiel, nécessaire pour la transforation des marchés électroniques en environnements efficaces dans le cadre du e-business.

Cet article analyse comment le cyber-crime et l'e-insécurité affectent l'économie globale et comment le développement et l'acceptation globale d'un cadre international d'e-sécurité contribueront au déploiement de la société de l'information. La validité d'un tel modèle exige une approche multidimensionnelle et novatrice de l'e-sécurité. Des recommandations sont données afin de guider la conceptualisation d'un cadre unifié d'e-sécurité, précisant sa dimension multidisciplinaire pour imposer la confiance accordée aux TIC dans un contexte international.

Trust and confidence in information and communication technologies are key factors to transform electronic markets place in effective environments to do e-business and e- activities.

This paper analyses how cyber crime and e-insecurity affect the global economy and how the development and overall acceptance of an international e-security framework will contribute to the deployment of the information society. The validity of such model requires a challenging multidimensional approach of e-security. Recommendations are given to guide the conceptualisation of an unified e-security framework, pointing out its multidisciplinary dimension to enforce trust and confidence in ICT in a international context.

1 Directrice de l'Institut d'Informatique et Organisation
Vice – Doyenne de l'Ecole des HEC
Ecole des HEC – INFORGE - Université de Lausanne
CH – 1015 Lausanne
Tel : +41 21 692 34 21 - Fax : +41 21 692 34 05
Courriel : sgh@hec.unil.ch - Site web : http://www.hec.unil.ch/sgh/

INTRODUCTION

Information and communication technologies become a new kind of mediators for the information society and knowledge economy.

These technologies must be :

- Accessible ;
- Timely useable (timeliness) ;
- Interoperable ;
- Scalable and flexible ;
- Affordable ;
- Open to party control ;
- Trustworthy.

Doing activities with information and communication technologies suppose that three major issues have been resolved.

First, network infrastructure must exist, be accessible, available, reliable and secure. Networks must offer as much bandwidth as necessary to support user's activities.

Systems and network management approaches and solutions could contribute to achieve this issue. Moreover, the cost of use must be in correlation with the performances and quality of services obtained. That supposes a valid underlying economical model and an effective cost management process.

Second, contents and services must answer the user's needs in term of quality, integrity, confidentiality and accessibility. That could be achieved trough improving quality and security of software development, reverse engineering processing and by management. As previously, cost must be effective.

Third, a consistent international well-known regulatory framework must have been defined. Responsibility of each actor involved in e-services delivery must be clarified. An enforceable legal framework had to exist to constraint actors of the digital world to support mechanisms that guarantee e-privacy and e-security. That will contributes to develop the information society.

SECURITY, PRIVACY AND TRUST ISSUES AND CHALLENGES

Based on Oxford Dictionary definition, the privacy is *« the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion »*. The free and unsupervised use of information and communications

technologies means confidentiality and integrity of data and flow, without active or passive listening. In digital environments (digital information, dematerialization of actors, computers and networks operating mode), technologies don't preserve, in native mode, user's privacy. To give only one example, an Internet Service Provider (ISP), has the opportunity to check traffic, emails, files, etc. which go through its infrastructure. This affects everyone privacy over the Internet.

Copy, logging, eavesdropping, are easy to realize. Network analysis traffic, actives auditing, intrusion detection systems, firewalls, etc. contribute to optimize network performances and security. In the same time, they can damage privacy of the user. The availability of management tools as protocols analyzer, associated to the exponential uses of e-services and to the number of 800 millions of Internet users estimated nowadays, emphasizes the importance of privacy needs over the Internet.

The majority of the Internet actors want to ensure that personal information is not abused and their right to privacy is protected. Nowadays, the need to privacy is not yet well identified and satisfied. *« In developing countries, human rights organizations understand the need for privacy but do not have the technology. Those in developed countries have the technology but do not think they need to protect privacy*[2]*»*. Digital traces are generated by any e-activities. They can be stored and handled on a legal basis or not. Justice and police investigation, computer forensic as commercial and marketing purposes or state and government policies could take advantage of personal data linked to digital traces to achieve specific objectives. Furthermore, illegal monitoring, illegal data obtaining and identity thief are a major concern for computer related crime. Therefore, technologies such as the Internet, sensors, global positioning systems (GPS), biometrics, smart durst, cameras and microphones, etc., are all around us. Pervasive computing is a reality. As IT resources continue to propagate and to be interconnected, it will become possible to gather information about virtually everything and everyone, anywhere and anytime. Therefore, privacy issues are becoming a major concern for information society citizens.

The privacy on the World Wide Web is a major issue. In September 2000, AMAZON has declared that its customers' data are intangible assets comparable to others.

Nowadays, data confidentiality and privacy protection are achieved in a no transparency way to the end user. Moreover, when a website requires personal information from an Internet user, it is not evident what will

[2] Robert Guerra, Managing director of Privaterra The pan European ministerial conference of the World Summit on the Information Society. Bucharest. (November 2002)

happen to that information. What websites will do with that information is not obvious. Will they share it with other entities ? And, how long they keep it ? Users cannot easily see or understand the role of cookies and the information gathered by them. Most often, cookies invade user privacy in a way or another. Users need to understand what cookies are used for and what means regarding their personal information. To satisfy users concerns, websites try to make their practices more transparent. But many privacy policies are models of legalistic complexity, while others have so little information as to be almost useless. Consequently, website privacy policies do not serve their goal of letting Internet users be informed about how their personal information is used.

It is not enough to promote development of connecting points to the Internet for accessibility. The information infrastructure must be reliable. Had hoc performances, services continuity and quality of services as quality of data must be guaranteed.

User's confidence in information and communication technologies will be achieved by addressing in complementary way: security and privacy protection issues.

The underlying problem lie on the level of security and trust offered and guaranteed by access, services and information and communication technologies providers. That could be sum up by the question: who controls infrastructures, accesses , uses, contents and security ?

Nowadays, security is done by obscurity.

E-security and e-privacy would contribute to define a trusted digital environment.

Effective privacy and security solutions will contribute to obtain confidence into information and communication technologies.

The notion of trust is central for computer security and does not rely only on technology tools. If trust is well placed, any system could be acceptably secure. If it is misplaced, the system cannot be secure. Security is a relative notion but security and trust are critical factors of success and enablers for the information society.

INFORMATION TECHNOLOGIES RISKS AND SECURITY THREATS

Focusing on security within open environments means to define the targets of threats. Without doing a risk analysis survey, the main targets of security threats are : end-user, network access point, network and all the infrastructures connected to the network as servers and information systems.

ICT dependency and vulnerability

Information and communication technologies are not reliable and not secure. Sources of vulnerabilities of the Internet are known. Multiple threats can occur at the environmental, physical, logical, informational and human levels.

Existing security technologies are fallible or could be circumvented, moreover it is difficult to define and support an effective security management process.

As the Internet as grown, so has connectivity, enabling also attackers to break into an increasing numbers of systems.

This is possible because more often non-secure systems are used and most systems cannot resist a determined attack if there are not well protected and monitored. Public attack tools are available. Security solutions or patches are not implemented. Management procedures and controls or system configuration and administration are defective. Human weaknesses are a reality.

A lack of an overall, global consistent and dynamic security approach and a lack of a good software development and implementation quality exist.

Opening computers and information resources through Internet, imply increasing dependency and vulnerability, so doing activities over the Internet is risky. Organizations and individuals can be hit by e-insecurity.

Cyber crime impacts

The negative impacts of security threats will affect not only systems or individuals actors but in a chained way organizations and society. Cyber crime is a reality. Usual criminals have gained new capabilities and e-delinquency could impact the economic actors. For example, economic crime can be enhanced such as: information warfare, competition distortion, internal theft, stock exchange influence, accountability unfairness, money laundering, etc. The market regulation can be weakened because traditional law enforcement is less effective, economic advantages can be given to unfair competitors, enterprise competitiveness can be reduced or cancelled by unfair information access.

The growing strength of criminal organizations that caring out large scale information technology crime is alarming.

Nowadays, cyber-criminal, hacker or cracker, what ever we call them, represent a real threat to the society, causing malicious harm to ICT resources, to individuals, organizations and states.

By their capacities to intercept data, to introduce into systems and access to data, cyber-criminals are able to affect users' privacy and business activities. Personal information, addresses, financial information, account information, passwords, etc. are precious targets for cyber-criminals that could use them to perform illegal actions.

« Identity theft round out the top seven categories of complaints referred to law enforcement during the year[3]*»*. The federal trade commission has reported in January 2004 that ID Theft Tops List of Costly Fraud Complaints. Identity theft and fraud cost Americans at least $437 million in 2003. Identity theft complaints numbered 215,000 reports, marking a 33 percent increase over the year before. Half of those who filed reports lost less than $228. The average incident cost Americans $1,868 because of a few large losses ($1 million-plus). The number of Identity Theft Complaints Registered by the U.S. Identity Theft Clearinghouse between 1999 and 2003 are as shown[4] on table 1 :

TABLE 1
The number of registered identity theft per year

Year	Number of registered Identity theft (in millions)
1999	1.4
2000	31.1
2001	86.2
2002	161.8
2003	210

The identity theft has increased in an exponential manner. The registered number of fraud in 2003 is about the quarter of the total number of the Internet users. This phenomenon cannot be ignored and will continue to be amplified since no action is taken to protect and to dissuade. The most utilized method to carry out such robberies is Trojans. Trojans are a kind of virus that can be hidden inside executables files (like mp3 songs, free games, pictures, movies). Once the file holding the virus is executed, the Trojan could provide information to the cyber-criminal in a transparent manner to the user. Most often, the Internet users have no idea that their private information has been stolen. This information could be used to perpetrate criminal actions. A stolen identity user is responsible of malicious activities that he didn't perform ! In this context,

[3] IFCC Annual Internet Fraud Report http://www.ifccfbi.gov/strategy/statistics.asp
[4] Source: Federal trade commission. September 2003.

he has to prove his innocence, which is difficult, even impossible without any help.

The fact that security solutions cannot guarantee privacy protection induces crucial consequences not only to the end users but also for overall organizations and society.

Computer related crimes are becoming significant. Old crimes are performed with new technologies and these ones induce new crimes ! Individual criminal as organized crime take advantage of Internet facilities. Police investigations in information and communication environments are more and more necessary and frequent. It relies on computer forensic and digital traces analyses that constitute an emerging scientific police specialization. This involves information gathering and flow and data monitoring. These processes must be well mastered and controlled in accordance of democracy principles. They raise privacy issues and need to be integrated in an appropriate legal framework, which must be enforceable, both at national and international levels.

SOME UNSATISFIED SECURITY NEEDS

E-security fundamentals are well known : availability, confidentiality, integrity, authentication, and non-repudiation. Master technological and informational risks have to be done in allowing an efficient use of information and communication technology, and also allowing privacy in respect of fundamental human rights.

Difficulty to secure dynamic and complex environments

Information and communication technologies form complex environments. It is complex because several independents and correlated infrastructures constitute them : human infrastructure, software, data, application infrastructures, hardware infrastructure, network infrastructure, maintenance infrastructure and environmental infrastructure. Each one is dynamic and can evolve separately, has its specific vulnerabilities, security requirements and its particular security solutions.

Moreover, security solutions have they own life cycle including several stages : risks analysis, policy specification, security implementation, maintenance, evaluation and optimization.

In this context some unsolved questions are raised, with no clear answers today, among them :

– How to obtain a minimum certified security level for each infrastructure ?

– How to obtain a certified global and consistent security level ?
– What can be certified ?
– What will be the validity of a static certificate in a dynamic environment ?
– What would be the dynamic certification process able to realize and to guarantee certification in a dynamic environment ?
– Who will be the certified authority (or authorities) authorized to deliver such certification at an international level?
– Who will control and manage certification processes, certification authorities and certificates ?
– Who will paid for certification ?
– Etc.

Lesson from the past

A wide range of stakeholders and players is present on the market such as : engineers, architects, developers, integrators, system administrators, managers, officers, lawyers, auditors, investigators, suppliers, manufactures, providers, clients and ends users.

Each one has diversity of interests, visions, solutions and languages. This reflects the evolution of the perception of handling security issues but does not lead to a better resolution of these issues.

Security is becoming more and more complex. From an historic perspective, security has been handling only through its technological dimension, and then others as managerial or legal dimensions have been taken into consideration. That is a good point, but the fact is, that they have been taken into account in an independence way instead of, a systemic and multidisciplinary approach.

More often we dispose of inefficient solutions, which introduce new weaknesses and vulnerabilities, or shift the responsibility of the security on others actors or entities, and produce a false sense of security.

Security solutions exist but are inefficient because :

– We think about tools only, not about tools, process and management ;
– Tools are not enough simple and flexible ;
– Tools offer a static and punctual answer to a dynamic and global problem ;
– Security international standards or recommendations exist but are not implemented ;
– There is no clarified share of responsibility and it is easier to move the responsibility of the security to the end-user ;
– Lack of training and competencies ;

– End-users have not an e-security culture ;

– Legal dispositions have been specified by people that does not fully integrated the user point of view and the technological, managerial or economical issues (mainly because it is too complex) ;

– No one wants to support the security cost.

The real challenge is to keep simple security handling.

That means that the security responsibility must be well defined at national and international levels and that security solutions must be :

– Transparent and cost effective for the end – user ;

– Cost - effective for the organization ;

– Enforceable for the regulator ;

– Flexible for information technologies provider.

Without offering simple and clear answers to this needs, e-security will remained an abstract concept of no use.

MULTIDISCIPLINARY ANG GLOBAL APPROACH

Security issues and stakes are human, technological, economical, legal and political.

Security tools can't replace an ethical behaviour and codes of conduct and an appropriate legal framework.

2002 OECD guidelines on the security of information systems and networks are a starting point to take into consideration security issues. But security is not only a cultural problem that has a technological dimension.

It is also a regulatory problem by the fact those technologies :

– Have become news kinds of mediators, which cannot be ignored at the individual, enterprise, organization or society levels ;

– Are used to conduct criminal behaviours ;

– Are the targets of criminality actions.

E-security issues from a user point of view

Security rules and tools must be usable and cost effective. That means that security mechanisms must be :

– Readily understood ;

– Configured with a minimum of effort by untrained users ;

– Designed with the right balance between efficiency, configurability, usability and costs.

Needs of awareness rising about risks assessments and risks management Needs of culture and education are real.

E-security issues from a managerial point of view

Information and communication services must be based on the use of secure systems, certified products and services.

That means to enforce use of standardized and certified solutions. ISO 15408 (Common Criteria) seems to be the best way to strengthen the fairness of the security market and that effective security offers exist.

Information technologies managers have to :

– Consider security as a permanent process that take into consideration resources, costs, and processes optimization within a risk management framework ;

– Define specifics security policies to support business activities (security reference model) and a crisis management policy (back-up solutions) ;

– Configure and manage hardware and software securely ;

– Be aware of they own penal responsibility in cases of major security incidents or crisis ;

– Develop information assurance and legal conformance ;

– Manage human resources (check personal background, define responsibility).

E-security issues from a technology point of view

To answer the need of monitoring and reaction, auditing mechanisms should be designed into critical systems. These mechanisms may report violations of a defined policy or actions that are considered to be security threats. The use of strong identification and authentication solutions, operational cryptographic mechanisms and one-time password are hardly recommended. Automated or semiautomatic techniques for guiding the selection of mechanisms for enforcing security policies and rules previously defined have to be designed. When necessary, certified and recognized third party authorities that have a regional, national and international recognition could be used. That means that such authorities exist with defined collaborative rules between them.

It is not necessary to define more security standards, but to promote certification processes by public institutions, based on the International Standard ISO 15408 - Common Criteria. That seems to be the best way to strengthen the fairness of the security market. Certification processes should be adapted to be more accurate for dynamic environment like Internet. Certified e-security solutions must be supported in a native node by information technologies.

Security can be improved by :

– Monitoring vulnerabilities and security solutions ;
– Finding computer and network security flaws ;
– Avoiding single points of failure ;
– Having an adaptability defensive mode.

E-security issues from a legal point of view

Law, legal institutions must exist to dissuade criminal behaviors and to pursue people who act in illegal ways.

Security solutions can protect a given environment in a particular context, but cannot prevent criminal behavior.

More often, computer and cyber crime are poorly pursued because :

– They can be automated, software embedded, and remotely realized ;

– The transnational dimension of that kind of crime requires an international and cooperative judicial system ;

– Criminals can also use someone else identity making their identification difficult ;

– It is difficult to qualify the facts ;

– Crime and evidence are related to immaterial resources.

A regulatory framework must be enforceable and effective both at the national level and at the international level. It had to be defined and supported by governments.

E-security from a market point of view

Technologies must have reduced vulnerabilities and improved quality and security code. The market must increase product liability, take into consideration the mobile world and must enforce authentication and privacy.

Only a parallel development of security control and privacy protection will allow confidence into information and communication technologies and in e-activities or e-transactions.

Market forces do not drive sufficient investment for :

– Users and contents identification and authentication ;
– Watermarking and fingerprinting ;
– Digital signature ;
– Public Key Infrastructure ;
– Tracking ;
– Confidentiality and Privacy management ;
– E-transaction payment ;
– User interface.

CONCLUSION AND RECOMMANDATIONS

There is no real technical obstacle to further development of e-security but the scope of deployment of effective local and international e-security services is very complex and the technical and management costs are not trivial.

Private and public partnership is desirable on a National, European and International levels to integrate security into infrastructures and to promote security culture, behaviour and tools .

Business, financial and organizational models are to be found to support effective deployment of security that could benefit to each one.

It is fundamental that the international community :

– Propose a unified e-security framework which take into consideration, in a complementary way the human, the regulatory, the organizational and economical, the technical and operational dimensions of e-security ;

– Promote an e-security culture (information on stakes and risks, diffusion of simple recommendations as for example: use secure systems, reduce vulnerability in avoiding dangerous situations or behaviours, etc.) ;

– Train and inform on security, privacy or data protection issues, existing solutions, legal dispositions, etc. ;

– Train and inform on information and communication technologies;

– Force information technologies and contents providers to improve security of their products and services ;

– Products or services must integrate in native simple and flexible security measures and mechanisms; they must be well documented and comprehensible (security mechanisms must be readily understood and configured easily by untrained users) ;

– Security must not be considered anymore as an option. As we trust in air transportation (in these contexts security is not an option for fortunate passengers), we must have confidence into information technologies ;

– Techniques must be defined to guide the selection of mechanisms that enforce a security policy ;

– In integrating at the beginning of their products development life cycle security processes, measures and solutions.

E-privacy stakes couldn't be dissociated of e-security stakes. Concrete, simple, efficient, flexible, comprehensible measures must be given to contribute to build confidence into information and communication technologies and services. This constitutes major

challenges for the XXI century for transforming our society into a safety information society.

Many stakes and challenges are related to users' privacy over the Internet. The basic rights of privacy must be respected and guaranteed to all users wherever they are located.

Effective e-security and e-privacy solutions should be implemented in information technologies resources in order to provide the minimum confidence level mandatory for an effective digital economy based on e-services.

A trusted information society where e-democracy is not a virtual abstract concept could be built, if and only if, security and privacy issues are solved taking into consideration civil and national security needs.

It is by taking into account the need of privacy protection and the need for security that should be defined an enforceable legal framework. Consistent and appropriate national, European and international laws related to the digital world, must be defined and applicable.

We had to deal with a major contradiction existing between justice and police investigation needs and privacy and freedom protection for individuals, corporations, government and countries needs.

It is of our responsibility to promote a safe and reliable cyberspace environment to contribute to design the emerging information society. A minimum level of security for information and communication technologies must be provided with an affordable cost. Security must not become an exclusion factor for everyone that would like to conduct private or business activities over the Internet.

Efficient e-security will result of a balance between security needs, financial and human processes, and viable technological and legal solutions, to be put in operation to satisfy e-security needs.

Security is a compromise between cost, security service level and time to deliver them. It is illusive to believe that these three factors could be satisfied together; choices have to be made between cost, level of security and time to deliver security. After a one-privileged criterion has been chosen, the others have to be adapted.

BIBLIOGRAPHY

AVATIS (M.A.), 2000, « Cybercrime before the senate judiciary committee, criminal justice oversight subcommittee, house judiciary committee and crime subcommittee », http://www.cybercrime.gov/vatis.htm

BISHOP (M.), 2002, *Computer security ; Art and Science*, Addison Wesley

GHERNAOUTI-HELIE (S.), 1998, *Stratégie et ingénierie de la sécurité des réseaux*, InterEditions - Dunod

GHERNAOUTI-HÉLIE (S.), 2003, « Challenges to develop and deploy a unified e-security framework », *UNECE Workshop on ESecurity and Knowledge Economy*, Geneva, Switzerland, 12nd February

GRITZALIS (D.) & AL., 2003, *Security and privacy in the age of uncertainty*, Kluwer Academic Publishers

KENDALL (S.), « Teen Hacker or Cybercriminal : How Do We Draw the Line ? », http://www.csoonline.com/talkback/120103.html

NARDELI (E.), POSADZIEJEWSKI (S.), TALAMO (M.), 2003, *Certification and security in eservices, from egovernment to ebusiness*, Kluwer Academic Publishers

THIBADEAU (R.), 2000, « A Critique of P3P: Privacy on the Web », http://dollar.ecom.cmu.edu/p3pcritique/

An education guide to privacy, http://lrs.ed.uiuc.edu/wp/privacy/

The Platform of Privacy Preferences specification, http://www.w3.org/TR/P3P/

Computer Crime Research Center, « To catch a cyber-criminal », http://www.crime-research.org/eng/library/Cybercriminal.html

Hacking and cracking, http://www.cyberangels.org/ hacking/index.html

Federal Bureau of Investigation National Computer Crime Squad, http://www.emergency.com/fbi-nccs.htm

Computer Crime Research Center, « Mission and vision », http://www.crime-research.org/about.html

IFCC Annual Internet Report, http://www.ifccfbi.gov/strategy/statistics.asp