FROM SECURITY CULTURE TO EFFECTIVE E-SECURITY SOLUTIONS

Prof. Solange Ghernaouti-Hélie
University of Lausanne, Switzerland
Tel. 00 41 21 692 34 21
Email: sgh@hec.unil.ch
Web: http://inforge.unil.ch/sgh

Abstract: Stakes and challenges of e-security are analyzed to point out key issues in mastering information technologies risks. Lessons from the past are summarized to explain why security solutions are not effective. The global deployment of the information society is constrained by the development and overall acceptance of an international e-security framework. The validity of such model requires a challenging multidimensional approach of e-security. Several reflection axis and recommendations to guide the conceptualization of a unified e-security framework are proposed.

Key words: Information society, threats, risks management, security needs and challenges, computer crime, multidimensional approach, unified e-security framework.

1. INFORMATION AND COMMUNICATION TECHNOLOGIES REQUIEREMENTS FOR THE INFORMATION SOCIETY

1.1 Basic requirements

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 define specially to clarify the responsibility of each actors involved.

1.2 Security and trust requirements

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? Security technologies solutions and management provide part of the answer.

E-trust could be achieved through e-security and e-security would contribute to define a trusted environment. 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.

2. 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.

2.1 Increasing 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.

2.2 Cybercrime impacts

The negative impacts of security threats will affect not only systems or individuals actors but in a chained way organizations and society. Cybercrime 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 canceled by unfair information access.

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

3. 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.

3.1 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 pay for certification?
- Etc.

3.2 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 more 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.

3.3 E-security challenges

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.

4. MULTI DIMENSIONAL AND GLOBAL APPROACH

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

Security tools can't replace an ethical behavior 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 that technologies:

- Have become news kinds of mediators, which cannot be ignored at the individual, enterprise, organization or society levels;
- Are used to conduct criminal behaviors;
- Are the targets of criminality actions.

4.1 E-security issues from an 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.

4.2 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).

4.3 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.

4.4 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.

4.5 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.

5. AREAS FOR IMPROVEMENT OF E-SECURITY

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, behavior 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 an 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 behaviors, 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 define 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.

6. CONCLUSION

It is 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, 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.

ACKNOWLEDGEMENTS

The author acknowledges Professor Stefano Spaccapietra to have given her the opportunity to share security global issues with people who are involved in the technological dimension of security.

REFERENCES

1. M. Bishop. Computer security; Art and Science. Addison Wesley 2002.
2. S. Ghernaouti-Hélie. Stratégie et ingénierie de la sécurité des réseaux. InterEditions - Dunod 1998.
3. S. Ghernaouti-Hélie. Internet et sécurité. Que-sais-je? n°3609. PUF 2002.
4. S. Ghernaouti-Hélie. Challenges to develop and deploy a unified e-security framework. UNECE Workshop on E-Security and Knowledge Economy, 12 February 2003, Geneva, Switzerland.
5. International standards ISO 15408, ISO 13335.