

Towards a Belgian Strategy on Information Security

By private associations and academia

September 2008

Signing organisations



Editors of this document:

Jean-Luc Allard	VP Information Security – ISACA Belgium, ISO/IEC JTC1 SC27 Belgian Shadow Committee (coordinator wg3)
Georges Ataya	VP international ISACA and ITGI, Professor Solvay Business School
Gautier Dallons	Coordinator of the Security Team and R&D Project leader, CETIC
Alain De Greve	ISO/IEC JTC1 SC27 Belgian Shadow Committee (coordinator wg1/wg4 – 27000 series)
Marijke De Soete	Vice-chair ISO/IEC JTC1 SC27, Member of the Board LSEC
Bart Moerman	President, ISSA Brussels European Chapter
Bart Preneel	Professor K.U. Leuven, ESAT/COSIC, Chairman Board of Directors LSEC, ISO-IEC/SC27 Belgian Shadow Committee (wg2)
Ulrich Seldeslachts	CEO LSEC
Thierry Villers	Director INFOPOLE Cluster TIC

Reviewers of this document:

Dany Van de Ven	Brigade General (retired), Director Agoria/BSDI
-----------------	---

Towards a Belgian Strategy on Information Security

Version 2

Introduction

This white paper originates from the need identified by our constituent (non-profit) organisations, which are directly involved in the field of information security in all economic sectors, to promote, create awareness and improve the coordination of initiatives in this area.

The organisations signing this document are:

- Belgian experts involved in ISO/IEC JTC1 SC27, an international standards committee on information security techniques, including Information Security Management System (ISMS) aspects.
- CETIC
- INFOPOLE Cluster TIC
- the Belgian Chapter of ISACA
- the Brussels European Chapter of ISSA
- K.U. Leuven, ESAT/COSIC
- LSEC (Leaders in Security)
- Solvay Business School

These signing organisations represent more than 3000 Belgian information security professionals from more than 500 private, public and research organisations.

The signing organisations have encountered a series of problems and shortcomings in the structure, regulation, education and threat or crisis communication in the information security field in Belgium. The organisations have made numerous international contacts during their business and networking activities and these show that in the field of information security Belgium lags behind most other European countries. In certain areas, it is even less developed than some Eastern European countries. However, our national experts enjoy a worldwide reputation, so these shortcomings are not due to a lack of knowledge or expertise.

Current governmental and parliamentary initiatives, such as those of the Commission de la Chambre de l'infrastructure/Kamercommissie voor infrastructuur and the Comité Ministériel du Renseignement et de la Sécurité/Ministeriële Comité voor Inlichting en Veiligheid (which instigated the Belgian Network Information Security platform, or BeNIS) show that the authorities realise that the federal (and regional) public administrations need reliable information security.

The undersigned have identified six strategic objectives necessary for improving information security and these will be elaborated on in this document. Meeting these objectives will be of great benefit to Belgium.

Background

Our society is highly dependent on information and information processes. For society to run smoothly both of these require a predetermined level of quality. Information security is about ensuring that this level of quality is not compromised by unacceptable risks. Nowadays it is ICT that provides the support for these information processes and it should make them more reliable and efficient. Improving information security requires setting specific objectives but how to respond to these objectives depends on the domain in which they are to be implemented.

ICT systems are becoming more and more pervasive in our society: most citizens and organisations are becoming increasingly depending on ICT services and applications. This has an impact on all economic players, including government administrations and critical infrastructures (e.g. energy, transport, health, telecommunications). This new environment means new risks: automated large scale attacks can be launched from anywhere in the world to target these ICT systems. For instance, there have been attacks on individuals (e.g. virus, spam), denial of service attacks on countries (e.g. against Estonia in 2007 [1]), as well as economic and industrial espionage (e.g. accusations that China penetrates the European countries' national systems [2]) and fraud (e.g. banking sector [3]).

Over the past two decades there has been substantial investment in research, development, deployment and auditing, which has resulted in better protection against some of these threats. But unfortunately numerous incidents show that overall information security is not really improving. There are several reasons for this:

- 1) Our information systems are evolving very quickly and becoming ever more complex (we link computers made of hundreds of millions of small components in networks consisting of hundreds of millions of computers) and as humans we are not very good at securing complex systems that have many failure modes.
- 2) As more and more applications go online, the greater the financial incentives for online criminal behaviour. However, it is important to note that we may not hear so much about such problems because it is not in the perpetrators' interest to publicise their successes.
- 3) Information security is highly interdisciplinary. Developing solutions requires an integrated management approach that combines technology with internal and external regulation. Economic and human or social factors also need to be studied and taken into account. So in order to make progress there needs to be close collaboration between government, companies and research institutions.

The development and deployment of secure ICT systems requires the development of standards, the evaluation of products or systems and global coordination and enforcement. Although many of these issues need to be addressed at an international level, it is clear that national governments share a major responsibility. In Belgium there is no information security body for providing recommendations and support to Belgian administrations, institutions and organisations, at any level. This is in contrast to the situation in many European countries, including most of Eastern Europe [see Annex A]. As a result, the work in this domain is not coherent, compatible and efficient.

Neither does Belgium have a scheme for the certification of security products and services, such as those based on the Common Criteria that are used by its European neighbours and countries such as Greece, Poland and Hungary [see Annex B]. Very often

this means that Belgian companies cannot participate in international tenders. So if we still want to participate it involves transferring our national know-how to other countries, which leads to loss of employment or delocalisation.

Strategic objectives

1. Information Security Awareness Forum

A Belgian Information Security Awareness Forum should be established. This forum would allow the exchange of information on information security initiatives, standards and experiences on implementation/certification, including information security management, risk management, information and IT security techniques, etc. It could also act as an effective communication platform for security initiatives for the national government and its governmental bodies, such as the federal police, or European bodies such ENISA [4].

Ideally, the forum should be based on collaboration between organisations that specialise in information security, such as the signing organisations and government, industry, services, education and research.

Another recommendation is the creation of a Belgian information security think tank. This would advise the Belgian governmental Information Security Body, which will be elaborated on later in this document. This think tank could be related to the forum.

The Information Security Awareness Forum could also establish WARPs (Warning, Advice and Reporting Points) on information security, similar to the WARPs established in the UK [5] and the Netherlands [6].

2. Information security standardisation

Minimal information and ICT security requirements based on international standards [see Annex C] should be specified and fully integrated into the various industry sector regulations. These should deal with aspects such as information security management and control framework, risk management, incident management, business continuity, evaluation and audit, reporting and compliance, etc. The requirements should also mention the need for accreditation for critical systems. The administration should lead the way for industries and private organisations where accreditation is not part of the implementation of security solutions.

A number of information security standards allow for evaluation/certification. Currently Belgian manufacturers and organisations need to go abroad for the certification of their information security products and services. In view of the increasing professionalism in the sector and the increased demand for certified products and services, Belgium should establish its own information security certification framework, based on international standards in accordance with Belgian law and regulations. In this case the Belgian Accreditation Body (BELAC) should accredit the required information security certification authority and any evaluation centre(s). This governmental information security certification authority would then be in a position to issue the required certified products and services. The initiative already begun in this area should continue to receive the necessary support in order to achieve these objectives.

The accredited information security certification organisation should collaborate with other national certification bodies within the EU through the Common Criteria Recognition Agreement [7]. The aim would be to establish a harmonious certification framework with

the other member states for the translation of standards enforced through European directives into the national certification programme. On a larger scale (worldwide) this body needs to establish frameworks with peer organisations for cross-certification.

Belgian efforts in international information security standardisation need to be better coordinated. Although excellent work is being delivered by Belgian experts in these forums, there is no support or recognition from the Belgian Standardisation Office (NBN). This coordinating role could, for instance, be fulfilled by Agoria, by acting as a single point of contact for the ICT sector (“sector operator”). These coordinated activities should be supervised by the Ministry of Economic Affairs and the Department of Scientific Policy.

3. Education, training and research

There is an urgent need to coordinate initiatives related to education, training and research in information security. Several university clusters and colleges in Belgium organise their own programmes, resulting in different curricula. At the very least, a common baseline should be defined and promoted.

A research platform in information security should be established and promoted (see examples in the Netherlands [8] and France [9]). It should take into consideration the deliverables of the strategic objectives as defined above.

4. Critical infrastructure and CERT

A Belgian plan and roadmap for the protection of our critical infrastructures should be developed in collaboration with industry and other European countries and link in with the European Framework that is being established under the dedicated European Programme. These infrastructures include energy, transport and health care, which have already received priority, as well as finance, food supply, water, dangerous goods, telecommunications and government [10].

This roadmap should also support the planned development of the ISO ISMS specific standards dedicated to the information security aspects of critical infrastructure.

The Belgian government should accelerate its scheme to provide a limited crisis plan. This could later be elaborated with larger scenarios and input from industry.

A Belgian CERT (Computer Emergency Response Team) [11, [12] needs to be established quickly. Its mission should be to protect the nation’s Internet infrastructure and to coordinate protection against and responses to cyber attacks across the country. All this needs to happen in close collaboration with industry, building on the expertise already present there. Collaboration with BELNET and inspiration from initiatives in various sectors (e.g. financial sector), coordination with ECSA (www.ecsa-eu.org) and CFS-CSF (www.csf-cfs.be) is strongly recommended in this area.

The law on electronic communication (Law of 13 June 2005, Art 113 and 114) is unclear on the operational role of BIPT/IBPT with regards to the national CERT. This lack of clarity could result in inaction.

5. Legal and regulations

Several Belgian laws relating to IT and information security (e.g. law on cryptography, computer criminality, etc.) need to be re-evaluated. At the very least, the laws relating to computer criminality and privacy need to be revised in order to provide unambiguous goals and interpretations. For example, companies offering penetration testing services should perhaps require a special status. The role of judiciary experts in information security issues should also be better defined and their contribution assessed.

There is a pressing need for regulations governing the privacy aspects [13] of new technologies such as e-identity, citizen localisation technologies and biometrics and the government should address these matters appropriately. How organisations eventually comply with the privacy law will depend on how precisely it is formulated. Terminology and requirements that are too vague result in poor compliance.

Adequate coordination and full cooperation between the Belgian Information Security Body and the existing Belgian Privacy Commission is vital. The Belgian Information Security Body, proposed below, should advise the Belgian government on how to establish and maintain a legal framework. The resulting law should be consistent with information security laws and regulations and it should take into account the vast amount of information security expertise already present in Belgium.

The above objectives will only be efficiently coordinated if a centralised strategy is created. This requires a sixth objective.

6. Belgian Information Security Body

A Belgian governmental Information Security Body should be established (similar for instance to BSI in Germany). This body should be responsible for deciding on the policy and strategy for information security in Belgium, collaborating closely with industry and other government departments. It should further define the standards/norms for information security to which the government and their (service) suppliers should adhere.

The establishment of this body would benefit from the expertise from BIPT/IBPT or any other suitable federal agency. But clearly it also requires the creation of an independent committee that would include the involvement of a number of private Belgian information security experts (both from industry and research), taking on board the experiences in our neighbouring countries and ENISA as appropriate. The strategy should be directed towards a European Framework and have direct links with European bodies such as ENISA as well as national bodies and agencies from other European countries.

The Information Security Body should be set up by the federal government to be independent from, but associated with, the most appropriate public entities (BIPT/IBPT, NVO/ANS, etc.). It should bring together all the relevant parties from the governments (federal, communities and regions) to define together with the industry a roadmap for information security, while providing government services, the federal state and the regions a clear vision for the future.

This body should also coordinate with the relevant Belgian bodies responsible for research in information security.

This body should coordinate the representation of Belgium in all international groups where our national interest requires our presence.

The signing organisations are ready to act as the proposed independent Belgian information security expert group until it has been officially established.

Conclusion

The signing organisations call upon the Belgian government for urgent action to be taken by relevant stakeholders in order to achieve the above-mentioned strategic objectives.

The signing organisations are prepared to get involved and assume responsibility in order to bring the Belgium information security environment to an adequate level.

More information in relation to this document can be obtained from the following representatives of the signing organisations: Jean-Luc Allard (ISACA) and Bart Moerman (ISSA).

References:

- CAWET Werkgroep 55: Beveiliging van Digitale Informatie, 26 oktober 2007, <http://www.kvab.be/downloads/CAWET/beveiliging%20van%20digitale%20informatie.pdf>
- “Voor een nationaal beleid van de informatieveiligheid”, *White Paper* opgesteld door het overlegplatform voor de informatieveiligheid (BeNIS)
- DOC 52 0898/001, Chambre 2e Session de la 52e Législature - Kamer 2de Zitting van de 52ste Zittingperiode 2007-2008, Commissie voor de infrastructuur, het verkeer en de overheidsbedrijven, uitgebracht door de Heer Roel Deseyn.

Background:

[1] Cases of attacks: Estonia

- Assessing the Cyber Security Threat (SDA Monthly Roundtable), A Security & Defence Agenda Rapporteur: John Chapman, Year of publication: 2008, Bibliothèque Solvay, Brussels

[2] Cases of attacks: China (presumed)

- Belgische Kamer van Volksvertegenwoordigers – Chambre des Représentants de Belgique
- CRIV 52 PLEN 035 – Plenumvergadering/Séance plénière donderdag/jeudi 08-05-2008 (pm)
- CRABV 52 COM 209 – Commissie voor Landsverdediging/Commission de la Défense Nationale: woensdag mercredi 14-05-2008 (avond/soir)

[3] Money mules in banking sector :

http://www.ecp.nl/nieuws/id=101482/Banken_pakken_money_mules_aan_met_start_campagne.html

Information Security Awareness Forum

[4] ENISA reference to Information Security Awareness:

www.enisa.europa.eu/pages/ENISA_Working_Group_on_Awareness_Raising.htm

WARP

- [5] WARP in the UK : www.warp.gov.uk
- [6] WARP in the Netherlands: www.onderwijswarp.nl, www.ictu.nl (NICC) and www.samentegencybercrime.nl

Information Security Standardisation

[7] For the CCRA: <http://www.commoncriteriportal.org/members.html>

Education and research

[8] Examples in the Netherlands: Veilig Verbonden: http://www.ictregie.nl/iip/pdf_pagina.php?pageId=34

[9] Examples in France: ANR programme Sécurité et Sûreté Informatique

Critical Infrastructure, CERT, CSIRT

[10] Critical infrastructures: <http://europa.eu/scadplus/leg/en/lvb/l33259.htm>

[11] For a complete overview of the current situation of CERTS in Europe:

http://www.enisa.europa.eu/cert_inventory/index_inventory.htm

[12] “Successful cyber defense requires a coordinated national approach” by Miguel De Bruycker, Belgian Defense, Computer Incident Response Capability & Urs E. Gattiker, CyTRAP Labs (<http://papers.weburb.dk/frame.php?loc=archive/00000149/>)

Legal & Regulations

[13] Privacy aspects recommendations:

- http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/walrave_en.pdf
- http://www.enisa.europa.eu/doc/pdf/Country_Pages/Belgium.pdf

Annex A

List of national information security bodies in Europe

Some of these are integrated within the National Security Authority, others not.

Spain	CNI	http://www.cni.es
Italy	AISE	
United Kingdom	CESG	http://www.cesg.gov.uk/
France	DCSSI	http://www.ssi.gouv.fr
The Netherlands	MIVB	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Germany	BSI	http://www.bsi.bund.de
Estonia	Information Board	
Poland	ABW	http://www.abw.gov.pl
Romania	ORNISS	http://www.orniss.ro
Sweden	Utrikesdepartementet SSSB	

Annex B

List of member countries of the CCRA (Common Criteria Recognition Agreement)

Europe:

Sweden, Spain, Norway, The Netherlands, Italy, Hungary, Greece, Germany, France, Denmark, Czech Republic, Austria, United Kingdom, Finland.

World:

USA, Turkey, Singapore, Malaysia, South Korea, Japan, Israel, India, Canada, Australia and New Zealand (together).

Annex C

List of potential standards to be promoted within the Belgian administration

ISO

- The whole ISO/IEC 2700x (e.g. 27001 'ISMS requirements' and 27002 'ISMS Good Practices') and ISO 2701X series (specific implementations of 27002, e.g. for critical infrastructure, e-government, etc.)
- ISO/IEC 15408 (Common Criteria for security evaluation) and related norms
- ISO/IEC 21827 (System Security Engineering – Capability Maturity Model)

ISF

- Standard of Good Practice for Information Security

ISACA

- CobiT 4.1

ENISA

- http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf

And many others published by the national bodies (Annex A) or national standards institutes (such as NIST in the USA).

NIST SP 800 : <http://csrc.nist.gov/publications/PubsSPs.html>

NST FIPS : <http://csrc.nist.gov/publications/PubsFIPS.html>

Who are we?

- The Belgian Chapter of ISACA, a worldwide professional organisation aimed at supporting IT governance professionals by research and education in IT assurance and audit, IT governance and information security management. ISACA certifies information security managers worldwide (more than 8000 certified professional) and has been active in Belgium since 1986. Major publications are regularly issued and distributed free of charge to increase information security awareness and proper governance.
- The Brussels European Chapter of ISSA, a worldwide professional organisation supporting information system security professionals by providing a platform for continuous professional education, awareness and training.
- LSEC (Leaders in Security), a Belgian non-profit organisation that is an association of the information security industry and includes members from research institutions, individual professionals and a wide variety of enterprises.
- INFOPOLE Cluster TIC, Walloon cluster of IT industries and research centres (private and public), some of which work in the security sector.
- CETIC (Centre d'Excellence en Technologies de l'Information et de la Communication) is active in applied research in software development, GRID technologies and electronic systems. CETIC is a connecting agent aimed at transferring technology between academic research and industries.
- K.U. Leuven, ESAT/COSIC, active in many IT security sectors, has set up a postgraduate programme in Information Security.
- Solvay Business School makes the link between technology and business management and organises masters, postgraduate programmes in IT Governance and IT Audit and Security.
- Belgian experts involved in ISO/IEC JTC1 SC27, an international standards committee in information security techniques, dealing with ISMS (WG1), cryptographic systems (WG2), evaluation, certification and assurance (WG3), technology security (WG4) and privacy and access management (WG5).