BSA | The Software Alliance

COUNTRY: **BELGIUM**

Belgium's Cyber Security Strategy was adopted by the government in 2012. The legal framework for cybersecurity in Belgium, however, remains somewhat unclear, and the information available on the implementation of the strategy is limited.

On the other hand, Belgium does have an established computer emergency response team, CERT.be, and a well-developed cybersecurity incident-reporting structure. Belgium also recently announced the launch of a new Cybersecurity Centre. There is active support in the country for public-private partnerships, through BelNIS, a government body that liaises closely with private and semi-private entities.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✓	The Cyber Security Strategy <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf> was adopted by the Belgian government in 2012. The Belgian Prime Minister issued the following statement in a press release issued when the draft strategy was presented to cabinet: "The Belgian e-strategy aims to identify the cyber threats, improve security and to respond to incidents. This project arose from the work of the consultation platform for security, BELNIS (Belgian Network and Information Security)". [Communication relative à la cyberstratégie belge, 21 December 2012 <www.presscenter.org/fr/pressrelease/20121221/communication-relative-a-la-cyberstrategie-belge>]
2.	What year was the national cybersecurity strategy adopted?	2012	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	◑	Belgium does not have a comprehensive critical infrastructure protection strategy or plan in place. Section 3 of the Cyber Security Strategy addresses, in part, the need for the government to work with entities engaged with critical infrastructure for the purposes of data protection and the development of improved incident management procedures. Legal definitions of critical infrastructure exist in the Law Relating to the Security and Protection of Critical Infrastructure 2011 <www.centredecrise.be/sites/5052.fedimbo.belgium.be/files/loi_epcip_2011.pdf>.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✗	Belgium does not have legislation/policy in place that requires the establishment of a written information security plan. The Act Concerning Classification and Security Clearances 1998 <www.ejustice.just.fgov.be/mopdf/1999/05/07_1.pdf> covers the main processes in evaluating which information should be classified and determining which individuals may be granted a security access level.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✓	The Act Concerning Classification and Security Clearances 1998 <www.ejustice.just.fgov.be/mopdf/1999/05/07_1.pdf> requires data, where disclosure may cause a threat to national security or the national interest of Belgium, to be classified. Article 4 of the act outlines a three-tiered system of classification levels. The levels are assigned according to the level of risk involved in disclosing the classified information.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✓	Article 9 of the Act Concerning Classification and Security Clearances 1998 <www.ejustice.just.fgov.be/mopdf/1999/05/07_1.pdf> maps security practices to assigned classification levels. These levels are set out in Article 4 of the act, and are assigned according to the level of risk involved in disclosing the classified information. Section 3.4 of the Cyber Security Strategy <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf> recommends the development of improved cyber safety standards and regulations, with a specific focus on the protection of ICT systems.

COUNTRY: BELGIUM

	QUESTION	RESPONSE	EXPLANATORY TEXT
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	Belgium does not have in place legislation or policy that requires an annual cybersecurity audit. Section 3.4 of the Cyber Security Strategy <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf> requires that networks which process classified and sensitive information complete compliance audits. The details of such an audit and the frequency with which it is to be carried out is not elaborated upon.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	Belgium does not have in place legislation or policy that requires a public report on the cybersecurity capacity of the federal government. The Belgium National Information Security (BelNIS), a coordinating workgroup comprised of representatives from relevant government agencies, and the Federal Public Service for Information and Communication Technology (Fedict) <www.fedict.belgium.be> have both published white papers and reports on topics regarding cybersecurity and the Belgian government. However, these publications are not published according to an official timeframe and are not necessarily endorsed by the Belgian government.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	Belgium does not have in an information security law that requires each federal agency to have a chief information officer (CIO) or chief security officer (CSO). Section 3.5 of the Cyber Security Strategy <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf> calls for an inventory of existing capacities of government departments to respond to cybersecurity incidents. It requires elaboration of cybersecurity incident processes and mapping to specific tasks according to the known cyber threats for that particular department.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	◑	The Law Relating to the Security and Protection of Critical Infrastructure 2011 <www.centredecrise.be/sites/5052.fedimbo.belgium.be/files/loi_epcip_2011.pdf> places the prerogative to identify a critical infrastructure incident with the "sectoral authority" responsible for the critical infrastructure affected. The law lists the factors that must be considered, including the number of potential victims, the potential economic impact, and impact on the population. Furthermore, Section 3.5 of the Cyber Security Strategy <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf> calls for the taking of an inventory of existing capacities of government departments to respond to cybersecurity incidents. It requires elaboration of cybersecurity incident processes and mapping to specific tasks according to the known cyber threats for that particular department.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	Legal definitions of critical infrastructure exist in the Law Relating to the Security and Protection of Critical Infrastructure 2011 <www.centredecrise.be/sites/5052.fedimbo.belgium.be/files/loi_epcip_2011.pdf>.
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	◑	The Belgian Cyber Security Strategy 2012 <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf> establishes the Centre for Cyber Security Belgium as the standards making body for cybersecurity. However, as of August 2014, the Centre had not yet been established and no specific cybersecurity standards or certification requirements have been published. Broader ICT standards and certification practices in Belgium are generally based on international standards.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT.be <www.cert.be> was established in 2008. It is responsible for coordinating security and incident response measures for government institutions and all Belgian companies.
2.	What year was the computer emergency response team (CERT) established?	2008	

COUNTRY: BELGIUM

QUESTION	RESPONSE	EXPLANATORY TEXT
3. Is there a national competent authority for network and information security (NIS)?	✔	The Cyber Security Strategy <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf> outlines the roles of the Centre for Cyber Security Belgium which would act as the national competent authority for network and information security, directly under the authority of the Prime Minister. The operating and functional status of the centre as of mid-2014 is, however, unclear. The Belgium National Information Security (BelNIS) is a coordinating workgroup comprised of members from relevant government agencies. It provides advice and proposals to government on the field of cybersecurity, and was involved in preparing the Cyber Security Strategy and proposing the Centre for Cyber Security Belgium. However its roles and powers are not that of a national competent authority. On 14 November 2014, the Belgian government announced the launch of a Cyber Security Centre in early 2015. A royal decree setting up this centre was subsequently published in the State Gazette on 21 November 2014. The centre will oversee and coordinate the handling of cybersecurity issues in Belgium.
4. Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT.be <www.cert.be> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as providing a reporting structure to log cybersecurity incidents.
5. Are national cybersecurity exercises conducted?	✔	Belgium conducted the cybersecurity exercise Belgocybex in 2012.
6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	Belgium does not have a clear national incident management structure in place. Section 3.5 of the Cyber Security Strategy calls for the taking of an inventory of existing capacities of government departments to respond to cybersecurity incidents. It furthermore requires elaboration of cybersecurity incident processes and mapping to specific tasks according to the known cyber threats for that particular department. Furthermore, the strategy indicates the Centre for Cyber Security is directly under the authority of the Prime Minister. It does not, however, set out a clear management structure for the purposes of responding to a cybersecurity incident.
PUBLIC-PRIVATE PARTNERSHIPS		
1. Is there a defined public-private partnership for cybersecurity?	◑	Belgium Network Information Security (BelNIS), established in 2005, acts as a coordinating workgroup that includes representatives from government agencies engaged with cybersecurity. It provides advice to the government on cybersecurity incidents and cybersecurity, but is not a centralised authority and does not have a publicly available central policy. Although its roles include liaising with the private sector, and some of its members are semi-private entities (such as the Belgian Institute for Postal and Telecom Services), it is difficult to consider it a public-private partnership. In addition, Belgium has signed a memorandum of understanding on cybersecurity with Luxembourg and the Netherlands, which includes cooperation and expertise-sharing on the development of public-private partnerships.
2. Is industry organised (i.e. business or industry cybersecurity councils)?	✔	There are multiple industry-organised and industry-engaged associations in Belgium that provide a platform for cooperation and collaboration on cybersecurity, including: • The Belgian Cybercrime Centre of Excellence, Training, Research, and Education (B.cCENTRE) <www.b-ccentre.be> is large-scale entity that brings together academic groups, industry stakeholders, and other organisations in order to facilitate cybersecurity research and training. It is based at KU Leuven. • Agoria <www.agoria.be> is a federation of technology companies. It promotes and supports cybersecurity as part of their advisory and policy advocacy role. • The Belgian Committee of the International Chamber of Commerce <www.iccbelgium.be> engages in discussions and initiatives organised throughout their international network. • Internet Service Providers Association of Belgium <www.ispa.be> organises workshops and participates in programs on the topic of cybersecurity and the safe use of the internet. • BELTUG <www.beltug.be> is an association of Belgian information and communications technology managers. BELTUG has highlighted security as one of their critical issues. • In addition, the independent Brussels-based think-tank, the Security and Defence Agenda (SDA) <www.securitydefenceagenda.org>, regularly partners and collaborates with industry on issues associated with cybersecurity.

COUNTRY: BELGIUM

	QUESTION	RESPONSE	EXPLANATORY TEXT
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	–	Belgium already has a public-private partnership dedicated to cybersecurity.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Belgium does not have sector-specific joint public-private plans in place.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been defined. However, Section 3 of the Cyber Security Strategy <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf> proposes the development of an inventory of existing capabilities of government departments to respond to cybersecurity incidents.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific risk assessments have not been published, as of August 2014.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	◑	Belgium's cybersecurity education strategy is built around promoting the Belgian Cybersecurity Guide <vbo-feb.be/Global/Nieuws%20-%20media/Nieuws/cyber%20security%20guide/icc_belsec_guide_LR_v2.pdf> through organisations like the Belgian Cybercrime Centre for Excellence. <www.b-ccentre.be> However the guide and related activities are mainly targeting higher education (e.g. colleges and universities) and businesses.