COUNTRY: **POLAND**

Poland has a comprehensive cybersecurity strategy with clear goals. It was adopted in 2013, thus most of the recommendations are still being implemented. The legal framework for cybersecurity is still not fully developed.

Poland has several computer emergency response teams (CERTs), including CERT.GOV.PL, which covers government and critical infrastructure entities. It also acts as the cybersecurity authority. CERT Polska is an academic CERT covering the entire .pl network in a semi-official capacity.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Cyberspace Protection Policy of the Republic of Poland <www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf> was adopted in 2013. The strategy is a principled approach that includes clear objectives, implementation and financing guidelines, and criteria for assessing the effectiveness of the policy.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The National Critical Infrastructure Protection Programme (NCIPP) <rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf> was adopted by the Polish government in 2013.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Poland that requires the establishment of a written information security plan.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Act of 5 August 2010 on the Protection of Classified Information <www.monitorpolski.gov.pl/du/2010/s/182/1228/D2010182122801.pdf> requires information that may adversely affect the national security, national interests, or civil order of Poland to be classified. The information is classified by a four-tiered classification system, as set out in the act. The classification 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?	✔	The Act of 5 August 2010 on the Protection of Classified Information <www.monitorpolski.gov.pl/du/2010/s/182/1228/D2010182122801.pdf> maps various security practices to assigned classification levels. These levels are set out in the act and are assigned according to the level of risk involved in disclosing the classified information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in Poland that requires an annual cybersecurity audit. The Cyberspace Protection Policy of the Republic of Poland <www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf> calls for the implementation of cybersecurity monitoring measures, however an auditing process is not specifically addressed.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	There is no legislation or policy in place in Poland that requires an annual cybersecurity audit.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	There is no legislation or policy in place in Poland that requires each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	The Cyberspace Protection Policy of the Republic of Poland <www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf> details a required incident reporting procedure, which includes the reporting of cybersecurity incidents.

COUNTRY: POLAND

	QUESTION	RESPONSE	EXPLANATORY TEXT
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The National Critical Infrastructure Protection Programme (NCIPP) <rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf> includes appropriate definitions for "critical infrastructure" and "critical infrastructure protection".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	◑	The Cyberspace Protection Policy of the Republic of Poland 2013 <www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf> contains a recommendation to establish minimum cybersecurity standards but no detailed standards have been developed, as of August 2014. The policy contains a broad commitment to international cooperation.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT.GOV.PL <www.cert.gov.pl> was established in 2008. It is responsible for coordinating security and incident response measures for Polish state authorities and entities engaged with critical infrastructure. CERT Polska <www.cert.pl> was established in 1996. It acts on behalf of the Research and Academic Network in Poland (NASK) <www.nask.pl> to coordinate incident response measures across .pl domain hosts.
2.	What year was the computer emergency response team (CERT) established?	2008	
3.	Is there a national competent authority for network and information security (NIS)?	◑	CERT.GOV.PL <www.cert.gov.pl>, in addition to its incident reporting and response functions and its public education programs, advises the government on cybersecurity issues. It does not act as a wider network and information security authority.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT.GOV.PL <www.cert.gov.pl> is tasked with managing the reporting of cybersecurity incidents. CERT.GOV.PL provides a multi-channel reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	◑	Poland has participated in cybersecurity exercises conducted by both the European Union and NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	A three-level National Response System for Computer Security Incidents is detailed in the Cyberspace Protection Policy of the Republic of Poland. <www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf>
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in Poland.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	While there is no industry-led cybersecurity platform in Poland, two chambers of commerce, the National Chamber of Commerce for Electronics and Telecommunications (KIGEit) <www.kigieit.org.pl> and the Polish Chamber of Information Technology and Telecommunications (PIIT) <www.piit.org.pl> engage with cybersecurity in the course of their operations.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	There are no new public-private partnerships being planned in Poland.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Poland 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.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific risk assessments have not been released.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The Cyberspace Protection Policy of the Republic of Poland 2013 <www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf> includes a set of principles on education and training, and a commitment to establish ICT security as a permanent topic in the higher education sector. Poland has also made a commitment to conducting a mass media cybersecurity campaign aimed at young people.