COUNTRY: **CYPRUS**

Cyprus adopted a national cybersecurity strategy in 2013. It includes a commitment to update key elements of the legal framework for cybersecurity. Cyprus also is working toward the establishment of a national computer emergency response team (CERT), which is expected to be operational in 2015. The country has also taken an interest in sector-specific approaches to the management of cybersecurity, with a potential focus on the energy and financial services sectors.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Cybersecurity Strategy of Cyprus was adopted in February 2013. As of August 2014, however, the contents of the strategy have not been made available to the public.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	Cyprus does not have a critical infrastructure protection strategy or plan in place. The critical infrastructure protection in general is under the responsibility of the Ministry of Interior and Civil Defence. <www.moi.gov.cy> Critical information infrastructure protection is under the responsibility of the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR). <www.ocecpr.org.sy> The work under the critical information infrastructure protection project is in progress as of August 2014. The academic sector, particularly the KIOS Research Centre for Intelligent System and Networks <www.kios.ucy.ac.cy> at the University of Cyprus, has published numerous research papers on Cypriot critical infrastructure.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Cyprus 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?	◑	Cyprus classifies sensitive information against a four-tiered classification system, however, there is no legislation or policy requiring the classification of particular data.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✖	Cyprus does not map specific security practices or requirements to risk levels.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in Cyprus that requires (at least) an annual cybersecurity audit.
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 Cyprus that requires a public report on cybersecurity capacity for the government.
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 Cyprus that requires each agency to have a chief information officer or chief security officer. The introduction of such a policy may occur in light of action in the Cybersecurity Strategy of Cyprus to introduce a national security policy.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	Cyprus has passed the Subsidiary Administrative Act Number 371/2013 that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✖	Cypriot legislation does not have an appropriate definition for "critical infrastructure protection".

COUNTRY: CYPRUS

	QUESTION	RESPONSE	EXPLANATORY TEXT
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	Not applicable	There are no specific cybersecurity standards or certification requirements for procurement in Cyprus, as of August 2014.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✖	Cyprus does not have an operational national CERT in place. However, the Department of Information Technologies of the Ministry of Finance is currently financing a project that will enable a government CERT to become fully functional by early 2015. The Cybersecurity Strategy provides for further work in evaluating a national CERT.
2.	What year was the computer emergency response team (CERT) established?	–	
3.	Is there a national competent authority for network and information security (NIS)?	◑	There is no clear national competent authority for network and information security in Cyprus. The Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR) <www.ocecpr.org.cy> is the regulatory authority for postal and electronic communications and, according to the European Union Agency for Network and Information Security, is the agency responsible for the implementation of a national CERT. <www.enisa.europa.eu/media/news-items/cyprus-cert-delegation-visit-to-enisa> The OCECPR does not have a national responsibility for network and information security. The current structure and the wider scope of the NIS authority will be evaluated under a specific action of the cybersecurity strategy in 2015.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✖	As of August 2014, there is not a clear incident reporting platform for the collection of cybersecurity incident data in Cyprus. The lack of a CERT or similar authority means cybersecurity incident data is not centrally logged.
5.	Are national cybersecurity exercises conducted?	◑	Cyprus has participated in multi-national cybersecurity exercises organised by the European Union.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is not a clear national incident management structure (NIMS) for responding to cybersecurity incidents in Cyprus.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	◑	The biennial CYpBER conference <www.cypber.com> provides a platform for Cyprus government and private sector representatives to liaise and exchange ideas relating to cybersecurity concerns, particularly those effecting the oil and gas industry. The conference produces significant, and publicly available, documentation covering topics addressed by the representatives. The national Cyber Security Strategy provides for a framework of a public-private partnership for cybersecurity, and also requires that any project should consider and follow the general policy of the public-private partnership framework of the government. Currently there is public-private cooperation in the fields of awareness for cybersecurity and in the creation of a cybercrime centre of excellence.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✖	Apart from the biennial CYpBER conference <www.cypber.com>, there is no significant industry-led platform for cybersecurity in Cyprus.
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 Cyprus.

COUNTRY: CYPRUS

	QUESTION	RESPONSE	EXPLANATORY TEXT
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	◑	Forums such as the CYpBER conference <www.cypber.com> indicate that the energy and oil sector remains a significant area of cooperation between the sector and government. However no sector-specific plans have been published.
2.	Have sector-specific security priorities been defined?	✖	There has been some discussion of cybersecurity risks in the energy sector, which appears to be a priority area for Cyprus. As of August 2014, work in this field is in-progress and there is no clear definition or priority <www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/presentations/costas-efthymiou-ocecpr-cyprus-2013-the-cyprus.pdf>.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Cyprus is undertaking a national Cyber Risk Assessment that includes sector-specific risks. As of August 2014, this work is in progress <www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/presentations/costas-efthymiou-ocecpr-cyprus-2013-the-cyprus.pdf>.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✖	Cyprus does not have a cybersecurity education program in place. Cybersecurity education, however, may be included in the recently announced national Cybersecurity Strategy (the strategy is not yet available to the public).