COUNTRY: **IRELAND**

Ireland's national legal and policy framework is very limited when it comes to cybersecurity. A cybersecurity strategy is being developed, but there is no clear timeframe for its release or adoption. Ireland is also one of the few countries in the European Union without an operational computer emergency response team, although it is in the process of establishing one.

While there is no formalised public-private partnership set up for cybersecurity, Irish private sector entities, including Infosecurity Ireland, appear to be quite active in this field. In addition, Ireland organised a number of successful individual cybersecurity education campaigns, such as the "Make IT Secure", which included releasing online resources alongside a television advertising campaign.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✖	According to the European Union Agency for Network and Information Security (ENISA), a cybersecurity strategy for Ireland is in development. <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ireland> According to the relevant minister, an Irish Cyber Security Centre was in development as of November 2013. <www.dcenr.gov.ie/Corporate+Units/Press+Room/Speeches/2013/Address+by+Minister+Rabbitte+at+the+IIEA+Cyber+Security+Conference.htm>
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	There is no critical infrastructure protection plan or strategy in place in Ireland.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Ireland 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?	✖	There is no legislation or policy in place in Ireland that requires an inventory of "systems" and the classification of data. The Official Secrets Act 1963 <irishstatutebook.ie/1963/en/act/pub/0001> provides the definition for an official secret, but does not detail a system for the classification of data.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✖	There is no legislation or policy in place in Ireland that requires an inventory of "systems" and the classification of data. The Official Secrets Act 1963 <irishstatutebook.ie/1963/en/act/pub/0001> provides general security requirements for data deemed an official secret, however these are broad and not mapped 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 Ireland that requires at least an annual 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 Ireland 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 Ireland 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?	✖	There is no legislation or policy in place in Ireland that requires the mandatory reporting of cybersecurity incidents. Ireland does not have a national CERT and does not have a centralised platform with which to collect incident data.

COUNTRY: IRELAND

	QUESTION	RESPONSE	EXPLANATORY TEXT
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✖	Irish legislation/policy does not have an appropriate definition for "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?	Not applicable	There are no specific cybersecurity standards or certification requirements for procurement in Ireland, as of August 2014.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	◑	The status of CSIRT-IE, the Irish national CSIRT, is unknown. Its roles and functions are not defined in government legislation, regulation or documentation and it has little online presence. IRISS-CERT <www.iriss.ie> was established in 2008. It serves to address the coordination of incident response measures for incidents that affect the Irish private, public, or non-Government sectors. IRISS-CERT is an independent not-for-profit company and is not an agency of the Irish Government.
2.	What year was the computer emergency response team (CERT) established?	–	
3.	Is there a national competent authority for network and information security (NIS)?	✖	Ireland does not have a national competent authority for network and information security. General information security responsibilities lie with the Department of Communications, Energy and Natural Resources. <www.dcenr.gov.ie>
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✖	The functions and services offered by CSIRT-IE are unspecified and it does not appear to provide an appropriate incident reporting platform for collecting cybersecurity incident data. There is no alternative government entity that is responsible for providing this service.
5.	Are national cybersecurity exercises conducted?	✔	According to the European Union Agency for Network and Information Security (ENISA) <www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012/at_download/fullReport>, Ireland conducted the national cybersecurity exercise Gaillean Exercise in 2010.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	Ireland do not have a national incident management structure in place for responding to cybersecurity incidents.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in Ireland.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	InfoSecurity Ireland <www.infosecurityireland.org> is an industry-led information security lobby-group whose members come from the private and academic sectors. Additionally, ICT Ireland <www.ictireland.ie>, a representative body for information technology companies in Ireland, engages with cybersecurity in the course of its 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 Ireland.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Ireland 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?	◑	Ireland does not have a comprehensive strategy for cybersecurity education. However, Ireland has run a number of successful individual cybersecurity education campaigns — for example, Make IT Secure, which includes online resources and TV advertising. <www.makeitsecure.org/en>