COUNTRY: **ESTONIA**

Estonia was one of the first countries to develop a national cybersecurity strategy in 2008, followed by the release of an updated strategy in 2014. The country also has a wide range of legislation that covers information security and cybersecurity. Estonia has a well-established computer emergency response team, CERT Estonia, under the control of the Information System Authority.

Further to national bodies, also notable is the fact that NATO's Cyber Security Centre of Excellence is based in Estonia.

While no formalised public-private partnerships exist, public entities do work closely with relevant private-sector organisations.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Cyber Security Strategy was released by the Estonian government in 2014. <www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf> It is an update of the 2008 strategy and is a continuation of the implementation of the 2008 goals, however it includes new threats and needs not covered in the previous strategy. The strategy is comprehensive and includes a thorough assessment of the cybersecurity threats faced by Estonia and the capability to respond to them — with reference to both operational capacity and the relevant legal framework. In addition, the strategy's declared goals and sub-goals are detailed and an implementation structure is provided.
2.	What year was the national cybersecurity strategy adopted?	2014	A previous strategy was adopted in 2008.
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Emergency Act 2009 <www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&pg=1&tyyp=X&query=H%E4daolukorra+seadus&ptyyp=RT&keel=en> identifies the critical infrastructure of Estonia and regulates the organisation and procedures involved in responding to related emergencies. Pursuant to subsection 40(2) of the Emergency Act, the Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets 2013 <www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf> regulates the organisation for the implementation of security measures for information systems in particular.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✔	Subsection 40, Paragraph 2 of the Emergency Act 2009 <www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&pg=1&tyyp=X&query=H%E4daolukorra+seadus&ptyyp=RT&keel=en> compels the government to establish security measures for certain vital information systems by means of regulation. Pursuant to this, the Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets was adopted in 2013.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The State Secrets and Classified Information of Foreign States Act 2007 <www.nsa.ee/files/State%20Secrets%20And%20Classified%20Information%20Of%20Foreign%20States%20Act.pdf> assigns information deemed appropriate to be treated as state secret a classification level, according to a four-tiered system. The requirements that deem information a state secret are organised by the agency or area to which the information relates.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✔	The State Secrets and Classified Information of Foreign States Act 2007 <www.nsa.ee/files/State%20Secrets%20And%20Classified%20Information%20Of%20Foreign%20States%20Act.pdf> maps security practices to the classification level assigned to information deemed a state secret. These classification levels represent the importance of the information to the various functions of the Estonian government and foreign governments, including the level of risk involved in disclosing the information.

COUNTRY: ESTONIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✔	The State Secrets and Classified Information of Foreign States Act 2007 <www.nsa.ee/files/State%20Secrets%20And%20Classified%20Information%20Of%20Foreign%20States%20Act.pdf> requires an annual inspection of the integrity of the storage in which state secrets assign the top or second tier classification level are contained. No further level of auditing or reporting is required by the Act. The Electronic Communications Act 2004 <www.legaltext.ee/text/en/X90001K4.htm>, as amended in 2011, entitles the Technical Surveillance Authority of Estonia to require that any communications provider carry out a security audit. There is no timetable that dictates when Technical Surveillance Authority is to require the security audits.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✔	The 2008 Cyber Security Strategy <www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf> requires that the Cyber Security Strategy Committee will monitor the implementation of the Cyber Security Strategy by submitting annual reports to the government, measuring the progress of the implementation against the Implementation Plan. The current Cyber Security Strategy <www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>, released in 2014, does not include this provision but does state that it retains the goals and objectives of the 2008 strategy.
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 requiring 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 Regulation on Security Measures for Information Systems of Vital Services and Related Information Assets 2013 <www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf> requires entities engaged with "vital services" to each appoint an individual to notify the Estonian Information System Authority <www.ria.ee> in the event of a security incident, including cybersecurity incidents. The entity must also submit a report to the Estonian Information System Authority following the resolution of the security incident.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Estonian Information System Authority <www.ria.ee> provides definitions for both "critical infrastructure" and "critical infrastructure protection", as well as the term "vital systems", which is used by the Estonian Government in legislation and policy related to information security.
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	The 2014 Estonian Cyber Security Strategy <www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf> includes a set of "principles and guidelines" for the procurement of national cybersecurity services and products. One of the principles encourages international cooperation. There are no local procurement requirements in place.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT Estonia <www.ria.ee/cert> was established in 2008. It is responsible for coordinating security and incident response measures across all Estonian networks.
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)?	✔	The Information System Authority <www.ria.ee> acts as Estonia's national competent authority for network and information security.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT Estonia <www.ria.ee/cert> is tasked with managing the reporting of cybersecurity incidents. CERT Estonia provides an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✔	Estonia has conducted two national cyber exercises, Cyber Hedgehog in 2010 and Cyber Fever in 2012. Estonia took part in multi-national cyber exercises organised by NATO in 2013. NATO's Cooperative Cyber Defence Centre of Excellence <www.ccdcoe.org> is based in Estonia.

COUNTRY: ESTONIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	National incident management procedures are outlined in the Emergency Act 2009. <www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&pg=1&tyyp=X&query=H%E4daolukorra+seadus&ptyyp=RT&keel=en> Cybersecurity incidents are not addressed in particular.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	◑	There is not a defined public-private partnership for cybersecurity in Estonia. The Information System Authority <www.ria.ee> operates in close cooperation with private sector. Vaata Maailma (the Look@World Foundation) <www.vaatamaailma.ee> is public-private partnership (founded in 2001) dedicated to promoting the use of the internet and ICT services. It is composed of Estonian and international telecommunications providers. The foundation runs various projects that are primarily educational in nature, covering safe internet and computer use.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	While there are no significant industry-led platform that engage with cybersecurity, the Estonian National Cyber Defence League <www.kaitseliit.ee/en/cyber-unit>, which is a cyber-response unit, is comprised of IT professionals and representatives from entities engaged with critical infrastructure. The league is specifically mentioned in Estonia's Cyber Security Strategy. <www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>
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 Estonia.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Estonia 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, 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?	✔	Estonia's Cyber Security Strategy 2008 <www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf> includes a comprehensive education program, including the following activities: • Organising information security awareness-raising for the wider public in cooperation with the private sector, with a particular focus on home users, small and medium-sized enterprises, employees of local governments and state agencies, teachers and students. • Conducting targeted media campaigns on cybersecurity and computer protection, and public advertising programmes. • Raising awareness of cyber culture in every Estonian agency and company by training senior executives and officials in the promotion of secure computer and Internet use in all fields. The 2014 Cyber Security Strategy <www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf> details the success of the implementation of these goals and commits to continuing the same educations outcomes.