COUNTRY: **HUNGARY**

The National Cyber Security Strategy of Hungary was adopted in 2013. The strategy covers key principles of cybersecurity, an overview of Hungary's current cybersecurity situation, and its future cybersecurity goals. Hungary has a limited legislative framework dedicated to cybersecurity.

Several public authorities play a role in cybersecurity, including the National Security Authority, which deals with information security, and the Cyber Security Centre, part of the intelligence services, which deals with cybersecurity. Hungary also has a computer emergency response team, CERT-Hungary, but its remit is limited to government institutions. Furthermore, while the National Cyber Security Centre is tasked with liaising with the private sector, there are no formalised public-private partnerships.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The National Cyber Security Strategy of Hungary <www.nbf.hu/legis.html> was adopted in 2013. The strategy covers key principles of cybersecurity, Hungary's current cybersecurity situation and future cybersecurity goals.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	◑	Act CLXVI of 2012 on the Identification, Designation and Protection of Vital Systems is the chief law for critical infrastructure in Hungary. In addition, the National Directorate General for Disaster Management, the agency responsible for critical infrastructure protection, published the document Three Pillars of Disaster Management <www.katasztrofavedelem.hu/letoltes/eng/szervezet/NDGDM_intro.pdf> in 2012. The document covers critical infrastructure protection in a limited way, but is not a critical infrastructure protection plan.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✔	Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies <www.nbf.hu/legis.htm> requires the relevant minister responsible for information security to prepare an annual monitoring plan, in conjunction with the ministers responsible for classified information protection and disaster prevention.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Act CLV 2009 on the Protection of Classified Data <njt.hu/cgi_bin/njt_doc.cgi?docid=126195.265401> requires data, of which disclosure may cause a damage to the public interest, to be classified. Paragraph 5, Subsection 4 of the act outlines a four-tiered system of classification levels. The levels are assigned according to the level of risk involved in disclosing the classified information. Act CLVI of 2010 on Greater Protection of Public Records within the Scope of National Data Assets <njt.hu/cgi_bin/njt_doc.cgi?docid=133022.240462> classifies all public data managed by a public body, public information, and all personal data that is of public interest as national data and outlines protection standards for dealing with such data.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✔	Act CLV of 2009 on the Protection of Classified Data <njt.hu/cgi_bin/njt_doc.cgi?docid=126195.265401> maps various security practices to assigned classification levels. These levels are set out in Paragraph 5, Subsection 4 of the act, and are assigned according to the level of risk involved in disclosing the classified information.

COUNTRY: HUNGARY

	QUESTION	RESPONSE	EXPLANATORY TEXT
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies <www.nbf.hu/legis.htm> requires the relevant minister responsible for information security to prepare an annual monitoring plan, in conjunction with the ministers responsible for classified information protection and disaster prevention. These plans are based on the current operations of the National Security Authority (NBF) <www.nbf.hu>. However, they are not a result of a defined auditing process. Additionally, Section 16/1a of the act allows the NBF to "check the relevant organisations' compliance with the statutorily defined security requirements and the related procedural rules". However, the NBF is not required to carry out this operation within a specific timeframe.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✔	The National Security Authority (NBF) <www.nbf.hu> is required by the Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies <www.nbf.hu/legis.htm> to prepare annual and ad-hoc reports on electronic information system security, the protection of vital information systems elements and the state of cyber protection. The authority must also provide quarterly reports to the National Cyber Security Coordination Council on security incidents, as well as domestic and international security trends. The authority is not required to publicly release these reports.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	Section 17 of Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies <www.nbf.hu/legis.htm> allows the relevant minister responsible for information security, upon receiving a proposal from the National Security Authority (NBF) <www.nbf.hu>, to appoint an information security supervisor for a fixed-term appointment. The appointment is not mandatory and is not required to be appointed to each agency,
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in place in Hungary that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems <njt.hu/cgi_bin/njt_doc.cgi?docid=155940.231269> includes an appropriate definition for the protection of critical systems.
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	The National Cyber Security Strategy of Hungary 2013 <www.nbf.hu/legis.html> contains a specific commitment to developing measures to: "ensure that the quality of IT and communication products and services necessary for the secure operation of the Hungarian cyberspace meet the requirements of international best practices, with special emphasis on compliance with international security certification standards".
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-Hungary <www.cert-hungary.hu> was established in 2013 and is responsible for coordinating incident response measures for Hungarian government institutions.
2.	What year was the computer emergency response team (CERT) established?	2013	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The National Security Authority <www.nbf.hu> acts as the national competent authority for network and information security in Hungary. The National Cyber Security Centre <www.cert-hungary.hu> operates within the Special Service for National Security and is tasked with the coordination of incident responses for breaches occurring within government networks or affecting critical information infrastructures.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-Hungary <www.cert-hungary.hu> is tasked with incident reporting and collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as having in place an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	◑	Hungary has participated in multi-national cybersecurity exercises conducted by NATO.

COUNTRY: HUNGARY

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	The National Cyber Security Coordination Council, established by Government Decision No. 1139/2013 on the National Cyber Security Strategy of Hungary <www.nbf.hu/legis.htm> is a government body comprised of a representative from the Prime Minister's Office and Ministers with responsibilities relevant to information and cybersecurity. The National Security Authority is required by the Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies <www.nbf.hu/legis.htm> to provide quarterly reports to the National Cyber Security Coordination Council on security incidents, as well as domestic and international security trends. The National Cyber Security Centre, CERT-Hungary <www.cert-hungary.hu> is required to report cybersecurity incidents that affect government networks and entities engaged with critical infrastructure.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	◑	While there is no dedicated public-private partnership for cybersecurity, the National Cyber Security Centre <www.cert-hungary.hu> is tasked with liaising with the private sector for the purposes of promoting information exchanges and developing long-term cyber strategies.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	There is no significant industry-led platform for cybersecurity in Hungary, the Hungarian Association of IT Companies — IZSV <www.ivvsz.hu> engages with cybersecurity as part 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 Hungary.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	◑	Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies <www.nbf.hu/legis.htm> provides consideration for Sectoral Incident Management Centres to act in conjunction with the Government Incident Management Centre. The act does not, however, make reference to particular Sectoral Incident Management Centres, nor does it establish or regulate Sectoral Incident Management Centres.
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 National Cyber Security Strategy of Hungary <www.nbf.hu/legis.html> includes a comprehensive set of recommendations and commitments on cybersecurity education. It states: "Hungary pays particular attention to integrating cyber security as a field in the information technology syllabus of primary, secondary and higher education, in training courses for government officials and in professional training courses".