RIVADA NETWORKS

www.rivada.com

Rivada Networks Submission to the

Irish National Cyber Security Strategy Draft Public Consultation - 2019.

Section	Recommendation
2.1	Create a centrally coordinated cyber security agency.
2.2.1	Focus the strategy on protecting the Irish way of life.
2.3	Create a strong deterrent through legal instruments and national/international alliances.
3.1	Expand the definition of critical infrastructure to include HEIs.
3.2	Greater alignment of risk management and IT activities at State level.
3.3	Initiative a Supply Chain Review for both State and OES suppliers.
3.4	Review Government and agency contractor cyber security.
3.5	Introduce unannounced cyber security audits for OES.
3.6	Review of tools to deter malicious cyber actors.
3.7	Enhance EU and international cyber threat cooperation.
3.8	Introduce protection mechanisms to ensure independence of cyber-security chiefs in OES.
3.9	Review foreign investment in OES and vendors to critical infrastructure.
3.10	Require interoperability for communications infrastructure in OES.
3.11	Introduce mandatory and graded OES cyber-attack drills.
4.1	Ireland seeks membership of the European Centre of Excellence for Countering Hybrid Threats.
4.2	Develop indicators and metrics for impact evaluation of hybrid threats.
4.3	Introduce mandatory hybrid threat assessment post-elections and referenda.
4.4	Launch campaigns to empower citizens to recognise hybrid threat actors and platforms.
4.5	Avoid censoring social media; respect the electorate and separation of media and government.
5.1	Initiate a full state body cyber security audit.
5.2	Introduce random state agency cyber security checks.
5.3	Introduce data access auditing within Government and State bodies.
5.4	Introduce Government Department cyber security incident drills.
5.5	Review personal device connectivity policies.
5.6	Educate Government employees on the dangers of coercion and blackmail from private online activities.

Section	Recommendation
5.7	Introduce restrictions on app downloads on government issued devices.
5.8	Review patient data protection measures in the Health Service, review foreign investment in health/biotech/DNA industries in Ireland, introduce legislation requiring explicit consent for patient data to be used in medical research.
6.1	Continue public information campaigns.
6.1.1	Investigate the possibility of launching a Private Citizen Cyber Security App.
6.2	Initiate SME campaigns, leveraging the insurance industry, GDPR and other issues important to business owners.
7.1	Promote Ireland as the leader in Cyber Security Education.
7.1.1	State Cyber Security agencies should have direct input into learning outcomes to education programmes at higher education level to ensure appropriate skill pool.
7.1.2	Introduce mandatory core modules in several areas of cyber security in identified programmes.
7.1.3	Introduce minimum standards and learning outcomes for cyber security courses.
7.1.4	Introduce computer science as a subject at primary school level.
7.1.5	Work with the private sector to develop recruitment strategies.
7.1.6	Introduce more attractive visa conditions for international students who wish to study cyber security in Ireland.
8.1.2	Ireland should advocate for strong and legally binding laws and policies in International, European and domestic maritime cyber security.
8.1.3	Ireland should advocate for international and European laws and policy for Space Cyber Security.
8.1.4	Introduce security checks for persons in HEIs who access space-located assets.
8.2.1.2	Develop policies around private enterprise reprisals for cyber-attacks.
8.2.1.3	Encourage and support the development of private enterprise collaborative forums in cyber security.
8.2.1.4	Review laws pertaining to Insurance coverage and cyber-attacks.
8.2.2	Introduce security checks for persons in private enterprise who access space-located assets.