Recommendation 1
For Governments

Prioritise cybersecurity in CSOs funding instruments.
Prioritise cybersecurity in CSOs funding instruments.

As the key funders of local CSOs, governments are well-positioned to shape the cyber resilience posture and environment of CSOs.

We recommend that governments prioritise cybersecurity in funding instruments for CSOs as the key strategy for enhancing their cyber resilience.

Given the limited budget available to CSOs, governments should provide funding for specific cybersecurity items, such as operations security, personnel security, and compliance, to guide CSOs into taking appropriate cybersecurity budgeting measures.
Recommendation 2
For Governments

Strengthen the local cybersecurity ecosystem to provide specific support for CSOs.
Strengthen the local cybersecurity ecosystem to provide specific support for CSOs.

We recommend that governments should create a more holistic cybersecurity support infrastructure for CSOs by strengthening the existing support ecosystem as well as creating cybersecurity entities (e.g., advisory, incident response) specific to CSO needs.

Either of the solutions points to the need for a new model for direct technical assistance to local CSOs – the support should be accessible, affordable and leverage existing support networks. Accessibility ensures contextually informed support from practitioners with regional and subject-matter expertise, while affordable solutions lower the cost barrier for CSOs, such as subsidising private companies to provide discounted or free security services to financially constrained CSOs. This new model also calls for maximising effective distribution of work among existing technical assistance providers available to CSOs.
Recommendation 3
For Governments

Provide capacity-building for CSOs
Provide capacity-building for CSOs.

Due to the limited internal IT and cybersecurity expertise amongst CSOs, governments should support CSOs to promote cybersecurity awareness and coordinate meaningful capacity-building. Such capacity-building efforts should take into account CSOs’ risk exposure as well as the local cybersecurity landscape, in terms of which actors and support mechanisms are available. CSOs should also be trained on the compliance requirements that affect their organisations – for example, compliance with the data protection regulations.

We recommend governments, especially the CSO-relevant cybersecurity entities to leverage their respective expertise and collaborate on regular awareness-raising, cybersecurity training, and capacity-building. Invariably, capacity-building should be framed towards cyber resilience in terms of preparing for, absorbing, recovering from, and adapting to adverse cyber incidents.
Recommendation 4
For Governments

Develop locally relevant cybersecurity resources for CSOs
Develop locally relevant cybersecurity resources for CSOs.

While there are many cybersecurity resources publicly available online that CSOs can use to improve their cyber resilience, there remains a need for resources that are locally relevant and sensitive to the context and situation of local CSOs.

We recommend governments to develop actionable general guidelines that capture the needs, practices, and context of the organisations. By incorporating existing mature cyber resilience approaches and frameworks, such as the NIST Cybersecurity Framework or the CIS controls, the security guidelines should empower the CSOs to make informed decisions towards better management of cyber resilience. Beyond guidelines and toolkits, there is an opportunity for governments to support the development of local technology solutions that improve the cyber resilience of CSOs.
ENHANCING THE CYBER RESILIENCE OF CIVIL SOCIETY ORGANISATIONS

Recommendation 5
For Governments

Strengthen cybersecurity threat intelligence research and communication
Strengthen cybersecurity threat intelligence research and communication.

Given the limited availability of data and reports on CSOs’ cybersecurity, we recommend that governments support research and analysis focused on the local cybersecurity threat landscape. This should involve developing the profiles of threat actors and the cyber-attack tactics, techniques, and procedures they employ; investigating the technical and operational cybersecurity practices of CSOs, as well as barriers to CSOs’ adoption of digital security tools and practices. Subsequently, this information could be shared with CSOs and relevant support networks, such as their technical assistance providers, to develop better, coordinated preparation and mitigation strategies against any future cyber threats.
Contact Us

+853 2871-2930

cyber-resilience@unu.edu

https://macau.unu.edu/