UNITED NATIONS
UNIVERSITY
Institute in Macau

ENHANCING THE CYBER RESILIENCE OF CIVIL SOCIETY ORGANISATIONS

Recommendation 1

For Civil Society Organisations

Undertake capacity-building for senior management.

Undertake capacity-building for senior management.

The majority of CSOs do not have sufficient and effective cybersecurity management policies, procedures, and processes in place. This reflects the CSOs' overall lack of cybersecurity capacity and their basic level of cybersecurity maturity; however, more importantly, this alludes to the senior management's limited capacity to manage organisational cyber resilience.

We recommend that CSOs undertake cyber resilience capacity-building for their senior management to enhance their understanding of organisational risk management, information technology management, and cybersecurity management; their awareness of the local cybersecurity landscape, their ability to develop and operationalise cybersecurity plans and strategies, as well as their understanding of the compliance requirements.

UNITED NATIONS
UNIVERSITY
Institute in Macau

ENHANCING THE CYBER RESILIENCE OF CIVIL SOCIETY ORGANISATIONS

Recommendation 2

For Civil Society Organisations

Adopt an appropriate cyber resilience management model.

Adopt an appropriate cyber resilience management model.

We recommend that CSOs roll out rigorous cybersecurity management strategies within their organisations, and make use of relevant cyber resilience management frameworks and models. Cybersecurity management, including the relevant frameworks, models, and tools, should be contextually informed – it should take into consideration CSOs' value-focused objectives, mission orientation, limited resources, and commitment to responsibly provide services to their clients.

Part of cyber resilience management should entail formulating and identifying controls across the prepare, absorb, recover, and adapt phases of cyber resilience and across the various cybersecurity domains. For example, CSOs should ensure that data protection is mainstreamed into all data processing operations, implementing standardised documentation of digital threats, coordinating with relevant stakeholders, including other CSOs, funders, and Cybersecurity Incident Response Teams, for information sharing and dissemination, and incident handling.

YOUR FAVORITE SOURCE OF
FREE BOOTSTRAP THEMES
Start Bootstrap can help you build better websites using the Bootstrap CSS framework!
Just download your template and start going, no strings attached!
FIND OUT MORE
Ps
Ai
Ae

UNITED NATIONS
UNIVERSITY
Institute in Macau

ENHANCING THE CYBER RESILIENCE OF CIVIL SOCIETY ORGANISATIONS

Recommendation 3

For Civil Society Organisations

Allocate and prioritise funding for cybersecurity.

Allocate and prioritise funding for cybersecurity.

We recommend that CSOs prioritise cybersecurity investments and allocate a dedicated budget line for cybersecurity expenditure. Budgeting for cybersecurity should be in line with the organisation's overall cybersecurity management strategy, which should be informed by the risk exposure, risk tolerance, and cybersecurity objectives of the organisation.

Cybersecurity investments should be prioritised across the various organisational units, domains, and processes – for example, in capacity-building and training, human resources, and communications. CSOs should prioritise cybersecurity investments that are essential to protect critical organisational assets which are most susceptible to cyber threats.

Grant-receiving CSOs should also include cybersecurity budgeting in their funding proposals.

UNITED NATIONS UNIVERSITY
Institute in Macau

ENHANCING THE CYBER RESILIENCE OF CIVIL SOCIETY ORGANISATIONS

Recommendation 4

For Civil Society Organisations

Undertake targeted organisation-wide capacity-building.

Undertake targeted organisation-wide capacity-building.

Organisational cybersecurity and cyber resilience are not only the responsibility of the management nor the cybersecurity personnel, although they do play a critical role. They are the responsibility of all personnel that is engaged and interact with the organisations. Therefore, enhancing organisational cyber resilience needs to be systemic and organisation-wide.

We recommend that CSOs undertake targeted cybersecurity capacity-building for different stakeholders, such as professional training for IT and cybersecurity personnel, basic cyber hygiene training for general personnel, and IT and cybersecurity management training for senior management. Depending on their capacity, we also recommend that CSOs undertake some level of cybersecurity awareness-raising for their critical partners (such as service clients and volunteers) who might otherwise be conduits of cybersecurity risks.

Undertake targeted organisation-wide capacity-building.

It is important for CSOs to build internal cybersecurity capacity, not only as part of organisational cybersecurity culture, but also to provide incident handling and response capability within the organisation. For core security processes and functions, internal personnel, with their understanding of the organisations’ operations, mission, and context, may be well positioned to manage and respond to cybersecurity threats.

YOUR FAVORITE SOURCE OF
Start Bootstrap can help you build better websites using the Bootstrap CSS framework!
Just download your template and start going, no strings attached!
FIND OUT MORE
Ps
Ai
Ae

UNITED NATIONS
UNIVERSITY
Institute in Macau

ENHANCING THE CYBER RESILIENCE OF CIVIL SOCIETY ORGANISATIONS

Recommendation 5

For Civil Society Organisations

Leverage external support and partnerships for cybersecurity.

Leverage external support and partnerships for cybersecurity.

In general, CSOs have limited human and financial resources to allocate to non-mission-core investments, such as IT and cybersecurity resources and operations. As such, CSOs outsource non-core functions and resource-intensive operations to third-party service providers and partners, when it is cost-effective to do so.

Notably, some research suggests that cybersecurity investments generate effective returns when resource-constrained organisations migrate from old and complex legacy systems to outsourced cloud applications and systems. Similarly, security products requiring more dedicated resources and professional expertise to maintain could be outsourced to a managed security service provider (MSSP).

Leverage external support and partnerships for cybersecurity.

We recommend that CSOs leverage the cybersecurity support available within their ecosystem, in terms of private sector service providers and public sector cybersecurity agencies, towards enhancing their cybersecurity operations. We also recommend CSOs to leverage partnerships with affiliate and peer organisations, in terms of information and knowledge sharing, and cybersecurity incident handling support. For example, CSOs could establish a dedicated IT team at the affiliation or headquarter level to offer subsidiary organisational units cybersecurity support.

UNITED NATIONS
UNIVERSITY
Institute in Macau

Contact Us

☎ +853 2871-2930

✉ cyber-resilience@unu.edu

🌐 https://macau.unu.edu/