JIU Recommendations on UNICC Cybersecurity Services

Cybersecurity services in the United Nations system organizations

Report of the Joint Inspection Unit (JIU/REP/2021/3)

In today's digitalized world, **cybersecurity** has emerged as a matter of importance for international organizations, and the United Nations is no exception. The potential consequences of a weak cybersecurity posture go beyond the disruption of ICT infrastructure and systems - rather, the ability of the United Nations to deliver its mandate is at stake.

In 2021, the United Nations Joint Inspection Unit (JIU), an independent external oversight body that conducts evaluations, inspections and investigations in the UN, reviewed the use of cybersecurity practices across the UN, with distinct recommendations for UN Agencies to leverage cybersecurity services from the **United Nations International Computing Centre** (UNICC) and for UNICC to establish a fund for donor contributions.

The JIU report, Cybersecurity in the United Nations system organizations (JIU/REP/2021/3), identifies common cybersecurity challenges and risks faced by the UN system, provides an analysis of responses to these threats and examines current inter-Agency dynamics as well as the potential for shared solutions. *Read the full report*.

The Director of the United Nations International Computing Centre should seek to establish by no later than the end of 2022 a trust fund for donor contributions, which would complement the capacity of the Centre to design, develop and offer shared services and solutions to enhance the cybersecurity posture of the United Nations system organizations.

The General Assembly of the United Nations should, no later than at its seventy-seventh session, take note of the recommendation addressed to the Director of the United Nations International Computing Centre to establish a trust fund for shared cybersecurity solutions and invite Member States wishing to reinforce the cybersecurity posture of the United Nations system organizations to contribute to the trust fund.

JIU report recommendations

UNICC Cybersecurity Services

UNICC's cybersecurity services cover cybersecurity oversight and governance as well as a whole spectrum of operational components. UNICC is certified with ISO 27001 and is a 2020 and 2017 CSO50 information security award winner. UNICC is a SWIFT cybersecurity service provider across many global locations.

+ Governance and CISO support
+ Threat Intelligence Network
+ Security Operations Centre
+ Security Incident and Event Management
+ Vulnerability Management
+ Phishing simulations
+ Penetration testing
+ Incident response and forensics
+ Information security awareness
+ Infrastructure and network support
+ PKI Digital Identity
+ Electronic Signature Services
+ Secure AuthN Federated Authentication

For more information, please reach out to **business@unicc.org**

Excerpts from the JIU report, Cybersecurity in the United Nations system organizations

A. Growing attention to cybersecurity, with different maturity levels

75. Frameworks generally complex, heterogeneous and multilayered. *The UNICC has developed a model to represent the different normative components of an Information Security Management System as layers, reflecting the highest level of abstraction on top and the broadest level of detail at the bottom, and has supported several United Nations system organizations in assessing and improving their existing regulatory and governance frameworks.*

111. Internal capacity varies. *To provide an alternative for entities that are not in a position to immediately establish a dedicated [cybersecurity] function, the Inspectors wish to highlight that the UNICC offers a service titled "security governance", sometimes also referred to as "chief information security officer as a service".*

B. Inter-agency mechanisms dealing with cybersecurity

143. Advantages & drawbacks of the UNICC business model. *The strict cost-recovery model under which the UNICC has operated since its inception has the advantage of ensuring a high degree of transparency in the costing of services, forces continuous coordination with clients, and keeps the scope of the service offer in check by requiring the closest possible alignment between what is really needed and what is developed and produced in response. […] The UNICC's service offer is dependent on clients providing seed funding to cover the costs of developing a new service to meet demand.*

144. The UNICC as a key player in the United Nations cybersecurity landscape. *As attested to by many of its clients, the Centre has accumulated considerable cybersecurity expertise and capacity and has gradually expanded its offer to include 13 specialized services in that area, commonly known under the brand name Common Secure. […] The services cover both dimensions of cybersecurity governance and operational aspects.*

145. Common Secure Threat Intelligence as the UNICC's flagship cybersecurity service. *Common Secure Threat Intelligence has been assessed in particularly positive terms by a clear majority of the Centre's clients and addresses a long-standing collective need formulated and repeatedly reiterated at the system- level. […] Common Secure Threat Intelligence can be considered the most promising cybersecurity service in terms of its potential to naturally attain full system-wide subscription and realize actual protection gains for the system.*

149. Opportunities for improvements within the existing boundaries of the UNICC's mandate. *The Inspectors believe that a great deal can be accomplished within the framework of the Centre's current mandate as revised in 2003, which already provides a sound basis for the implementation of solutions that could come alive with a little more engagement of all stakeholders.*

157. Operationalizing the trust fund. *The main aim of the fund could be to finance research and development for the purpose of launching cybersecurity services for which there is clear interest among organizations but no initial critical mass of users who are prepared to share the seed funding needed. Similarly, the fund could be used to extend the scope or depth of the existing services for which there is a clear demand and which require seed funding, or the cost of which would need to be lowered to enable more organizations to join sooner.*

E. Opportunities for a closer alignment of physical security and cybersecurity

163. Desirability and suitability of a harmonized approach. *Bearing in mind that the UNICC participates in the Inter-Agency Security Management Network, the Inspectors noted that the Centre had expressed its readiness to play a role in consolidating and communicating information on cybersecurity incidents to national authorities on behalf of the United Nations system organizations, if formally entrusted with such a role.*

Advantages of Engaging UNICC

- Intimate knowledge of the system and needs of UN system organizations
- Long-standing experience with customized services
- Subject to same administrative rules and structures
- Engagement with relevant inter-Agency forums
- Progressive decrease in cost of services as UNICC's Partner Organizations base grows
- Not-for-profit and cost recovery services delivery
- Inherent and shared objectives of rendering the system more secure for all
- Ability to learn from UNICC's Partner Organizations, scaling lessons learned for a collective benefit
- Bird's eye view of the system as a whole and all its parts
- Neutral, apolitical and - due to its cost-recovery model - disinterested broker of system-wide solutions

For more information, please reach out
to **business@unicc.org**

UNICC

SUSTAINABLE DEVELOPMENT GOALS