United Nations

A/77/88/Add.1

General Assembly

Distr.: General
7 June 2022

Original: English

Seventy-seventh session
Item 145 of the preliminary list*
Joint Inspection Unit

Review of cybersecurity in the United Nations system organizations

Note by the Secretary-General

The Secretary-General has the honour to transmit to the members of the General Assembly his comments and those of the United Nations System Chief Executives Board for Coordination on the report of the Joint Inspection Unit entitled "Cybersecurity in the United Nations system organizations" (see A/77/88).

* A/77/50.

I. Introduction

1. In the report of the Joint Inspection Unit entitled "Cybersecurity in the United Nations system organizations" (see A/77/88), the Unit presents its review of cybersecurity in the United Nations system organizations, the main objectives of which are to: (a) identify and analyse common cybersecurity challenges and risks faced by United Nations system organizations individually, as well as their respective response thereto, bearing in mind organizations' context-specific requirements (vertical perspective); and (b) examine current inter-agency dynamics facilitating a system-wide approach to cybersecurity for better coordination, collaboration and information-sharing among the United Nations system organizations, and, where appropriate, the potential for shared solutions (horizontal perspective).

II. General comments

2. Organizations welcome the report and its findings, which have the potential to enhance the cybersecurity posture of the United Nations system. They further appreciate the fact that the review promotes: (a) a business risk-based approach that goes beyond the more traditional approach, which is centred on information and communications technology (ICT); (b) inner entity view/processes; and (c) strong support for a common and shared basic level of security protection/measures across the United Nations system in order to bridge the maturity gap between entities and improve cyberresilience throughout the United Nations system.

3. Organizations support the recommendations set out in the review.

III. Comments on specific recommendations

Recommendation 1
The executive heads of the United Nations system organizations should prepare, as a matter of priority and no later than 2022, a comprehensive report on their cybersecurity framework and present it to their respective legislative and governing bodies at the earliest opportunity, covering the elements contributing to improved cyberresilience examined in the present report.

4. Organizations support this recommendation.

5. In some entities, existing regular governance reporting on cybersecurity may already meet the needs underlying the recommendation through, for example, reporting to governing bodies, audit and oversight committees, internal information technology boards at the enterprise level and external expert advisory boards for technology.

6. When preparing the recommended reports, entities underscore the importance of ensuring that these public documents do not provide any detail that would either acknowledge specific information about detection of attacks and the detection capabilities of the respective organizations or provide any information that a potential adversary could leverage to increase the likelihood of specific attacks succeeding.

Recommendation 2
The legislative and governing bodies of the United Nations system organizations should consider the reports on the elements contributing to improved cyberresilience prepared by the executive heads and provide strategic guidance on further improvements to be implemented in their respective organizations, as necessary.

7. Organizations note that this recommendation is addressed to the legislative and governing bodies.

8. The expected strategic guidance must consider that additional resources would be required to strengthen the local security posture and facilitate collaboration with the United Nations International Computing Centre (UNICC).

Recommendation 3
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.

9. Organizations note that this recommendation is addressed to the Director of UNICC.

10. Smaller entities lacking resources and skills in cybersecurity could benefit from the additional and focused shared services that UNICC would develop. Entities working through private-public partnerships in the implementation of their digital development and humanitarian programmes are eager to continue to receive direct support from Member States for the delivery of their digital programmes, including aspects related to their cybersecurity, and in that regard some entities interpret the scope of this recommendation to mean that it covers the internal cybersecurity posture of their offices worldwide and the cybersecurity posture/risks related to the external work with private-public partners.

11. If this recommendation is implemented, some UNICC member organizations note that they envision playing a role in the discussions on governance, funding, implementation and access to the trust fund, including through engagement in the context of the Digital and Technology Network, before any proposal is finalized.

Recommendation 4
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.

12. Entities note that this recommendation is addressed to the General Assembly and reiterate the comments provided in response to recommendation 3.

Recommendation 5
The Secretary-General should present a report to the General Assembly of the United Nations no later than at its seventy-eighth session exploring further opportunities to draw upon the convergence between physical security and cybersecurity so as to ensure a more holistic protection of United Nations personnel and assets and indicating necessary measures to strengthen the existing structures accordingly, giving particular attention to the potential role of the Department of Safety and Security in this regard.

13. Organizations note that this recommendation is addressed to the Secretary-General.

14. The United Nations Secretariat has already initiated such a process. In addition to informal and ad hoc collaboration between the Office of Information and Communications Technology and the Department of Safety and Security, the latter is

a member of the recently established hybrid cyberattack response network. In addition, under the capital investment plan for ICT operations, necessary investments will be considered to strengthen existing structures, personnel, assets and services, with a view to benefiting from the convergence between physical security and cybersecurity.

15. With regard to the convergence of physical and cybersecurity functions, some organizations see a potential conflict in the language of paragraph 164 of the report. While the Inspectors recognize that the physical security unit must not absorb cybersecurity functions, they proceed to recommend convergence, which might create a situation in the various agencies that could lead to the very result that the Inspectors do not recommend. Those organizations suggest that it should be stressed that cybersecurity functions must not be absorbed into physical security units.

16. Although there is ongoing collaboration between the Department and the Office on cybersecurity matters, it should be noted that the Office will take the lead and that the role and resources of the Department will be confined to ensuring the physical security of United Nations staff and premises, given that cybersecurity does not fall under its purview. This partnership is activated when addressing hybrid cyberattacks[1] on the United Nations, in which case the Department and the Office collaborate on conducting security risk assessments and developing and implementing recommendations concerning preventive and mitigating measures.

[1] In this context, hybrid cyberattack can be described as the use of digital technology or a physical attack against information technology infrastructure to cause deliberate harm to United Nations programmes and activities that results in significant physical security vulnerability at United Nations premises or heightened risk of harm to staff members.