Joint Inspection Unit
of the United Nations System

www.unjiu.org

"Independent
system-wide
inspection, evaluation
and investigation"

Review Highlights JIU/REP/2021/3
October 2021

CYBERSECURITY IN THE UNITED NATIONS SYSTEM ORGANIZATIONS

Inspector Jorge Flores Callejas
Inspector Aicha Afifi
Inspector Nikolay Lozinskiy

Background

In today's digitalized world, cybersecurity has emerged as a matter of importance for international organizations, and the United Nations is no exception. The digital transformation, the increasing dependence on information and communications technology (ICT) and cyberenabled solutions, and the fact that cyberthreats are constantly growing, have led to an unprecedented augmentation of cybersecurity risks facing the United Nations system. 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, and its credibility vis-à-vis its members states and beneficiaries, is at stake. While cyberattacks may affect organizations with diverse mandates and structures differently, the menace is a real and shared one.

Objectives

The main objectives of the JIU were to: (a) Identify and analyse common cybersecurity challenges and risks faced by the United Nations system, 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 United Nations system organizations, and where appropriate, the potential for shared solutions (horizontal perspective).

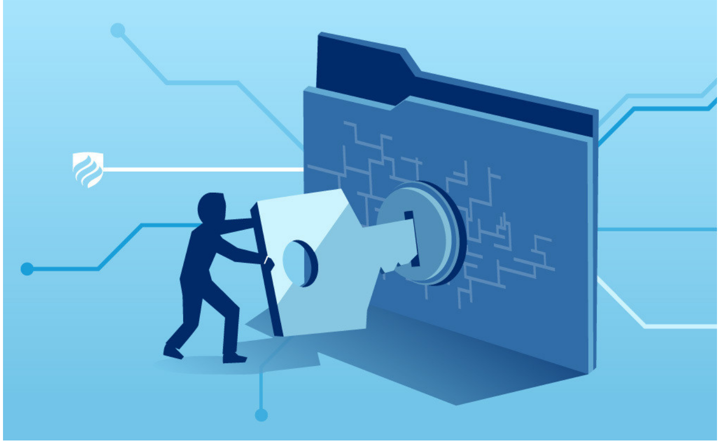
Approach & Methodology

In accordance with JIU internal standards and working procedures, the Inspectors used a range of qualitative and quantitative data collection methods from different sources to ensure the consistency, validity and reliability of their findings. Data collection instruments included:

- Desk review of relevant components of the applicable regulatory frameworks (governing body resolutions, corporate strategies on ICT, and specific policies and procedural guidance documents on information security and cybersecurity where they existed) as well as reports from internal and external oversight bodies. Analysis of the reports of the committees and networks of CEB, mainly the Digital and Technology Network and its Information Security Special Interest Group.

- 2 corporate questionnaires answered by JIU participating organizations and a series of questions addressed to UNICC management.

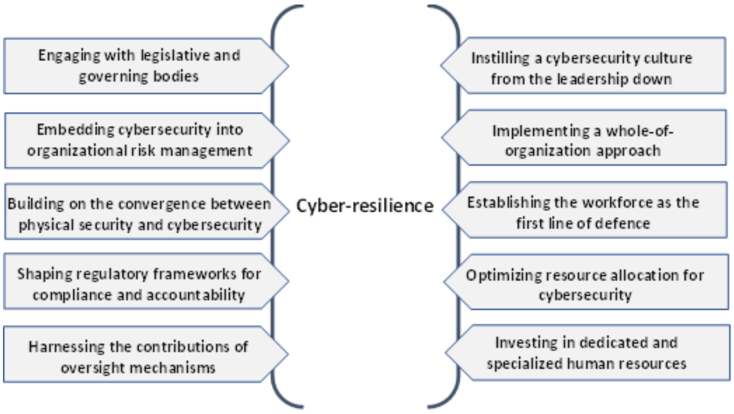
- 45 interviews with officials in charge of ICT and cybersecurity more specifically, as well as with senior officials to provide a broader organizational perspective. Interviews were also conducted with representatives of oversight bodies, the United Nations Department of Safety and Security and the UNICC.



Click to access the full report

What the JIU found

A strong cybersecurity posture for any organization results from a multifaceted, whole-of-organization approach cutting across several organizational domains and competences, including information and communications technology, risk management, physical safety and security, and information and knowledge management more broadly. In a system-wide perspective, the weak individual cybersecurity posture of one organization has the capacity to represent a collective problem for the system as a whole.


Engaging with legislative and governing bodies
Embedding cybersecurity into organizational risk management
Building on the convergence between physical security and cybersecurity
Shaping regulatory frameworks for compliance and accountability
Harnessing the contributions of oversight mechanisms
Cyber-resilience
Instilling a cybersecurity culture from the leadership down
Implementing a whole-of-organization approach
Establishing the workforce as the first line of defence
Optimizing resource allocation for cybersecurity
Investing in dedicated and specialized human resources

1. Cybersecurity deserves legislative and governing bodies' attention

Few organizations have recognized the potential of active engagement with the legislative and governing bodies on cybersecurity matters, and among those who have, most did so only after a major attack necessitated increased attention and interaction at the intergovernmental level. Legislative and governing bodies should step up their engagement on the matter and provide high-level strategic guidance, including through the formulation of an explicit risk appetite statement and the corresponding allocation of resources to contribute to attaining the desired level of protection. To enable them to do so, organizations are called upon to consider further developing their reporting to legislative and governing bodies by devising appropriate methodologies for collecting and sharing relevant cybersecurity metrics, and by anticipating escalation protocols to be followed in the event of attack.

2. Need to embed cybersecurity into organizational risk management efforts

The utility of applying a risk management lens to cybersecurity has already been recognized in various fora, although the implications of viewing cybersecurity this way in practice have yet to be fully understood and absorbed in many parts of the system. In practice, treating cybersecurity as a corporate-level risk management issue carries several concrete benefits that are further detailed in the report. Beyond embedding cybersecurity formally in the organization's enterprise risk management framework, the emphasis in future needs to be on developing effective and meaningful risk mitigation measures in conjunction with robust business continuity planning. Cybersecurity experts' contribution to and full involvement in internal risk management processes, from design to implementation and monitoring, will be crucial to achieve these objectives.

3. There is potential in building on the convergence between physical and cybersecurity

Even though there is no shortage of examples of the ways in which cyber and physical security intersect in practice, institutionalized links between the two domains remain sporadic across the organizations surveyed. The corporate architecture of only two participating organizations reflects an actual integration of the physical safety and security and the cybersecurity management frameworks. There is potential in building on the convergence between the two domains to the benefit of both and towards a more holistic approach to the protection of organizational personnel and assets. This is also true from a system-wide perspective and the report highlights several areas for further consideration both at the level of individual organizations and among the relevant inter-agency coordination mechanisms, building on the expertise already available.

4. Need to shape regulatory frameworks for compliance and accountability

Participating organizations refer to a wide range of industry standards, sometimes more than one, and most are either already certified, planning to get certified under ISO 27001, or have chosen to voluntarily align their framework with it without seeking formal certification. The Inspectors found that cybersecurity was routinely referenced in the ICT strategies of the organizations and specific cybersecurity policies exist or are being developed in many of them. These frameworks are generally complex, heterogeneous and multi-layered, and scattered across a set of strategic, policy, procedural and technical guidance documents. Against this backdrop, the need for simple, non-technical and engaging language and messaging that focuses on making the consequences of risky cyberbehaviour palpable for the individual is apparent. In addition, to reinforce individual accountability, incentives for reporting of incidents without fear of repercussions and a more nuanced – more easily deployable, less formal and invasive – sanction system for poor cyber-hygiene would go a long way to encourage individuals to take responsibility for their unsafe or risky practices.

5. Harnessing the contribution of oversight mechanisms

Internal and external oversight mechanisms were found to have been attentive to cybersecurity matters even in the absence of specific references in their mandates to the topic as such. The review contains several examples of corporate enhancements made to the cybersecurity framework of participating organizations that had originated in oversight recommendations, thus highlighting their added value. To maximize that value, it is important to ensure that the knowledge and experience of the cybersecurity experts within an organization can systematically inform and feed into the work of the oversight function.

Click to access the full report

6. Need to instil a cybersecurity culture from the leadership down

The cybersecurity posture of an organization is also a matter of a strong internal culture, which starts with the attention and priority given to the issue by executive management – the tone at the top. The Inspectors consider it the responsibility of the executive head to instil such a culture in all functions and all locations where the organization is present, since an attack or intrusion anywhere could lead to a compromise everywhere. The first step is for senior leadership itself to be aware of the associated risks and the implications of inaction and poor cyberhygiene. Continued commitment and engagement must go beyond statements profiling cybersecurity as a corporate priority. A key element would be seeing the occurrence of incidents not as a failure but rather as a starting point for addressing a shared problem and for better protecting the organization and its assets.

7. Need to implement a whole-of-organizational approach

Responsibility for cybersecurity cannot rest with ICT departments alone, and the majority of participating organizations have recognized that administrative as well as substantive departments have a role to play. In light of the recent trend observed in many organizations towards decentralization and delegation of authority to mid-level managers, mainstreaming of cybersecurity considerations into the policies governing the work of respective departments and their practices would contribute to ensuring more direct organization-wide ownership and accountability by spelling out related responsibilities where they would be more readily consulted by each stakeholder in their respective role. One encouraging practice encountered across several participating organizations was the availability of role-based cybersecurity training opportunities and awareness raising measures, which should be further expanded to equip all stakeholders optimally for their respective contribution to organizational cyber-resilience.

8. Establishing the workforce as the first line of defence

The "human factor" has gained in importance in the global cybersecurity threat landscape, as reflected in the growing concern among participating organizations over individual end-users being increasingly targeted through social engineering techniques. It is therefore evident that empowering users to play an active role in improving organizational cyber-resilience is imperative and basic digital literacy of each member of the workforce is a non-negotiable starting point. The review confirmed the existence of mandatory training sessions on cybersecurity for staff members in a majority of the organizations. However, compliance with mandatory training alone is rarely a meaningful indicator of awareness, nor does it provide sufficient assurance regarding the attainment of actual behavioural change. Organizations should therefore aim to develop a comprehensive training and awareness-raising programme with clear objectives defined for each category of stakeholder in accordance with the risks they may represent for the organization. In this context, attention to all categories of personnel is necessary.

9. Need to optimize financial resource allocation for cybersecurity

In the organizations' own assessment, despite an overall increase in the resources allocated to cybersecurity in recent years, resource constraints were found to have most severely impacted the human resource capacity and the availability of in-house expertise; the ability to make appropriate ICT infrastructure investments; and the ability to replace obsolete applications. More important than the question of how much should be spent on cybersecurity is the question of where the resources should be allocated so as to have the most meaningful impact. In the view of the Inspectors, attention to keeping cybersecurity investments firmly grounded in and linked with business requirements and sound risk management practices is imperative to avoid both overinvesting and underresourcing a key business continuity function.

10. Investing in dedicated and specialized human resources

The majority of participating organizations have invested in hiring specialized expertise to cover the different dimensions of cybersecurity, sometimes placed under the leadership of a dedicated chief information security officer (CISO). The scope of the function extends beyond the digital sphere and is not limited to providing technical know-how. Irrespective of the organizational placement of cybersecurity – under ICT or independently from it –, it is important to safeguard the opportunity for cybersecurity considerations to be voiced and heard by the responsible decision-makers without restriction. The function should therefore be situated where it can address executive management independently and effectively contribute to other corporate frameworks such as enterprise risk management, information and knowledge management, physical safety and security, and oversight. Having dedicated and specialized cybersecurity expertise within each organization contributes to reinforcing the posture not only of that organization but of the system as a whole and is therefore a worthwhile investment.

Technological preparedness: select issues for closer attention

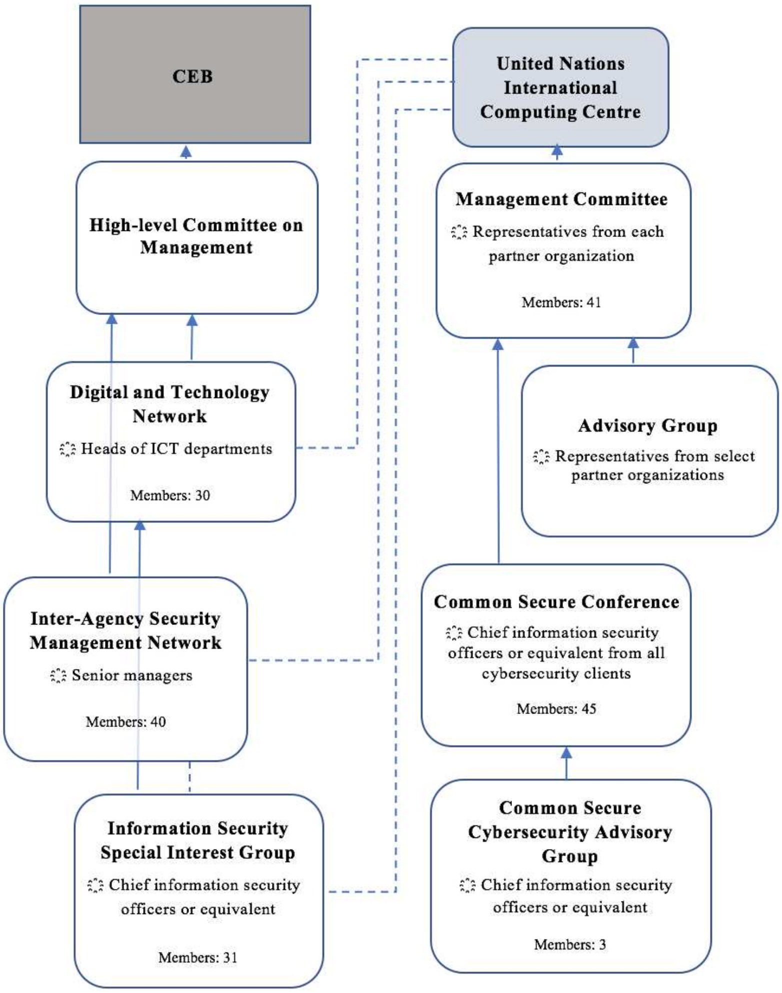
Without aiming for a comprehensive assessment of technological preparedness, the Inspectors identified some common issues for attention in areas that have recently been subject to more dynamic development:

- **End point device management:** the security of tools facilitating remote work was brought into focus by COVID-19 and should be expanded;
- **Legacy systems:** upgrading or retirement of ageing, often custom-built systems to be reviewed to reduce vulnerabilities;
- **Cloud security:** comprehensive risk assessment, vendor management and compliance monitoring essential as accountability, even when using external providers, remains internal;
- **Vulnerability management:** adequate resources needed for regular, systematic assessments and continuous detection and patching efforts;
- **"Shadow IT":** balancing the need for risk control against the legitimate interest of users to innovate and avail of alternate solutions in a safe computing environment.

Cybersecurity: a system-wide priority?

Despite the existence of several important resources and mechanisms within the system, including apparent political will, there continue to be insufficient linkages between system-wide strategic direction and operational capacity that the system could mobilize towards strengthening its cybersecurity posture. The inter-agency machinery dealing with cybersecurity was found to be long established and generally functioning. At the same time, there is no single entity formally tasked with driving the agenda of a harmonized approach. The Information Security Special Interest Group, which operates under the auspices of the High Level Committee on Management, reports to the Digital and Technology Network, thereby mirroring the prevailing set-up observed within most organizations whereby the chief information security officer reports to the head of his or her respective ICT department, with all the benefits and limitations that such a set-up implies. Furthermore, in the absence of decision-making authority to compel action directly at the system level, the impact of the considerable body of work produced by the Information Security Special Interest Group has been limited in several ways, including by the fact that it has no operational capacity to implement agreements reached or recommendations made.

Inter-agency institutional and operational arrangements regarding cybersecurity



CEB
United Nations International Computing Centre
High-level Committee on Management
Management Committee
Representatives from each partner organization
Members: 41
Digital and Technology Network
Heads of ICT departments
Members: 30
Advisory Group
Representatives from select partner organizations
Inter-Agency Security Management Network
Senior managers
Members: 40
Common Secure Conference
Chief information security officers or equivalent from all cybersecurity clients
Members: 45
Information Security Special Interest Group
Chief information security officers or equivalent
Members: 31
Common Secure Cybersecurity Advisory Group
Chief information security officers or equivalent
Members: 3

Role of the United Nations International Computing Centre

The United Nations International Computing Centre, an inter-agency facility operating under the WHO financial rules and regulations, has been filling some of the gaps in this respect. About two thirds of the United Nations system organizations have benefitted from UNICC cybersecurity services on an opt-in basis for a number of years, with this area of the Centre's service catalogue having seen considerable and diverse growth. The Centre's business model is based on a cost-recovery and shared service model. Its offer is thus dependent on clients providing seed funding to upfront the costs of developing a new service to meet demand, while many can only afford to buy the service so developed once a critical mass of clients has already subscribed to it.

The Inspectors consider that the establishment of a trust fund to complement existing funding mechanisms with voluntary contributions earmarked for shared cybersecurity solutions benefiting the system has the potential to become a game changer in addressing some of the stumbling blocks towards an enhanced operational capacity for the system. In addition, there is an opportunity to build into the trust fund's governance mechanism an element of consultation with the competent inter-agency bodies that could further contribute to improving the somewhat strained dynamics between the mandated inter-agency mechanisms for the system and the UNICC as a privileged cybersecurity service provider. The executive heads of the participating organizations are further invited to reconsider current corporate arrangements and revisit opportunities for utilizing the Centre's 13 existing cybersecurity services and harness its as yet unrealized potential to assume a bigger role as an "operational arm" for cybersecurity in the system.

What the JIU recommends

The report includes five formal recommendations, which are complemented by 35 informal or soft recommendations as additional suggestions that, in the view of the Inspectors, could enhance the cybersecurity posture of the United Nations system.

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.

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.

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.

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.

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.

Click to access the full report

October 2021

JIU Reports 2020/2021

JIU/REP/2021/2, Review of United Nations system support for landlocked developing countries to implement the Vienna Programme of Action

JIU/REP/2021/1, Review of management and administration in the World Meteorological Organization

JIU/REP/2020/8, Review of mainstreaming environmental sustainability across organizations of the United Nations system

JIU/REP/2020/7, Blockchain applications in the United Nations system: towards a state of readiness

JIU/REP/2020/6, Multilingualism in the United Nations system

JIU/REP/2020/5, Enterprise risk management: approaches and uses in United Nations system organizations

JIU/REP/2020/4, Review of management and administration in the Economic Commission for Latin America and the Caribbean

JIU/REP/2020/3, Review of common premises in the United Nations system: current practices and future prospects

JIU/REP/2020/2, Policies and platforms in support of learning: towards more coherence, coordination and convergence

JIU/REP/2020/1, Review of the state of the investigation function: progress made in the United Nations system organizations in strengthening the investigation function

For all reports visit: https://www.unjiu.org/content/reports

For further information, please contact jiucommunications@un.org

ABOUT THE JIU

The Joint Inspection Unit is the only independent external oversight body of the United Nations system mandated to conduct evaluations, inspections and investigations system-wide.
Visit the JIU website for more information at www.unjiu.org