Executive Summary
In October 2022, the United Nations International Computing Centre (UNICC) hosted its annual Common Secure Conference with the special goal of bringing its cybersecurity clients and Partner Organizations together to expand the UN family cybersecurity community, share intelligence on cyber best practices and provide feedback on the UN Common Secure threat intelligence network and other services.

The five-day agenda included sessions by cybersecurity thought leaders and practitioners on topics that impact the UN family and the cybersecurity threat landscape, data protection and challenges in applying UN Privileges and Immunities in the digital world. The event also hosted networking activities, FIRST Security Incident Response Training, a Capture the Flag event and tabletop exercises.

Cyber criminals are collaborating more and more, so cybersecurity professionals need to step up on sharing information and intelligence to keep pace with cyber criminals. Common Secure member agencies need to connect with each other to share information and keep our UN Agencies secure and aware.

In October 2022, the United Nations International Computing Centre (UNICC) hosted its annual Common Secure Conference with UNDP and FIRST Security Incident Response Training.

Key Takeaways

1. Internationally accepted best practices and standards
   - Drawing lessons from the Common Secure model, the use of standardized frameworks, processes, and metrics will help improve cybersecurity practices across agencies, increasing common approaches towards UN consensus on cybersecurity.

2. Capacity building, cybersecurity awareness and training
   - Capacity building is crucial in organizational resilience and critical with regard to changing roles and responsibilities. Security awareness is the first line of defense and the best way to protect organizational assets and prevent incidents from taking place. Investing in awareness helps us in understanding the bigger picture.

3. Cloud security and data governance
   - As digital solutions are increasingly cloud-based, cloud security drives on-demand business continuity and resilience. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously. Prevention is the best protection. The Common Secure model is crucial in cloud environments.

4. Threat intelligence networks and threat data correlation
   - Sharing threat intelligence within the UN cybersecurity community builds trust and reduces risk. Leveraging threat intelligence across agencies increases offer vector detection and fast threat remediation. Incorporating a threat intelligence network and sharing threat data across agencies is critical in protecting against cyber threats.

5. Zero trust
   - A zero trust-based cybersecurity architecture is the way forward. Zero trust empowers users to engage with cloud providers on issues related to data sovereignty and UN Privileges and Immunities.

6. Data protection
   - UN Security is crucial to bridge the gap between legal and technical realities where UN data is at risks to data privacy. Cybersecurity is a serious concern for the UN, therefore, data protection and privacy are crucial. The Common Secure model is an approach to protecting privacy.

7. Cybersecurity in the form of cybercrime.
   - Cybersecurity experts need to play a direct role in chronic Management to better live with the COVID pandemic.

8. Sharing threat intelligence within the UN cybersecurity community builds trust and reduces risk. Leveraging threat intelligence across agencies increases offer vector detection and fast threat remediation.

9. Cybersecurity awareness is the first line of defense and the best way to protect organizational assets and prevent incidents from taking place.

10. Capacity building is crucial in organizational resilience and critical with regard to changing roles and responsibilities.

11. As digital solutions are increasingly cloud-based, cloud security drives on-demand business continuity and resilience.

12. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

13. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

14. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

15. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

16. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

17. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

18. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

19. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

20. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

21. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.

22. Preventing data loss is a problem data protection, exploitation and analysis always occur simultaneously.