UNICC Common Secure Conference with UNDP and FIRST

3 - 7 October 2022

Executive Summary

In October 2022, the United Nations International Computing Centre (UNICC) hosted its annual Common Secure Conference with the 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 UNICC 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 system such as cybersecurity threat landscapes, data protection and challenges in applying UN Privileges and Immunities in the digital world. The event also featured networking sessions, 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 intelligence and information to keep pace with cyber criminals. Common Secure members can envision a UN family to collect and share information to keep our UN Agencies secure and aware.*
>
> **Tima Soni** | Chief, Cybersecurity Division, UNICC

22

UN Agencies

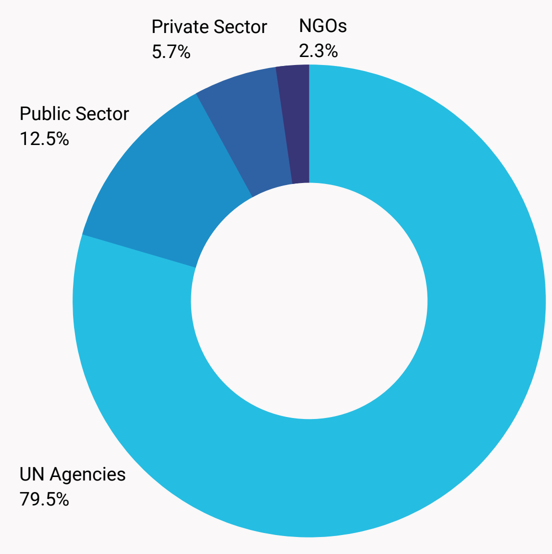

Figure 1. Onsite participants

260+

Participants

178

Remote

88

Onsite

Key Takeaways

1 Internationally accepted best practices and standards

Strengthening the organizational cybersecurity posture maximizes business value and misson-delivery effectiveness. Best-practices frameworks and standards can address high-severity risks and high impact breaches. Scientific, analytical methods optimize inflection points and advance innovative technologies to counteract human cognitive biases, just as cybersecurity capacity-building and learning create a culture of awareness. 'Secure by default' controls, automatically incorporated into digital product development, are better than trying to retro-fit last-minute, self-defeating security controls.

There is no way that we can get to the outcomes that we all want - that we all need - without leveraging science and technology, with adequate capacity building.

Amandeep Singh Gill
UN Secretary-General's Envoy on Technology

2 Collaboration during the pandemic and forming a new normal

The COVID pandemic has pushed businesses and individuals to form new normal, hybrid work practices, with more home office work (with non-organizational security controls) and more data exchange across borders, increasing possible attack vectors. Endpoint management, effective crisis response, cross-boundary collaboration and organizational resilience enable secure and high-functioning business operations. With this new normal, cybersecurity experts are increasingly in demand.

Cybersecurity experts need to play a larger role in crisis management to better 'live with COVID-19.'

Lyle McFayden
Senior Solution Architect, UNICC

3 Capacity building, cybersecurity awareness and training

Capacity building is crucial to organizational resilience and to deal with the shortage of cybersecurity professionals. Security awareness and training for UN personnel reduces cyber-attacks and prevents intrusions from threat actors. Learning techniques like gamification can foster a cultural code of conduct that helps to mitigate real-world security incidents and make cyber awareness and learning both fun and rewarding.

Security awareness is the springboard for security intelligence.

Sandy Jourdain
Information Security Analyst, UNDP

4 Threat intelligence networks and threat data correlation

Sharing threat intelligence within the UN cybersecurity community builds trust and mitigates risks. Meaningful threat data correlation creates in-depth intelligence and successful responses to UN Agency threat environments. Enriching and automating threat intelligence enhances cybersecurity tools and platforms, enriching cybersecurity analysts' work and ensuring a proactive approach to protecting international organizations.

Leveraging threat intelligence to enrich security incidents helps us in understanding the bigger picture.

Martin Paulinyi
Cybersecurity Operations, World Health Organization

5 Cloud security and data governance

As digital solutions are increasingly cloud-based, cloud security drives organizational cybersecurity initiatives. Cloud security has a data problem: data collection, exchange and analysis always involves risk and requires adequate privacy and protection. Preventive controls like threat intelligence automation in cloud environments reduces security incidents.

Security must be built-in and managed at scale.

Kathleen Moriarty
Chief Technology Officer, Center for Internet Security

6 Zero trust

A zero trust-based cybersecurity architecture is the way forward. Zero trust architecture means identifying protection surfaces, building security controls to protect organizational assets and monitoring access with the aim to prevent data breaches.

The Common Secure conference was great, maybe adding even more sessions on common issues among our organizations and more on how different organizations are approaching those issues, with lessons learned it would be even better.

Anonymous survey respondent
Common Secure Conference 2022

7 Data privacy and protection

UN Agencies need to bridge the gap between legal and technology teams when it comes to data protection and privacy. It is important to build technical and legal controls to protect sensitive information before it is stored with cloud providers. UN Agencies must come together to negotiate with cloud providers on issues related to data sovereignty and UN Privileges and Immunities.

Cybersecurity officers are best placed to assess risks to data and can provide valuable advice to their organizations regarding the most appropriate security controls to protect data and manage its implementation

Sebastian Vanegas
Data Protection Specialist, WFP