Session Outcome Document

How .POST powered services build Cyber Resilience within the global Postal and Logistics Sector

Universal Postal Union

Thursday 10 July 2025 – 09:00 to 10:00 am

https://www.itu.int/net4/wsis/forum/2025/Agenda/Session/195

Tangible Outcomes of the session

- **Digital Transformation of Postal Services**: Postal services are rapidly expanding their digital offerings far beyond traditional mail, acting as multi-sector digital service providers for e-commerce, financial services, e-government, and health services, often serving as "one-stop shops" for digital inclusion.
- **Significant Cybersecurity Gaps**: Despite this digital expansion, the postal sector exhibits suboptimal cybersecurity hygiene, with low implementation rates for critical practices like cybersecurity training, risk management, and incident response plans.
- **Regional Disparities**: Developing regions, specifically Latin America and the Caribbean, Asia and the Pacific, and Africa, show the lowest adoption rates of cybersecurity best practices and inadequate budget allocations.
- **Budget-Workload Mismatch**: Cybersecurity budgets are not keeping pace with increased workloads; less than half of posts increased their budgets despite 70% experiencing higher cybersecurity demands.
- **Global Nature of Threats**: Cyber threats, including brand impersonation, phishing, ransomware, and supply chain attacks, are a universal phenomenon affecting postal services in both developed and developing countries, often exploiting public trust in postal brands.
- **Human Element as Weakest Link**: The human layer remains a critical vulnerability, necessitating comprehensive awareness training for both postal employees and citizens alongside technical measures.
- **Importance of Collaboration**: International and cross-sector collaboration—through formal agreements, sector-specific CERTs, and information-sharing platforms—is essential for strengthening postal cybersecurity resilience.
- **Role of Posts in Digital Inclusion**: Posts are positioned as critical infrastructure and trusted community hubs that can provide human-touch access points for digital services, especially beneficial for underserved populations.

Call to action:

- Continue rolling out the UPU .POST domain initiative to provide a secure digital identity and services for postal operators in their e-business. (WSIS Action line C7)
- Implement the Postal Sector Information Sharing and Analysis Centre (POST-ISAC) to enable secure and confidential threat intelligence sharing among posts and supply chain stakeholders.
- Expand the UPU SECURE.POST platform to include comprehensive cybersecurity testing and learning resources, in addition to its current URL checking service.
- Continue implementing UPU digital readiness assessments in member states through partnerships like the CTU-UPU MOU.
- Maintain and expand joint incident response simulations and real-time monitoring partnerships between national cybersecurity authorities and postal services, as demonstrated by Albania
- Provide special funding packages for Small Island Developing States (SIDS) and Least Developed Countries (LDCs) to support their secure digital transformation efforts.
- Prioritise continued upskilling of postal staff in digital literacy, platform-specific training, and cyber hygiene practices.

Key Recommendations and Forward-Looking Action Plan for the WSIS+20 Review and Beyond (2–5 bullet points presenting concrete actions and guidance to inform the WSIS+20 Review by UNGA and build the multistakeholder vision of WSIS beyond 2025)

- **Enhance Cybersecurity Training and Awareness:** Implement comprehensive cybersecurity training programs for postal employees and end-users, focusing on risk management, incident response, and safe digital practices to mitigate human vulnerabilities.

- **Strengthen Financial Investments in Cybersecurity:** Advocate for governments and postal operators to align cybersecurity budgets with the increasing demands of digital transformation, ensuring adequate funding for cybersecurity initiatives, especially in developing regions.

- **Facilitate International Collaboration:** Promote the establishment of formal agreements and cooperative frameworks for cross-sector information sharing, including the formation of sector-specific CERTs and global threat intelligence platforms tailored for postal services.

- **Support Digital Inclusion Initiatives:** Encourage postal services to leverage their unique position as trusted community hubs, actively engaging in digital inclusion efforts that provide access to e-commerce, financial services, and other critical digital tools for underserved populations.

- **Expand and Promote Digital Security Frameworks:** Accelerate the rollout of the UPU .POST domain initiative to strengthen digital identities for postal operators, implement the POST-ISAC for secure threat intelligence sharing, and enhance the UPU SECURE.POST platform to capitalize on cybersecurity testing and learning resources.