ITUEvents

Regional Cybersecurity Summit for Africa

20-23 November 2023
Kampala, Uganda

itu.int/go/_RCSSA

Supported by: Hosted by: Organized by:

The International Telecommunication Union (ITU) in collaboration with the Uganda Communications Commission (UCC) and the Uganda Computer Emergency Response Team (UgCERT) and with the support of AfricaCERT jointly organised a Regional Cybersecurity Summit for Africa in Kampala, Uganda from 20 - 23 November 2023.

In our progressively interconnected global landscape, cybersecurity is becoming paramount for the safeguarding of delicate data, fortification of vital infrastructure, and bolstering trust in our digital transactions. The ITU Plenipotentiary Resolution 130, which underscores the need to reinforce the role of the ITU in building confidence and security in the application of ICTs, acts as a central and guiding principle for this Regional Cybersecurity Summit.

This summit, dedicated to addressing security and cyber resilience of critical infrastructure and digital services , also conformed to multiple other key resolutions such as WTSA Resolution 50 concerning cybersecurity, WTSA Resolution 58 advocating for the creation of national computer incident response teams, and WTDC Resolution 69 which supports the formation of computer incident response teams (CIRTs), especially in underdeveloped nations, along with fostering their collaboration. The summit also recognized and abided by WTDC Resolution 45, which endorses enhanced cooperative strategies in the realm of cybersecurity, including fighting and reducing spam.

Furthermore, the summit's goals were aligned with the priorities of Africa's regional initiative 3, which emphasized trustworthiness, safety, and security in the deployment of telecommunication/ICTs as well as the protection of personal information, and WTSA Resolution 89 that proposes the use of ICTs to bridge the gap in financial inclusion.

The Summit gathered **183 participants** from **39 countries** across the first three days (20-22 November 2023) and **47 participants** from **17 countries** for the meeting of ITU-T Study Group 17 Regional Group for Africa (SG17RG-AFR). It was composed of the following themes/events:

- **20 November 2023 -** Theme: Strengthening security in the digital economy
- **21 November 2023 -** Theme: Security and cyber resilience of critical infrastructure and digital financial services
- **22 November 2023:** CyberDrill

- **23 November 2023:** Meeting of ITU-T Study Group 17 Regional Group for Africa (SG17RG-AFR)

A two-part bridging the standardization gap (BSG) training also took place during the Summit as the final session on 21 November and as part of the meeting of the ITU-T Study Group 17 Regional Group for Africa (SG17RG-AFR) on 23 November.

The Summit achieved the following objectives:

- Introduced the work of ITU-T Study Group 17 and showcased several key standards on security including Recommendations ITU-T X.1060 on "*Framework for the creation and operation of a cyber defence centre*", ITU-T X.1150 "*Security assurance framework for digital financial services*" and ITU-T X.1352 "*Security requirements for Internet of things devices and gateways*";
- Facilitated the exchange of best practices, experiences and lessons learned on security baselines for digital infrastructure and security for emerging technologies;
- Explored approaches to assess cyber resilience of critical infrastructure in telecommunication networks with a focus on critical infrastructure and security for digital financial services;
- Showcased the ITU DFS security lab and the practical guidance available on implementing robust security assurance frameworks for digital financial services;
- Promoted the ITU-T Bridging Standardization Gap programme in supporting standardization, capacity building on regulation in developing countries and facilitating participation of developing countries in international standardization in ITU-T; and
- Provided a platform for cybersecurity experts from Africa to participate in hands-on cybersecurity simulation exercises and strengthen their preparedness, resilience and coordination to safeguard critical infrastructure and respond to emerging threats in the cybersecurity landscape.

The presentation material, session recordings and photos are available at: https://itu.int/go/_rcssa.

Summary of Day 1 - Theme: Strengthening security in the digital economy

The first day of the summit explored diverse dimensions of cybersecurity, starting with a keynote that highlighted the human element in cybersecurity. It stressed the need for personalized approaches, addressing challenges faced by different demographics, and called for relentless awareness, digital literacy, and a positive organizational culture. The first session delved into the adoption of international cybersecurity standards, with emphasis on Recommendation ITU-T X.1060 and urging all stakeholders to consider the adoption of international standards, including Rec. X.1060, for comprehensive cybersecurity measures. The second session focused on security baselines for digital infrastructure. It highlighted the proactive and continuous nature of cybersecurity efforts, covering aspects from deploying skilled teams to balancing security with usability and keeping up to date with regulatory changes. The third session explored evolving strategies for emerging technologies, advocating for collaboration, data utilization, and a holistic approach. Finally, Day 1 concluded with a session dedicated to providing a complete view of ITU-D's activities on cybersecurity.

The discussion in each session is summarised as follows:

i) Keynote: The human element in cybersecurity

In addressing the human element of cybersecurity, the presentation highlighted the diverse challenges faced by different demographics. From susceptibility to fake news for adults to the risks of children downloading games and clicking links, the focus is on tailoring cybersecurity awareness to individual needs. The call to action emphasizes fostering a relentless awareness of cybersecurity, promoting digital literacy, and cultivating an organizational culture that influences positive behavioural change.

A crucial aspect is communicating cyber empowerment over fear, utilizing clear “dos” and “don'ts”, and employing relatable language to make cybersecurity concepts accessible. The presentation highlighted the personal and financial impacts of cyber threats, emphasizing the continuous nature of cybersecurity efforts. Parental involvement is encouraged, urging conversations with children about responsible online behaviour, data protection, AI, and the potential risks associated with clicking on links.

ii) Session 1: Enhancing national cybersecurity frameworks with international cybersecurity standards - CDC framework and transition strategies

The session underscored the important role of adopting and implementing international standards as the cornerstone for robust and resilient cybersecurity in the national cybersecurity strategy. Recommendation ITU-T X.1060 stands out as an exceptional tool in enhancing cybersecurity resilience of public and private organizations. The standard provides a succinct common language for cybersecurity, codifying services, and listing security services as best practices. It offers a structured approach to establish and operate CDCs effectively with a catalogue of 64 services in 9 categories. The presentation highlighted the importance of aligning existing security functions, such as Security Operations Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs), with the X.1060 framework, ensuring a comprehensive and strategic approach to cybersecurity management. The successful implementation of this framework standard complemented with unique local specifications, as exemplified by Algeria Telecom, further reinforces its efficacy.

Additionally, insights from AfricaCERT highlight the significance of statistics they shared, revealing that only about 50% of respondents from their survey have started implementing the CDC. This emphasises the urgency for nations to prioritise and accelerate the adoption of comprehensive cybersecurity measures.

iii) Session 2: Security baselines for digital infrastructure

The focus was to share experiences on establishing security baselines for digital infrastructure, specifically within the contexts of e-government services and telecommunications. The first presentation shared the experience of Uganda in developing security baselines for e-government services with key takeaways emphasizing the importance of deploying a skilled and competent team, having a comprehensive plan that considers industry adversarial profiles and stakeholder concerns, and enforcing uniformity through documentation and automation. The second presentation outlined the security architecture framework for e-government services in Côte d'Ivoire, covering aspects such as a strategy for achieving zero paper by 2030, legal and policy considerations, and digital trust services. The final presentation addressed security baselines for digital infrastructure from a telecommunication operator’s perspective in Uganda, discussing approaches and challenges, including resource constraints, the complexity of digital infrastructure, and the need to balance security and usability.

The overall theme of the session highlighted the continuous and proactive nature of creating, implementing, and enhancing security baselines. It emphasized the need for organizations to address challenges systematically, such as resource constraints, the evolving technological landscape, and the human factor, by combining technology solutions with robust training programs and staying informed about regulatory changes. By doing so, organizations can establish and maintain a resilient security posture for their digital infrastructure.

iv) Session 3: Evolving security strategies for emerging technologies

The focus was on evolving security strategies for emerging technologies, exploring innovative approaches to regulation using statistical insights to fortify regulatory frameworks in the rapidly changing digital landscape. The first presentation delved into the crucial role of data and statistics in supporting cybersecurity, emphasizing the importance of defining cybersecurity, learning from industry and ITU, and leveraging collaboration for effective cybersecurity measures. General lessons highlighted the empowerment, communication, and impact that data and statistics bring, emphasizing stakeholder buy-in, a culture of data, and the need for collaboration and awareness. Looking ahead, the direction pointed towards enhanced collaboration, technology integration, and further automation.

The second presentation tackled evolving security strategies for artificial intelligence (AI), emphasizing the crucial role of an effective Security Operations Center (SOC) enhanced by AI to counter evolving cyber threats. The discussion covered challenges and opportunities in AI security, comparing traditional security measures with AI-specific strategies, and the importance of preventing bias in AI models for fairness and ethical use. The final presentation addressed IoT security in the evolving threat landscape, providing implementation-guiding best practices to secure innovative progress. It covered the IoT threat landscape, global standards, industry history, and anti-abuse measures, stressing the importance of addressing threats from increasing IoT device numbers and growing bandwidth for botnet traffic. Overall, the session highlighted the holistic approach needed, combining technical measures, organizational responsibility, and ongoing vigilance in the face of evolving technologies.

v) Session 4: Facilitating a trusted cyberspace for all - Overview of ITU-D activities

This session introduced the activities of the Telecommunication Development Sector (ITU-D) (https://www.itu.int/itu-d/sites/cybersecurity/) in supporting the ITU membership – particularly developing countries – to increase cybersecurity capabilities at the national level, in order to enhance security and resilience, build confidence and trust in the use of ICTs – making the digital realm more safe and secure for everyone. The presentation covered the areas of intervention spanning technical support, strategy support, cybersecurity inclusion and data & advisory as well as various initiatives and methods applied to develop impact including CyberDrills, national CIRT establishment & enhancement, support in development of national cybersecurity strategies, the Women in Cyber mentorship programme, the Her CyberTracks Project, the Cyber for Good project as well as an overview of the activities undertaken under and the Global Cybersecurity Index (GCI) and its impact.

Summary of Day 2 - Theme: Security and cyber resilience of critical infrastructure and digital financial services

Day 2's sessions covered a diverse range of topics related to security of critical infrastructure and digital financial services (DFS). The first session addressed cybersecurity challenges to critical infrastructure, emphasizing the need for a proactive and collaborative approach in defending against evolving threats like DDoS attacks, ransomware, and social engineering. The second session featured a panel discussion on the roles of regulators and DFS providers in enhancing cyber resilience, showcasing insights from various stakeholders in the DFS ecosystem. The third session delved into the ITU's work on security and cyber resilience for DFS, covering the Digital Financial Services Security Lab, Cyber Resilience Assessment Toolkit, and the cybersecurity landscape for fintech and digital financial services. The fourth session highlighted country experiences in implementing the ITU DFS Security Lab, emphasizing collaboration between governments, regulatory bodies, and DFS providers to enhance cybersecurity. Finally, the fifth session provided a deep dive into Blockchain Secure Authentication (BSA) technology, addressing the cybersecurity threats faced by African countries and proposing BSA as a revolutionary solution for passwordless authentication in mobile payments. The day concluded with a session on Bridging the Standardization Gap, aiming to empower developing countries in participating effectively in the ITU's standards-making process, emphasizing the importance of inclusivity, skill-building, and creating relevant standards through engagement in regional groups.

Overall, the sessions provided comprehensive insights into strategies, challenges, and innovations in enhancing cybersecurity and digital financial services. The discussion in each session is summarised as follows:

i) Session 1: Addressing cybersecurity challenges to critical infrastructure

This session shared insights on strengthening cybersecurity for critical infrastructure and showcase some security considerations applied towards addressing cybersecurity challenges and enhancing cyber resilience of critical digital infrastructure.

The first presentation highlighted the importance of cyber resilience against abusive threats to infrastructure, particularly in the context of evolving DDoS attacks. The discussions delved into defending against DDoS attacks, the significance of data and statistics, and best practices in countering threats like ransomware and social engineering. It also addressed emerging threats such as artificial intelligence abuse, quantum computation, increased device counts, bandwidth implications, and supply chain vulnerabilities. The second presentation shared security considerations of Uganda for critical digital infrastructure, particularly the protection of e-government services. It emphasized the role of the National Information Technology Authority-Uganda (NITA-U) and the Computer Emergency Response Team/Coordination Center (CERT.UG/CC) in safeguarding critical information infrastructures. The importance of e-government services, cyber threats, data privacy, and measures for securing government networks were discussed, along with considerations for identity authentication, secure development practices, incident response planning, user awareness, regulatory compliance, collaboration with the private sector, and international cooperation.

Session 2: Panel discussion - The role of regulators and DFS providers in enhancing cyber resilience within the DFS ecosystem

This session delved into the roles of different stakeholders in the DFS ecosystem in bolstering cyber resilience within the DFS ecosystem. The panel discussion featured representatives from various stakeholders, including a payment aggregator i.e., Financial Technologies Service Providers Association (FITSPA), the banking sector i.e., representatives from the Central Bank of Uganda representative, and the Ghana Association of Banks (GAB) and from a DFS service provider i.e., MTN Mobile Money, Uganda. The panel provided valuable insights into the multifaceted roles of different entities, emphasizing the importance of a coordinated and comprehensive approach to cybersecurity in the DFS sector.

ii) Session 3: ITU work on security and cyber resilience for DFS

This session explored the guidance available from the ITU on security and cyber resilience for digital financial services.

The first presentation provided an in-depth overview of the ITU's Digital Financial Services Security Lab, detailing security recommendations, collaboration strategies with regulators and providers, and the DFS Security Lab's objectives. The second presentation introduced the ITU Cyber Resilience Assessment Toolkit, providing a self-assessment methodology for DFS entities to evaluate their cyber preparedness. It outlined phases, questions, and guidance results for a comprehensive assessment, contributing to the identification of threats and risks specific to digital financial services.

The final presentation discussed the cybersecurity landscape for fintech and digital financial services, presenting Recommendation ITU-T X.1150, *Security assurance framework for DFS*. The rise of fintech and digital financial services was explored in the context of their transformative impact on financial transactions. The challenges, trends in cyberattacks on the financial sector, and the security assurance framework, aligning with established standards, were highlighted. The session emphasized the importance of continuous monitoring of cyber threats, prioritizing security in DFS, and fostering a resilient cybersecurity approach, especially as DFS evolves globally.

iii) Session 4: Country experiences on DFS Security

The session focused on country experiences in implementing the ITU DFS Security Lab and the knowledge transfer as well as adoption of security best practices and standards for digital finance and fintech.

Uganda presented its experience in implementing the ITU DFS Security Testing Lab, emphasizing collaboration with telecommunication operators, the Central Bank, and DFS providers. The presentation also highlighted the lab's methodology for conducting security tests on mobile DFS applications and its role in providing guidance for implementing security recommendations. Tanzania, in its experience, also outlined their approach in adopting key ITU recommendations, including addressing SS7 vulnerabilities, SIM-related risks, and implementing security best practices for mobile apps. Knowledge transfer through training sessions and the continuous operation of the testing lab, with quarterly tests, are key aspects of Tanzania's approach. Additionally, the session covered the adoption and implementation of ITU DFS Security Recommendations in the Southern African Development Community (SADC) by the Communications Regulators' Authority of Southern Africa (CRASA).

The insights from these country experiences highlighted the collaborative efforts between governments, regulatory bodies, and DFS providers in enhancing cybersecurity in the digital financial space. The adoption of ITU recommendations and the operation of security labs were highlighted as effective measures to address evolving threats and promote a secure environment for digital financial services.

iv) Session 5: Deep dive on Blockchain Secure Authentication and deployment for passwordless authentication for DFS

In this session, the focus was on Blockchain Secure Authentication (BSA) technology and its application for passwordless authentication in mobile payments. The presentation highlighted the cybersecurity threats faced by African countries in the realm of access security, emphasizing the lack of cybersecurity protocols in about 90% of African businesses. The financial sector emerged as the primary target, with 68% of successful attacks directed at this sector, followed by telecommunications companies. Notably, the session pointed out the vulnerability of existing passwordless solutions, with 97% susceptible to phishing and push attacks.

The presentation also delved into the challenges and limitations of current access controls, including issues with passwords, multi-factor authentication (MFA), device vulnerabilities, and the growing threat landscape in cloud environments. Blockchain Secure Authentication (BSA) was presented as a revolutionary solution, adhering to a Zero Trust Framework and designed for security, privacy, and trust. Transitioning into the introduction of BSA, it was described as a fourth-generation authentication system that leverages hybrid blockchain technology for secure identity and access management. The session concluded with insights into the BSA technology overview, entities involved, a live demo, and its potential implementation in Digital Financial Services (DFS), including the development of a sandbox/testbed environment for testing passwordless authentication solutions based on blockchain. The standardization efforts in SG17 were also highlighted, underlining the commitment to secure authentication based on Distributed Ledger Technology.

v) Session 6: Bridging the Standardization Gap (Part 1)

The last session focused on the Bridging the Standardization Gap training, which aimed to enhance standardization capability of developing countries and empower effective participation in the ITU's standards-making process. The training introduced ITU, its objectives, and the structure of ITU-T, including Study Groups, Focus Groups, and workshops/symposia. Emphasis was placed on the importance of bridging the standardization gap to foster inclusivity in standards development, build skills for efficient participation, and create relevant standards through engagement in regional groups. Initiatives like the DFS Security Lab and United for Smart Sustainable Cities were highlighted, showcasing efforts to bridge this gap.

The session further introduced the work of Study Group 17, its structure, and the role of the Study Group 17 Regional Group for Africa. Opportunities for participation were outlined, emphasizing consistency of effort, communication, organizational strategy, collaboration, and resource utilization. The benefits of participation were highlighted, including capacity development, networking, and access to standards and recommendations. Lessons and recommendations were provided to address challenges, encouraging a proactive approach to enhance engagement in the standardization process.

Summary of Day 3 - CyberDrill

Day 3 began with a keynote emphasizing the importance of cybersecurity preparedness, highlighting the need for cyber simulation exercises, offering various types tailored to different needs. Following the keynote, a cyber drill experience sharing session was conducted featuring multiple speakers who provided insights into their experiences conducting cyber drills.

The cyber drill exercises followed which comprised of three distinct scenarios, each offering a unique focus and approach to enhance cybersecurity preparedness: website defacement investigation, DFS cyber resilience self-assessment, and phishing email/malware analysis. These hands-on exercises provided practical insights, fostering a proactive approach to cyber threats, and enhancing overall cybersecurity readiness. The CyberDrill is summarised as follows:

i) Keynote: Cyber drills: A tool to develop a proactive and robust security posture or the importance of security simulations

The keynote highlighted the significance of cybersecurity preparedness and incident response, emphasizing the design and review of incident response plans. It reviewed cyber threat trends and statistics for 2023, noting the increasing attack surface trend, with a focus on the Metaverse, artificial intelligence, deep fakes, rampant bots, and heightened attacks on critical infrastructures. The trends observed over the past 12 months included a targeting of accounting and financial data, sophisticated malware, ransomware, social engineering, payment through cryptocurrencies, and the growth of the Internet of Things industry. The increasing cost of cybercrime, predicted to reach $8 trillion in 2023, was also highlighted and the need for a cyber incident response plan was stressed. The structure of such a plan was outlined, covering incident response team, detection, assessment, communication, containment, investigation, documentation, training, and plan maintenance.

The keynote highlighted the importance of conducting cyber simulation exercises, citing their role in improving readiness, identifying weaknesses, providing training opportunities, fostering collaboration, and enhancing overall cybersecurity readiness. Different types of exercises, including table-top, capture the flag, red team vs blue team, and full-scale cyber-attack simulations, were presented, with considerations for choosing the appropriate method based on factors such as the number of participants, duration, financial resources, and organizational experience.

ii) Cyber drill experience sharing

The cyber drill experience sharing session featured speakers from Mauritius, Ghana and Uganda who provided insights into their experiences conducting cyber drills. The emphasis was placed on the significance of these exercises in bolstering the cybersecurity posture of a country. Various speakers shared practical knowledge and lessons learned from organizing cyber drills, highlighting the importance of such proactive measures in preparing for and mitigating cyber threats. Overall, the session contributed valuable insights and best practices drawn from real-world experiences to emphasize the role of cyber drills in fortifying national cyber resilience.

iii) Cyber drill exercises

The cyber drill exercises comprised three distinct scenarios, each offering a unique focus and approach to enhance cybersecurity preparedness.

Scenario A, facilitated by AfricaCERT, centred on a cyber-attack involving website defacement of a bank. The objective was to investigate the unauthorized access and modification of the bank's website, particularly understanding the methods used for defacement and potential vulnerabilities related to session/cookie exploitation. The scenario aimed to uncover insights into addressing these vulnerabilities and strengthening the overall cyber resilience of the targeted website.

Scenario B, facilitated by ITU/TSB, introduced the DFS Cyber Resilience Toolkit through an interactive tabletop session. Participants were divided into groups, each concentrating on a specific aspect of cybersecurity, including risk management, governance, testing, training & awareness, protection, and incident response. The toolkit facilitated a self-assessment for DFS entities, users, and actors in the telecommunication sector of the DFS ecosystem, aiming to improve overall infrastructure posture and prepare against cyber threats.

Scenario C, facilitated by UG-CERT, focused on phishing email and malware analysis. Participants took on the role of cybersecurity analysts tasked with scrutinizing a phishing email and investigating a suspicious document for potential hidden malware. The goal was to identify vulnerabilities, understand the malicious payload, and enhance capabilities in analysing and responding to such cyber threats.

Day 4 - Meeting of ITU-T Study Group 17 Regional Group for Africa (SG17RG-AFR)

Participation in the SG17RG-AFR meeting on 23 November 2023 was limited to Representatives of ITU Member States, ITU-T Sector Members and Academia from the African region, as well as Associates that belong to ITU-T Study Group 17 and the African region, in addition to participants invited by the regional group Chair, as defined in WTSA Resolution 54 (Rev. Geneva, 2022) (Resolves 4-6).

Access to meeting documents including the outcomes of the meeting are accessible to ITU-T members: https://www.itu.int/go/tsg17rgafr.

____