South Sudan School of Internet Governance (SS-SIG) 2026

- **Theme:** Shaping the Future of the Internet in South Sudan
- **Organized by:** ISOC South Sudan Chapter in collaboration with the SS-IGF Secretariat
- **Policy brief topic:** Strengthening Cybersecurity Preparedness in South Sudan
- **Session facilitator:** Innocent Vukeni Joseph_Head of SS-CIRT
- **SIG Training dates:** 20th – 22nd May 2026
- **Venue :** Scinius Hub

Executive Summary

As South Sudan expands digital services, the citizens, businesses, and institutions face growing cyber risks, including phishing, scams, account takeovers, ransomware, data breaches, and misinformation. The SS-SIG 2026 participants stressed that cybersecurity is not only a technical issue, but also a matter of trust and national development.

Discussions and simulations showed that low awareness, weak institutional capacity, poor reporting, and limited coordination continue to hinder cyber resilience. South Sudan now has an opportunity to strengthen its digital ecosystem before cyber incidents become more frequent and costly.

This brief recommends improving cybersecurity awareness, building incident response capacity, strengthening coordination, investing in skills development, and promoting early reporting and digital trust.

The Challenge

South Sudan's digital growth is increasing the exposure to cyber threats, while awareness and response capacity remain limited. Many users still fall victim to phishing, fraud, impersonation, and misinformation. Many institutions also lack trained staff, response procedures, and resources to detect and manage incidents.

During the simulation exercise, participants noted that organizations often struggle to separate rumors from verified incidents, leading to delayed responses and reduced public trust.

Key issues raised by participants

- Low public awareness of cyber threats.
- Weak cybersecurity capacity in institutions.
- No clear reporting channels for incidents.
- Misuse of social media for scams and misinformation.
- Poor coordination during cyber incidents.
- Limited investment in cybersecurity skills.

Prepared by: Richard Mawa Michael_IGF/SIG Rapporteur

To access online visit: www.internetsociety.org.ss or www.ssigf.org.ss

- **Why this issue matters to the public;**

Cybersecurity is essential for digital trust. People will only use digital services if they believe their data is safe and institutions can respond effectively to threats.
A major cyber incident affecting government, finance, telecoms, or public information systems could damage confidence in digital transformation. Building preparedness now is vital for development, service delivery, and national security.

Insights from the SS-SIG 2026 Practical Exercise

The simulation, which involved phishing, website defacement, misinformation, and alleged data breaches, highlighted five lessons:
1. Verify Before Acting: Confirm facts before making public statements.
2. Report Early: Report incidents immediately to designated focal points.
3. Coordinate Responses: Government, technical teams, law enforcement, telecoms, media, civil society, and affected organizations must work together.
4. Communicate Responsibly: Public communication should be timely, factual, and transparent.
5. Protect Rights and Trust: Responses must respect privacy, freedom of expression, and due process.

- **Policy Recommendations**

1. Strengthen the national CIRT/CSIRT to coordinate reporting, alerts, threat sharing, and technical response.
2. Integrate cyber hygiene into schools, universities, government institutions, and community programs.
3. Encourage users to enable multi-factor authentication, use strong, unique passwords, check suspicious links and messages, update devices and software, back up data regularly, and report incidents quickly.
4. Investing in training, certifications, simulations, and professional development.
5. Creating cooperation mechanisms among government, telecoms, financial institutions, academia, civil society, media, and technical communities.
6. Provide trusted reporting channels and encourage sharing lessons learned without blame.

- **Key Message**

South Sudan has a chance to build cybersecurity preparedness early in its digital journey. Cybersecurity should be seen as a shared national responsibility for protecting trust, services, institutions, and citizens. By investing in awareness, coordination, capacity, and response, South Sudan can build a safer digital future.

Discussion's guiding question

How can the government, private sector, civil society, academia, media, and the technical community work together to make cybersecurity everyone's responsibility in South Sudan?

Prepared by: Richard Mawa Michael_IGF/SIG Rapporteur

To access online visit: www.internetsociety.org.ss or www.ssigf.org.ss