APRICOT 2026

Fellowship Completion Report

Personal & Programme Information:

Full Name	Md Mahedi Hasan
Current Role	Senior Cybersecurity Analyst
Organisation	University of Dhaka
Country	Bangladesh
Fellowship Programme	Practical Cybersecurity for Internet Operators (PCIO) MasterClass, APRICOT 2026
Event Dates	4 – 12 February 2026
Venue	Sheraton Gandaria City, Jakarta, Indonesia

1. BACKGROUND AND MOTIVATION

I currently serve as Senior Cybersecurity Analyst at the University of Dhaka, where I am responsible for securing digital infrastructure used by more than 50,000 students, academic staff, and administrative personnel. The scope of this responsibility demands not only strong technical competence but also continuous, structured professional development aligned with the evolving threat landscape.

My engagement with the regional Internet community began at SANOG40, where I attended an APNIC security training programme. That experience was a turning point. It clarified how much structured, expert-led training remained ahead of me and introduced me to a broader community of practitioners navigating the same operational challenges across South and Southeast Asia.

The APRICOT 2026 Fellowship represented the most significant next step in that journey. It provided an opportunity to receive intensive, hands-on training from internationally recognised instructors, to engage with the Asia-Pacific operator community at a high level, and to contribute back through both active participation and a conference presentation.

2. PCIO MASTERCLASS: TECHNICAL TRAINING

The Practical Cybersecurity for Internet Operators (PCIO) MasterClass, delivered by the Network Startup Resource Center (NSRC), was the centrepiece of my fellowship. The three-day programme combined structured instruction with hands-on laboratory exercises across a comprehensive range of cybersecurity topics directly relevant to Internet operators and institutional network administrators. Instructors **Philip Paeps (NSRC)**, **Tashi Phuntsho (FLEXOPTIX/NSRC)**, and **Warren Finch (ISOC)** brought both technical depth and practical operational experience to each session.

Day-1: Infrastructure Security Foundations

The first day established a disciplined security methodology and covered the practical fundamentals of network infrastructure hardening, including structured security thinking, credential management with a hands-on password vault lab, and Layer 1/2/3 best practice configurations. Management network design, out-of-band (OOB) access architecture, and router and host security configuration each supported by practical lab exercises gave immediate, applicable depth to the instruction.

Switching security was addressed through VLAN segmentation, BPDU Guard, Dynamic ARP Inspection (DAI), and IP Source Guard. These controls are frequently deprioritised under operational pressure, yet they close significant attack vectors at the network access layer.

Day-2: Routing Security and BGP Best Practices

The second day addressed routing security, the most operationally critical area for any Internet operator. Sessions covered wireless security risk management, Layer 3 device security in Layer 2 environments, and a structured introduction to routing security principles. Practical laboratory work included router hardening procedures, eBGP configuration with transit providers, and the application of BGP best current practices in alignment with RFC 7454 and the MANRS framework.

Working through these exercises in a fully virtualised lab environment bridged the gap between theoretical understanding and hands-on competence. This is the kind of operational confidence that translates directly into production network improvements.

Day-3: Advanced Defensive Techniques and Incident Response

The final day covered advanced defensive mechanisms and incident preparedness. Unicast Reverse Path Forwarding (uRPF), a BCP 38-aligned control for defeating IP source spoofing, and Remote Trigger Blackhole (RTBH) filtering for real-time DDoS mitigation were each covered with hands-on labs. The RPKI Operations sessions were among the most directly impactful of the programme. We deployed an RPKI validator cache from scratch and configured route origin validation on routers, addressing BGP route hijacking risks that are a pressing concern for operators across our region.

The programme concluded with a Seven Layers of Basic Cybersecurity strategic framework, vulnerability management methodology, a session on firewalls and packet filters, and a tabletop incident response exercise. The tabletop exercise was particularly instructive. It demonstrated that composure, clear communication, and defined ownership are as critical as technical knowledge when responding to a live security incident.

Key Technical Outcomes

- **RPKI and Route Origin Validation:** Completed end-to-end deployment of an RPKI validator cache and router configuration, acquiring the practical skills to implement route origin validation on our university network.
- **RTBH Filtering:** Understood and practised both local and upstream RTBH signalling, establishing a viable DDoS mitigation capability for our infrastructure.

- **uRPF and BCP 38 Compliance:** Configured Unicast Reverse Path Forwarding in strict and loose modes, reinforcing source address validation as a network-wide operational standard.
- **BGP Hardening:** Applied RFC 7454 and MANRS best practices to eBGP sessions, including prefix filtering, max-prefix limits, and route policy discipline.
- **Layer 2 Security:** Implemented BPDU Guard, Dynamic ARP Inspection, and IP Source Guard, with improvements now planned for deployment across our campus network.
- **Incident Response:** Practised structured crisis decision-making through a tabletop exercise, reinforcing the value of documented runbooks, defined roles, and clear communication protocols.

3. FELLOWS SKILLS WORKSHOP, 8 FEBRUARY 2026

On 8 February, I attended the invitation-only Fellows Skills Workshop, facilitated by Aftab Siddiqui, William Stockbridge, and Terry Sweetser. This full-day session complemented the technical training with a focus on professional leadership, effective communication, and community contribution. These are the capabilities that determine how effectively technical expertise translates into lasting regional impact.

- **Technical Communication:** Structured exercises on presenting complex technical content clearly and persuasively to diverse professional audiences, directly applicable to my role as a conference presenter and internal trainer.
- **Leadership Under Pressure:** Scenario-based role-playing exercises simulating high-stakes security incidents, developing composure, prioritisation skills, and decisive communication under time-critical conditions.
- **Community Leadership:** Facilitated discussion on the professional responsibilities of fellowship recipients as future mentors and advocates within the regional Internet community, reinforcing the expectation of active contribution beyond individual organisational roles.

4. CONFERENCE PARTICIPATION AND COMMUNITY CONTRIBUTION

Alongside the MasterClass and Skills Workshop, I attended the main APRICOT 2026 conference from 9 to 11 February. Sessions on IPv6 deployment strategy, Internet exchange point (IXP) operations, DNS security, routing policy, and network automation provided important regional context. They offered a broad view of where the Asia-Pacific operator community is focused and what challenges practitioners are actively working to solve.

I was honoured to present at the conference, delivering a session titled ***"From Compromise to Resilience: A Practical Journey of Security Transformation,"*** which documented the University of Dhaka's experience recovering from a significant security incident and rebuilding a more resilient institutional network security programme. Presenting this experience to an international audience of operators underscored the community value of transparency, honest reflection, and shared operational learning.

Engagement with the NOC, the Peering Forum, and peer conversations throughout the event provided equally substantive learning. These interactions offered candid, practitioner-level insight into how operators across the region are managing the same infrastructure security challenges we face in Bangladesh.

5. KNOWLEDGE TRANSFER AND COMMUNITY IMPACT

The fellowship obligation does not conclude at the conference venue. The value of this training is fully realised only when it is carried back to the networks, teams, and communities that could not be present in Jakarta.

I have maintained an active commitment to knowledge sharing throughout my career, contributing to regional platforms including BDSAF, SANOG, bdNOG, APAN, Phoenix Summit, and BIGF. Each event I attend generates materials and insights that I share through presentations, internal training sessions, and published documentation. APRICOT 2026 has produced the most substantive body of transferable knowledge to date.

The following knowledge transfer commitments are currently in progress:

- **Regional Forum Presentations:** Presenting APRICOT 2026 learnings at upcoming bdNOG and SANOG events to share operational knowledge with the broader Bangladesh and South Asian operator community.
- **Fellowship Mentorship:** Actively encouraging and supporting the next cohort of fellowship candidates from Bangladesh, sharing both the application process and the professional value of sustained regional engagement.
- **Published Reference Materials:** Making workshop notes, lab summaries, and configuration guides from the PCIO MasterClass openly available to community peers who were unable to attend.

6. CONCLUSION

APRICOT 2026 was a professionally defining experience. The PCIO MasterClass equipped me with practical, immediately deployable technical skills. The Fellows Skills Workshop strengthened my capacity to lead, communicate, and contribute at a regional level. The conference programme and peer engagement provided the broader operational context in which those skills must be applied.

This fellowship was a direct investment in the security and resilience of the networks, institutions, and communities I serve. I am fully committed to honouring that investment through rigorous knowledge transfer, continued community contribution, and sustained engagement with the Asia-Pacific Internet community.

I extend my sincere gratitude to the APRICOT 2026 organising committee, the APNOG Board, APJII as the host organisation, and the fellowship sponsors for their commitment to building technical capacity across the region. Their investment makes a measurable difference.