BRUNEI CYBERSECURITY ASSOCIATION

December 2025 Newsletter

HAPPENING IN DECEMBER:

- BCSA appreciation dinner for CySec volunteers
- Cyber673 Session #14: CTF and Chill
- BCSA × ITE Singapore Overseas Learning Journey to Brunei
- Cyber Threat Intelligence Report
    - Iran-Nexus Threat Actor UNC1549 Takes Aim at Aerospace

ANNOUNCEMENT!

We are excited to share that the Brunei Cyber Security Association (BCSA) has moved to a new official website!

NEW WEBSITE	https://www.bcsa.bn
OLD WEBSITE	https://www.pksbrunei.org (***no longer in use***)

Please update your bookmarks and visit our website for the latest updates and events!

BRUNEI CYBERSECURITY ASSOCIATION

[Nabilah Salihin]

BCSA appreciation dinner for CySec volunteers

CYSEC Appreciation Night 2025 was held on **5 December 2025** at An-Naura Hall, Yayasan Complex, to honour the dedication and commitment of CYSEC 2024 and 2025 volunteers. The event brought together volunteers, leaders, and guests in a warm and meaningful gathering. The programme began with registration and the presentation of certificates to participating volunteers, followed by a Doa Selamat recited by Muizzuddin Mahdi. Opening remarks were delivered by Vice President Azizul Hasrin, who expressed sincere appreciation for the volunteers' continued support and contributions to CYSEC initiatives.

A highlight of the evening was the presentation of tokens of appreciation to distinguished recipients, namely Zara Laila Cheong, recognized for her achievement at the Top Women in Security ASEAN Region Awards, and Azizul Hasrin, recipient of the AJCCA Cyber Resilience Award. The evening concluded with refreshments, a lucky draw featuring five winners, and entertainment performances by Dayat Ahim and Danyel Shahjohan, creating a relaxed and celebratory atmosphere for all attendees.

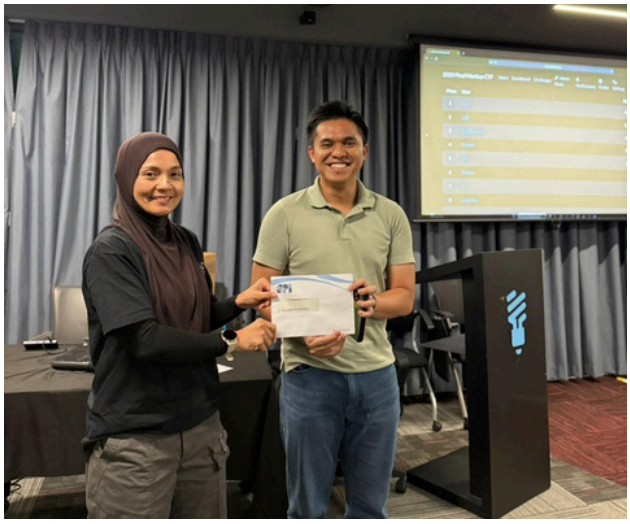
Cyber673 Session #14: CTF and Chill

cyber673 closed out 2025 with a chill, beginner-friendly mini-CTF celebrating 12 months of community meetups. Held on 10 December at Brunei Innovation Lab, the solo-format event featured bite-sized challenges spanning web, digital forensics, and misc categories—complete with a live scoreboard and progressive hints.

The evening wrapped up with year-in-review highlights, community shoutouts, and prizes for the top 3 participants, generously sponsored by Brunei Cyber Security Association and SPI BN Sdn Bhd.

Thanks to Swarmnetics, NitroSec, and SPI BN for powering the session, and Brunei Innovation Lab for hosting.

Here's to another year of learning, hacking, and growing together!



BRUNEI CYBERSECURITY ASSOCIATION

[Danial Asyraf]

BCSA × ITE Singapore Overseas Learning Journey to Brunei

The BCSA × ITE Singapore Overseas Learning Journey to Brunei, held from **14–19 December 2025** in Bandar Seri Begawan, brought together students, educators, and industry professionals from Brunei and Singapore to strengthen regional collaboration and cybersecurity talent development. Organised by the Brunei Cyber Security Association (BCSA) in collaboration with the Institute of Technical Education (ITE) Singapore, the programme combined institutional and industry visits, hands-on workshops, tabletop exercises, and interactive activities.

Participants gained valuable exposure to Brunei's cybersecurity ecosystem through visits to key organisations including Cyber Security Brunei (CSB), AITI, UNN, Politeknik Brunei, CyberSafe Brunei, EVYD Technology, Dynamik Technologies, and Universiti Teknologi Brunei (UTB). The learning journey enhanced understanding of cybersecurity operations, regulatory frameworks, incident response, and technical skills, while fostering cross-border knowledge exchange, professional networking, and ASEAN-level cooperation in cybersecurity.

BRUNEI CYBERSECURITY ASSOCIATION

Cyber Threat Intelligence Report

Iran-Nexus Threat Actor UNC1549 Takes Aim at Aerospace

Iran-nexus threat actor UNC1549 has conducted a sophisticated cyber espionage campaign targeting the aerospace and defense sectors and leveraging third-party relationships, spear-phishing, and custom malware to gain and maintain access. Operating from late 2023 through 2025, UNC1549 exploited trusted third-party vendors and virtual desktop infrastructure (VDI) to infiltrate high-security environments. Once inside, they used advanced lateral movement techniques, such as stealing victim source code for spear-phishing campaigns that use lookalike domains to bypass proxies and abusing internal service ticketing systems for credential access. Post-exploitation activity involves custom tools, including the TWOSTROKE backdoor for command-and-control (C2 or C&C) communication, the Lightrail tunneller, and the Deeproot file manager. The actor also uses a tool called DCSYNCER.SLICK to extract NTLM password hashes from domain controllers and SIGHTGRAB for visual data capture. To evade detection, the group deletes forensic artifacts and uses SSH reverse tunnels to hide activity from endpoint detection and response (EDR) agents.

Click **here** to read more

BRUNEI CYBERSECURITY ASSOCIATION

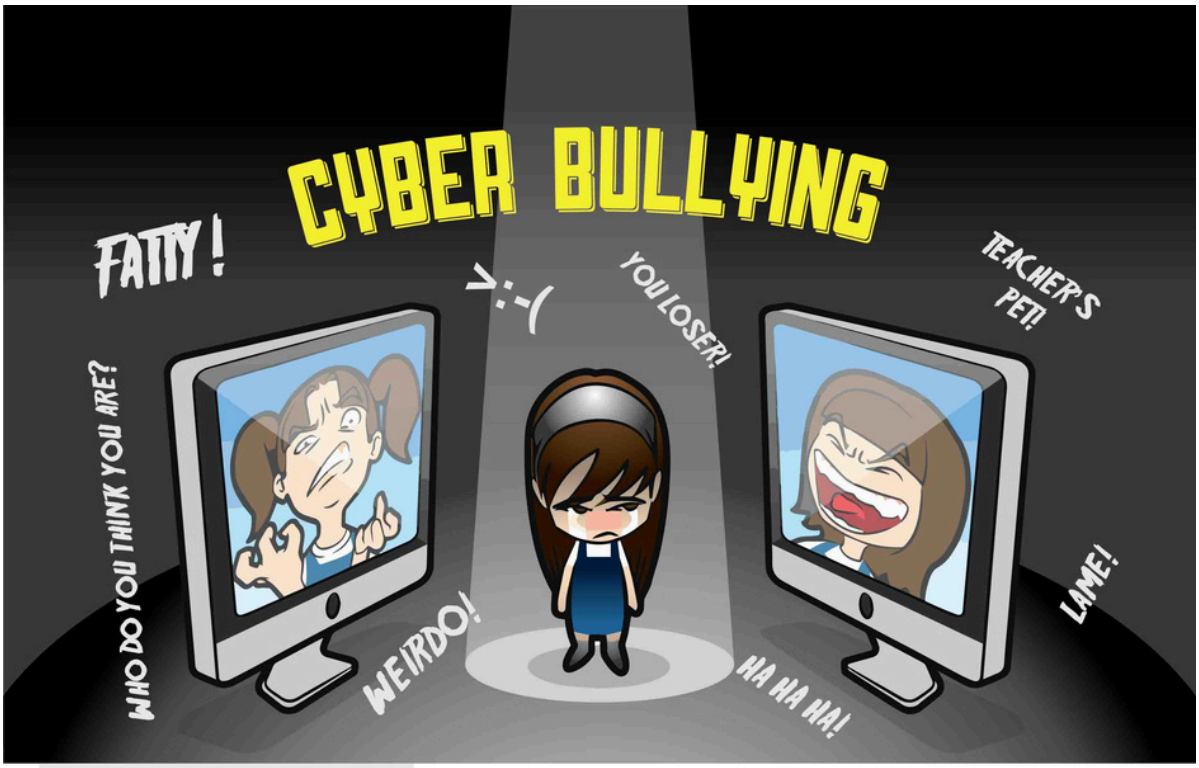
Professional Training & Certification Program Schedule 2026

BRUNEI CYBERSECURITY ASSOCIATION

Professional Training & Certification Program January 2026

BRUNEI CYBERSECURITY ASSOCIATION

Be Smart. Be Safe.
Say No to Cyber Bullying



Cyber bullying occurs when the Internet or mobile phones are used to harm other people in a deliberate, repeated, and hostile manner. This includes threatening, intimidating, harassing, or causing embarrassment to the victim. It often occurs in social networks, blogs, through SMS, email or instant messaging. In Brunei, it is common for people to express their anger or frustration through social networking sites such as Facebook, Twitter and MySpace. If these online posts are directed at a specific person, it could lead to cyber bullying.

Most cyber bullies are often motivated by anger, revenge or frustration. Many do it for their own entertainment or to get a reaction.

IF YOU ARE BEING CYBER BULLIED

» Do not react to a bully. It might only motivate them more.

» Do not reply to any messages from a bully.

» If you are being cyber bullied by someone on a social network, you can "Block" or "Unfriend" them.

» If you are being cyber bullied by phone, you could change your phone number.

» Do not delete messages from a bully. They can serve as evidence when you lodge a report about the bullying.

» Report the bullying to your parents or even to the police.

» Many social networking sites allow users to report cyber bullying. For example, you can report bullying on Facebook's Help Center.

BEST PRACTICES

» Be careful what photos and personal information you post on the Internet. Keep in mind that anything you post might be seen by anyone in the world.

» If someone has posted something negative about another person, do not "Like" the post. When you "Like" it, you are supporting the bully's behaviour.

» Do not assume a picture of someone you met online is real. Often, what you see on the Internet or on social networking sites is not true.

An initiative by BRUCERT (Brunei Computer Emergency Response Team)

A team under CSB (Cyber Security Brunei)

Learn more about online safety

SVC secure verify connect

www.SecureVerifyConnect.info

@bruneicert

Report any Cybersecurity Incident here

BRUNEI CYBERSECURITY ASSOCIATION

Stop the Leak: Protect Your Digital Identity

184 Million Passwords Leaked

Is Your Account at Risk?

A massive data breach exposed 184 million usernames and passwords. Popular platforms like Facebook and Google are affected

Why You Should Be Concerned

Leaked passwords can be used to:

- Break into your accounts
- Steal your identity
- Make unauthorized payments

Even if you haven't been targeted yet, your info could be out there.

How to Check if You're Affected

- Go to **haveibeenpwned.com**.
- Enter your email to see if it's in the breach.
- If yes, you need to update your passwords immediately.

What You Should Do

- Use unique, strong passwords or passphrases
- Turn on Multi-Factor Authentication (MFA)
- Change passwords regularly (email, banking, work)

Best Practices

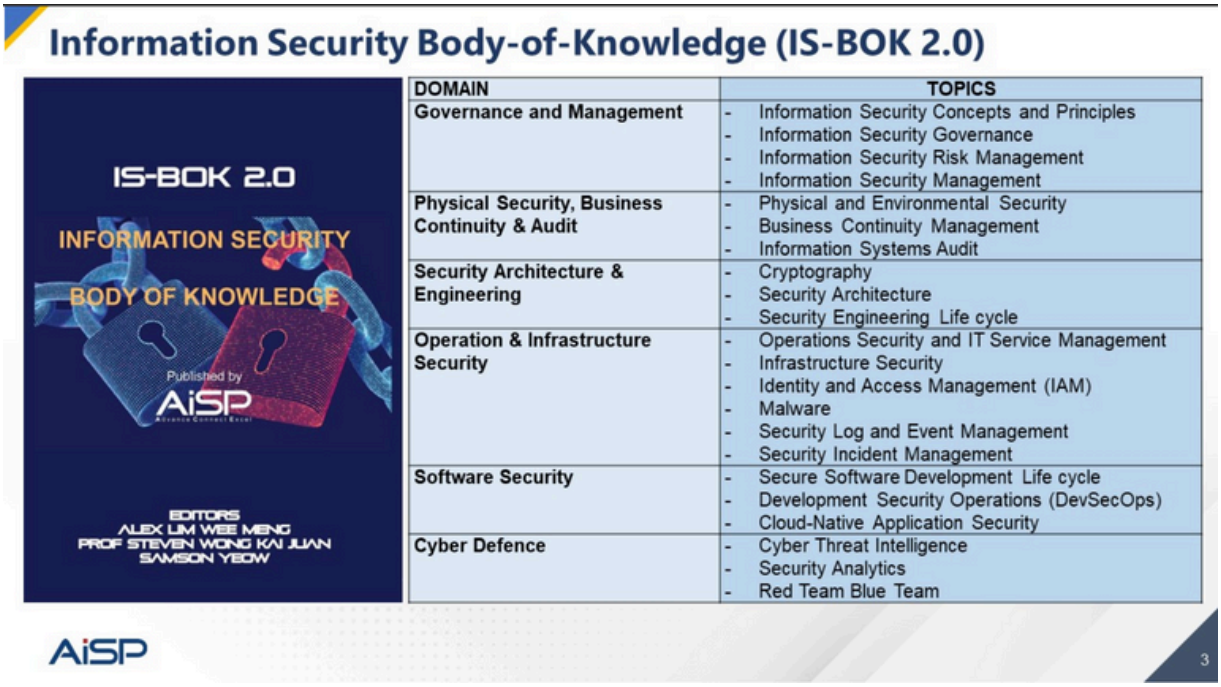
- Don't reuse passwords
- Log out of unused sessions
- Remove saved passwords from browsers
- Backup data offline
- Avoid suspicious links and downloads

BRUCERT | SVC secure verify connect

Report any Cybersecurity Incident here

BRUNEI CYBERSECURITY ASSOCIATION

Preorder IS-BOK 2.0 Information Security Body of Knowledge Published by AiSP



Since 2009, the Association of Information Security Professionals (AiSP) has developed the Information Security Body of Knowledge (IS BOK) to support professionals in building and updating their expertise. The latest BOK 2.0 aligns with Brunei's cybersecurity landscape, referencing the Skills Framework for Infocomm Technology. Continuously evolving, it prepares professionals for industry applications and is covered in the NICF – AiSP Qualified Information Security Professional (QISP®) Course.

For more information, click here

BRUNEI CYBERSECURITY ASSOCIATION

Nitro Security T-Shirt Order

Click here or scan the QR Code to order

BRUNEI CYBERSECURITY ASSOCIATION

Preorder Brunei Cybersecurity Association Polo-Shirt

Type	Sizes	Price (BND)
Short Sleeve	XS - 2XL	$20
	3XL	$21
	4XL	$22
Long Sleeve	XS - 2XL	$22
	3XL	$23
	4XL	$24

Preorder here

www.bcsa.bn contact@bcsa.bn @bcsa.bn +673 8382272

BRUNEI CYBERSECURITY ASSOCIATION

Join Our Membership!

PROFESSIONAL / FELLOWSHIP: BND45

BENEFITS

- Exclusive access to resources, events, and recognition
- Mentorship and leadership opportunities
- Get discounts on training programs
- Advance your career with our high-level network

REQUIREMENTS

- **EXPERIENCE:** Minimum three (3) years of experience in relevant fields with a recognized degree OR five (5) years of experience with a non-related degree or no degree.
- **CV SUBMISSION:** Required.
- **PROFESSIONAL INVOLVEMENT:** Demonstrates significant engagement in information security or related areas.
- **COMMITTMENT:** Must adhere to a code of conduct and actively participating in BCSA activities.

ORDINARY: BND30

BENEFITS

- Access to a wealth of resources and professional development opportunities
- Discounts on training and certifications
- Be represented in industry and government forums

REQUIREMENTS

- **EXPERIENCE:** Minimum one (1) year of experience in relevant fields with a recognized degree OR three (3) years of experience with a non-related degree or no degree.
- **CV SUBMISSION:** Required.
- **COMMITTMENT:** Must adhere to a code of conduct and actively participating in BCSA activities.

AFFILIATE: BND20

BENEFITS

- Connect with industry professionals and explore partnerships
- Get discounts on training programs
- Your voice in the cybersecurity landscape

REQUIREMENTS

- **INTERESTS:** Open to individuals who are passionate about cybersecurity, regardless of their formal background in the field.
- **COMMITTMENT:** Encouraged to engage in BCSA events and activities to deepen their knowledge and involvement.

STUDENT: BND15

BENEFITS

- Access to essential resources and networking events
- Exclusive discounts on training and certifications
- Get discounts on training programs
- Mentorship and career development opportunities

REQUIREMENTS

- **ELIGIBILITY:** Open to any students currently enrolled in an educational institution with a valid student status.
- **COMMITTMENT:** Encouraged to engage in BCSA events and activities to deepen their knowledge and involvement.

Register your interest here!

www.bcsa.bn contact@bcsa.bn @bcsa.bn +673 8382272