Asian Institute of Insurance

(Formerly known as Malaysian Insurance Institute)

Cyber Risk & Cybersecurity Briefing for Board Members

DATE:
July 17, 2025

TIME:
9.00 a.m. – 5.00 p.m.

VENUE:
Aii Training Room, level 2,
AICB Building, Kuala Lumpur

CPD HOURS:
7 Hours

Proficiency Level: Mastery

FSF
FUTURE SKILLS FRAMEWORK
MALAYSIA

31 Prime Skills
14 Power Skills

**Fully HRDC Claimable
Under Focus Area Course:**

REGISTERED HRDCORP TRAINING PROVIDER

HRDCORP CLAIMABLE

Training Programme No.:
10001550358

This programme is designed specifically to equip board of directors with the the awareness and knowledge to understand the global landscape and state of cyber risks facing organisations and nations alike

www.aiiasia.org

LEADERSHIP PROGRAMME

PROGRAMME OVERVIEW

In Q2 2024, Check Point Research saw a 30% YoY increase in "reported" cyber attacks globally, reaching 1,636 attacks per organization per week. The scale and acceleration of cyber attacks have made Cybersecurity a top discussion point at every Board Meeting. How prepared are Board members in understanding, advising and challenging issues that arise in this critical area?

This half day Cyber Risk & Cybersecurity briefing will provide Board Members with the awareness and knowledge to understand the global landscape and state of cyber risks facing organisations and nations alike. It will bring the latest insights and research on threats that will hit the shores of Asia and sophisticated cybercrime deployment that all businesses and organization must know to be prepared for the wave of attacks that will only ramp up in the months to come.

The briefing will walk through the forensics of major cyberattacks for Board members to witness the unfolding of the crisis and where the triggers or preventions could have taken place before-during- and post attack media communications. It will also address best practices in "Cybersecurity Reporting Indicators" that should be incorporated to ensure cyber resilience in every organization for the BOD to review and hold the Management team accountable for.

The finale of the briefing will deep dive into the future of cybersecurity to build Cyber Resilience with the advancement of AI and Quantum Computing and how unpreparedness will lead to major negative disruption in organisations. It would introduce innovative solutions and stealth technology that are being deployed in the US and Europe that would be critical in making organisation more resilient in the face of rising threats.

PROGRAMME SUMMARY

This cyber risk briefing is designed for Board Members to enable them to have better foresight of upcoming disruption, ability to advise their CTO/CISO teams, practice responsible governance and be prepared to effectively manage cybersecurity crises. In today's digital age, protecting your organization from cyber threats is paramount, and this briefing will enlighten you to the most recent innovations needed to build cyber resilience in your business.

01 Global Cyber Risk Landscape

02 Responsible Governance to enhance Cyber Resilience

03 Future of Cybersecurity

BENEFIT AND IMPACT

- ❑ Gain critical awareness of the global and regional cyber threat landscape.
- ❑ Understand the forensics behind major cyber incidents and how to respond.
- ❑ Learn best practices in cybersecurity governance and reporting for Boards.
- ❑ Enhance ability to hold Management accountable for cyber risk preparedness.
- ❑ Discover innovative technologies shaping the future of cyber resilience.
- ❑ Network with peers and cybersecurity experts to benchmark strategies.

PROGRAMME AGENDA

Time	Session
8.30 am – 9.00 am	**Registration**
9.00 am – 9.15 am	**Opening Speech –** Dennis Loong, Director, Faculty, Asian Institute of Insurance
9.15 am – 10.30 am	**Global Cyber Risk Landscape** *Speaker: Danny Kim, Founder and CTO of FullArmor Corp, and CEO of CyberArmour* ➢ The Cyber threat landscape: Current trends, threat actors strategic direction change, ecosystem that enables them. ➢ Vulnerabilities of current cybersecurity solutions. ➢ Deconstructing how hackers enter into your organisation and systems: **Insurance Industry Specific Case Forensics Walk Thru.** ➢ Cybersecurity framework and best practices: Understanding attack chains.
10.30 am – 11.00 am	**Morning Break**
11.00 am – 12.30 pm	**The Criticality of Board Governance** *Speaker: Danny Kim, Founder and CTO of FullArmor Corp, and CEO of CyberArmour* ➢ Board's role in overseeing and implementing a robust governance framework that enables cybersecurity. ➢ Resilience & agility: Will directors be liable in the future? ➢ Board's oversight and reporting: Learning to construct a **Cybersecurity Technical Balance Sheet** for board reporting & analysis (identifying risks, vulnerabilities and metrics that hold management accountable). ➢ Incident response planning & forensics. ➢ Communications & cybersecurity crisis management for boards and senior leaders' discussion & debrief. ➢ Cyber insurance considerations.
12.30 pm – 1.30 pm	**Lunch Break**

PROGRAMME AGENDA

Time	Session
1.30 pm – 2.30 pm	**Case Studies Interactive Discussion**

Facilitators:

1. *Danny Kim, Founder and CTO of FullArmor Corp, and CEO of CyberArmour*
2. *Jeremiah Abraham Selvaraj, Head of Cybersecurity Solutions Business Unit, Cyberarmour*

➢ Ransomware Attack Case.
➢ Zero-Day Attack Case.
➢ Espionage via Phishing Case.

2.30 pm – 3.30 pm   **Future of Cyber Security**

Speaker:

Jeremiah Abraham Selvaraj, Head of Cybersecurity Solutions Business Unit, Cyberarmour

➢ The accelerated vulnerabilities and threats with the advancement of AI, ML, IoT, Blockchain and Quantum Computing.
➢ Stealth-based cybersecurity technology.

3.30 pm – 5.00 pm   **Q&A and Closing Thoughts**

TARGET AUDIENCE

- Board Members, C-Suite Executives and Senior Management.
- Chief Technology Officers (CTOs), and Chief Information Security Officers (CISOs).

PROGRAMME FEE

	Aii Member	Non-Member
Early Bird Fee *(Register before June 30, 2025)*	Single: RM 2,600 / USD 590	Single: RM 3,000 / USD 680
Normal Fee	Single: RM 3,000 / USD 680	Single: RM 3,500 / USD 800

Danny Kim
Founder and CTO of FullArmor Corp, and CEO of CyberArmour

Danny Kim is a technology leader and innovator with over 30 years of experience in the enterprise and cyber security industry. As the Founder and CTO of FullArmor Corp, he has been at the forefront of developing security, compliance, and access management products. He pioneered FullArmor's strategy to partner with leading tech firms like Microsoft, Citrix, and F5, successfully scaling products to market. FullArmor Corp. has been a Microsoft Gold Certified Partner for over 20 years and has won several awards for its products and services.

Danny has taken on a new venture in Southeast Asia as the CEO of CyberArmour based out of Malaysia, with the vision to empower and build communities of Cybersecurity Professionals, STEAM based learning communities and Entrepreneurs in the region.

Danny is also deeply invested in educational initiatives, leading programs that inspire students in STEAM fields with hands-on learning experiences. He and his team led the first ever high school team to win the prestigious Shell XPRIZE Ocean Discovery competition. As the CEO of Quest Institute, he spearheaded various STEAM related educational programs including a unique initiative partnering with NASA and other organizations to launch student- designed experiments to the International Space Station. Danny Kim has also been a speaker and mentor at various events and programs for young entrepreneurs and innovators.

As the VP/Director AMSE and R&D, Valley Christian Schools, he leads the Applied Math Science and Engineering (AMSE) STEM program at Valley Christian Schools, contributing to future STEM growth and innovation.

Danny graduated from Cornell University with a degree in computer science and electrical engineering. He is a visionary leader and a role model who has demonstrated excellence and integrity in his work and life. He is a faith- driven entrepreneur who believes that God has a purpose for his life and business and has made significant contributions to the fields of technology, education, and space exploration.

SPEAKER PROFILE

Jeremiah Abraham Selvaraj
Head of Cybersecurity Solutions Business Unit, Cyberarmour

With 12 years of extensive experience in the tertiary education sector, Jeremiah is a highly skilled IT professional specializing in IT and Cyber Security, delivering large-scale & technical IT infrastructure support & solutions. Currently, Jeremiah head the Cybersecurity Solutions business unit at Cyberarmour, a boutique cybersecurity company focused on cutting-edge threat surface reduction/removal and stealth technology for servers. His role involves leveraging his deep understanding of IT security integration, encompassing Microsoft Security, Norton, Sophos, ScanNow, Zscaler, Cisco, Fortinet, Windows Active Directory & Group Policy, to drive the development and delivery of Cyberarmour's specialised solutions.

Jeremiah also extends his expertise as a consultant to CTOs and CISOs on Enterprise IT infrastructure, including cloud services & virtualization such as Citrix, VMWare, Serverpark VDI, and SCCM. His commitment to fostering cybersecurity knowledge is further demonstrated through his active engagement with Cyberarmour Academy. In this capacity, he contributes to teaching and learning initiatives aimed at spreading cybersecurity awareness and best practices among working adults and even school children.

Jeremiah is a proud member of ISC2 and CompTIA, holding certifications in CompTIA Security+, PRINCE2 Foundation, and Certified ISO Internal Auditor. He holds a Bachelor of Engineering and a Diploma in Mechatronics Engineering. A committed individual, Jeremiah seeks to build leadership & character within his team and among the younger generation. He excels in providing top-notch customer service, possesses exceptional communication skills, profound computer & IT competencies, and maintains an unyielding passion for IT security.

FSF SKILLS

Skills Developed by Attending this Programme

Prime Skills

Digital and Data Integration	1. Data Governance 2. Data Protection 3. Disruption Management 4. Big Data Analytics 5. Security Monitoring 6. Security Architecture 7. Threat Intelligence and Management	8. Artificial Inteliigence (AI) Management 9. DevSecOps 10. Emerging Technology Synthesis 11. Enterprise Architecture 12. Penetration Testing
Growth and Partnerships	1. Global Perspectives 2. Scenario Planning and Analysis	3. Disruption Management
Risk Management, Governance and Regulatory Compliance	1. Internal Governance 2. Regulatory Compliance 3. Risk Management 4. Risk Governance 5. Operational Risk Management 6. Crisis and Disaster Recovery Management 7. Business Continuity Management	8. Business Continuity Planning 9. Enterprise Risk Management 10. Technology Risk Management 11. Artificial Intelligence, Ethics and System Governance 12. Monitoring and Surveillance 13. IT Audit 14. Risk Modelling and Validation
Sustainable Finance and Insurance	1. Sustainable Stewardship Development	2. Sustainability Risk Management

Power Skills

Innovation & Delivery	1. Adaptability and Resiliency 2. Business Acumen 3. Critical Thinking 4. Change Management 5. Innovative Thinking	6. Digital Fluency 7. Learning Agility 8. Problem Solving 9. Sustainability Awareness
Social Intelligence	1. Collaboration 2. Communication 3. Influencing and Negotiation 4. Coaching & Mentoring 5. Conflict Management	

REGISTER NOW

Asian Institute of Insurance
197701004772 (35445-H),
Level 6, Bangunan AICB,
No. 10 Jalan Dato' Onn,
50480 Kuala Lumpur, Malaysia

For further information, please contact:
Email: sales@aiiasia.org