SURUHANJAYA SYARIKAT MALAYSIA
COMPANIES COMMISSION OF MALAYSIA

2026

SSM TRAINING

BOARD OF DIRECTORS: IF CYBER SECURITY IS NOT A TOP PRIORITY, YOUR BUSINESS IS AT HIGH RISK

Perhentian Island, Terengganu

Corporate Topic Series

BOARD OF DIRECTORS: IF CYBER SECURITY IS NOT A TOP PRIORITY, YOUR BUSINESS IS AT HIGH RISK

COURSE INTRODUCTION

No matter the size or industry of the organization, cybersecurity has become a top priority in today's constantly evolving digital landscape. Boards of Directors play a pivotal role in ensuring effective oversight of cybersecurity practices. Cybersecurity is no longer just an IT issue; it must be integrated into every facet of an organization's decision-making. The repercussions of cyber risk extend far beyond technology, potentially affecting operations, reputation, and financial stability. Boards must therefore understand both the breadth and depth of cybersecurity risks and their potential impact on the organization.

Although most boards acknowledge that cybersecurity is important, many still struggle to translate that priority into effective oversight and resilience. Surveys from 2024–2025 highlight ongoing gaps in preparedness and understanding: while a majority of board members now view cybersecurity as a material business risk and have increased their focus on cyber strategy and reporting, a significant portion still do not feel adequately prepared to handle attacks, with just over half saying their organizations are unprepared to cope with a material cyber incident in the next 12 months.

Additionally, recent industry reports show that nearly 60% of global board members consider emerging technologies such as generative AI a security risk, underscoring how boards must grapple with not only traditional threats but also evolving ones linked to advanced technologies.

Despite growing awareness and increased cybersecurity budgets, gaps remain between awareness and actionable preparedness. Boards must continue to enhance their cyber literacy, integrate cyber into enterprise risk frameworks, and establish clear governance practices that support proactive risk management rather than reactive oversight.

COURSE OBJECTIVES

This course will introduce the board of directors to the latest cybersecurity threats and enlighten them on what are the defense technologies available with details on why and when the company needs to invest in them. This course also highlights the roles and responsibilities of board of directors in cyber risk management based on guidelines issued by regulators.

COURSE CONTENTS

Latest Attack Trends: 100% Live Demo

Objective: Understand the latest attacks in the wild contributing to increase in cyber risk.

- AI based attacks.
- Business Email Compromise (BEC).
- File-less malware attacks.
- Firmware attacks.
- Mobile phone attacks.
- Web attacks.
- Email spoofing.
- USB / File attachment attacks.
- Identity based attacks.
- Social media attacks.
- Payment based attacks.

Cyber Resilience

Note: this module is based on guidelines provided by Bursa Malaysia, Security Commissions, and Bank Negara.

- Security obligations by role for a cyber resilient organisation.
- Managing cyber risk through a governance framework.
- 3rd party risk.
- Vulnerability management.
- Zero trust architecture and strategy.
- Improved detection and response strategy and framework.
- Cyber threat intelligence.
- Mitigating risk through cyber insurance.
- How to handle during and after a breach?

BOARD OF DIRECTORS: IF CYBER SECURITY IS NOT A TOP PRIORITY, YOUR BUSINESS IS AT HIGH RISK

LEARNING OUTCOMES

By attending this course, participants will be able to:

- Learn about the latest attacks, how these attacks are carried out with DEMOS and how to improve your existing cybersecurity defence strategy and cyber resilient framework.
- Attendees will learn on evolution of cyber resilience framework with roles and responsibilities for board and senior management.

WHO SHOULD ATTEND

Open for all Board of Directors, Senior Management and C-Level professionals.

ABOUT THE TRAINER

Dr. Clement Arul is an internationally recognized cybersecurity leader, strategist, and thought leader with over 25 years of experience spanning cybersecurity governance, threat intelligence, digital forensics, cloud security, and enterprise risk management. He is the Founder and Chief Executive Officer of Cybertronium, where he advises boards, C-suites, and global organizations on building cyber-resilient, business-aligned security programs.

Renowned for bridging the gap between technology and executive decision-making, Dr. Arul has pioneered the adoption of advanced security capabilities such as EDR, XDR, SOAR, firmware vulnerability management, and cloud detection and response across the region. He is also a strong advocate for cybersecurity education, having developed ISO 17024-certified professional certification programs aligned with global frameworks including NICE and MITRE, making high-quality cybersecurity training accessible across ASEAN and emerging markets.

Dr. Arul's impact on the global security community was recognized in 2022 when he was ranked #2 in the IFSEC Global Top 20 Cybersecurity Professionals & Influencers, underscoring his influence and leadership on the world stage.

His contributions have earned him numerous accolades, including Global Cybersecurity Visionary of the Year, Cybersecurity Innovator of the Year, and Gold Globee Winner – CTO of the Year (Security Services). He has also been recognized as Cybersecurity Professional and Educator of the Year (Asia).

A sought-after keynote speaker and advisor, Dr. Arul regularly engages with boards, regulators, and industry leaders on topics such as cyber resilience, emerging threats, AI security, and executive cyber governance. His work continues to shape how organizations approach cybersecurity as a strategic business imperative rather than a purely technical function.

BOARD OF DIRECTORS: IF CYBER SECURITY IS NOT A TOP PRIORITY, YOUR BUSINESS IS AT HIGH RISK

ADMINISTRATIVE DETAILS

Date	31 March 2026	
Venue	Virtual platform	
Time	09.00 am – 05.00 pm	
Training Methodology	Presentation, live demos and discussion	
Fee	RM550.00	Standard
	RM450.00	Licensed Secretary. Member of MAICSA, MIA, Malaysian Bar, MACS, MICPA, Sabah Law Society & Advocates Assoc. of Sarawak.
SSM CPE Points	8 points	

HOW TO REGISTER?

STEP 1

Strictly via online registration at **www.ssm4u.com.my/ecomtrac**

STEP 2

NEW USER (First Time Login)

- Click on **SIGN UP**
- Key in **REGISTRATION INFORMATION**
- Click on **REGISTER**
- Key in **USERNAME** and **PASSWORD**

EXISTING USER

- Key in **USERNAME** and **PASSWORD**
- Click on **SIGN IN**

STEP 3

- Select training
- Check on Available Seat
- Click on Add Participant
- Key in participant's information
- Click on Submit
- Check participant's details
- Click on Submit Payment

Note: Please submit your application within 15 minutes. Otherwise the system will automatically cancel your transaction and you will lose your seat(s). Please re-apply if you wish to proceed. Full payment shall be made at the point of registration.

BOARD OF DIRECTORS: IF CYBER SECURITY IS NOT A TOP PRIORITY, YOUR BUSINESS IS AT HIGH RISK

TERMS & CONDITIONS FOR TRAINING PROGRAMMES

PROGRAMME FEE

- Fee is payable to SURUHANJAYA SYARIKAT MALAYSIA.
- Admittance to training programme shall be granted only upon registration and full payment is received.

PAYMENT MODE

- Registrations and payment for training programmes MUST be made through online at e-COMTRAC (www.ssm4u.com.my/ecomtrac). Upon submitting the registration application, participants are deemed to have read and accepted the terms and conditions herein.
- Payment by cash and cheque is not acceptable effective from January 2021.

CLASSROOM TRAINING

- For classroom-based training, a confirmation e-mail will be sent to participants at least 1 working day prior to the programme.
- Participants are required to present Malaysia's identification card and foreign participants are required to present passport at the registration counter for verification and admission to training programme.
- Admittance may be denied upon failure to present identification card / passport.

LIVE WEBINAR TRAINING

- A notification e-mail with the webinar access link will be sent to participants at least 1 working day prior to the webinar.
- The access link is unique for registered participants and should not be forwarded or shared with others.

E-LEARNING TRAINING

- Upon successful registration, an email will be sent containing the access link to the pre-recorded webinar and accompanying material will be sent on the start date of the programme.
- Access will be available for a fixed duration of seven (7) days starting from the session's commencement date. After this period, the link will expire, and access to the webinar and materials will no longer be available.

CERTIFICATE OF ATTENDANCE

- Upon full attendance of the programme and payment is received, participants will be issued an e-Certificate of Attendance.
- Participants can download the e-Certificate of Attendance from e-COMTRAC platform in three (3) working days after the programme or in seven (7) working days for conference / symposium. Please take note that the certificate is available for download up to 30 days from the conclusion of the programme. An administrative fee of RM30.00 per copy is chargeable for downloading the certificate after the 30th day. Any replacement of certificate due to errors in name or identification card number wrongly filled by participant / representative during registration or loss of certificate, etc will incur a fee of RM30.00 for reissuance.

CANCELLATION / ABSENT

- No refund will be given to participants who failed to attend the programme.
- Replacing registered participant is not allowed.

TRANSFER

Transfer of registration fee to another training programme is not allowed.

PERSONAL DATA PROTECTION NOTICE

Your personal data and other information provided in this application and including any additional information you may subsequently provide, may be used and processed by COMTRAC/SSM as a reference in future to communicate with you on our training programmes/events. In line with the Personal Data Protection Act 2010, we wish to obtain your agreement and consent for using your personal data. If you do not consent to the processing and disclosure of your personal data, you should send an e-mail to us at comtrac@ssm.com.my.

HUMAN RESOURCES DEVELOPMENT CORPORATION

SSM is registered as a training provider with HRD Corp under GOV1000117857. All trainings are claimable under SBL Scheme subject to HRD Corp approval. Participant's employer needs to apply for grant at least one day before the commencement of training.

COPYRIGHTS

The materials of the training programme are solely for participants' personal use. No part of these materials may be stored, reproduced or transmitted in any form or by any means, including photocopying, e-mailing and recording, without the written permission of the author or SSM. Information contained in these documents is understood to be correct at the time of writing. The assessments and views expressed in these materials shall be treated/ regarded purely for public information and discussion and it does not constitute formal advice. The views provided are for general information to provide better clarity and understanding of the subject matter. It should not be relied upon as an alternative to specific legal advice from your lawyer or other professional service provider. If you have any specific issues and/ or questions about any legal matter, you should consult your lawyer or other professional service provider. In no event shall the SSM be liable for any damages, whether in an action of contract, negligence or other tort, arising from the contents in these materials.

EXCLUSION OF LIABILITY

The speaker(s) or trainer(s) is independent and shall not represent SSM, act as its agent or otherwise represent that their personal views are endorsed by SSM. The assessments and views expressed during the programme are entirely the speakers'/trainers' own. SSM shall not be liable for whatever circumstances arising from any engagement between the speaker(s) or trainer(s) and the participant(s).

DISCLAIMER

SSM reserves the right to cancel the programme, change date(s), venue(s), speaker(s) or any other changes due to any unforeseen circumstances that may arise without prior notice to participants. SSM also reserves the right to make alternative arrangements without prior notice. SSM accepts no responsibility for death, illness, injury, loss or damage of any property belonging to, or financial loss by any persons attending the programme, whatever the cause. SSM shall not be responsible for any costs, damages or losses incurred by participants dues to the changes and / or cancellation. SSM is not responsible for the integrity of participants' computer or device, your internet signal bandwidth, or any other consideration outside of the control of SSM.

SSM shall not be responsible for any problems or technical malfunction, including, without limitation, the acts, omissions, problems or malfunctions of any telephone network or lines, computer online systems, servers, computer equipment, software, failure of e-mail, traffic congestion on the internet or at any web or combination thereof.

All information contained in the brochure is correct and accurate at the time of publication.