Understanding the Evolving Cybersecurity Landscape

FACULTY
Clement Arul

WHO SHOULD ATTEND
- Directors of financial institutions
- Anyone else who may find the programme helpful

www.iclifgovernance.org
PROGRAMME OVERVIEW

In today’s cybersecurity landscape, the only secure system is one that is unplugged, turned off and in a locked room. However, since it is clearly not practical to leave our systems turned off or shutdown, it is critical that we understand the risks our systems are exposed to and take the necessary measures to defend them.

This programme is designed to help participants understand, assess and take a proactive posture in cybersecurity; and understand why cybersecurity is a board level responsibility, and how to manage and mitigate cyber risks.

Learning Objectives

• Learn the anatomy of a cyber attack;
• Gain knowledge about the threat environment including the latest trends in cyber attacks;
• Gain understanding on the regulatory requirements in Bank Negara Malaysia’s Risk Management in IT Guidelines and the Securities Commission’s Cybersecurity Guidelines;
• Gain understanding on how to map security obligations by role across the organisation;
• Provide directors with handles on what to look out for in overseeing cybersecurity risks;
• Learn takeaway tips for protecting company and personal information.

FACULTY

Clement Arul is the Chief Operating Officer – Technology and R&D at Vigilant Asia. He has more than 20 years of experience as principal security consultant, penetration tester, ethical hacker, and security trainer. He specializes in Internet of Things, big data, payment gateway hacking, web application security and penetration testing. He is a frequent speaker at security events in Asia Pacific including those organized by Microsoft, the Malaysian government agencies, corporates and universities.

Clement Arul is a two time National Award winner of Cyber Security Professional of the Year in 2014 and 2017 and two time Regional Award winner of Cyber Security Professional of the Year APAC in 2017 and 2019. He was also awarded as APAC Cyber Security Educator of the Year 2019.
Session 1: Introduction — Anatomy of an Attack
This session will explore the basics of security and outline the cyber attack lifecycle.

- What is security, vulnerabilities and 0 days?
- Cyber attack lifecycle
- Different attack vectors
- Threats versus risks
- Why perimeter defences are failing?
- Why anti-virus is not enough?
- Financial implications of a cyber attack
- Why cybersecurity is a board responsibility?

At the end of the session, participants will be able to identify the lifecycle of a cyber attack and the different types of cybersecurity risks; explain the financial implications of cyberattacks and the importance of cyber security oversight.

Session 2: Latest Attack Trends — 100% Demo
In this session, participants will learn the latest trends in cyber attacks and how these are carried out via live demonstrations.

- Business Email Compromise
- Ransomware
- Advanced Persistent Threat
- Malvertising
- Mobile Malwares
- Web Attacks
- Identity theft
- Social media based attacks
- Wireless (WiFi) attacks
- Account takeover and stuffing

At the end of the session, participants will gain greater awareness on current cyber threats and risks, and appreciate the need to practise good hygiene in ensuring cybersecurity.

Session 3: Regulatory Guidelines
This session will discuss the regulatory guidelines issued by Bank Negara Malaysia and the Securities Commission on cybersecurity:

- Risk Management in IT Guidelines (BNM)
- Cybersecurity Guidelines (SC)

At the end of the session, participants will be able to articulate the regulatory requirements on cybersecurity from BNM and the SC. More critically, it will also highlight the role of the board in providing cybersecurity oversight.

Session 4: The Way Forward — Mitigating & Managing Cybersecurity
This session will outline security obligations by role across the organisation. It will also provide understanding on how to handle a cyber breach — during and after the incident — to make the organisation more cyber resilient.

At the end of the session, participants will gain greater clarity on the different cybersecurity roles within the organisation; and what to do in the event of a breach and after a breach.

- Security obligations by role
- Risk management framework
- Managing cyber risk through a governance framework
- Mitigating risk through cyber insurance
- Applying business intelligence to cybersecurity
- What to do during a cyber breach?
- What to do after a cyber breach?
- Role of the board and questions they must ask
# REGISTRATION FORM

**Understanding the Evolving Cybersecurity Landscape**

**FEE:** RM3,500 before SST

<table>
<thead>
<tr>
<th>NAME</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DESIGNATION</td>
<td></td>
</tr>
<tr>
<td>COMPANY</td>
<td></td>
</tr>
<tr>
<td>ADDRESS</td>
<td></td>
</tr>
<tr>
<td>CONTACT TEL. NO. (COMPANY)</td>
<td>(PERSONAL)</td>
</tr>
<tr>
<td>FAX NO.</td>
<td></td>
</tr>
<tr>
<td>EMAIL ADDRESS</td>
<td></td>
</tr>
<tr>
<td>NAME OF SECRETARY</td>
<td></td>
</tr>
<tr>
<td>CONTACT TEL. NO.</td>
<td></td>
</tr>
<tr>
<td>EMAIL ADDRESS</td>
<td></td>
</tr>
</tbody>
</table>

## PAYMENT

Iclif is registered to charge Service Tax (“SST”) for programmes conducted in Malaysia under the laws of Malaysia (SST registration no.: W10-1812-32000095).

Payment should be made within **30 days** from the invoice date or in advance of the programme date, whichever is sooner. Your place is only secured once payment has been received within this period.

- Cheques should be made payable to **THE ICLIF LEADERSHIP AND GOVERNANCE CENTRE**
- For telegraphic transfer, kindly remit payment to account number: **5140 1138 4115** at **MAYBANK BERHAD KL MAIN BRANCH, 50050 KUALA LUMPUR**

Please email a copy of the payment receipt to **finance@iclif.org** and cc to **fide@iclif.org**

## TERMS AND CONDITIONS

Terms and conditions apply. Please visit [www.iclifgovernance.org](http://www.iclifgovernance.org) for our terms and conditions and additional information on the programme.

## PERSONAL DATA PROTECTION

The Iclif Leadership and Governance Centre respects your personal data and have taken steps to be fully compliant to the Personal Data Protection Act 2010 (Malaysia). The types of data, purpose of use, and a list of your rights under the Act are explained in our Privacy Policy And Notice ([www.iclif.org](http://www.iclif.org)).

I consent to the use of my personal data in the manner and for the purposes stipulated in the Privacy Policy And Notice.

With regards to promotional and marketing materials, would you like to receive news and updates on Iclif’s services/offers?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

Agreed and confirmed by:

……………………………

Signed by:

Date: