CYBERSECURITY: A BOARDROOM AGENDA

COURSE INTRODUCTION

With all the news and stories about hackers, botnets and breaches involving personal information, it is easy for the security message to sound over-used and tired. It is easy for one to say, “It won’t happen here.”

Studies and surveys repeatedly show that the human factor (what employees do or don’t do) is the biggest threat to information systems and assets. People, just like computers, store, process and transfer highly valuable information. Yet people remain highly insecure due to lack of education on this. As a result, cyber attackers are actively targeting the human element. Until you address the human issue, technology alone cannot secure your organization. Humans are the weakest link in the IT security chain clubbed with technology and process vulnerabilities are making it worse.

COURSE OBJECTIVES

This training prepares members of the board and other senior management of an organization to understand, assess and take a proactive stand in cybersecurity. Along the way, members of the board will be introduced to the threats from Ransomware, BEC, Malwares and Social Engineering to Advanced Persistent Threats that can decimate an organization. Understand why cybersecurity is a board level concern and how to mitigate and manage it.

COURSE CONTENTS

Introduction to Cyber Security

- What is security, vulnerabilities & O-Days, attack life cycle, different attack vectors?
- Threats vs. risks, why perimeter defences are failing? Why anti-virus is not enough?
- Financial implications of a cyber attack.
- Why cybersecurity is a C – level activity?

Latest Attack Trends

- Business email compromise (BEC) (Demo).
- Ransomware (Demo).
- Advanced persistent threat (Demo).
- Mobile malwares (Demo).
- Identity theft (Demo).
- Web data breach (Demo).
- Technologies, policies and strategies to defend these attacks.

LEARNING OUTCOME

By attending this course, the participants will be able to:

- Understand why cyber security is a boardroom activity.
- Learn the security obligations by role.
- Appreciate the risk management framework.
- Manage cyber risk through a governance framework.
- Mitigate risk through cyber insurance.
- Apply business intelligence to cybersecurity.
- Handle situation during and after a breach

WHO SHOULD ATTEND

Members of the board, senior management of an organization, Company directors, company secretaries, company secretarial assistants, lawyers, accountants, corporate consultants and anyone who wants to learn about cyber safety.

Note: No IT knowledge required. Open for all who use computers / smart devices

ABOUT THE TRAINER

Clement Arul is Chief Executive Officer, Kaapagam Education Services Sdn. Bhd. He is a National and Regional award-winning Cybersecurity Professional with twenty two years of IT experience in security, ethical hacking, cyber security framework, security risk & governance, systems analysis, big data, IoT, design, development, secure coding, implementation, digital forensics and project management. Clement is a security consultant for many multi-national and leading IT companies in APAC region. A frequent speaker in security events in APAC.

Awards and Recognition:

- IFSEC GLOBAL TOP 20 CYBERSECURITY PROFESSIONALS 2020, IFSECGLOBAL, UK
- APAC Cyber Security Professional of the Year 2020, 2019, and 2017, Global Cybersecurity Excellence Awards.
- Cyber Security Professional of the Year 2017, 2014, National Cyber Security Awards, MOSTI, Govt. of Malaysia.

ADMINISTRATIVE DETAILS

DATE	PLATFORM	EVENT CODE
22 September 2021	Webinar @ Microsoft Teams	122/21/CEP/WEB

Time	9.00 a.m. - 5.00 p.m.	
Training Methodology	Presentation, Live Demos and Discussion	
Fee	**RM300.00** **RM250.00**	Standard Licensed Secretary. Member of MAICSA, MIA, Malaysian Bar, MACS, MICPA, Sabah Law Assoc. & Advocates Assoc. of Sarawak.
CPE points	4	