CERTIFIED SECURITY AWARE CxO

CSACxO

Duration: 1 day; Instructor-led | Virtual Instructor-led

OVERVIEW

Members of the board and other senior management of an organization can learn how to understand, evaluate, and adopt a proactive stance toward cyber security with this course. Members of the board will be exposed to all the most recent threats along the way, such as Mobile Hacking, WhatsApp-based attacks, Web Application Compromise, File-less Malwares, Ransomware, Advanced Persistent Threats, Business Email Compromise, and Social Engineering that can completely destroy an organization.

Discover more by looking at Use Cases of Recent Attacks, which include SingHealth, Equifax, British Airways, Schneider Electric, and many others.

Learn why cyber security is a board level issue, how to manage it, and what the CXO and board members' responsibilities are in pre-breach, breach, and post-breach scenarios.

These challenges are addressed in this high-impact security awareness training. By making sure your users are aware that they are targets, training them how to use technology safely, and ensuring your company stays compliant, it motivates and alters behavior. Additionally, you move beyond just prevention and start establishing human sensors, building a much more resilient company, by training your users the indicators of compromise and how to report occurrences.

OBJECTIVES

- Understand all the Latest Attacks and ways to mitigate them.
- Understand on Why Cyber Security is a Boardroom activity.
- Understand the Way to Move Forward: Mitigating & Managing Cyber Security for your organization.
- Learn how to handle During and After Breach scenarios.
- Map Security Obligations by Role in your organization.

AUDIENCE

This awareness is designed for C-Level and board members who wish to improve organization's capacity to anticipate and react to cyber-attacks without inundating them with technical jargons.

COURSE CONTENTS

Module 1: 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?
- Business and Finance Implications of a Cyber Attack
- Why Cyber Security is a C – Level Activity?
- Statistics on Software Vulnerabilities and related dark web ecosystem
- Cybersecurity Landscape in Malaysia
- Latest Attack Use Cases
- Case study: 2022 Smishing attacks – OCBC Bank
    - Case study: 2021/22 Double and Triple Extortion Ransomware Attacks
    - Case study: 2021 Identity Theft – UOB Bank
    - Case study: 2021 Telco 3rd Party vendor's security breach
    - Case study: 2020/21 Supply Chain Attack
    - Case study: 2021 Manufacturing based Attack
    - Case study: 2020 Online Payment Tampering Attack
    - Case study: Cyber insurance and Cybercrime

Module 2: Latest Attack Trends: 100% Live Hacking Demos

- Business Email Compromise (BEC) (Demo)
- Ransomware (Demo)
- Advanced Persistent Threat (Demo)
- Mobile Malwares (Demo)
- Identity Theft (Demo)
- Web Data Breach (Demo)
- Supply Chain attack (Demo)
- Technologies, Policies & Strategies to Defend these attacks

Module 3: Way to Move Forward: Mitigating & Managing Cyber Security

- Again, Why Cyber Security is a Boardroom activity?
- Secure Software Development Life Cycle and its components
- Security Obligations by Role: CEO, CFO, COO, CISO, CHRO, CRO
- Risk Management Framework
- Managing Cyber Risk through a Governance Framework
- Mitigating Risk through Cyber Insurance
- How to handle During and After a Breach?
- Security Commission Guidelines for Cybersecurity Risk Management
- Bank Negara Risk Management in IT guidelines