AjarAble

CERTIFIED SECURITY AWARE CxO

CSACxO

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

OVERVIEW

This training prepares members of the board and other senior management of an organization to understand, assess and take a proactive posture in cyber security. Along the way, members of the board will be introduced with Live Hacking demos to all the latest threats including Mobile Hacking, WhatsApp based attacks, Web Application compromise, File-less Malwares, Ransomware, Advanced Persistent Threats, Business Email Compromise, and Social Engineering that can decimate an organization.

Dig deeper with Use Cases of Latest Attacks including SingTel, Solarwinds, SingHealth, Equifax, British Airways, Schneider Electric and many more.

Understand why Cyber Security is a Board level problem and how to Mitigate and Manage it and what are the roles of the CxO & board members during pre-breach , breach, and post-breach scenarios. Also, learn the way to move forward Mitigating & Managing Cyber Security with Cyber Risk management and Governance framework and Cyber Insurance.

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.

PREREQUISITES

- Do you use a Smart phone / Laptop / Email / Internet? If the answer is a Big Yes, then, you are eligible to attend this training.
- No technical knowledge required. Open for all ages

AUDIENCE

- Anyone

CERTIFICATION

Cybertronium Certification: Certified Security Aware CxO

- Exam Platform: KALAM
- Exam Format: Multiple Choice Question (MCQ)
- Exam Questions: 25 Questions
- Exam Duration is: 60 Minutes
- Exam Pass Mark: 70%
- Exam Fees: Inclusive in the Course Fees
- Free Add-on: Free Membership access to KALAM Cybersecurity Collaboration & Community Skills Validation Platform

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?
- Use Cases of Latest Attacks including SingHealth, Equifax, British Airways, Schneider Electric and many more
- Financial Implications of a Cyber Attack
- Why Cyber Security is a C – Level Activity?

Module 2: Latest Attack Trends

- Mobile Malwares (Live Demo)
- Web Data Breach (Live Demo)
- Business Email Compromise (BEC) (Live Demo)
- WhatsApp based attacks (Live Demo)
- Ransomware (Live Demo)
- Advanced Persistent Threat (Live 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?
- Security Obligations by Role
- Risk Management Framework
- Managing Cyber Risk through Governance Framework
- Mitigating Risk through Cyber Insurance
- Applying Business Intelligence to Cybersecurity
- How to handle During and After a Breach?