Cyber Security for the Board, Senior Executives and Management

Take a Proactive Stance in Cyber Security

Discharge your due diligence requirements, increase your cyber resilience

The World Economic Forum (WEF) has placed cybersecurity as a top 10 corporate risk in its annual World Economic Forum Report, and the Australian Securities and Investments Commission (ASIC) expects directors within Australian organisations to be cyber prepared and improve resilience.

This course addresses the critical subject of management's due diligence. It is designed to provide guidance to members of the board, senior executives, and management as to why they need to assess the emergent nature of risks associated with cyber security and the action steps they should be considering.

You will benefit from having a clear understanding of the essential knowledge and skills required to conduct risk assessments and select appropriate management frameworks, leading to identification of future state needs, highlighting gaps and formulating an improvement plan to address these.

The course can be presented in full day, half-day and 2-hour format.

FURTHER DETAILS OVERLEAF ►

Cyber Security

AUSTRALIA'S NUMBER ONE TECHNOLOGY TRAINING PROVIDER

www.alccyber.com.au

Cyber Security for the Board, Senior Executives and Management

A Custom Solution to Taking a Proactive Stance in Cyber Security

Key Objectives

- Examine the NIST Cybersecurity Framework and other key frameworks that need to be considered
- Understand the importance of performing enterprise risk management and how to incorporate cybersecurity risk
- Identify roles and responsibilities of the board, senior executives, management, employees and specialists
- Understand cybersecurity governance, risk and compliance (GRC) as an ongoing requirement.
- Understand the important distinction between being secure and being resilient

Can be presented in full day, half day and 2-hour format. Content is customisable to your situation.

Key Topics

1. Introduction

- A definition for cybersecurity
- Common terminology
- Assessing which of your assets are at risk from cyber threats
- The importance of managing risk correctly for Board Members, C-Suite and Management

2. Identifying Cyber Security Threats and associated Risks

- Why is cyber security so difficult to define?
- Related privacy, legislation and regulatory concerns
- Examining how high the stakes are

3. The Enterprise Risk Management Process incorporating Cyber Security

- Enterprise Risk Management, Governance and Compliance
- Systemic risks arising from realistic cybersecurity threats
- Risk treatment options and when to use cybersecurity insurance

4. Guidance for Board Members, C-Suite and Management

- A framework for identifying and assessing cybersecurity threats and risks
- Incorporating cyber security governance models and oversight into existing practices
- Responsibilities of the Board Members, C-Suite and Management

5. Resilience versus Security

- Security and resilience are not synonyms: one is about hunkering down, the other is about doing business
- It's not a matter of if, but when.
- Security can't stop all attacks. Preparing for and surviving the inevitable
- Resilience is not an IT issue
- Responding to cyber security breaches

6. Additional Tools Provided as Part of the Course

- An actionable checklist and self-assessment questionnaire
- Draft high-level roadmap which can be used as a basis for a Cyber Security Action Plan

alc

Contact Peter Nikitser for more details

Phone **(07) 3870 9318** or email **peter.nikitser@alc-group.com**

www.alccyber.com.au