alc

A tesserent Company

CYBER SECURITY FOR DIRECTORS & THE BOARD

DURATION: 1-2 HOURS

CYBER SECURITY

This presentation is designed specifically for directors and board members to provide a thorough understanding of their legal and fiduciary liabilities and responsibilities and a sound insight into the diverse nature of the threats and how these can be addressed in order to enhance business capability and increase cyber resilience.

WHO SHOULD ATTEND

Board of Directors: Members of the board who provide strategic guidance and oversee the company's operations.

Non-Executive Directors: Independent directors who contribute their expertise without holding executive roles.

Chairperson: The individual responsible for leading board meetings and ensuring effective governance.

Board Members: All members of the board, including those with financial, legal, technical, and industry-specific expertise.

Shareholders: Individuals or entities with ownership stakes in the company.

Investors: Individuals or organisations with financial interests in the company's success.

LEARNING OUTCOMES

Directors and board members play a critical role in shaping an organisation's cybersecurity posture and ensuring its resilience to cyber threats. This course is designed to equip attendees with the knowledge and understanding necessary to: fulfill their fiduciary duty by overseeing cybersecurity governance. Make informed decisions about cybersecurity investments and risk management. Effectively engage in discussions about cybersecurity strategy and incident response. Understand the legal and regulatory implications of cybersecurity for the organisation. Enhance the company's overall cybersecurity culture and awareness.

By attending this course, directors and board members will contribute to the organisation's ability to protect sensitive data, maintain trust with stakeholders, and minimisae the impact of cyber incidents.

CYBER SECURITY
WE HAVE YOU COVERED

1300 767 592
customerservice@alc-group.com
alctraining.com.au

ALC.Training
@alcgroup
alc-training

COURSE CONTENTS

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

IDENTIFFYING CYBER SECURITY THREATS & ASSOCIATED RISKS

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

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

GUIDANCE FOR BOARD MEMBERS

- 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

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

ADDITIONAL TOOLS

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