

Cyber Security Risk

Course outline

Acknowledgements

Written and designed by:

Robbie Sinclair, Security, Governance and Risk Executive Specialist

Copyright

Copyright strictly reserved. No part of these course materials covered by copyright should be reproduced or copied in any form or by any means without the written permission of Governance Institute of Australia.

© Governance Institute of Australia Ltd 2022

Course Outline

In today's world, everything is digital. Information and systems are increasingly becoming an organisation's greatest asset, and their greatest threat. Cyber security incidents can result in financial, legal and regulatory, reputational, and customer impacts. A significant cyber security incident could mean the end of an organisation. Community expectations have changed, and organisations can no longer afford to overlook its cyber security threats and management activity.

The aim of this course is to examine key areas of information security risk faced by organisations and to discuss the standards, guidelines, frameworks, and methodologies available for their effective management.

The key objectives are to:

- Understand key concepts in security risk
- Understand how to develop a governance framework for approaching more complex security risks
- Examine a 'defence in depth' approach to the management of current security risk challenges
- Form and express a view on steps that your organisation can take to develop security risk resilience.

Course content

1 Introduction

- 1.1 Scope and context of this course
- 1.2 What is the aim of this course?

2 Information security risk

- 2.1 What is information security?
- 2.2 Information security vs. cyber security
- 2.3 Information security principles

3 Cyber security frameworks

- 3.1 Introduction to cyber security frameworks of thinking
- 3.2 NIST
- 3.3 Essential Eight
- 3.4 Other Information Security Frameworks and Standards

4 Governance imperatives

- 4.1 The role of the board
- 4.2 Characteristics of effective governance
- 4.3 Defining the Information Security Program
- 4.4 Why information security governance is needed
- 4.5 Key governance questions

5 Risk identification and assessment

- 5.1 Identification and assessment
- 5.2 Assessing possible consequences
- 5.3 Policy implications

6 Threat event case studies

- 6.1 Large Melbourne Hospital – Australia 2021
- 6.2 Colonial Pipeline ransomware attack
- 6.3 JBS S.A. Cyber attack
- 6.4 Internet of Things (IoT) hack
- 6.5 Threat events
- 6.6 COVID-19 as a threat vector
- 6.7 Additional COVID-19 security measures

7 Technology security risk

- 7.1 Key terminology

- 7.2 Data security
- 7.3 Cloud technology
- 7.4 Cloud technology services & threats
- 7.5 Technology governance
- 7.6 Emerging technologies
- 7.7 Global technology risks

8 Cyber security risk

- 8.1 Cyber security strategy
- 8.2 Cyber security threat mitigation

9 The link between cyber and physical security

- 9.1 Domain 1: 'People' security
- 9.2 Domain 2: 'Asset' (physical and intangible) security
- 9.3 Domain 3: 'Virtual' security (Technology and Systems)

10 Conclusion

11 Resources

- 11.1 Legislation and regulators
- 11.2 Standards and guidelines
- 11.3 Governance Institute resources
- 11.4 Reference books
- 11.5 Reports and articles
- 11.6 Further resources

12 Appendices

13 Readings