

PRESENTERS



John Bergamasco, Marsh Ltd, Wellington

John is head of the Marsh cyber specialty for Marsh New Zealand, responsible for the direction and assistance of current and prospective clients in understanding, evaluating and managing cyber risks and exposures.

Prior to joining Marsh, John has held positions of Associate Director for Grant Thornton New Zealand, Director for Information Security/CISO for a prominent US-based law firm, Senior IT Audit Manager for the third largest retail bank in the UK, and several senior IT audit and information security audit roles in public accounting and the United States Federal Government.



Andrew Simpson, KPMG, Christchurch

Andrew leads the South Island Advisory team in Christchurch. He has more than 20 years' experience in IT Auditing, IT Consulting, Internal Audit and risk management. He specialises in helping businesses with their strategic systems initiatives and has worked on many complex IT projects in the UK, Europe, Australia and New Zealand. He also advises businesses on their cyber security defences and controls. He has worked across multiple business sectors and works closely with business leaders to help fuel their success.

CONTENTS

MANAGING CYBER RISKS	1
INTRODUCTION	1
<i>What is cyber/information security?</i>	1
<i>What is information confidentiality, integrity and availability?</i>	1
<i>What is cyber risk?</i>	2
<i>What is a cyber-attack?</i>	2
<i>What is the cyber landscape?</i>	2
<i>The widespread adoption of new technologies is increasing corporate and personal vulnerability:</i> ..	3
<i>Prevailing attack vectors and related agents are the following:</i>	3
<i>Major challenges are aggravating the cyber threat landscape – such as the following:</i>	4
<i>The Risk Connection:</i>	5
<i>A lack of effective information risk management and governance may lead to the following:</i>	5
<i>How can cyber risk be managed?</i>	6
<i>Actions to build cyber resilience</i>	7
<i>Six Actionable strategies in maturing the cybersecurity posture</i>	8
<i>Business disruption and the path to recovery</i>	8
<i>Risk Transfer and Cyber Insurance:</i>	9
<i>Why doesn't traditional insurance cover cyber loss(es)?</i>	9
<i>Terrorism Exclusion – Typical policy wording</i>	10
<i>Exposure</i>	10
KEY AREAS TO REDUCE AND MITIGATE CYBER RISKS AND EXPOSURE.....	11
<i>Information Risk Management Regime</i>	12
<i>Network Security</i>	12
<i>User Education and Awareness</i>	12
<i>Malware Prevention</i>	12
<i>Removable Media Controls</i>	13
<i>Secure Configuration</i>	13
<i>Managing User Privileges</i>	13
<i>Incident Management</i>	14
<i>Monitoring</i>	14
<i>Home and Mobile Working</i>	14
<i>How do we achieve cyber governance and increased cyber resilience?</i>	15
<i>How do we evaluate the effectiveness of our organisation's cyber risk program?</i>	16
CLOUD COMPUTING – OVERVIEW AND UNDERSTANDING OF BENEFITS AND INFORMATION SECURITY RISKS	24
<i>Points to consider</i>	25
CONCLUSION	26