

PRESENTER



Michael Wigley, Wigley and Company, Wellington

Michael's clients include many IT companies, telcos and ICT customers. He has a focus on complex disputed issues, risk, regulation including competition, and public law. He has considerable experience over 15 years in advising on cybersecurity and privacy issues faced by companies and the public sector, as well as extensive involvement in advising on directors' liabilities and duties, a major consideration in relation to cybersecurity, ICT and disruptive technologies. Michael is based in Auckland and Wellington, and he often advises clients as part of a multi-disciplinary team, such as technical, media, and economics.

CONTENTS

LEGAL ASPECTS OF CYBERSECURITY.....	1
INTRODUCTION	1
WHAT IS CYBERSECURITY?.....	2
GC100: WHY DOES CYBER SECURITY WORRY SENIOR MANAGERS?.....	2
GC100: WHAT ARE THE LEGAL CONCERNS FOR BUSINESS AROUND CYBER SECURITY?	3
STANDARD OF CARE REQUIRED OF COMPANIES AS TO CYBERSECURITY	4
WHAT IS REQUIRED FOR A “REASONABLE” STANDARD?.....	5
TEAMWORK AND THINKING LIKE A PIRATE, NOT A NAVY CAPTAIN	5
CASE STUDY – TALKTALK IS HACKED – IN THREE PHASES	6
<i>The First Phase- October 2015.....</i>	6
<i>TalkTalk – The Second Phase: 3 months later</i>	9
<i>The Third Phase: Another problem at TalkTalk.....</i>	9
<i>Closer to home</i>	10
THE LEGAL ‘DEFENSIVE SHIELD’ FOR CYBERSECURITY	10
A FOOTNOTE – CYBERSECURITY WEAK POINTS IN LAW FIRMS	10
APPENDIX: WHAT FOOT AND MOUTH CAN TEACH US ABOUT CYBERSECURITY	13
<i>Overview</i>	13
<i>The detail.....</i>	13
<i>Why is Foot and Mouth relevant to cyber security?.....</i>	13
<i>What standard of care must a company exercise to avoid negligence liability?</i>	14
<i>What this means in practice</i>	15