

# Contents

---

	<i>Foreword</i>	<i>xi</i>
	<i>Miles Templeman, Director General, Institute of Directors</i>	
	<i>Contributors' notes</i>	<i>xiv</i>
<b>Part 1: Information at risk</b>		
1.1	The information security management system <i>Alan Calder, IT Governance Ltd</i>	3
1.2	The business case for IT security <i>Andrew Steggles, EMEA Nokia Enterprise Solutions</i>	8
1.3	Recent attack trends <i>The Fraud Advisory Panel's Cybercrime Working Group</i>	12
1.4	The fine art of elephant husbandry – a practical guide to patch management <i>Chris Knowles, Computacenter</i>	18
1.5	Gone phishing <i>Frank Coggrave, Websense</i>	23
1.6	The marketing dimension <i>Michael Harrison, Harrison Smith Associates</i>	26
<b>Part 2: Points of exposure</b>		
2.1	Web security <i>Suheil Shahryar, VeriSign UK</i>	33
2.2	Broadband <i>Paul Collins, NTL Business</i>	48
2.3	Don't indulge in unprotected wireless <i>Ian Kilpatrick, Wick Hill Group</i>	54
2.4	No phishing: protecting employees from e-mail fraud <i>Ed Rowley, CipherTrust Europe Ltd</i>	57
2.5	Network vulnerabilities <i>Peter Crowcombe, NetScreen Technologies Inc</i>	63
2.6	Wireless applications <i>Andrew Steggles, EMEA Nokia Enterprise Solutions</i>	67