

# Contents

---

<i>Foreword</i>	xiii
<i>George Cox, Director General, Institute of Directors</i>	
<i>Introduction</i>	
<i>Adam Jolly</i>	xv
<b>Part 1: Information at risk</b>	
1.1 The business case for information security	3
<i>Nick Coleman, Head of Security Services, IBM and Chairman, SAINT</i>	
1.2 The demand for continuous information	12
<i>Rick Cudworth, Partner, KPMG LLP</i>	
1.3 The threat from cybercrime	18
<i>The Fraud Advisory Panel, Cybercrime Working Group, ICAEW</i>	
1.4 Recent attack trends	22
<i>Stuart Eaton, Centrinet</i>	
1.5 Recognising the enemy within	26
<i>Declan Grogan, Security Designers</i>	
1.6 Cyberliabilities in the workplace	33
<i>Richard Woudberg, Legal Counsel, Integralis</i>	
1.7 Data complacency	37
<i>Humphrey Browning, Head of Technical Consultancy, Nexor</i>	
1.8 The marketing dimension	41
<i>Michael Harrison, Chairman, Harrison Smith Associates</i>	
Stamping out the bugs	47
<i>Tony Neate, Industry Liaison Officer, National Hi-Tech Crime Unit (NHTCU)</i>	
<b>Part 2: Points of exposure</b>	
2.1 Email	53
<i>Indicii Salus</i>	
2.2 Web security	61
<i>Sam Green, Zeus Technology</i>	

2.3	Network vulnerabilities	66
	<i>Peter Crowcombe, EMEA Marketing Manager, NetScreen Technologies Inc.</i>	
2.4	Remote working	71
	<i>Paul Drew, Tekdata</i>	
2.5	Protecting online privacy	73
	<i>Simon Stokes, Tarlo Lyons Solicitors</i>	
2.6	Online payments	79
	<i>Colin Whittaker, Head of Security, APACS</i>	

	Case Study: Wellbeing.com takes a dose of ClearCommerce medicine	82
--	--	----

	Corporate profile: Proseq	84
--	---------------------------	----

**Part 3: Software protection**

3.1	Intrusion detection	93
	<i>Stuart Eaton, Centrinet</i>	
3.2	Firewalls	96
	<i>Stuart Eaton, Centrinet</i>	
3.3	Virus attack	98
	<i>Natasha Staley, Anti-Virus Consultant, Sophos Anti-Virus</i>	
3.4	Authentication and encryption	102
	<i>Tim Pickard, EMEA Strategic Marketing Director, RSA Security</i>	
3.5	Digital signatures	108
	<i>Bart Vansevenant, GlobalSign</i>	
3.6	Digital rights	113
	<i>Simon Mehlman, Macrovision</i>	
3.7	Electronic licensing	118
	<i>Simon Mehlman, Macrovision</i>	

**Part 4: Security policies**

4.1	Countering cybercrime	125
	<i>The Fraud Advisory Panel, Cybercrime Working Group, ICAEW</i>	
4.2	Security as standard	134
	<i>British Standards Institute (BSI)</i>	
4.3	Adequate security	139
	<i>Chris Knowles, Computacenter</i>	
4.4	A multi-layered response	145
	<i>Paul Barker, Technical Architect, Integralis</i>	
4.5	Managed security services	152
	<i>Stuart Eaton, Centrinet</i>	
4.6	Security testing	157
	<i>Roy Hills, NTA Monitor</i>	
4.7	Open source in the enterprise	160
	<i>Paul Smeddle, Positive Internet Company</i>	

**Part 5: Organisational back-up**

5.1	Employee confidentiality and a culture of security <i>Peter Wilson, Tarlo Lyons Solicitors</i>	165
5.2	Electronic contracting <i>William Kennair (John Venn &amp; Sons, UK), Chair, ICC Commission on E-Business, IT and Telecoms Task Force on Security and Authentication</i>	168
5.3	Information security training <i>John Harrison, Associate, SAINT and Smart421</i>	175
5.4	Beyond 'off the shelf' <i>Ken Watt, INSL</i>	183

**Part 6: Contingency planning**

6.1	Business continuity and crisis management <i>Dr David Smith FBCI, Chair, Education Committee, British Continuity Institute</i>	189
6.2	Data recovery <i>Gordon Stevenson, Managing Director, Vogon International</i>	199
6.3	Crisis management <i>Peter Power, Managing Director, Visor Consultants</i>	202
6.4	Forensics <i>Clifford May, Principal Consultant, Integralis</i>	207