# Contents

**Acknowledgements**

xvii

**Foreword**

xix

**Introduction**

xxi

## 1 Power to the people

- The power is out there . . . somewhere  1
- An information-rich world  2
- When in doubt, phone a friend  3
- Engage with the public  4
- The power of the blogosphere  4
- The future of news  5
- Leveraging new ideas  5
- Changing the way we live  6
- Transforming the political landscape  7
- Network effects in business  8
- Being there  9
- Value in the digital age  9
- Hidden value in networks  10
- Network innovations create security challenges  12
- You’ve been de-perimeterized!  14
- The collapse of information management  15
- The shifting focus of information security  15
- The external perspective  17
- A new world of openness  18
- A new age of collaborative working  19
- Collaboration-oriented architecture  20
- Business in virtual worlds  21
- Democracy . . . but not as we know it  22
- Don’t lock down that network  23
- The future of network security  24
Can we trust the data? 25
The art of disinformation 27
The future of knowledge 28
The next big security concern 30
Learning from networks 31

2 Everyone makes a difference 33
Where to focus your efforts 33
The view from the bridge 34
The role of the executive board 35
The new threat of data leakage 36
The perspective of business management 38
The role of the business manager 39
Engaging with business managers 40
The role of the IT function 41
Minding your partners 42
Computer users 43
Customers and citizens 44
Learning from stakeholders 44

3 There’s no such thing as an isolated incident 47
What lies beneath? 47
Accidents waiting to happen 48
No system is foolproof 49
Visibility is the key 49
A lesson from the safety field 50
Everyone makes mistakes 52
The science of error prevention 53
Swiss cheese and security 54
How significant was that event? 55
Events are for the record 56
When an event becomes an incident 57
The immediacy of emergencies 57
When disaster strikes 58
When events spiral out of control 58
How the response process changes 59
No two crises are the same 60
One size doesn’t fit all 61
The limits of planning 62
Some assets are irreplaceable 63
It’s the process, not the plan 63
Why crisis management is hard 64
Skills to manage a crisis 65
Dangerous detail 67
The missing piece of the jigsaw 67
Establish the real cause 68
Are you incubating a crisis? 69
When crisis management becomes the problem 70
Developing a crisis strategy 70
Turning threats into opportunities 71
Boosting market capitalization 72
Anticipating events 73
Anticipating opportunities 74
Designing crisis team structures 75
How many teams? 76
Who takes the lead? 77
Ideal team dynamics 77
Multi-agency teams 78
The perfect environment 79
The challenge of the virtual environment 80
Protocols for virtual team working 81
Exercising the crisis team 81
Learning from incidents 83

4 Zen and the art of risk management 85
East meets West 85
The nature of risks 86
Who invented risk management? 87
We could be so lucky 88
Components of risk 89
Gross or net risk? 90
Don’t lose sight of business 91
How big is your appetite? 92
It’s an emotional thing 93
In the eye of the beholder 94
What risk was that? 96
Living in the past 96
Who created that risk? 97
It’s not my problem 98
Size matters 99
Getting your sums right 99
Some facts are counterintuitive 101
The loaded dice 101
The answer is 42 103
It’s just an illusion 103
Context is king 104
Perception and reality 105
It’s a relative thing 107
Risk, what risk? 107
Something wicked this way comes 108
The black swan 109
Double jeopardy 110
What type of risk? 111
Lessons from the process industries 112
Lessons from cost engineering 113
Lessons from the financial sector 113
Lessons from the insurance field 115
The limits of percentage play 116
Operational risk 116
Joining up risk management 117
General or specific? 119
Identifying and ranking risks 120
Using checklists 122
Categories of risks 122
It’s a moving target 123
Comparing and ranking risks 124
Risk management strategies 125
Communicating risk appetite 126
Risk management maturity 127
There’s more to security than risk 128
It’s a decision support tool 129
The perils of risk assessment 130
Learning from risk management 131

5 Who can you trust? 133
An asset or a liability? 133
People are different 134
The rule of four 135
The need to conform 136
Understand your enemies 137
The face of the enemy 137
Run silent, run deep 138
Dreamers and charmers 139
The unfashionable hacker 140
The psychology of scams 142
Visitors are welcome 142
Where loyalties lie 144
Signs of disloyalty 144
The whistleblower 145
Stemming the leaks 146
Stamping out corruption 147
Know your staff 148
We know what you did 149
Reading between the lines 151
Liberty or death 153
Personality types 154
Personalities and crime 156
The dark triad 157
Cyberspace is less risky 157
Set a thief 159
It’s a glamour profession 160
There are easier ways
I just don’t believe it
Don’t lose that evidence
They had it coming
The science of investigation
The art of interrogation
Secure by design
Science and snake oil
The art of hypnosis
The power of suggestion
It’s just an illusion
It pays to cooperate
Artificial trust
Who are you?
How many identities?
Laws of identity
Learning from people

6 Managing organization culture and politics

When worlds collide
What is organization culture?
Organizations are different
Organizing for security
Tackling ‘localitis’
Small is beautiful
In search of professionalism
Developing careers
Skills for information security
Information skills
Survival skills
Navigating the political minefield
Square pegs and round holes
What’s in a name?
Managing relationships
Exceeding expectations
Nasty or nice
In search of a healthy security culture
In search of a security mindset
Who influences decisions?
Dealing with diversity
Don’t take yes for an answer
Learning from organization culture and politics

7 Designing effective awareness programs

Requirements for change
Understanding the problem
Asking the right questions
The art of questionnaire design 214
Hitting the spot 215
Campaigns that work 216
Adapting to the audience 217
Memorable messages 218
Let’s play a game 220
The power of three 221
Creating an impact 222
What’s in a word? 224
Benefits not features 225
Using professional support 226
The art of technical writing 227
Marketing experts 228
Brand managers 229
Creative teams 230
The power of the external perspective 230
Managing the media 231
Behavioural psychologists 232
Blogging for security 233
Measuring your success 234
Learning to conduct campaigns 235

8 Transforming organization attitudes and behaviour 237
Changing mindsets 237
Reward beats punishment 238
Changing attitudes 240
Scenario planning 241
Successful uses of scenarios 242
Dangers of scenario planning 243
Images speak louder 244
A novel approach 245
The balance of consequences 245
The power of attribution 248
Environments shape behaviour 248
Enforcing the rules of the network 250
Encouraging business ethics 251
The art of on-line persuasion 251
Learning to change behaviour 252

9 Gaining executive board and business buy-in 255
Countering security fatigue 255
Money isn’t everything 256
What makes a good business case? 257
Aligning with investment appraisal criteria 257
Translating benefits into financial terms 258
Aligning with IT strategy
Achieving a decisive result
Key elements of a good business case
Assembling the business case
Identifying and assessing benefits
Something from nothing
Reducing project risks
Framing your recommendations
Mastering the pitch
Learning how to make the business case

10 Designing security systems that work
Why systems fail
Setting the vision
What makes a good vision?
Defining your mission
Building the strategy
Critical success factors for effective governance
The smart approach to governance
  Don’t reinvent the wheel
  Look for precedents from other fields
  Take a top down approach
  Start small, then extend
  Take a strategic approach
  Ask the bigger question
  Identify and assess options
Risk assessment or prescriptive controls?
In a class of their own
Not all labels are the same
Guidance for technology and people
Designing long-lasting frameworks
Applying the fourth dimension
Do we have to do that?
Steal with caution
The golden triangle
Managing risks across outsourced supply chains
Models, frameworks and architectures
Why we need architecture
The folly of enterprise security architectures
Real-world security architecture
The 5 Ws (and one H)
Occam’s Razor
Trust architectures
Secure by design
Jericho Forum principles
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Harnessing the power of the organization</td>
<td>311</td>
</tr>
<tr>
<td></td>
<td>The power of networks</td>
<td>311</td>
</tr>
<tr>
<td></td>
<td>Surviving in a hostile world</td>
<td>311</td>
</tr>
<tr>
<td></td>
<td>Mobilizing the workforce</td>
<td>312</td>
</tr>
<tr>
<td></td>
<td>Work smarter, not harder</td>
<td>313</td>
</tr>
<tr>
<td></td>
<td>Finding a lever</td>
<td>313</td>
</tr>
<tr>
<td></td>
<td>The art of systems thinking</td>
<td>314</td>
</tr>
<tr>
<td></td>
<td>Creating virtuous circles</td>
<td>315</td>
</tr>
<tr>
<td></td>
<td>Triggering a tipping point</td>
<td>315</td>
</tr>
<tr>
<td></td>
<td>Identifying key influencers</td>
<td>316</td>
</tr>
<tr>
<td></td>
<td>In search of charisma</td>
<td>318</td>
</tr>
<tr>
<td></td>
<td>Understanding fashion</td>
<td>318</td>
</tr>
<tr>
<td></td>
<td>The power of context</td>
<td>319</td>
</tr>
<tr>
<td></td>
<td>The bigger me</td>
<td>320</td>
</tr>
<tr>
<td></td>
<td>The power of the herd</td>
<td>321</td>
</tr>
<tr>
<td></td>
<td>The wisdom of crowds</td>
<td>322</td>
</tr>
<tr>
<td></td>
<td>Unlimited resources – the power of open source</td>
<td>323</td>
</tr>
<tr>
<td></td>
<td>Unlimited purchasing power</td>
<td>324</td>
</tr>
<tr>
<td></td>
<td>Let the network to do the work</td>
<td>324</td>
</tr>
<tr>
<td></td>
<td>Why is everything getting more complex?</td>
<td>325</td>
</tr>
<tr>
<td></td>
<td>Getting to grips with complexity</td>
<td>327</td>
</tr>
<tr>
<td></td>
<td>Simple can’t control complex</td>
<td>327</td>
</tr>
<tr>
<td></td>
<td>Designing freedom</td>
<td>329</td>
</tr>
<tr>
<td></td>
<td>A process-free world</td>
<td>330</td>
</tr>
<tr>
<td></td>
<td>The power of expressive systems</td>
<td>331</td>
</tr>
<tr>
<td></td>
<td>Emergent behaviour</td>
<td>332</td>
</tr>
<tr>
<td></td>
<td>Why innovation is important</td>
<td>332</td>
</tr>
<tr>
<td></td>
<td>What is innovation?</td>
<td>333</td>
</tr>
<tr>
<td></td>
<td>What inspires people to create?</td>
<td>335</td>
</tr>
<tr>
<td></td>
<td>Just one idea is enough</td>
<td>335</td>
</tr>
<tr>
<td></td>
<td>The art of creative thinking</td>
<td>336</td>
</tr>
<tr>
<td></td>
<td>Yes, you can</td>
<td>336</td>
</tr>
<tr>
<td></td>
<td>Outside the box</td>
<td>337</td>
</tr>
<tr>
<td></td>
<td>Innovation environments</td>
<td>339</td>
</tr>
<tr>
<td></td>
<td>Turning ideas into action</td>
<td>339</td>
</tr>
</tbody>
</table>