# Contents


***Acknowledgements*** **xvii**
***Foreword*** **xix**
***Introduction*** **xxi**

**1 Power to the people** **1**
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 160
I just don't believe it 161
Don't lose that evidence 162
They had it coming 163
The science of investigation 164
The art of interrogation 165
Secure by design 167
Science and snake oil 167
The art of hypnosis 169
The power of suggestion 170
It's just an illusion 171
It pays to cooperate 172
Artificial trust 173
Who are you? 173
How many identities? 175
Laws of identity 176
Learning from people 178

**6 Managing organization culture and politics 181**
When worlds collide 181
What is organization culture? 182
Organizations are different 184
Organizing for security 186
Tackling 'localitis' 186
Small is beautiful 187
In search of professionalism 188
Developing careers 190
Skills for information security 191
Information skills 192
Survival skills 194
Navigating the political minefield 195
Square pegs and round holes 196
What's in a name? 197
Managing relationships 199
Exceeding expectations 200
Nasty or nice 201
In search of a healthy security culture 202
In search of a security mindset 204
Who influences decisions? 205
Dealing with diversity 206
Don't take yes for an answer 207
Learning from organization culture and politics 208

**7 Designing effective awareness programs 211**
Requirements for change 211
Understanding the problem 212
Asking the right questions 213

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 259
Achieving a decisive result 259
Key elements of a good business case 260
Assembling the business case 261
Identifying and assessing benefits 261
Something from nothing 263
Reducing project risks 263
Framing your recommendations 264
Mastering the pitch 264
Learning how to make the business case 266

**10 Designing security systems that work 269**
Why systems fail 269
Setting the vision 270
What makes a good vision? 270
Defining your mission 272
Building the strategy 274
Critical success factors for effective governance 275
The smart approach to governance 276
Don't reinvent the wheel 276
Look for precedents from other fields 277
Take a top down approach 277
Start small, then extend 278
Take a strategic approach 278
Ask the bigger question 279
Identify and assess options 280
Risk assessment or prescriptive controls? 280
In a class of their own 282
Not all labels are the same 283
Guidance for technology and people 284
Designing long-lasting frameworks 285
Applying the fourth dimension 286
Do we have to do that? 287
Steal with caution 289
The golden triangle 290
Managing risks across outsourced supply chains 291
Models, frameworks and architectures 292
Why we need architecture 293
The folly of enterprise security architectures 294
Real-world security architecture 295
The 5 Ws (and one H) 296
Occam's Razor 297
Trust architectures 298
Secure by design 299
Jericho Forum principles 299

Collaboration-oriented architecture 300
Forwards not backwards 301
Capability maturity models 301
The power of metrics 302
Closing the loop 303
The importance of ergonomics 305
It's more than ease of use 305
The failure of designs 306
Ergonomic methods 307
A nudge in the right direction 308
Learning to design systems that work 308

**11 Harnessing the power of the organization 311**
The power of networks 311
Surviving in a hostile world 311
Mobilizing the workforce 312
Work smarter, not harder 313
Finding a lever 313
The art of systems thinking 314
Creating virtuous circles 315
Triggering a tipping point 315
Identifying key influencers 316
In search of charisma 318
Understanding fashion 318
The power of context 319
The bigger me 320
The power of the herd 321
The wisdom of crowds 322
Unlimited resources – the power of open source 323
Unlimited purchasing power 324
Let the network to do the work 324
Why is everything getting more complex? 325
Getting to grips with complexity 327
Simple can't control complex 327
Designing freedom 329
A process-free world 330
The power of expressive systems 331
Emergent behaviour 332
Why innovation is important 332
What is innovation? 333
What inspires people to create? 335
Just one idea is enough 335
The art of creative thinking 336
Yes, you can 336
Outside the box 337
Innovation environments 339
Turning ideas into action 339

Steps to innovation heaven 340
The road ahead 341
Mapping the future 342
Learning to harness the power of the organization 344

**In conclusion** **347**

**Bibliography** **353**

**Index** **357**