

CONTENTS

CHAPTER 1: Becoming an Entrepreneur in the Security Business	1
1.1 Context	1
1.2 Competitive intelligence	2
1.3 Linking business intelligence to our operating environment	7
1.4 Examining appropriate intellectual property rights (IPR) in order to protect business ideas and enterprise	8
1.5 Emerging markets	13
1.6 Targeting consumer markets and marketing	18
1.7 Business funding	21
1.8 Reviewing operations management	28
1.9 Business networking	34
2.0 Social media marketing	42
2.1 Negotiation	46
2.2 Company structures, corporate returns and regulation	51
References	55
Chapter 2: Becoming a Developed Security Manager.....	65
2.1 Context	65
2.2 Role of security director	66
2.4 Fitting security into a wider context of resilience	70
2.5 Sub-disciplines of organisational resilience: Security, emergency planning and business continuity	73
2.6 Management and balancing important priorities	74
2.7 Adding value: Developing the business that clients require	80
2.8 Why do businesses fail?	85
2.9 The requirement for professional proficiency	89
References	107
Chapter 3: Security Legislation and Regulation.....	113
3.1 Context	113
3.2 Types of law in UK	113
3.3 UK human rights laws	114
3.4 Other UK laws relating to security management	117
3.5 Other UK laws relating to corporate management and workplaces	124
3.6 International law, conflict and human rights	140
3.7 Prominent business laws related to international business	146

References.....	148
VIDEOS.....	149
Chapter 4: Private Investigations.....	151
4.1 Context.....	151
4.2 Role of private investigators.....	153
4.3 Affidavits and process serving.....	154
4.4 Tracing missing people.....	156
4.5 Surveillance techniques.....	164
4.6 Technical surveillance.....	171
4.7 Witness statements.....	175
4.8 Crime scene analysis.....	181
4.9 Evidence: What is it? Why is evidence so flawed?.....	182
References.....	188
Chapter 5: Information Security.....	195
5.1 Context.....	195
5.2 Why target our information?.....	196
5.3 Intelligence and espionage.....	200
5.4 Internal risks.....	211
5.5 Cyber security.....	214
5.6 Mitigation: Developing a security policy.....	219
References.....	229
Chapter 6: Protective Security.....	237
6.1 Context.....	237
6.2 Methods of risk assessment.....	240
6.3 How to conduct a person-focused threat assessment.....	246
6.4 Ethos and expectations of protective security roles; 'adaptive practitioners'.....	250
6.5 Anti-piracy; market, counter-measures and agencies.....	253
6.6 Firearms.....	259
6.7 Managing people in protective security environments.....	266
References.....	273
Chapter 7: Safe Business Travel.....	281
7.1 Context.....	281
7.2 Government help and basics.....	282
7.3 Before you go: Safety and security tips.....	287
7.4 Reporting and responding to crime in-country.....	290
7.5 Business travel insurance.....	292
7.6 Kidnap for ransom, kidnap and countermeasures.....	295

7.7 Corporate liability laws and business travel.....	301
7.8 Protective security approaches to travel security.....	304
7.9 Due diligence.....	306
References.....	308
Chapter 8: Personal and Organisational Resilience.....	313
8.1 Context.....	313
8.2 Personal resilience.....	314
8.3 Personal resilience initiatives in the workplace.....	315
8.4 Developing team resilience from personal resilience techniques.....	317
8.5 Crisis management and personal resilience.....	320
8.6 Crisis management and communications.....	321
8.7 Social media and crisis management.....	325
8.8 Crisis management standards and guidance.....	328
References.....	331
ITG Resources.....	337