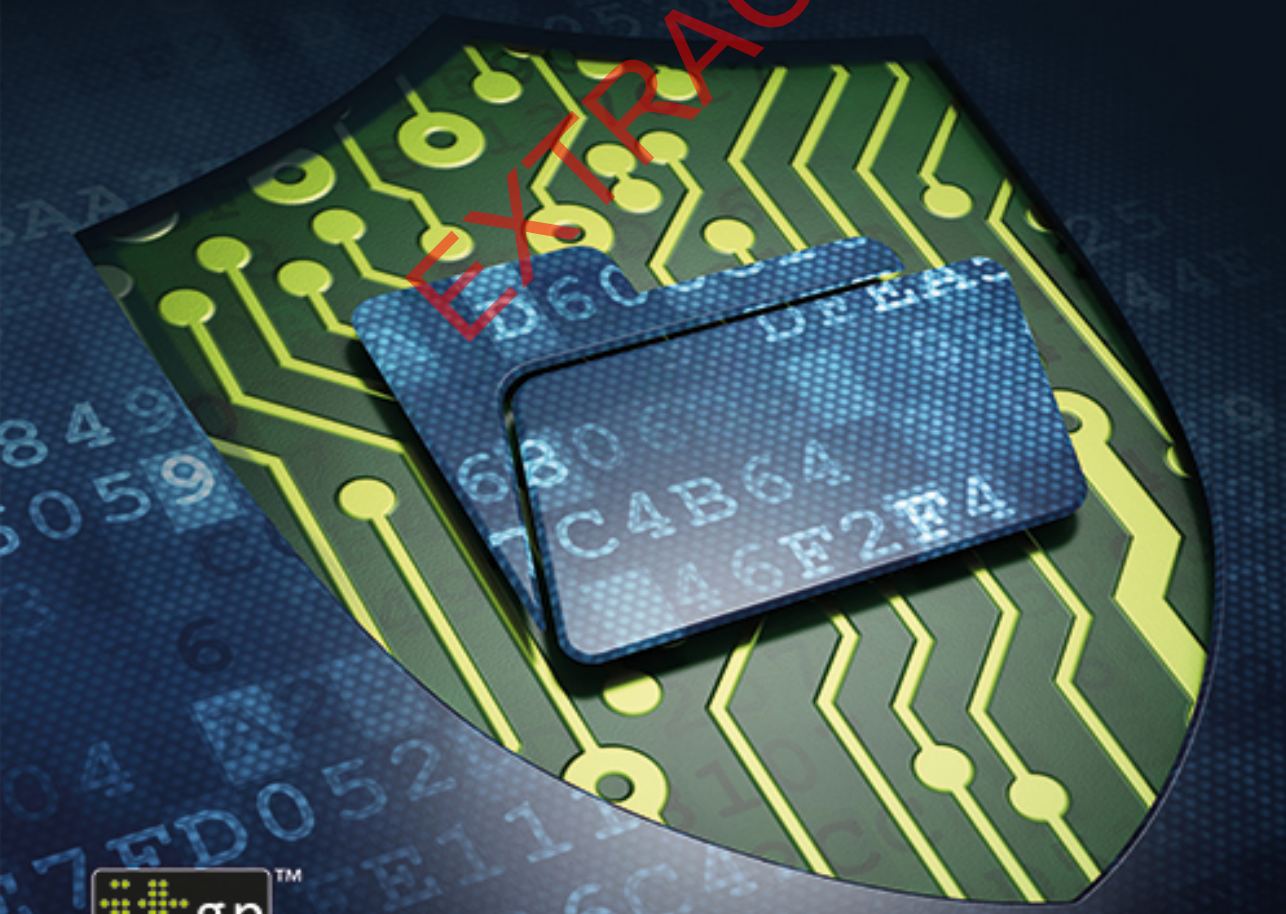
THE SECURITY CONSULTANT'S HANDBOOK

Richard Bingley



itgp™

The Security Consultant's Handbook

RICHARD BINGLEY

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

First published in the United Kingdom in 2015
by IT Governance Publishing

ISBN 978-1-84928-749-4

ABOUT THE AUTHOR

Richard Bingley is a senior lecturer in security and organisational resilience at Buckinghamshire New University, in the United Kingdom. Richard is co-founder of CSARN, the popular business security advisory network with offices in the UK and Australia. He has more than 15 years' experience in a range of high-profile security and communications roles, including as a close protection operative at London's 2012 Olympics and in Russia for the 2014 Winter Olympic Games. Richard has previously authored two popular books: *Terrorism: Just the Facts* (2004) and *Arms Trade: Just the Facts* (2003). Richard is a licensed close protection operative in the UK and holds a postgraduate certificate in teaching and learning in higher education.

FOREWORD

Welcome to *The Security Consultant's Handbook*.

This book is *not* a training manual about the security industry, or any subdiscipline within it. There are hundreds, or thousands, of specialist security training services and guidance manuals out there that can explain and evaluate their niche and technical specialisms far better than I.

Yet several years have now passed since a range of very decent generalist support books for security managers and practitioners have been produced. A lot has happened since: economic crashes, national security data haemorrhages, nuclear reactor meltdowns, nihilistic international terrorism and a social media revolution that has brought about individual and corporate liberation and tyranny; possibly in equal measure.

My purpose, therefore, is to set out to provide a compendium of business approaches, opportunities and risks that fairly reflect those faced by the modern security entrepreneur and practitioner, at this point in time. I say *entrepreneur* because – whether we are sole contractors, employees, or public authority officials – most of us nowadays are required to innovate and adopt entrepreneurial approaches by our paymasters.

More than ever before, a failure to read and adapt to our operating environments, can leave us short of perceived value. The business world is more accessible, but possibly less forgiving, than ever before.

In this book, I therefore aim to provide a holistic oversight of essential core knowledge, emerging opportunities and approaches to corporate thinking that are being increasingly demanded by employers and buyers in the security market. This book aims to provide options and directions for those who are ambitious to succeed in security, either individually or as part of a team.

I also hope to stimulate some fresh ideas and new routes to market to consider for security professionals who may feel that they are under-appreciated and over-exerted in traditional business domains. I do hope that each of the eight chapters really does help the reader to enjoy a renewed sense of passion and control over their entrepreneurial activity.

This book will therefore unapologetically seek to encourage and facilitate the reader's own lateral thinking in relation to existing markets, management and business approaches. Near the beginning, we provide some foundation

knowledge of so-called emerging markets, even though these markets – such as Brazil, India, Russia and China – have now been maturing for several decades.

Moreover, I attempt to encourage the reader's own skills and knowledge, by linking much of our content to further opportunities for training, higher education and longer-term professional development.

Possibly the biggest barrier to our own success is an individual and collective impatience with *reflective learning* techniques. Our inability to sensibly review or admit to various faults, is a fundamental recurring weakness for us information-rich, but knowledge-poor, human beings.

Since time immemorial, *cognitive bias* has been a significant contributor in the causation of wars, industrial-scale accidents and bankruptcies. Being caught in an activity trap, or constricted by tunnel vision, prevents us from exploiting so many nearby opportunities to improve and excel. I therefore very much hope that this book encourages readers to reach beyond their comfort zones, yet still remain within the bounds of law and sanity!

Today's world does unequivocally provide a treasure trove of opportunity for entrepreneurs and innovators, I believe. It's surely the dilemma as to which doors to open or close that tends to vex us entrepreneurs.

This said, I hope that our readers' decision-making capabilities may be well assisted by discovering lots of new facts and case studies across the eight chapters. These sections seek to cover foundation knowledge in the domains of: entrepreneurial practice; management practice; legislation and regulation; private investigations; information and cyber security; protective security; safer business travel; personal and organisational resilience.

For context, I'm a security management lecturer and security contractor. I first conceived the idea for this book as I was travelling from Belorussky railway station northwards towards Moscow's Sheremetyevo Airport, on a sleek, bullet-shaped, Aero Express shuttle train. The 2014 Sochi Winter Olympics had safely concluded a few hours before.

I had taken some time out from university teaching and accepted a brief security contract. My role on this occasion was as a protective security agent for an American client organisation in Russia.

Our company had had some Olympic guests travelling back through Moscow from Sochi, mainly towards the United States. Some were a little apprehensive about their transit. Understandably so. Suicide bombings at Russian rail stations had occurred a few weeks before the Games. Moreover, 100 or so suicide

bombings during the last decade and a half had hit the Russian people hard. But our people were safely through and back in various planetary quarters. Job done.

As I boarded the train, a bilingual announcement told us that chemical weapons or firearms were – thankfully – not permitted on this train. Passengers around me curled up into their coats with the same type of melancholic gloom reserved for any pre-dawn, Monday morning, midwinter commute anywhere in the world.

My Wi-Fi connection suddenly kicked in. Emails pulsed through from my own students in Iraq, the UAE, Canada and US. My project bosses in Florida had also pinged me a message or two about returning items. Another colleague sent me an SMS: should we add a brief evaluation of ongoing events in Ukraine to my daily threat assessment? Ukraine's President had been toppled by protestors 48 hours before. 'Nftr' I responded (Nothing further to report). As things stood, all our guests had safely left the region.

Moments later I received a text message from a Chamber of Commerce boss in Russia. Another text streamed in, this time from my mother. My old dog Floyd was asleep by her home hearth. She expressed genuine surprise that I was still alive. Perhaps even a small suspicion that I hadn't been in Russia at all, because I wasn't even slightly incapacitated.

How perspectives can vary. I instantly thought back to the previous night's dinner on Moscow's neon-illuminated boulevard, *Novy Arbat*. A Russian friend recoiled in dismay when I told them that western visitors to Moscow actually required a physical security detail: "We have far less crime than New York", they moaned.

So there we have it. The world *has* closed in, just as the Scorpions sang back in 1991 after the Berlin Wall was hammered down. Today our planet is a global village. We global citizens can talk to one another and see one another, although we may all live in wildly different time zones. We all share the same data sets and read the same news blogs. We are all – I hope – more interested in developing intercontinental business alliances, rather than intercontinental ballistic missiles.

Yet human perspectives can remain poles apart; entrenched by different experiences, cultures, approaches and interpretations.

Knowing in essence who and what to believe, and also what to do if certain scenarios occur, does actually get to the heart of what constitutes working life as a security operative. Beneath the corporate-enshrined authority of an executive boardroom, there really aren't many company roles with such a significant sense of duty and responsibility, than that of a professional security officer.

For those interested in progression within the security profession, the world is your operating environment. Therefore, good subject matter knowledge is not so much a route to power, but a fundamental duty of your day job role, which is to keep your colleagues and assets safe and secure.

This may be quite a daunting statement.

This publication is therefore designed to be a practical and enabling guide for security officers and contractors. Its purpose is to plug information gaps, or provoke new ideas, rather than to be treated as a fully garrisoned academic tome.

My aim was to provide a 'real-world' support tool for those who want to offer safe, proportionate and value-driven security services to their clients.

By carrying out some 50 interviews with leading security practitioners, and reviewing a large range of credible literature, which now supports business security activity, I have tried wherever possible to suspend personal opinions and philosophies. I wanted to let the experts and facts speak for themselves.

Nevertheless, personal leanings and preferences will be evident, such as the choices I have made around chapter topics. These editorial choices tend to reflect my philosophy and my own experiences within the profession, as to what topics have emerged to be significant from a corporate world viewpoint.

I apologise if this book's menu does not suit every reader's taste. Please do let me know if significant areas of interest have been omitted and we will seek to include such omissions in subsequent editions.

In closing, I would like to thank the many interviewees who shared their insights both for open-source and background contexts. Face-to-face interviews were conducted during 2013, 2014 and early 2015 in mainland Britain, Northern Ireland, Lebanon, the US, the Czech Republic and Russian Federation. I also express sincere thanks to a fantastic range of students at Buckinghamshire New University's growing Department of Security and Resilience, based in the UK, where I teach as a senior lecturer.

For context, many, if not all, of my undergraduate and postgraduate students can claim to be officially *mature* because they are over 25 years old. They also work as full-time security consultants and managers in some of the world's most complex and volatile environments. Each student works viscerally hard in their day job. They somehow study in their non-existent 'spare' time. More often than not each learner defeats exceptional life constraints. Their motivation and application continues to inspire me. Some were able to share their own work experiences for learning purposes within this book. I am hugely indebted that so

many found the time and patience to teach and support me, when it should of course be the other way around.

I would particularly like to thank Phil Wood MBE, former Head of Academic Department at Buckinghamshire New University, for his support when I joined his team of academics. Likewise, a 'thank you' also to our new Head of Academic Department, Emma Parkinson, for her support and endless sympathy as I came to conclude writing this book. I am also indebted to my fellow security management lecturers, Simon King and Gavin Butler, alongside Dianne Cameron, Dianne Dunn and Peter Brown (senior registrar) in our university's Blended Learning Unit. They all bore the brunt of my research and book writing diversions. For context, Simon King also very kindly contributed subsections 4.5 (surveillance techniques) and 4.6 (electronic surveillance, the law and ethics) of this book's Private Investigations chapter. Gavin Butler also very kindly supplied some of the chapter subheadings and was pivotal in shaping the list of contents for this edition. I would like to record my gratitude for all of those who contributed quotes, ideas and interviews to this book. These include: Antoni Bick, Thomas Black, Scott Brant, John Paul Breed, Paul Brown, Lee Caines, Daniel Cogan, James Gess, Jon Hill (Polaris), Tom Hough, Tracey Hough, Simon Hull, Jason Layton, Brett Lovegrove, Seth Martin, Paul Morgan, Chris Phillips, Robert Newman, Lisa Reilly, Thomas Richmond, Rob Scott (SCG Security), Adam Smith, Jason Towse (Mitie Total Security), John Tristram and Andy Williams (ex-Marriott EMEA security director).

Some have chosen to remain uncited.

I do also wish to specifically thank my publishers at IT Governance, including Vicki Utting, for her patience and compassion, as my book deadline did require a couple of extensions, following the passing of my father, Randal Bingley. A big further 'thank you' to my mother, Amanda Bingley, who has provided me with consistent love and support. My final 'thank you' is directed toward PC Milena Bauerova, of London's famous Metropolitan Police Service. PC Bauerova came to my rescue during a sunny afternoon in June 2013, on London's picturesque Hampstead Common. Clearly, without her kind intervention back then, this book may never have witnessed the light of day.

The errors in this material are all mine.

Richard Bingley, London, 2015

CONTENTS

CHAPTER 1: BECOMING AN ENTREPRENEUR IN THE SECURITY BUSINESS

1.1 Context

> *"You miss 100% of the shots you don't take."* – Wayne Gretzky, NHL Hall of Fame.

Whether as an employee, senior manager, or self-employed consultant, we are all expected to be entrepreneurs. Growing a successful business, your own enterprise or somebody else's, is one of the most satisfying experiences during anybody's working life. Winning new contracts is a thrilling endorsement of conceptual plans, existing skills, prior investment and experiences. On paper, becoming a *successful* entrepreneur within the security sector can be viewed as relatively straightforward by those on the outside of our profession. There is a popular perception that the private security market is awash with money, especially around high-value assets where niche specialisms and uber-exciting professional backgrounds may well be required by clients. Two recent conversations that I've had spring to mind. The first, with a young law undergraduate at my boxing gym. After sparring me out of the ring, my pal wanted to chat about how he could 'diversify' into security. (Doesn't being a barrister pay enough?) Secondly, a talk with Jason Towse, a managing director at one of the UK's biggest security operators. He told me that margins from manned-guarding had all but evaporated. Success was hard-earned and cumulatively accrued, he said, "from building long-standing strategic relationships". Longer-term relationships enabled the client and vendor to develop a trusted synergy based upon an intuitive understanding of one another. There had to be a 'cross-cultural fit' between both organisations, Towse reflected (1).

The truth is, of course, that security markets are, in essence, volatile. Furthermore they remain vulnerable to changing commercial market conditions, like any other private enterprise. Security markets mirror wider global market conditions, unless specific local incidents or security cultures emerge. That is, if they are lucky! Some three or four years after the noughties banking crisis, major financial institutions in London were still laying-off dozens of security staff, despite the international terrorism threat level either being designated 'severe' or 'substantial' (2). Yet elsewhere, often in fragile spheres of instability and conflict, the private security market has boomed beyond the wildest imagination of most practitioners. For example, after almost a decade of military intervention in Afghanistan, by 2010, the

US Department of Defense employed around 20,000 private contractors and licensed 37 companies in Afghanistan. Circumstances again changed rapidly that year. Afghanistan's President, Hamid Karzai, issued a decree prohibiting private security companies and established an Afghan Public Protection Force (APPF). The APPF was tasked to replace all non-diplomatic private security management functions (3). Yet four years later, following significant security lapses, and consideration for wider national security concerns, the outgoing President revoked his 2010 force nationalisation decree. Thus, market continuity planning, to militate against inconsistent customers and uncertain markets, will be a recurring theme for entrepreneurs as we travel through this book.

Taking on the role of business planner, when the sands of politics and economics are permanently shifting, can absorb and expend a lot of energy and enthusiasm. It may even sap individual and team morale after a while. Chronic uncertainty causes fatigue. Yet, there is a positive side for security practitioners because surrounding instability, even adversity, should really play to our strengths. Uncertainty and adversity are the very reasons why our clients look for our services. After all, if a security consultant does *not* survive and thrive on instability, then why on earth should an external client ever need to have confidence in you?

As we will see in this chapter, and subsequent sections of the Handbook, information is a critical success factor to any enterprise. Knowledge is, de facto, commercial power – a mix of leverage, authority and trust in us to do the right thing, at the right time. Those who take time to properly research, analyse and make sense of surrounding business environments, will reap longer-term dividends. Not least, because a greater sense of authority and resilience will emerge about your enterprise in the eyes of your putative clients and market peers. By positively embracing uncertainty, and shining a torch of leadership in difficult and unpredictable environments, the modern day security practitioner is ideally equipped to add real value to most organisations, including their own. Security practitioners and successful entrepreneurs have many shared characteristics: adaptability, a preference for back-up plans, and, above all, psychological resilience and stamina. "There's no such thing as a setback", said self-help guru business mogul, Tony Robins, who declared this enjoyable truism after his latest TV series was cancelled by producers (4). Just a nudge in another direction, perhaps.

1.2 Competitive intelligence

> *"Competitive Intelligence is not an invention of the 20th Century."* – (Leonard Fuld, 2013)

Enterprises thrive due to many factors; desirable products, effective marketing, blindly optimistic and wealthy investors, dynamic working cultures and, of course, good leadership and motivated employees. Nevertheless, in all likelihood, a business can only survive and prosper in the longer-term by remaining actively aware and adaptive to its operating environment. Such alertness includes keeping a careful and most respectful eye upon similar organisations fishing in the same waters.

Security sector job roles are more fragile than others. Services and consultancies are in many cases contracted out, licensed and regulated by government departments and public authorities. This extra political dimension – sometimes influenced by a swift change in public opinion, or a new ministerial appointment – means that projects or administrative regimes can be uprooted or radically changed with very little notice. Commercial security and risk services are often tasked around delivery into higher-risk domains, where the approach by government agencies could be more volatile and uncertain. The only consistent feature of many higher risk environments is their inherent inconsistency. Governments will often seek to take direct control of a crisis situation or contagion of negative events. Authorities may wish to extend their reach over a perceived, troublesome sector, such as security, by issuing a raft of measures that may be impracticable and toxic to continued business. Security risk management thus attracts a high degree of interest from media and NGOs which makes public authorities even more susceptible to intervening within this sector. Sudden alterations to the operating environment imposed by governments and public authorities, can lead to damaging losses if the new conditions are not quickly anticipated. On the positive side, riskier security or operating environments provide fantastic opportunities for security enterprises to shine and excel. Companies that know their operating environments well, and also uphold professional practices around individual and organisational resilience (those that we delve into across this book's eight chapters), will gain competitive advantage over their commercial peers.

Case studies: Four overnight game-changers to a private security operating environment

1. The introduction of British troops into Northern Ireland in 1969 to separate warring

factions, and provide protection for civilians. This UK Government move followed the escalation of widespread sectarian and terrorist violence in Northern Ireland, and concerns in relation to the neutrality of some public services including domestic police functions.

2. The shooting and killing of several citizens in Baghdad by a small handful of employees working for the US security company, Blackwater, during 2007. The company was immediately ejected from Iraq by the domestic government. A national and international clamp-down on overseas-based private security contractors followed. This tragic event contributed, somewhat, as a catalyst for 'Montreux Document': also known as the *International Code of Conduct for Private Security Service Providers* (ICoC), a Swiss Government initiative. ICoC was codified into sector guidance by security trade association, ASIS, who later published the widely practiced *Management System for the Quality of Private Security Company Operations* (ANSI/ASIS PSC 2012).
3. Establishment of the Afghan Public Protection Force (APPF) by President Hamid Karzai's administration, following his declaration in 2010 that all Private Security Contractors (PSCs) will be disbanded and services provided direct by the APPF. Karzai repealed his decision four years later.
4. A last-minute decision by UK Government ministers and officials to deploy several thousand Armed Forces personnel to guard the London 2012 Olympics sites, following an admission by the central security contractor, G4S, that there was a significant service delivery shortfall in required security guards. The British Security Industry Authority had warned about significant potential shortfalls more than two years beforehand. Those well-mobilised private companies that anticipated the shortfall were able to pick up the slack and win last-minute contracts, including for specialised services, such as close protection.

What is competitive intelligence?

"Competitive Intelligence is not an invention of the 20th century," reports Leonard Fuld, a pre-eminent expert in the field. It is just another form of intelligence gathering, specifically tasked to gather actionable and high-grade information about activities, strengths and weaknesses of market competition. Fuld points to a historical example of nineteenth century British financier, Nathan Rothschild, who, "managed to corner the market on British government securities by receiving early warning of Napoleon's defeat at Waterloo". Fuld adds: "He used carrier pigeons, the email of his day. He knew the information to watch and how to make sense of it; in the end, he used this intelligence to make a killing in the market" (5).

Competitive intelligence (CI) gained ground in American business journals half a century ago. Competitive intelligence is a process which identifies and researches various important market information sets, which when integrated together, provide a company with insightful information and therefore a 'competitive advantage'

over others in the field. We will take some time in the next sub-chapter (1.3) to look at management tools which enable us to build and achieve competitive intelligence products; perhaps the most famous being Harvard Professor Michael Porter's *Five Forces Model*. With Porter's work, CI gained a greater business educational grounding in the US. His 1980 study, *Competitive Strategy: Techniques for Analyzing Industries and Competitors*, is deemed a seminal paper by corporate strategists. Security planners confidently deploying Porter's modelling will undoubtedly impress potential clients! Porter summarises his findings by saying: "Customers, suppliers, substitutes and potential entrants are all 'competitors' to companies in the industry and may be more or less prominent depending on the circumstances. Competition in this broader sense might be termed *extended rivalry*" (6). An important document emerged in 2008 that attempted to pull together the range of definitions and parameters set by CI practitioners and academics. The Society of Competitive Intelligence Professionals (SCIP) published a definition in its journal: "… a necessary, ethical business discipline for decision making based on understanding the competitive environment" (7). Stephen Miller, formerly an editor of SCIP's journal, describes CI as a *positive* corporate business function: "CI enables managers in companies of all sizes to make decisions about everything from marketing, R&D and investing tactics, to long term business strategies" (8).

Competitive intelligence includes the following traits and focus:

- Its core focus is on the external business environment
- There is some form of process involved, or established business function/s, whereby information and knowledge is gathered and processed into an actionable 'intelligence product'
- CI could also act as a radar-like 'early warning system' for a company to be made aware, sooner rather than later, of possible major market changes or incidents

Case Study: Fund's ten principles of competitive intelligence

1. Competitive intelligence is information that has been analysed to the point where you can make a decision.
2. Competitive intelligence is a tool to alert management to an early warning of both threats and opportunities.
3. Competitive intelligence is a means to deliver reasonable assessments.
4. Competitive intelligence comes in many flavours [sic].
5. Competitive intelligence is a way for companies to improve their bottom line.
6. Competitive intelligence is a way of life, a process.

7. Competitive intelligence is part of all best-in-class companies.
8. Competitive intelligence is directed from the executive suite.
9. Competitive intelligence is seeing outside yourself.
10. Competitive intelligence is both short and long term (9).

How can we stay on the right side of the law?

With real-time global interconnectedness, and greater commercial pressures for transparency, Open Source Intelligence gathering (OSINT) has become big business. Decent OSINT briefings can provide real value-added services to clients. OSINT can also provide tangible internal organisational value. Unfortunately, the line between legitimate intelligence activities and unlawful espionage is sometimes crossed. One company, IT hardware manufacturer Hewlett Packard, was made to pay around $14m in fines, and its contracted private investigator was jailed, following unlawful intercepts carried out on senior employees' telephones. The *Fuld Gilad Herring Academy of Competitive Intelligence* runs the Competitive Intelligence Certification Program. Its President, Dr Ben Gilad, stated: "If more companies took care to thoroughly train their managers and executives in how to produce and how to use intelligence in all levels of the organization, fiascos such as those at HP … would be much less likely to occur" (10). It's a good point and for that reason we more comprehensively cover the laws and regulations which regulate intelligence gathering activities in chapters 3, 4 and 5 of this book.

Pitfalls of competitive intelligence

Despite a huge amount of media and political anxiety around functions associated with intelligence gathering within the security sector, the fact remains that research, monitoring and evaluations of the competitive environment are routinely carried out by all types of organisations, including by the very same newspapers and politicians who may sometimes stoke up political firestorms related to intelligence-topic controversies! If this is the case, it is often under the guise of more benign terminology. Job titles, such as research assistant, or analyst, often do indicate some form of business intelligence role. Nevertheless, the iron-rule is to conduct research and analysis of competitors in a fair and lawful manner. Moreover, you may wish to ask a stack load of questions before accepting or seeking to fulfil an intelligence-related contract. For example, if a client is seeking to buy in CI services, their motivations may be vague: because how do they know what they really need to know? Seek to develop clarity around the task, or project, before you set off launching various lines of inquiry, or commissioning endless

investigative reports. Moreover, can external security practitioners really step into other corporate environments and cultures, and credibly tell them what their risk exposure is? Be confident that you and your team can deliver. Before accepting a contract, consider other questions that might also need to be answered. Such as, to what extent is the client's executive team behind this initiative? Or are you being recruited to serve a more personalised or discreet agenda? If so, why? For those individuals and companies undertaking competitive intelligence functions, *The Society of Strategic and Competitive Intelligence Professionals* exists to help you tackle such challenging questions (11).

1.3 Linking business intelligence to our operating environment

Each organisation is different, with a unique culture, mix of employees and a unique combination of incoming events which undoubtedly impact it. Therefore, it may well be that many organisations establish their own ways to read, anticipate and map-out their own operating environments. Management tools which help us to draw a map of our business environment are as critically important to the lives of private companies as navigation charts are to the survival of sailors. It is therefore worth familiarising ourselves with some widely familiar business-environment analysis models. If deployed correctly, these management tools can hugely assist enterprises to harness control of resources and target operations to optimum effect.

Three business management models: PESTLE, Porter's Five Forces and SWOT

A widely favoured business tool is for business researchers and analysts to work to the PESTLE (Political, Economic, Sociological, Technological, Legal and Environmental) model to evaluate important external and internal forces that can impact an organisation. On the positive side PESTLE can provide structured information that can then be exploited by a company, because it has a coherent list of forces at work in its own operating environment. PESTLE, and other variations to this famous mnemonic out there, really does help business planners to dig under the skin of an operating environment. PESTLE challenges organisational autopilot and collective comfort zones. Like all of these business analysis tools that we're looking at in this chapter, PESTLE provides for a crucial episode of corporate *reflective learning*. This management tool also nurtures a sense of belonging and corporate purpose, to all executives who play their part in devising the PESTLE.

Professor Michael Porter's *Five Forces Model* helps companies to summarise the five competitive forces that provide a risk, or opportunities for them, within an industrial sector (12). These can literally be identified and listed under the following categories, Porter suggests:

- Threat of new entrants
- Threat of substitute products or services
- Bargaining power of buyers
- Bargaining power of suppliers
- Competitive rivalry between companies.

However, it might be that a company chooses to look more internally at the Strengths, Weaknesses, Threats and Opportunities (SWOT): the team, product and brand that it has at its disposal to take on the world. SWOT analysis, credited to management academic, Albert Humphrey, has been a very popular management tool deployed for several decades. This model enables teams, and companies, to articulate and address some weaker points in a positive and transformational manner … rather than allocating individual blame to individuals or departments. This is because SWOT analysis tends to be collectivist and can be concluded by focusing on the more positive organisational elements (strengths and opportunities) towards the end of the exercise. This modus operandi should leave the team forum satisfied and reassured, if not entirely exhilarated.

The three management models above can all be considered effective and well-known corporate business tools to provide intelligence-led decision making. If you get five or ten minutes to address a C-suite (senior executive board) officer, give consideration to deploying some, or all of these, in a presentable and engaging manner to your target audience. Moreover, do bear in mind that bad news is best delivered in a sandwich of diplomacy and provisos.

1.4 Examining appropriate intellectual property rights (IPR) in order to protect business ideas and enterprise

As you set about establishing your enterprise, knowledge about how to best protect your expanding corporate intellectual property becomes critical. For security practitioners, familiarity and professionalism in this field is additionally important from a reputational point of view because potential clients and industry peers will expect your company to possess proficiency in this sphere. Information asset protection is a fast-growing business-line, as we shall see later

(during the Information and Cyber Security pages of Chapter 5). Therefore, developing advanced capability and expertise in this important sphere may well help you to win new clients, and also expand revenue streams from existing buyers.

Common types of intellectual property rights include: copyright, industrial design rights, patents, trademarks, trade dress, and in some jurisdictions, trade secrets. Common definitions can be found within each country's designated supervising agency. For example, in the United Kingdom, the UK Intellectual Property Office (IPO) is responsible for supporting and advising businesses in this area. All emerging security companies, and those responsible for intellectual property protections, would do well to familiarise themselves with baseline definitions and frameworks helpfully provided by the IPO, or any corresponding agencies in your country of operation (13).

Definitions, laws, protocols and rules can also be made or agreed by supranational organisations, such as the European Union (EU). The UN's World Intellectual Property Organisation (WIPO) based in Geneva is vested with overall global authority and responsibility for issuing guidance and resolving disputes (14). Issues and resolutions can also often be handled by delicate and detailed state-to-state negotiations ('bilaterals') or multinational forums, such as the G8 and G20 groupings on major national and emerging economies (15).

Patents: A patent grants an inventor exclusive rights to make, use, sell and import an invention for a limited period of time, in exchange for the public disclosure of the invention. An invention is a solution to a specific technological problem which may be a product or a process (16).

Copyright: A copyright gives the creator of the original work the exclusive rights to it, usually for a limited time. Copyright may apply to a wide range of creative, intellectual, or artistic forms, or works. Copyright does not cover ideas and information themselves, only the form, or manner, in which they are expressed (17).

Industrial design rights: An industrial design consists of the creation of a shape, configuration or composition of pattern or colour, or combinations thereof, in three dimensional form, containing aesthetic – and thus significant commercial – value. An industrial design can be a two- or three-dimensional pattern used to produce a product, industrial commodity or handicraft (18).

Trademarks: According to the United States Trademark and Patent Office (USTPO): "A trademark is a word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods of one party from those of others" (19).

Trade dress: is “a legal term of art that generally refers to characteristics of the visual appearance of a product or its packaging (or even the design of a building) that signify the source of the product to consumers”, explains the University of Princeton website (20).

Trade secrets: according to USTPO, a trade secret is “a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known or reasonably ascertainable, by which a business can obtain an economic advantage over competitors or customers (21)”. In the US, trade secret law is primarily handled at the state level under the Uniform Trade Secrets Act, which most states have adopted, and a federal law, and the Economic Espionage Act 1996, which makes the theft or misappropriation of a trade secret a Federal crime.

IP: International governance and protocols

Patents and trademarks are territorial and must be filed in each country where protection is sought. Since the rights granted by any country’s patent office, such as the USPTO in America, extend only throughout the territory of that sovereign territory (or state in some cases), and have no effect in a foreign country, an inventor who wishes patent protection in other countries must apply to the relevant nation state or regional patent offices. Almost every country has its own patent laws. A full list of national authorities responsible for IP is published by the World Intellectual Property Organisation. Specific guidance has been produced for small and medium-sized companies (SMEs) and some of this advice is amplified by interviews carried out with smaller scale security companies by the author in the next section (22).

USPTO usefully provides *toolkits* for IP-related issues as they pertain to specific countries. This provides a mix of general and location-specific guidance and findings including white papers from interest groups, such as the *American Chinese Chamber of Commerce*. A link to USPTO’s advice is provided in the end-chapter references list (23).

Difficulties with managing IP for start-ups and partnerships

Intellectual property cases are usually complex, ambiguous and resource-heavy for companies that seek recourse in this area. Public authorities and non-profit organisations in some countries offer mediation services, in order to help resolve issues between organisations and avert them from escalating into costly and very public legal battles. Modern, highly mobilised work patterns can complicate

governance and parameters around intellectual property. Employees with expertise and sought-after skills, particularly those at a senior level, often move between new employers or different geographic markets with alacrity. Moreover, directors and executive-level staff or contractors with access to sensitive operational details, can often be employed, or retained, by several different organisations; possibly companies with a conflict of interest.

These are just some of the challenges to sensibly retaining critical information within key groups of collaborators and enterprises. But add in to the mix 'real-time' digital communications, international business collaborations, increased expectations of product scrutiny (at exhibitions, etc.), then intellectual property protection becomes an almost fanciful concept. Trade shows and exhibitions, technology magazines, journals and digital information, and self-publication, have all extensively proliferated in modern times. Dominant trade publications and journals now expect access to all products and employees!

Moreover, sometimes there are cultural barriers which can scupper plans to protect information or designs during business trips. Some cultures tend to reject that knowledge and research should be privately owned. Development and progress is seen as a fraternal human obligation. Lessons for security contractors, which arose from several first-hand experiences of IP fragmentation, do raise the issue of teamwork and trust: "transparency among one another, and an awareness of the value of our information to everybody else, is vital", reports Rob Scott, a UK-based security contractor (24). Tips from a range of security contractors include:

- Be clear from the outset; what information are you providing to the company? Also, be clear in your own mind, what will you retain copyright over?
- Be proactive in registering intellectual property with national authorities. Despite media horror stories, they can actually be helpful and informative.
- Perception is reality. Entrepreneurs sometimes start out in teams or alliances of individuals coming together to fill a market gap. You may all be juggling a variety of commercial interests. Therefore, if you have a perceived *conflict of interest* in the eyes of your team members (remember, you might not think so, but we are talking about *perception*), then be really clear from the outset about your commercial aims and interests. Full disclosure is always better than falling out.

Counterfeiting and piracy

> *"Counterfeiting is the ultimate technology for people who want to get something for nothing."* – (Financial writer, Marshall Brain, '*How Counterfeiting Works*')

The Organisation for Economic Co-operation and Development (OECD) estimated that up to $200bn (US) of world trade is made up of counterfeit goods. OECD statisticians admit that this figure is magnified to "several hundred billion dollars or more" because they were unable to calculate "domestically produced and consumed" so-called 'knock-off goods'. The OECD is just one high-profile organisation urging national governments and industry sectors to share information in relation to useful anti-counterfeiting strategies, and busily issues various missives upon domestic police agencies and prosecutors to "enhance enforcement" (25).

Counterfeiting and *piracy* are terms used to describe a range of illicit activities at the core of IP infringement. The impact upon business communities has become so severe that the World Trade Organisation (WTO) enshrined provisions relating to fair play and honest business practices when it was established by the Marrakesh Agreement (1994). Provisions within the *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS) do form a continuous workstream for some of the WTO's 600 staff in Geneva, Switzerland (26). This body, which has the unenviable task of liberalising trade barriers, replaced the well-known 1948 General Agreement on Tariffs and Trade (GATT). TRIPS brought in provisions of expected standards and dispute resolution procedures. This body attempts to provide global governance, controls and policy direction around: trademarks, copyrights, patents and design rights, as well as a number of related entitlements.

Business impact of IP breaches

Counterfeiting and piracy are longstanding problems which are growing in scope and magnitude, argues the OECD and many likeminded organisations. They are of concern to both government and industrial sectors because of the profound damage that information theft can bring into societal and industrial levels of innovation. Moreover, many IP breaches pose a clear and present danger to the welfare of consumers, such as poor or fake medical products and equipment. Counterfeiting and piracy activity does tend to channel substantial cash and functional resources that can be used by criminal networks and organised crime groups, that profoundly corrode the normal functioning of everyday civilian life, argues the OECD.

Furthermore, companies are also badly disadvantaged by knock-off products and unlicensed goods or operators that can undercut existing, lawful, business enterprises. Moreover, the incentive for companies to invest in their own research and development is massively undermined if they are unable to enjoy the benefits of such effort and expense.

Business and law enforcement responses

Despite international protocols and emerging agreements between international organisations and states, legal recourse against counterfeiting and piracy is usually addressed within the country where suspected offences are committed. Nevertheless, some domestic police forces, such as the UK's City of London Police, and the US's Federal Bureau of Investigation (FBI) are chasing down British and American-based persons and companies involved in large-scale IP criminal activity (27). Action Fraud is the UK's National Fraud Reporting Centre (NFRC). The service is run by the new National Fraud Authority, the "government agency that helps co-ordinate the fight against fraud in the UK" (28). In terms of gathering information, the NFRC is part-supported by the City of London Police's National Fraud Intelligence Bureau. Suspected counterfeiting, and other frauds, can be reported into Action Fraud.

Under the clever strapline *'Fake costs more, I'll buy real'*, the International Chamber of Commerce (ICC) launched an impressive research and publications programme, in order to identify and offer solutions in response to counterfeiting activity. Several years on, the ICC-run *Business Action to Stop Counterfeiting and Piracy program* continues to keep business communities well briefed in relation to areas of IP risk. The ICC also provides a toolkit for public authorities, such as policy-makers, police and prosecutors, to strengthen proceeds of crime legislation (29). Should you wish to develop your knowledge in this area, the following report is recommended: *Controlling the Zone: Balancing facilitation and control to combat illicit trade in the world's free trade zones*, produced by the ICC (2013), listed in the references section below (30).

1.5 Emerging markets

> *"The twenty first century may well be the time when the balance of power shifts to Brazil, Russia, India and China, nations collectively referred to as BRICs. These nations constitute the shape of the future, giving rise to a new world economy."* – William C Hunter, Dean of University of Connecticut Business School (31)

The concept of new *emerging markets* (EMs) does generate much excitement among entrepreneurs. This optimism has been compounded by the global economic downturn from 2007, which has subsequently remained resilient across most of the established, so-called, advanced industrial economies (AIEs). Cost-cutting, which has driven lots more innovation, ICT dependency and efficiency, has occurred across almost all commercial and public sector domains since. So, what is it that is actually driving forward globalisation and an enthusiasm for emerging markets?

- The rapid growth of *middle income* purchasing power for non-essential goods in emerging economies (including Brazil, Russia, India, China … commonly now known as *BRIC* markets). The products include domestic appliances, cars, computers and smartphones. For example, analysts at the *Economist Intelligence Unit* report that by 2020 China will be a larger domestic automotive market than America, and Russia will topple Germany as Europe's biggest car market (32).
- The rapid spread of interactive ICT (Web 2.0) due to accessibility of digital and social media and ecommerce platforms. There is also now instant access to information sources for market and competitor intelligence.
- The untapped markets still to come: at the time of writing, India had 250 million internet users, and ecommerce penetration was relatively low compared to developed markets, such as the UK, where 19 out of 20 citizens now buy online (33). This type and profile of untapped market is hugely exciting to entrepreneurs, who may well reflect upon Ferdinand Porsche's splendid motivational quote: "We build cars that nobody needs but everybody wants to have."
- A rapid 'catch up' of productivity levels in emerging economies to close the 'productivity gap' in comparison to established AIEs.
- Expansion of international and supranational organisations, such as the G8, IMF and World Bank, which marshal trade liberalisation and development strategies within some emerging markets.
- An 'infrastructure boom' led by the BRIC quartet, with India predicted to implement a one trillion dollar investment in national infrastructure between 2013-17 (34).
- The rise of 'city economies'. According to eminent global management consultants' company, McKinsey, the gross domestic product (GDP) of global cities will surge by $30 trillion during the period between 2010 and 2025. Some 47% will be generated in 440 'emerging market centres'; most of these are to be found in Asia, Africa and Latin America, say McKinsey's researchers (35).

What is an emerging market?

In 1981, World Bank economist, Antoine W Agtmael, coined the phrase 'emerging market economy'. Although parameters around a definition are widely set, Agtmael's thoughts did include reference to, "an economy with low to medium per capita income" (36). Emerging markets are transitional. They are usually perceived to be on the move, from a closed (controlled) economy, surrounded by barriers to entry, towards participation into international markets. Some common features of emerging markets can be expected. In order to achieve greater accessibility and international leverage, leaders in potentially successful emerging markets will often seek to introduce reforms to business and taxation policies, such as promoting fiscal transparency, uniform levels of legal compliance, and also the removal of barriers, such as anti-foreign property laws, as well as the privatisation (sale) of many state-owned enterprises. Such a process will usually displace some of the economic and political *ancien regime*. Thus, do not be tempted to 'put all your eggs in one basket'. Ongoing power struggles and regular changes of influential personnel are hardly uncommon in emerging markets. Some countries have also been able to 'emerge' and flourish due to a decline in armed conflict; for instance, Indonesia and Colombia are fast becoming tigers in Pacific Asia and Latin America respectively.

Where are these 'emerging markets'?

Since Agtmael's definition became broadly accepted, the world's most successful emerging economies were spread quite evenly around the globe. Six of the top 20 markets (also four of the top six) were located in East Asia, as identified by business monitoring organisation, Bloomberg. These being: China (first), South Korea (second), Thailand (third) and Malaysia (sixth) (37). Headline hype around the vitality of certain emerging economies does need to be further examined by potential investors and visitors alike. Seldom do headlines and selected data used by news organisations actually relate back an accurate and actionable picture. For instance, many economists do predict that the impact of the 2007/8 global economic crash upon emerging markets may well have been initially slower, and far less visible, than was the case in advanced industrial economies (AIE), such as the US, UK and Germany. These aftershocks have continued well into the following decade because quantitative easing programmes only came to closure five years later. Hence, emerging markets are not always the commercial 'promised land'. Another concern is that productivity in AIEs has continued to stagnate or fall, almost a decade after the economic crash. To some extent, the fate of emerging markets is intertwined because stagnation of major economic powers will also continue to take orders out of the supply chain in many emerging

economies, including Russia, East Europe and Latin America (6). Other age-old economic problems persist in emerging market zones, caused by serious political or military instability, the rise and fall of oil prices, and significant natural disasters. Thus a neutral and open-minded application of sensible business intelligence analysis techniques, such as PESTLE and SWOT, is strongly advised before the establishment security functions and consultancies in emerging markets.

Economic aid

Efforts to open up economies to international trade and to carry out market liberalisation reforms, will often attract international development aid from supportive national states, the IMF and the World Bank. Moreover, in 1970, the United Nations passed Resolution 2626 which stipulated that advanced industrial societies should each contribute at least the equivalent of 0.7% of their GDP directly to international development assistance (38). Development efforts and aid were consolidated by an agreement at the UN of eight millennium development goals (MDG). These MDGs are due for revision in 2015, possibly expanding the range of contributing countries and nature of their contributions. This could expand or reduce investment by aid organisations or government initiatives that directly invest in security management functions related to aid and humanitarian assistance projects.

Networks, such as the European Interagency Security Forum (EISF), ensure that security managers working for NGOs are able to share good practice, mutual aid and educational support between one another, and across many complex and fragile overseas environments, including many officially designated emerging markets (39). According to Lisa Reilly, chairperson of EISF, there are several attributes that will give some security practitioners an advantage over competitors. Reilly stated: “Consultants need to really understand the ethos and mandate of the organisations they wish to work for. Just using the term ‘humanitarian’ does not mean that training or services to be provided are appropriate in content or approach, and practitioners who do not understand this can cause more security risks than they resolve” (40).

Further information about emerging markets

The website *Emerging Markets: News, Analysis and Opinion (www.emergingmarkets.org)* is an increasingly important hub for financial and political information, even running awards ceremonies for economists and bankers in emerging zones, and employing Nobel Prize winning economists,

such as Joseph Stiglitz, as columnists (41). *Forbes Magazine* in the US and London's *Financial Times* (FT) provide upbeat, strategic market information that can be critically examined and corroborated via further in-country reports. Industry forums, such as the Chambers of Commerce and their in-country websites, are often excellent hubs for advice and further decent business contacts. Forbes' does estimate that emerging economies will experience financial growth at some two to three times the pace of AIEs (42). Of the old guard, only Japan and the US are likely to remain as the world's top six largest economies, with India, Russia and Brazil due to usurp Germany, France and Britain in the financial 'pecking order'. According to Forbes' analysis: "… another benefit for investors is the diversification that the EM's provide, because they tend to perform differently than developed markets, and have been successful at decoupling from the greater, longer term woes of the mature economies of the West" (43).

The largest four emerging markets – Brazil, Russia, India and China – were coined as 'BRIC' economies by international investment bank, Goldman Sachs, in a seminal published report in 2001 (44). Another global investment bank, Morgan Stanley, has also reported on the emerging markets and has developed criteria to classify economies based around accessibility, size and liquidity. Morgan Stanley began this now well-known index back in 1988, when only ten economies satisfied their strict economic development criteria; now some 23 cross the threshold of investor opportunity. These are:

Latin America: Brazil; Chile; Mexico; Colombia; Peru

Europe, Middle East and Africa: Czech Republic; Egypt; Greece; Hungary; Poland; Qatar; Russia; South Africa; Turkey; United Arab Emirates

Asia: China; India; Indonesia; Korea; Malaysia; Philippines; Taiwan; Thailand

Source: Morgan Stanley, Emerging Market Index 2014 (45)

Figure 1: Morgan Stanley's emerging market index

Risks of emerging markets

Emerging markets generally do not have the level of market efficiency and strict standards in accounting and securities regulation to be on par with advanced industrialised economies. But emerging markets will typically have developing financial infrastructure including banks, a stock exchange and one unified currency.

Emerging markets can offer decent potential returns for security companies, not just by way of protective security contracts. Often lacking in stability and

political certainty, inward investors do turn to physical security providers for employee safety reassurance and, possibly, also to achieve some form of 'force projection' that may act as a deterrent to potential adversaries. Security risk management companies that routinely deploy threat and risk assessment services, as core business for their clients, will also therefore correspondingly develop a very rich knowledge-bank of refined information about the in-country operating environment. The sourcing of local, dependable chaperones, translators, business network organisations, and also the processes of carrying out various reconnaissance and site surveys, does mean that security risk management can diversify beyond protective roles and into business enabling services, such as by launching business and market intelligence and analysis products (either as a value-added service or specifically intended separate revenue stream.)

Understanding what an 'emerging economy' actually is can be most helpful to a security department. Further research and clarity about the specific operating environment that is being targeted is essential; because sometimes a raft of credible assertions that a market is 'emerging' (often backed up by enthusiastic newspaper articles, government promotions and the march of semi-adventurous tourists) can sometimes lead to a disproportionately optimistic news narrative. Such positive terminology may encourage investors to walk blind-sided with their employees into a new market, and assume – quite incorrectly – that risk levels have reduced. Security practitioners should therefore be aware that emerging economies are still very much high-risk political/economic pendulums that can quickly and violently swing backwards, instead of forwards. Clients will undoubtedly expect their security teams to demonstrate strong, forward-thinking awareness around opportunities and threats in less stable markets. Moreover, it should be the case that at times of uncertainty and change, well-prepared security practitioners will actually be in their commercial and personal element.

Traditional markets: the brave old world

Before we close this section, it is worth reminding ourselves that more traditional, established domestic security markets still offer plenty of opportunity. ASIS and the Institute of Financial Management (IOFM) reported in a 2012 report (that interviewed some 400 security industry executives) that the US security market *alone* was worth $350 billion (around £220 billion) (46).

Key findings of the report include:

- $350 billion market breaks down into some $282 billion in private sector spending and $69 billion of federal government spending on homeland security.
- Operational (non-IT) private security spending is estimated to be $202 billion, with expected growth of 5.5% in 2013; IT-related private security market is estimated at $80 billion, with growth of 9% projected for 2013.
- Number of full-time security workers is estimated to be between 1.9 and 2.1 million.
- 42% of respondents indicated spending on training would increase in 2013, with 12% anticipating a rise of 10% or more.
- The private investigator is one of the fastest growing occupations; with anticipated growth of 21% projected through 2020; several IT positions are anticipated to grow 22% through 2020.

1.6 Targeting consumer markets and marketing

> *"Market intelligence is a must-have tool for all security directors planning their departmental and personnel budgets and resource needs, as well as for industry suppliers planning their marketing and product growth."* – RD Whitney, Executive Director at Institute of Financial Management (47)

Entrepreneurs usually start companies to solve problems. They believe that something necessary is missing from the market and that they provide the unique approach to fix the marketplace. Hopefully, during the initial period of establishing a business, there is clarity of vision and a sense of common purpose. The business has a clear understanding of its competitors, its finances, its goals, and the direction of its own market position. Most successful entrepreneurs write down and communicate their business plan and strategy. Nevertheless, a feature of a successful business start-up, is that it swiftly generates pace and momentum of its own. Hundreds or thousands of decisions must be made, equipment purchased, problems solved, etc. This activity curve is both an immensely rewarding window of opportunity for entrepreneurs, but also a period of substantial risk. A new, uncontrolled project is always at some risk from hurtling off the rails. The power and the velocity of an enterprise that gathers momentum can sometime surprise its founders. The brand may gather a level of momentum and generate a scale of interest that surpasses existing competences and capacity. Or an unexpected revenue stream may come in, which can move the entrepreneur some distance away from their company's original vision. Control and co-ordination of market navigation is

critical. Nowhere is this more important than in the sphere of developing a marketing strategy.

The 'marketing mix': the four Ps

Marketing is defined by the *Chartered Institute of Marketing* as the process "responsible for identifying, anticipating and satisfying consumers' requirements profitably" (48). The business leadership company, *Mindtools*, identify marketing as: "putting the right product in the right place, at the right price, at the right time" (49).

A dominant formula within the marketing industry that aims to help enterprises understand their commercial strategy, product development and positioning is known as the *marketing mix*. The mix demands that companies carry out structured analysis around their own products, prices, places and promotions – the four Ps. The marketing mix for every business will be different.

When marketing, companies need to create a successful mix of:

- The right product
- Sold at the right price
- In the right place
- Using the most suitable promotion (50).

Source: Business Case Studies website www.businesscasestudies.co.uk

Figure 2: The marketing mix

To create the right marketing mix, businesses have to meet the following conditions:

- **Product:** must have the right features to address market need. For example, it must look good and work well.
- **Price:** the price must be right and build in profit (unless it's a deliberate promotional loss leader). Discounts and margins must be accurately calculated.
- **Place:** the goods must be in the right place at the right time. Ensure on-time storage, delivery and accuracy. Develop channels.

- **Promotion:** the target group needs to be made aware of the existence and availability of the product through promotion.

The *Business Case Studies* website gives some excellent case studies of how the 4Ps formula works within some exciting global enterprises including: Manchester United, supermarket Aldi, Red Bull Formula 1 racing team and the National Trust, a British charity. Integrating the elements, business processes, marketing, sales, finance, compliance, communications, security, and so on, will contribute to more powerful and relevant marketing. Marketing departments, like any other busy office functions, can be prone to slipping into silos. But how on earth can marketing be successful if marketing professionals don't know the nuts and bolts, and strengths and weaknesses, of other business functions? This quandary for marketing professionals, who are often cajoled by boardrooms to 'get to know the business better', is not dissimilar to some complaints levelled against security functions! Thus, here exists an opportunity for security entrepreneurs and managers; explore together what functions are mutually supportive. You may find that synergies exist, such as around sharing business and market intelligence information, providing safety and security bulletins and workshops, or working together to invest and develop the company in exciting new emerging markets.

Much underestimated by some security professionals, marketing and sales strategy is the engine that propels forward any company in any sector. Carefully considered planning, coupled with accurate market analysis, will invariably determine just how successful your company and collaborations become. "Focus on the core problem your business solves and put out lots of content and enthusiasm and ideas about how to solve that problem", is a piece of great advice from Laura Fitton, founder of *oneforty.com* (51). Moreover, beware of launching 'loss leaders'; free or low-cost products or product samples. They can exhaust and bankrupt you as the following case study demonstrates:

Case Study: Free holiday offer cleans out Hoover

The UK company, Hoover, ended up paying out £50m in legal bills including compensation, and being sold off to an Italian competitor, after devising a ruinous marketing campaign that offered customers free flights to Europe (later extended to America), if they bought products worth a minimum of £100. Between 1992 and 1993 a trickle of customers claimed the flights. But soon demand became an avalanche, as this wonderful news spread. Customers could literally fulfil their travel dreams merely by buying an expensive but useful domestic appliance. The marketing tag-line for Hoover was: 'Two Return Seats – Unbelievable'.

It soon was. Hoover quickly appeared to renege on its deal by cancelling the offer to existing customers. The *Hoover Holiday Pressure Group* was formed by one customer, Harry Crichy. Such was the outrage of customers that a Hoover engineer was kidnapped on a call-out after reportedly telling his customer: "If you think buying a washing machine's going to get you two tickets to America, you must be an idiot" (52).

The pressure group estimated that it had 8,000 members at its peak. Questions were asked by MPs in Parliament. Hoover ended up being forced to provide some 220,000 free flights after losing prolonged legal actions by customers which lasted six years in some cases. Hoover's UK division was sold to Italian manufacturer, Candy. The managing director of Hoover Limited and president of Hoover Europe, and the two directors most closely involved with the promotion – the Hoover vice-president of marketing, and the director of marketing services – were dismissed by Hoover. By 1998, the company had paid out £50 million in legal bills.

1.7 Business funding

The success of winning investment involves entrepreneurs 'stepping into the shoes' of potential investors; what will encourage them about your company and vision? Conversely, what avoidable factors may dissuade an investment group away from your enterprise? It is worth accepting from the outset that – as in a job interview – applying for funding and then accepting a potential investor is a mutual, two-way, process. A poor investor match, based on poor information sharing, or divergent business philosophies, can sink an enterprise faster than an unexpected torpedo attack.

Moreover, if your capital investment is endogenous (perhaps derived from your own hard-earned savings), then it is essential for you to apply the same cost-benefit assessment models that others might apply to a decision about whether to invest in you. Imposing strict cost controls and carrying out regular cost benefit and profit and loss monitoring from the outset, will install a habit and, then, a culture of self-discipline and accountability. Further down the line, the benefits of cost control and prudence will be magnified, because it might mean that –

thanks to your prudence – you will not be forced to release so much equity in the company, or sign up to unfavourable business finance terms, when it comes to the point that you might need to access extra funding. Being able to choose and carefully select an appropriate investor into your business, can be one of the most exciting and optimistic times for entrepreneurs who wish to expand and drive their business into its next development phase.

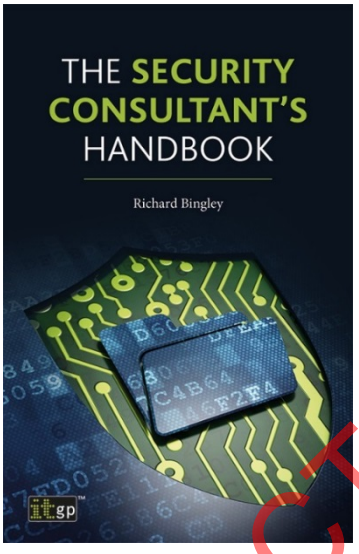
Demonstrating to your potential investor your competences and vision for the target marketplace is essential in unlocking investment for any business. But security companies in hazardous environments, or perceived to operate in risky environments, will need to provide extra reassurance to investors as to the legality, security and resilience of their own business. Investors will often look at the security market with a mix of trepidation and excitement around the return on investment (ROI).

As security practitioners, our skills and experience in delivering contingency planning and business continuity strategies for clients, are hopefully second-to-none. But we sometimes take these capabilities for granted. Potential investors, especially those with non-security career backgrounds, are likely to be far more welcoming if security companies demonstrate their own in-house business resilience strategies within any business plan and pitch that is supplied to the investor.

A clear sense of where liabilities and responsibilities exist is absolutely essential in collaborations and joint venture (JV) operations. The report of investigation by Statoil, one of three JV parties who owned the In Amenas oil plant in Algeria at the time of the 2013 terrorist attack, demonstrates just how complex and exhausting the security and legal arrangements of JVs can be in relation to claims for loss and damages (53).

<<< END OF EXTRACT >>>

The Security Consultant's Handbook



- Essential direction for ambitious professionals who want to succeed in security
- A wealth of knowledge for the modern security practitioner
- Featuring case studies, checklists and helpful chapter summaries, *The Security Consultant's Handbook* aims to be a practical and enabling guide for security officers and contractors

"The author has produced a most assured work; a book for our times; and one for the newcomer to security and anyone wanting to refresh themselves or get a grip on 2015 in general. A cracking book from a man who is giving the security industry a good name."

Mark Rowe

Buy your copy today

www.itgovernance.co.uk/shop/p-1726-the-security-consultants-handbook.aspx

www.itgovernanceusa.com/shop/p-1487-the-security-consultants-handbook.aspx

www.itgovernance.eu/p-1140-the-security-consultants-handbook.aspx