Corporate Security Intelligence and Strategic Decision Making

Justin Crump
CONTENTS

Foreword by David Burrill OBE  xiii
Introduction and Acknowledgments  xv
About the Author  xix

SECTION I  Rationale

1  What Is Corporate Security Intelligence?  3
   Chapter Objectives  3
   Introduction  3
   Intelligence Defined  4
   Introducing Decision Advantage  7
   The Corporate Security Environment  8
   The History of Corporate Intelligence  9
   A Typical Corporate Security Department  12
   Challenges to Effective Corporate Security  14
   Overcoming These Challenges: The “Business of Resilience”  15
   The Role of Intelligence in Enterprise Risk Management  18
   Conclusion: Toward Truly Intelligent Security and Businesses?  22

2  The Corporate Security Operating Environment  23
   Chapter Objectives  23
   Introduction  24
   Geopolitical Risk  24
      Unknown Unknowns  26
   Terrorism  28
   Cyber Issues  36
      State-Level Threats  38
      Cyber Crime  38
      Cyber Activism  39
      A New Paradigm  39
   Conventional Espionage and the “Insider Threat”  40
## CONTENTS

Single-Issue Activism and Political Violence 42
   The Move toward All Liberation Struggles Being “As One” 43
   Secondary Targeting of Customers, Suppliers, and Shareholders 44
   Internationalization of Single-Issue Campaigns 44
   Political Extremism 45
   Use of Social Media in Single-Issue Protest and Political Activism 46

Organized Crime 46
   The Wide Reach of Serious Organized Crime 47
   Threats to Corporate Security 48
Emerging Threats—What’s Next? 49
Conclusion: A Complex and Multifaceted World 52

### 3 Legal Drivers for Corporate Security Intelligence 53

Chapter Objectives 53
Introduction 53
   Protecting the Heath, Safety, and Security of Employees:
   An Employer’s Duty of Care 55
   Relevant Laws in the United States 56
   Relevant Laws in the United Kingdom 60
   Relevant Laws in the European Union 63
   Developing Causes of Action: Negligent Failure to Plan 63
   Duty of Care: Summary 64
Corporate Responsibility, Compliance, and Business Ethics Concerns 65
   United Kingdom Law: The UK Bribery Act 67
   Sanctions Regimes in the United States and United Kingdom 71
   Corruption, Compliance, and Sanctions—Summary 72
Conclusion: The Legal Imperative 72

### 4 Operational Drivers for Corporate Security Intelligence 75

Chapter Objectives 75
Introduction 75
General Corporate Security Intelligence Operating Framework 77
Risk-Management Standards 79
How Corporate Security Intelligence Saves Money 80
How Corporate Security Intelligence Makes Money 82
Conclusion: Intelligence and the Four Ps 84
SECTION II  Theory

5 The Fundamentals of Intelligence  89  
Chapter Objectives  89 
Introduction  89 
The Information Hierarchy  90 
The Intelligence Cycle  92 
  Criticism of the Intelligence Cycle  96 
  A Suggested Model for the Corporate Security Intelligence Cycle  97 
Principles of Intelligence: CROSSCAT  99 
Dramatis Persona: Roles and Responsibilities  101 
  Intelligence Manager  101 
  Collectors  102 
  Collators  103 
  Analysts  103 
  Administrators  103 
  Consumers  104 
Types of Intelligence  105 
The Systems Approach  106 
Predicting, Forecasting, and Probability  107 
Conclusion: All Parts in a Harmonious Whole  108 

6 Management and Direction  111  
Chapter Objectives  111 
Introduction  111 
Intelligence Requirements and Product Definition  113 
Managing People and Processes  116 
Managing Clients and Promoting the Role of Intelligence in the Business  123 
Knowledge Management  124 
Conclusion: An Essential Juggling Act  125 

7 Intelligence Collection  127  
Chapter Objectives  127 
Introduction  127 
Sources  128 
OSINT: The Open World  131 
  The Internet and Security: An Intelligence Perspective  132
## CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Social Media: Networks within a Network</td>
<td>134</td>
</tr>
<tr>
<td></td>
<td>News Media: A Similar Perspective</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>HUMINT: The Human Element</td>
<td>137</td>
</tr>
<tr>
<td></td>
<td>Company Sources</td>
<td>138</td>
</tr>
<tr>
<td></td>
<td>The Collection Management Process</td>
<td>139</td>
</tr>
<tr>
<td></td>
<td>Planning</td>
<td>139</td>
</tr>
<tr>
<td></td>
<td>Execution</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>Source Gathering Techniques: OSINT</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>Source Gathering Techniques: HUMINT</td>
<td>142</td>
</tr>
<tr>
<td></td>
<td>Source Gathering Techniques: Company</td>
<td>144</td>
</tr>
<tr>
<td></td>
<td>Information Archiving</td>
<td>144</td>
</tr>
<tr>
<td></td>
<td>Verification</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td>The Review Process</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td>Conclusion: Better Equipped than Ever?</td>
<td>147</td>
</tr>
<tr>
<td></td>
<td><strong>8 Collation</strong></td>
<td>149</td>
</tr>
<tr>
<td></td>
<td>Chapter Objectives</td>
<td>149</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>149</td>
</tr>
<tr>
<td></td>
<td>Key Principles</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td>Structured versus Unstructured Data</td>
<td>152</td>
</tr>
<tr>
<td></td>
<td>Databases and Automated Collation</td>
<td>153</td>
</tr>
<tr>
<td></td>
<td>Big Data</td>
<td>155</td>
</tr>
<tr>
<td></td>
<td>GIS</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>Conclusion: Getting the Ducks in a Row</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td><strong>9 Analysis</strong></td>
<td>159</td>
</tr>
<tr>
<td></td>
<td>Chapter Objectives</td>
<td>159</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>159</td>
</tr>
<tr>
<td></td>
<td>Three Models of Corporate Intelligence Processing</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>Decomposing the Task</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>Assessing Sources</td>
<td>163</td>
</tr>
<tr>
<td></td>
<td>Collation</td>
<td>164</td>
</tr>
<tr>
<td></td>
<td>Intelligence Analysis in the Corporate Sector</td>
<td>165</td>
</tr>
<tr>
<td></td>
<td>The Role of the Analyst</td>
<td>165</td>
</tr>
<tr>
<td></td>
<td>Ensuring Credibility and Access</td>
<td>166</td>
</tr>
<tr>
<td></td>
<td>Analytical Techniques and Thought Processes</td>
<td>166</td>
</tr>
<tr>
<td></td>
<td>Analytical Fallacies and Psychological Traps</td>
<td>172</td>
</tr>
<tr>
<td></td>
<td>Avoiding the Pitfalls</td>
<td>177</td>
</tr>
<tr>
<td></td>
<td>Articulation and Testing of Assumptions</td>
<td>178</td>
</tr>
</tbody>
</table>
CONTENTS

Asserting Conclusions and Forecasting 180
Conclusion 181

10 Dissemination 183

Chapter Objectives 183
Introduction 183
Why Do We Disseminate Material? 184
Balancing Operational Security 185
Report Formats 188
Writing Guidance 188
Presentation Guidance 193
Quality Assurance 195
Showing Return on Investment 197
Conclusion 199

SECTION III Practice

11 Operational Models 203

Chapter Objectives 203
Introduction 203
A Corporate Solution: The Security Intelligence Decision Advantage Research Model (SiDeARM) 204
What Does SiDeARM Consist Of? 204
  Management 204
  Direction 206
  Collection 206
  Collation 207
  Analysis 208
  Dissemination 208
  Clients 209
  Other Factors 209
Countering Crime: The National Intelligence Model (NIM) 209
  NIM at a Glance 210
  NIM in Practice 211
  NIM Considered 212
Conclusion 214
CONTENTS

Travel Security 232
New Market Entry 236
Scenario Planning 240
Depth Due Diligence 244
  Screening 244
  Enhanced Due Diligence 245
  Investigative Due Diligence 246
Power Mapping 247
Country/Geopolitical Risk Analysis 249
Executive and Event Protection 252
Exercises and “Red-Teaming” 253
Crisis Support 254
Threat and Reputational Monitoring 255
Summary 255

14 Conclusion: Reinforcing Intelligent Security 257

References 259
  Case Law References 264
  Statute Law References 264

Index 267
CHAPTER OBJECTIVES

1. To discuss why it is useful to have a model of intelligence to help guide structures, processes, and the deployment of resources.
2. To introduce a simple security intelligence model, applicable to any scale of deployment.
3. To discuss aspects of a common dedicated countercrime model (the National Intelligence Model).

INTRODUCTION

Having talked through the reasons why we should (and, indeed, must) have corporate security intelligence and addressed the theory, it now seems only fair to help the reader work out how to put this into practice. The purpose of this chapter is therefore to talk through a couple of useful models that work in quite different ways. In reality, all operational models will differ, and this is all to the good, as the doctrine should be applied to the task rather than the other way around. However, they also all have common elements, and having a model provides a degree of assurance that everything is in fairly good shape and that nothing important has been forgotten.
A CORPORATE SOLUTION: THE SECURITY INTELLIGENCE DECISION ADVANTAGE RESEARCH MODEL (SIDEARM)

Remember the piece earlier in the book, where we talked about the need to hook people on occasion and be theatrical in order to get a point across? I freely admit that the name of this model reflects that imperative. Joking aside, SIDEARM is designed to be the convenient safety net to help any size organization seeking to implement intelligence in an effective and efficient fashion. Put simply, it incorporates all the theory we have discussed, and quite a bit of best practice, in order to present a template to follow. It does not mandate particular products, unlike the National Intelligence Model for policing (see discussion later in this chapter). Rather, it lays out a framework and approach within which cohesive intelligence outputs can be delivered.

SIDEARM, as an approach, can be embedded in any intelligence team. Even one person for whom intelligence consumes just a fraction of their time can make use of it. In effect, it helps ensure that what is being produced is intelligence rather than just information, and it does so by bringing in a structured and disciplined approach.

WHAT DOES SIDEARM CONSIST OF?

SIDEARM closely echoes the modified version of the intelligence cycle introduced in Chapter 5, the “hub and axle” or “engine and driveshaft” model. It is therefore broken down under the various functions within the cycle. Again, even just one person can do all of these, especially if they are using the model as a guide to help them remember which “hat” they should be wearing at which time! The SIDEARM model is shown in Figure 11.1. The key point of the model is the structural and architectural aspects it suggests. It’s easiest to understand this by briefly looking at each stage in the cycle. (Note that templates for each of the supporting functions mentioned are available on the website accompanying this book.)

Management

Three are four important things to consider under the Management heading. These are:

- *Mission and vision statement:* It is important to define what, exactly, the function is meant to be doing. This helps to set the tone and
keeps all involved (including external stakeholders) focused on what is trying to be achieved.

- **Resource matrix**: This can vary, but the aim is to have clarity on what resources are available at what time, and what intelligence requirements (IRs) they are allocated to. This is usually kept as a spreadsheet by the manager, although if you have access to SharePoint, a combination of tasks and a calendar are also useful for keeping track.

- **SOPs and policies**: The exact number of these will vary; where possible, corporate policies should be distilled for relevant points or otherwise leveraged. Often, effort here revolves around understanding what exactly corporate policies dictate and then communicating these (some people refer to this as the “BS filter”). The minimum required is probably operations security (OPSEC), research guidance, process diagrams, and writing standardization
guidance. However, it is good to check against the list provided earlier in the book for an exhaustive assessment of what may be included!

- **Lessons learned and blue-sky process**: These are strictly different things, but they are to some extent related as management functions. Blue sky challenges the current assumptions and is often overlooked, since it is a “nice to have” function. However, it is very important in terms of countering those pesky high-impact/low-probability events. Meanwhile, lessons learned are more related to dissecting and analyzing failures (part and parcel of intelligence work). Both together are however about boosting long-term effectiveness and are integral to a healthy system.

**Direction**

Direction is both the start and end point of the intelligence cycle (if a cycle really has as such, which some would argue it doesn't). There are two main things to consider when looking at direction:

- **Intelligence requirements register**: We have discussed at length how these are the things that energize the process. It is all too easy to let these slide. SIDeARM mandates that a register of intelligence requirements be kept. This is assigned against the resource matrix and collection plan in order to ensure that tasks are managed coherently.

- **Feedback process**: It is vital to collect feedback from clients, and there must be a formalized process for doing so. Again, there is no mandated standard for these; rather, the process must be given consideration, and adequate arrangements be made. This includes ensuring that the consequences of feedback are acted upon and communicated both to the team and the client from whom feedback was elicited.

**Collection**

The collection process similarly has two main enabling documents:

- **Source lists**: These are highly confidential if they refer to human sources, open-source lists less so. Source lists are highly dynamic and require active management, so SIDeARM recommends that they be reviewed as a matter of routine by the intelligence
manager. This prevents lists of dead links and ensures that new sources are being identified and added. Note that the resource plan may identify that there are gaps in sources that need to be filled. This should also be reflected in the source lists themselves, as a reminder/prompt to the collectors. For maximum effectiveness, though, this should clearly be issued to someone as a task.

- **Collection plan**: This brings the source list and IRs to life, allocating resources and sources to objectives. As this implies, there are tight linkages between the various documents that have been established to guide and shape activity. This is a critical document, and yet it is so often overlooked.

### Collation

The main aim of collation is to ensure that information can readily be accessed and connected as part of analysis. “Joining the dots” is a critical feature of intelligence work, after all. Time invested here is vital.

- A key feature is the *knowledge base*. This can take many forms: shared drives, SharePoint libraries, cards in a box—technology is making this ever simpler, and yet also adding layers of complexity. Ultimately, this is an archive space where documents and other material can be stored and indexed. This can include in noting programs such as OneNote and Evernote. All knowledge/information should, where possible, be kept inside one “wrapper” in order to help OPSEC and also allow for ready searching across the entire data/knowledge set.

- **GIS** (geographical information systems) are also critical. SIDeARM breaks these out, as this is a factor that is often forgotten until someone realizes that a map would be useful—often when a database is already huge and geo-coding it would take months. Work this in from the start where possible; it’s time well spent, as visualization is incredibly useful. Obviously this is dependent on the circumstances, but geographic and temporal analysis has many uses.

- **Data validation**: As discussed in Chapter 8 on collation, a key part of data retrieval comes from having common standards. Effective data entry and consistent capture require attention, guidance, and discipline, else they will break down. Guidelines must therefore
be clear, and the process of validation must not be allowed to be eclipsed by timing issues, overload, etc. To do so is to put in place short-term gain at the expense of long-term pain and inefficiency.

**Analysis**

Effective analysis relies to a large extent on the individual’s mindset and the processes in place, which allow the analyst to overcome inherent limitations. Support is therefore provided under SIDeARM in two areas;

- **Tools**: This can include a compendium of techniques, reference guides, and of course technology, particularly as regards data visualization. This is becoming more and more important with the rise in the ability to capture and store huge amounts of data.
- **Processes**: Sound analytical processes must be embedded and to some extent come from careful structuring, allowing people to have the time and space to do the task properly, and the access to support where required. The traps and pitfalls were discussed at length in earlier chapters; time spent on considering analytical processes will greatly help the quality of the output.

**Dissemination**

The dissemination stage is when material gets sent to the client. Timeliness and accuracy are important at this stage; relevancy and “actionability” should have been covered by having good IRs, sources, and collection plans. Saving time on distribution is therefore essential. Moreover, OPSEC is a big issue here, as product readily links. There are therefore a number of things to consider.

- **Standard templates**: These help speed up distribution and help clients absorb information quickly and easily. They should not constantly change, but there should be efforts periodically to tweak these based on feedback to improve usability both for analysts and for clients.
- **Distribution lists**: Again, contact should be quick and easy. It is pointless putting in all this work throughout the intelligence cycle to then fail to get it to clients due to not having their address at hand!

208
• **Platforms**: Consider what other platforms and vectors can be used. There almost certainly needs to be an archive available to clients to put reports into context. Can you make greater use of this to support wider distribution of information? (Push vs. pull again.)

• **Quality assurance**: This is often underrated. As a minimum, I recommend “four eyes” and proofing where possible. That said, this shouldn’t unduly affect timeliness, at least not for critical information.

**Clients**

Much client input is captured through the direction–feedback process. However there is one discrete input.

• **RoI/Value process**: This requires a different sort of engagement with clients to try and put a financial value on the service. This can be related to key performance indicators (KPIs), where appropriate, or use a “real recognized value saved” system, as previously discussed.

**Other Factors**

Although not broken out here, SIDeARM also highlights enabling structures of technology and infrastructure. These are not mandated, but rather should be applied and considered by the manager throughout.

---

**COUNTERING CRIME: THE NATIONAL INTELLIGENCE MODEL (NIM)**

It can be seen from the previous section that SIDeARM is a conceptual model for a healthy functioning system. It does not mandate particular standards; rather, it recommends a series of components that together make for an effectively managed whole.

For contrast, let’s now look at the National Intelligence Model (NIM), launched by the UK National Criminal Intelligence Service (NCIS) and adopted by the Association of Chief Police Officers (ACPO) in 2000, and set out a national model for an intelligence-led approach to policing. For the purpose of NIM, intelligence refers to “information that is subject
to a defined evaluation and risk assessment process in order to assist with police decision making,” with the model setting out a standard for all UK police forces in order to ensure that policing practices are guided by fully researched, developed, and analyzed intelligence to provide strategic direction and support tactical and operational decision making. Nonetheless, the model at its core does not aim at providing an in-depth technical guide on information management; rather, it serves as a standardized practical approach to information collection, storage, and dissemination in any security environment in accordance with set legal and ethical standards. Accordingly, its core principles can be applied in any risk management environment to accurate, timely, and ethical information and intelligence management within and between organizations.

**NIM at a Glance**

In its broadest form, NIM is a product-oriented service that defines a process for setting priorities and a framework in which the identified problem priorities can be solved. NIM is therefore adaptable to not only police or intelligence services, but also to any areas of business requiring a guided, informed, and standardized approach to risk management.

The model defines three levels of operational practice:

- **Local**: Managing a smaller geographical area
- **Regional**: Focusing on issues affecting more than one local area, which may require cooperation and an interagency approach
- **National or international**: May often include cross-border impact and require the management of issues that also combine the first two levels

These levels of operational practice are not necessarily interdependent; rather, the operational practices work codependently, dependent on each level’s requirements. The mechanisms behind the exchange and sharing of intelligence are therefore crucial to ensure effectiveness and maintain consistency of intelligence products that can be applied to:

- Crime and criminality at all levels, including perpetrators
- Non-crime-related issues, such as reputational risks and deviation from code of practices
- Interagency partnerships
- National and international cooperation and coordination
With the main goal of the National Intelligence Model being to ensure that any actions steering decision making are based on researched and analyzed information, NIM provides a standardized approach to this by ensuring:

- Operational security and effectiveness
- An informed approach to identification of threats, risks, and key priorities
- Inter- and intra-agency consistency
- Informed resource allocation (financial and human)
- Greater compliance with legislation (e.g., human rights, RIPA)

**NIM in Practice**

The National Intelligence Model is designed to put intelligence at the front of every action—to steer and guide the direction of decision making on operational, tactical, and strategic levels. To achieve this, the approach focuses on four intelligence products (which are produced at each of the three levels of operational practice outlined previously):

**Strategic assessment**: A document produced by intelligence units to provide a wider overview and predictions of a situation locally, regionally, or nationally over a six-month period. This document provides a foundation for a Strategic Tasking and Coordinating Group (T&CG), which typically consists of senior decision makers and stakeholders. Based on the strategic assessment, the group also sets out the control strategy and intelligence requirements for the three levels of operational practice for the forthcoming period. This provides direction as to what information and intelligence should be collected in relation to the set priorities and other emerging issues in order to identify further trends and patterns that may pose an ongoing threat or constitute immediate or long-term risks.

**Tactical assessment**: A document that outlines predictions to direct tactical priorities at a more immediate time frame (every two weeks). Also produced by the intelligence function at all levels, the document is reviewed by the Tactical T&CG. The outcomes of the meeting and the tactical directions are then reviewed at the next Tactical T&CG, allowing for the evaluation of measures taken and identifying areas for improvement.
**Problem profile:** This is typically commissioned by the Tactical T&CG to identify the scale of a particular issue within any of the three levels of operation in order to evaluate priorities for further direction of resources.

**Target profile:** This is also typically commissioned by the Tasking T&CG, focusing on a profile of suspects or offenders to identify patterns in behavior, networks, and geographical areas in order to identify areas for tactical operational priorities.

These products are supported by a guided process of information collection, evaluation, and dissemination, including source protection. To ensure that best practices are standardized across a range of agencies, NIM includes a set of standard guidelines, referred to as the 5×5×5 system.

The system grades the source by five letters (A to E) and the information by scores of 1 to 5, and it sets out any applicable dissemination limitations based on the sensitivity of the information and source protection in the same way (an example of a 5×5×5 sheet can be found in Figure 11.2). Although a dedicated intelligence team, often consisting of researchers and analysts, will ensure that the process is followed correctly, the information itself can be collected from an array of sources, including the public, organizational assets, and/or partner agencies. Once correctly researched, evaluated, and sanitized, this information will be used to feed the four products described here in order to identify gaps in intelligence, identify risks, direct tactical resources, and identify strategic priorities.

**NIM Considered**

Similar to its role in intelligence-led policing within the law enforcement sector, NIM provides a standardized guidance to intelligence management by promoting partnerships and information sharing in any security environment. The basic components of NIM can therefore be readily applicable as a standardized approach to risk management in an array of businesses in order to improve any entity’s ability to mitigate risks and threats. Information management is therefore not simply a goal; it is a tool to support and enhance decision making at operational, tactical, and strategic levels.

The National Intelligence Model does not form a technical solution to risk management within a corporate security environment, but can rather serve as a guideline to a more standardized intelligence-led approach that can aid in gaining an accurate picture of the business as a
### Template 1

**NOT PROTECTIVELY MARKED UNTIL COMPLETED**

<table>
<thead>
<tr>
<th>GPMS:</th>
<th>RESTRICTED</th>
<th>CONFIDENTIAL</th>
<th>SECRET</th>
</tr>
</thead>
</table>

#### 5×5×5 Information Intelligence Report Form A

<table>
<thead>
<tr>
<th>ORGANISATION AND OFFICER</th>
<th>DATE/TIME OF REPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)</th>
<th>REPORT URN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### SOURCE AND INFORMATION/INTELLIGENCE EVALUATION TO BE COMPLETED BY SUBMITTING OFFICER

<table>
<thead>
<tr>
<th>SOURCE EVALUATION</th>
<th>INFORMATION/INTELLIGENCE EVALUATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Always Reliable</td>
<td>1 Known to be true without reservation</td>
</tr>
<tr>
<td>B Mostly Reliable</td>
<td>2 Known personally to the source but not to the person reporting</td>
</tr>
<tr>
<td>C Sometimes Reliable</td>
<td>3 Not known personally to the source but corroborated</td>
</tr>
<tr>
<td>D Unreliable</td>
<td>4 Cannot be judged</td>
</tr>
<tr>
<td>E Untested Source</td>
<td>5 Suspected to be false</td>
</tr>
</tbody>
</table>

### REPORT

<table>
<thead>
<tr>
<th>PERSON RECORD:</th>
<th>DoB:</th>
<th>NIB CRO:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPERATION NAME/NUMBER:</th>
<th>S</th>
<th>I</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### INTELLIGENCE UNIT ONLY

<table>
<thead>
<tr>
<th>HANDLING CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>To be completed by the evaluator on receipt and prior to entry onto the intelligence system.</td>
</tr>
<tr>
<td>To be reviewed on dissemination.</td>
</tr>
</tbody>
</table>

#### 5×5×5 REVIEWED BY:

<table>
<thead>
<tr>
<th>RE-EVALUATED</th>
<th>CROSS-REF URN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

#### DISSEMINATED TO:

<table>
<thead>
<tr>
<th>PERSON DISSEMINATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME/DATE OF REVIEW:</td>
</tr>
</tbody>
</table>

#### DETAILED HANDLING INSTRUCTIONS:

| PUBLIC INTEREST IMMUNITY: |
| INPUT ONTO AN INTELLIGENCE SYSTEM | Yes | No |

| SIGNATURE (PAPER COPY): |

#### GPMS: | RESTRICTED | CONFIDENTIAL | SECRET |
|---------|------------|--------------|--------|

---

**Figure 11.2** Example of a 5 × 5 × 5 information intelligence report form. (From ACPO [2010]. With permission of the Association of Chief Police Officers, 2010.)
whole, including its capabilities, understanding the risk and threat environment, and identifying high-risk areas in order to ensure effective and efficient resource allocation against problems. Similarly, implementing a NIM-based approach does not necessarily require separate allocation of resources. A standardized intelligence-led approach will instead aid in allocation of often-limited resources: By applying the problem-solving approach, resources can be better focused at identified high-risk areas, targeting the problems through informed strategies.

With the ever-evolving risk and threats facing businesses and corporations worldwide, adoption of a standardized approach to information sharing can:

- Reduce definitional differences by following set guidelines
- Reduce duplication of efforts by appropriately documenting and storing intelligence
- Reduce duplication of efforts by sharing intelligence
- Increase cooperation and collaboration within and between organizations
- Increase operational and tactical consistency
- Increase awareness of risks impacting businesses
- Increase awareness of best practices in risk mitigation
- Increase source protection

**CONCLUSION**

These are two very different models, with different purposes in mind. They also approach the underlying topic in different ways. Neither is better (although I would argue that SIDeARM is more broadly applicable to corporate work than the NIM). However, both can provide guidance to someone who is looking to establish a function or who wishes to “health-check” their own function against a set of criteria. As ever, there is no right answer, and systems depend on people, process, and technology rather than just one aspect; weaknesses in one area can often be countered by strength somewhere else. That said, having the right balance of ingredients helps a lot, and architecture designed to fully support intelligence production will reward those who invest the time and effort.
FOREWORD

By David Burrill Obe

Intelligence expert and former Chief Security Officer

Corporate Security Intelligence is a fundamental part of the basis on which business security decisions should be made. Few would deny that this is a prerequisite for decision making and yet it is, sadly more often than not, treated with lip service. The need for threat and risk analysis, activities which depend on good and timely intelligence, to influence the delivery of security, corporate or otherwise, can be found in most security policies. Unfortunately, it is common to discover that such analyses are infrequently conducted and infrequently subjected to even the most rudimentary re-assessment. In short, key company decisions are therefore made on the basis of ignorance; ignorance of fact and ignorance of professional projections on future developments.

The impact of what I consider to be corporate negligence has significance way beyond what is traditionally, and wrongly, considered to be the narrow confines of corporate security measures. Good corporate security intelligence is crucial to, amongst others, the due diligence process required for mergers and acquisitions, to entering new markets, and to the management of crises.

The unfortunate picture that I paint is caused by amateurism on the part of corporate security departments, executive committees and boards, and all stakeholders focused on the enablement of business, the projection of outstanding reputation and governance of the highest standards. If they “do not get it,” “it” being the potential return on investment of corporate security service which is underpinned by timely and accurate corporate security intelligence, then re-education is long overdue. A growing number of companies do take a professional approach. They set a benchmark against which weaker performances will be measured; informally for the most part but formally, sometimes in law, when weakness may be perceived in the aftermath of incidents, particularly major incidents, as being causal or responsible for inadequate mitigation.

Given the context that I have described, I am delighted that Justin Crump has decided to produce this timely work on corporate security intelligence.
I recommend it to all professionals in the field of security and risk, and to all stakeholders, especially key corporate decision makers. Most especially, I recommend it to all whom hither “have not got it.” Given the world today, it is about time they did!

David Burrill

November 2014

David is the former deputy director Intelligence Corps and chief of staff of the Intelligence and Security Centre, UK Armed Forces. On leaving the military he became chief security officer of British American Tobacco. In more than twenty years of private sector work, he became president of the International Security Management Association; remains an emeritus member of the Risk and Security Management Forum; and was the first co-chairman of the UK Foreign and Commonwealth Office’s Security Information Service for Business Overseas (SISBO)—a public/private sector partnership initiative of which he was one of the key architects.

David was awarded an OBE in the 2004 New Years Honours List for services to international security management. In 2005, David was honored by CSO Journal with a Compass Award for visionary leadership, and by ASIS International as the first recipient of its European Leadership Award. In November of that year he also became the first foreigner to receive a distinguished achievement award from the Overseas Security Advisory Council of the US Department of State, and is the first foreigner to be granted alumni status of the distinguished council. Finally, in July 2006, he was recognized by the Association of Security Consultants with the award of the Imbert Prize for distinguished achievement from citations submitted by ASIS International, the British Security Industry Association, and The Security Institute. He remains highly active coaching, training and mentoring emerging leaders in the security field and also helping identify and drive action around emerging trends.
Despite a long history, the art and science of corporate security has long been a neglected topic, and the study of intelligence within this setting remains even more so. However, this trend is changing. The increasing size, scale, and sophistication of corporate activities on the world stage—coupled with increasing legislative attention—is driving an increasing focus on this topic area, and the traditional gap between “business” (which makes money) and “security” (a corporate cost center) is markedly narrowing.

It is perhaps hardly surprising that this topic should not traditionally have received the attention it deserves. After all, the wider issue of intelligence in the national security context, which has justifiably drawn much more academic and public attention, is in itself still poorly understood. Although most commonly included under political science, the study of intelligence cuts across a huge range of human endeavor, incorporating organizational science, psychology, business, literature, and drama, to name just a few areas of relevance. In a similar vein, the practitioner must be both an artist and a scientist, comfortable with working with words and numbers, and presenting both in written and verbal fashion; be a humble influencer; and be an introverted extrovert. Practitioners must be comfortable with failure and be able to overcome this and keep “kicking on”; they must similarly be at home with complexity and thrive in frustrating and uncertain environments. Moreover, they must be able and willing to put themselves forward and present a view that may be unpopular without taking reactions personally.

It is hard not to have respect for those who do this job in the public sector, where they are at least part of large apparatuses that provide structure, support, certainty of employment, clear career paths, and rigor. How much harder, then, to do this in the corporate or NGO sector, where few of these benefits apply! Corporate analysts will often be working solo, or in a very small team; may be seen ultimately as a cost to the business; and will constantly be evaluated as to their value and worth on the strictest of scales. There is no certainty of support or funding, and there
is no “fudge factor” to hide behind. Moreover, power and organizational structures are often shifting, and clients are won or lost on influence. The corporate intelligence practitioner—as with any responsible corporate security operator—must therefore be an astute business operator with a whole range of soft skills as well as the hard skills relevant to the trade.

The last few years have seen a renaissance in this industry, as the understanding of intelligence-led security operations seeps into the corporate sector. After all, intelligence drives efficiency in response and helps prevent threats from harming the company, its people, and its assets; protects them from harm; prepares them for possible threats; and ultimately drives profits through its support of management decision making at all levels.

This book therefore serves to address the current void of awareness about and study of the corporate security intelligence environment. It draws on the increasing volume of material relevant to national security intelligence work, but it also incorporates a great deal of personal and organizational experience gained supporting corporate clients worldwide through a variety of challenging circumstances. It has been supported by key members of the International Security Management Association (ISMA), which forms the worldwide association for chief security officers; by ASIS, the largest corporate security organization globally; and by the UK’s Resilience and Security Management Forum (RSMF). I am also grateful to all members of the Analysts’ Roundtable network, with many offering encouragement, stories, and support throughout the process of writing this book to specifically address the topic.

This work would not have been possible without the support of a great number of people. A number of more personal thanks are also in order, for those key individuals who have helped with this process. Firstly, to David Burrill for helping correct the first proofs and kindly offering to write the foreword. His lifetime of relevant experience has been a great help. All members of the Sibylline team have also been immensely helpful in providing support, encouragement and research/writing; particular thanks must go to Rick Moyes, Matthew Friibance, Ashlea Cliff, Maria Fjeldstad, and Ollie Fairbank, all of whom provided excellent input at a critical time. Jonathan Dunbar, Peter Gordon-Finlayson and Helen Clamp also all provided extremely useful feedback during a very hectic summer, and very much helped get this book over the line. All are not just colleagues, but also friends, and I hope that in turn they will continue to find the lessons from the book useful.
Critically, I have to thank two wonderful American women. Firstly, Dr. Nicole Lipkin for planting the seed; supporting her as she wrote her second book was an eye-opening experience, which made this work possible. She taught me much. Liz Chamberlin meanwhile has been a support throughout and without her this would not have been achieved. It is strangely fitting that she was able to celebrate with me somewhere in mid-Atlantic at 35,000 feet when the work was finally complete. . . .

Last, but very much not least, fantastic thanks are due to the very supportive, patient, and encouraging team at CRC Press. Prudy, Suzanne, Kate, Jennifer, Shayna, Kathryn and Mark (who initially bought my pitch over coffee at ASIS—how long ago now) are all brilliant. I'm very grateful that they have helped bring the lessons of the last twenty years to life, and hope that the end result does them justice.
ABOUT THE AUTHOR

Justin Crump has been working in the risk, intelligence and analysis field for over twenty years. A graduate of Durham University and King’s College London, he initially worked with the Conflict Studies Research Centre (CSRC), then based at the Royal Military Academy, Sandhurst, UK. As part of this work he was primarily responsible for examining the post-Cold War evolution of Russian maritime strategy. This included work on a number of varied and exciting projects for the Royal Navy, and has fueled a lifelong interest in Russian military capability.

In 1998 Justin gained employment with Chase Manhattan as an Investment Banking analyst, based in London, Geneva and New York. Following a highly intensive training program—equivalent to a degree in banking in just four months—he rotated between departments including Mergers and Acquisitions; Financial Sponsors Debt Capital Markets; and the Chase Private Bank. This period saw a great deal of fluctuation in emerging markets, including the Argentine default and Russian crash, and so this was a particularly fascinating time to help clients negotiate these issues.

The events of September 11, 2001 drove a radical change in Justin’s career. Having joined the British Reserve Forces in 1995, he volunteered for full-time service and was mobilized to the Queen’s Royal Hussars, an armored regiment equipped with the Challenger 2 tank. By November 2001 he was therefore deployed on operations in the Balkans, initially serving as a staff officer in Regimental Headquarters, before taking over a troop in the Brigade Operations Squadron—specialized group undertaking operations across the north-east of the country.

Following the successful completion of this tour, Justin undertook advanced technical training on the Challenger 2 before taking over a tank troop in Germany. This involved intensive training to support operations in Iraq, including learning Arabic to a colloquial level, before deploying to
the country in late 2003. This operational tour initially saw Justin assume responsibility for reconstruction and development of a swath of territory north of Basra, but in early 2004 he was moved to Maysan to support the police force; during this period he saw firsthand the failure of policies, especially regarding the Shia militias, as a result of which he saw weeks of combat in and around the provincial capital, al-Amara.

On return from Iraq Justin joined PA Consulting, the leading UK management consultancy. During this period he was involved in the development of national security programs which remain classified. This involved exposure to both human and technical aspects of intelligence work, which influenced his subsequent career. However, he also had a role as the Aide to Major General the Duke of Westminster KG, the first Reservist officer of that rank since before the Second World War. The General was immensely active, helped by his private resources, and so Justin was soon called to focus on this role full time. From 2004–2007 he was therefore based in the Ministry of Defence in Whitehall, having exposure to policy at Ministerial level during a particularly interesting and critical time. The role also involved an extensive overseas visit program, giving the opportunity to meet key senior foreign personalities and develop relationships. A particular focus were continued protracted visits to operations in the Balkans, Iraq and Afghanistan, where Justin was able to spend time on the ground in Kabul and Kandahar.

In 2007 Justin returned to civilian life, becoming a country risk analyst for the niche British consultancy Stirling Assynt, working alongside a number of former senior intelligence officers. This role saw him embedded with Unicredit, the leading Italian bank, based in Milan. In recognition of his performance, he was promoted in 2008 to become Head of Threat Intelligence, running all the firm’s routine analytical output. This saw responsibility for developing a fast-growing team, with offices in London and Hong Kong, and analysts embedded in a number of major companies. In 2010, the firm’s analysis was featured in an exclusive report on the front page of the South China Morning Post, which led almost overnight to Justin being in demand as a media commentator, focusing on intelligence affairs. This has included being invited to be a blogger on security and intelligence for the Huffington Post, and he routinely appears on international news channels, both as an expert commentator and during topical debates, where he has appeared alongside senior government figures.

Justin founded his own successful firm, Sibylline Ltd, in 2010 with the aim of focusing more on emerging areas of intelligence in the corporate environment. This includes aspects such as cyber operations and social
media collection, as well as developing the approach and theories outlined in this book. Sibylline now supports a large number of companies, ranging from blue chips to medium-sized enterprises, as well as governments, and since 2010 Justin has built the company up in line with his vision to professionalize corporate intelligence work. The firm also runs the Retail Industry Security Centre in the US, providing threat information to hundreds of malls; retail chains; and law enforcement personnel nationwide. In 2011, this work led Justin to be invited to brief the main gathering of the State Department’s Overseas Security Advisory Council Annual Briefing. He is a regular speaker at industry conferences, including regional OSAC meetings, as well as for ISMA—the leading association for Chief Security Officers. This experience both reflects and maintains Sibylline’s position as thought leaders in corporate intelligence.

In 2013 Justin became Head of Intelligence for the ANVIL Group, following a strategic partnership with Sibylline. He also supports the not-for-profit City Security Resilience Networks (CSARN), a business and security networking and briefing organization founded by leading figures in the UK security industry. In what is laughingly called “spare time,” he continues to serve as a Reservist, currently having the great privilege to command a Challenger 2 Squadron based in the south-west of the UK.