BUSINESS ESPIONAGE
Risk, Threats, and Countermeasures

BRUCE WIMMER, CPP
PART I UNDERSTANDING THE PROBLEM OF BUSINESS ESPIONAGE

Chapter 1 Understanding the risks

Introduction
Risk Methodology
Risk Formula
Summary

Chapter 2 Characteristics of business spies

MICE
CRIME
BECCA
Project Slammer
U.S. FBI
Summary

Chapter 3 High-Threat Locations for Business Espionage

Asia-Pacific
Latin America
Europe
Africa
Middle East
More Examples
Business Espionage in Singapore
Business Espionage in Vietnam
Korea, Japan, and India ................................................. 38
Business Espionage in Latin America ................................. 39
United States ................................................................. 41
Vulnerabilities Identified in Examples .................................. 43
Summary ........................................................................ 44

Chapter 4 Espionage by Electronic Means ......................... 47
Introduction ...................................................................... 47
Cases of Electronic Eavesdropping ...................................... 50
Vulnerabilities Identified .................................................... 57
Summary ........................................................................ 58

Chapter 5 Espionage by Force: Physical Theft or Other Appropriation ........................................... 59
Introduction ...................................................................... 59
Cases of Business Espionage by Physical Theft or Other Appropriation .................................................. 60
Vulnerabilities Identified .................................................... 71
Summary ........................................................................ 72

Chapter 6 Facing Espionage While Traveling .................... 75
Introduction ...................................................................... 75
Cases of Travelers Becoming Victims of Business Espionage .................................................. 76
Vulnerabilities Identified .................................................... 81
Conclusion ...................................................................... 82

Chapter 7 Insider Threat ................................................... 85
Introduction ...................................................................... 85
Cases of Insider Espionage ................................................ 87
Vulnerabilities Identified .................................................... 96
Summary ........................................................................ 97
## Part 2 BUSINESS ESPIONAGE COUNTERMEASURES

### Chapter 8 Protecting Your Most Critical Resources
Focus on protecting the most critical information and resources

### Chapter 9 Physical and Personnel Security Countermeasures

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>114</td>
</tr>
<tr>
<td>Business Espionage Security Awareness Training</td>
<td>116</td>
</tr>
<tr>
<td>Business Espionage Reporting Program</td>
<td>119</td>
</tr>
<tr>
<td>Travel Security Program that Includes Business Espionage Threat</td>
<td>120</td>
</tr>
<tr>
<td>Clear, Demonstrated Senior Leadership Support</td>
<td>122</td>
</tr>
<tr>
<td>Identifying and Properly Classifying Sensitive Information</td>
<td>123</td>
</tr>
<tr>
<td>Conduct a Holistic Risk Assessment</td>
<td>126</td>
</tr>
<tr>
<td>Access controls</td>
<td>134</td>
</tr>
<tr>
<td>Control of Office Machines</td>
<td>139</td>
</tr>
<tr>
<td>Use of Tiger and Red Team Testing</td>
<td>140</td>
</tr>
<tr>
<td>Non-Disclosure, Non-Compete, and Other Legal Agreements</td>
<td>141</td>
</tr>
<tr>
<td>Limiting Where/How Company Information Can Be Worked On or Discussed</td>
<td>142</td>
</tr>
<tr>
<td>Develop Special Measures for Marketing and Sales Staff</td>
<td>144</td>
</tr>
<tr>
<td>Liaise with Counterespionage Government Agencies</td>
<td>146</td>
</tr>
<tr>
<td>Offensive Counterespionage</td>
<td>146</td>
</tr>
<tr>
<td>Summary</td>
<td>147</td>
</tr>
</tbody>
</table>

### Chapter 10 Technical Electronic and Computer Countermeasures

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>150</td>
</tr>
<tr>
<td>Technical Surveillance Countermeasures (TSCM)</td>
<td>151</td>
</tr>
<tr>
<td>Computer countermeasures</td>
<td>157</td>
</tr>
<tr>
<td>Mobile Device Countermeasures</td>
<td>161</td>
</tr>
<tr>
<td>Summary</td>
<td>162</td>
</tr>
</tbody>
</table>
Chapter 11  Comprehensive Countermeasures .......................... 163

Introduction ........................................................................... 163
Formal Integrated Approach to IT and Physical Security .......... 166
Summary ................................................................................. 171

Conclusion .............................................................................. 173

Index ..................................................................................... 187