

---

## Contents

---

<b>List of Figures</b> . . . . .	ix
<b>List of Scenarios</b> . . . . .	xiii
<b>Preface</b> . . . . .	xv
<b>Introduction</b> . . . . .	xix
<b>Part 1. Information Systems: Technologies and People</b> . . . . .	1
<b>Chapter 1. Components with Known Purposes: Technologies</b> . . . . .	3
1.1. Up to the end of the 19th Century: decreasing transmission time . . . . .	4
1.2. From the end of the 19th Century: decreasing processing time. . . . .	14
1.3. From the end of the 20th Century: facing massification. . . . .	21
<b>Chapter 2. Components with Interpretive Aspects: People</b> . . . . .	25
2.1. Tacit knowing or, how do we know? . . . . .	26
2.1.1. The existence of tacit knowledge . . . . .	26
2.1.2. Sense-giving and sense-reading: knowledge is tacit. . . . .	27
2.2. The interpretative framework, the filter through which we create our knowledge . . . . .	31

---

2.2.1. A tool for tacit knowing . . . . .	31
2.2.2. The different types of interpretative frameworks . . . . .	34
2.2.3. The commensurability of interpretative frameworks . . . . .	37
2.3. The concept of incommensurability . . . . .	38
2.3.1. From partial communication to incommensurability . . . . .	39
2.3.2. Language – linking words to nature . . . . .	41
2.3.3. Revolution – changing the meaning of words . . . . .	44
2.4. Mental models, representations of reality . . . . .	46
2.4.1. Incomplete representations . . . . .	47
2.4.2. Cognitive representations . . . . .	49
2.4.3. Shared mental models . . . . .	50
2.4.4. Explaining mental models. . . . .	51
<b>Part 2. The Insider Threat . . . . .</b>	<b>59</b>
<b>Chapter 3. The Three Categories of Insider Threats . . . . .</b>	<b>61</b>
<b>Chapter 4. Unintentional . . . . .</b>	<b>69</b>
4.1. The quality of the stolen information . . . . .	73
4.2. The case of apparently insignificant information that has hidden value . . . . .	74
4.3. The case of information that can simply be asked for . . . . .	78
4.4. The case of the information that will help you . . . . .	81
<b>Chapter 5. Intentional and Non-Malicious . . . . .</b>	<b>83</b>
5.1. Conflict between productivity and security . . . . .	85
5.2. Workarounds, a factor for innovation or risk . . . . .	88
5.2.1. Workarounds are an innovation . . . . .	89
5.2.2. Workarounds are a risk . . . . .	89
5.3. On non-malicious violations . . . . .	90
5.3.1. Intentional behavior . . . . .	91
5.3.2. Personal benefit without malicious intent . . . . .	91
5.3.3. Voluntary breaking of the rules . . . . .	92
5.3.4. Possible damage or risk to security. . . . .	92
<b>Chapter 6. Intentional and Malicious . . . . .</b>	<b>95</b>
6.1. The information is known; why not exploit it? . . . . .	96

6.2. Organizational environment and cognitive processes of committing the act . . . . .	99
6.2.1. For the organization, deterrence prevents maliciousness . . . . .	100
6.2.2. For the employee, moral disengagement justifies maliciousness. . . . .	103
6.3. Ease of deterrence. . . . .	105
<b>Conclusion</b> . . . . .	111
<b>Bibliography</b> . . . . .	117
<b>Index</b> . . . . .	127