

INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES

ADVANCES IN INFORMATION SYSTEMS SET



**Volume 10**

# **Insider Threats**

**Pierre-Emmanuel Arduin**

**ISTE**

**WILEY**



## Insider Threats

*Being simple is complicated*

(Être simple, c'est compliqué)

**Advances in Information Systems Set**

coordinated by  
Camille Rosenthal-Sabroux

Volume 10

---

**Insider Threats**

---

Pierre-Emmanuel Arduin

**iSTE**

**WILEY**

First published 2018 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

ISTE Ltd  
27-37 St George's Road  
London SW19 4EU  
UK

[www.iste.co.uk](http://www.iste.co.uk)

John Wiley & Sons, Inc.  
111 River Street  
Hoboken, NJ 07030  
USA

[www.wiley.com](http://www.wiley.com)

© ISTE Ltd 2018

The rights of Pierre-Emmanuel Arduin to be identified as the author of this work have been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

Library of Congress Control Number: 2017963958

---

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library

ISBN 978-1-84821-972-4

---

---

# 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



---

## List of Figures

---

<b>Figure 1.</b> A Hollerith punch card in 1890 . . . . .	xvi
<b>Figure I.1.</b> Example of a successful Carbanak phishing e-mail accompanied by a compressed configuration file in .rar format . . . . .	xxi
<b>Figure 1.1.</b> Artifacts supporting an information system in the second Century BCE. . . . .	5
<b>Figure 1.2.</b> Artifacts supporting the Roman army’s information system in the first Century. . . . .	8
<b>Figure 1.3.</b> Chappe’s Telegraph, an artifact supporting the information system of the French State in the 19th Century . . . . .	11
<b>Figure 1.4.</b> “Correspondence Cinéma – Phono – Télégraphique”: artifacts supporting an information system in the year 2000, as seen in 1910 by Villemard . . . . .	13
<b>Figure 1.5.</b> First page of the August 30, 1890 Scientific American showing how the artifacts supporting an information system made it possible to reduce processing time . . . . .	16

**Figure 1.6.** Control console of the LEO I in 1953. For the first time, a computer system supported an information system in a business . . . . . 19

**Figure 1.7.** Audio and video interface with screen sharing in 1968, confusion developed between “computer system” and “information system”. . . . . 21

**Figure 1.8. a)** The ARPANET in 1977 and  
**b)** the Internet in 2015. . . . . 22

**Figure 2.1.** Sense-giving and sense-reading constitute tacit knowing, the basic structure of the knowledge transfer. . . . . 29

**Figure 2.2.** Knowledge is tacit: this formula, although explicit, is useless for the cyclist. Moreover, for someone who does not grasp its meaning, which is tacit, this remains uncomprehended 30

**Figure 2.3.** The transfer of tacit knowledge . . . . . 32

**Figure 2.4.** The different types of interpretative frameworks: intrusion or non-intrusion into the environment, which is judged analyzable or non-analyzable . . . . . 36

**Figure 2.5.** a) Weak and b) strong commensurability of interpretative frameworks . . . . . 38

**Figure 2.6.** Commensurability in mathematics: here  $a = 2u$  and  $b = 3u$ ,  $a/b = 2/3$  is a rational number,  $a$  and  $b$  are therefore commensurable . . . . . 39

**Figure 2.7.** A representation of the solar system according to Aristotle, extract from the *Cosmographicus liber* of Petrus Apianus in 1524 . . . . . 42

**Figure 2.8.** Mendeleev’s table, the periodic classification of elements, in 1869. . . . . 43

---

<b>Figure 2.9.</b> A communication breakdown: the two people link terms to nature differently. For example here when $A \neq B$ . . . . .	45
<b>Figure 2.10.</b> Mental models are internal representations of external reality at the root of reasoning, decision-making and behavior . . . . .	48
<b>Figure 2.11.</b> Using the flow of water to explain electrical currents, an example of copying an existing mental model to explain an unknown domain . . . . .	49
<b>Figure 3.1.</b> Taxonomy of threats aimed at the security of information systems. . . . .	64
<b>Figure 3.2.</b> Two dimensions and three categories of insider threats. . . . .	66
<b>Figure 4.1. a)</b> Phishing and b) spear phishing: the insider threat can be unintentional in the absence of awareness. . . . .	72
<b>Figure 4.2.</b> A seemingly harmless e-mail . . . . .	77
<b>Figure 4.3.</b> A web page simulating a Microsoft Windows error screen . . . . .	81
<b>Figure 5.1.</b> Workarounds: an adjustment between constraints on the ground (bottom-up) and strategic pressures (top-down) . . . . .	87
<b>Figure 5.2.</b> A caricatural workaround showing the innovation and risk aspects . . . . .	88
<b>Figure 5.3.</b> The fragile balance of security when the threat is internal, intentional and non-malicious: workarounds. . . . .	90
<b>Figure 6.1.</b> The Security Pacific National Bank building in 1971. . . . .	97

**Figure 6.2.** Straub–Welke’s security action cycle . . . . . 100

**Figure 6.3.** a) A deterrent public health poster in 1942 b) and an information systems security deterrent poster in 2003. . . . . 101

**Figure 6.4.** Point between a fully malicious employee (right), fully non-malicious employee (left) and one likely to use neutralization techniques (center) . . . . . 105

**Figure 6.5.** Ease of deterring a violation of the information system security policy when the threat is internal, intentional and malicious . . . . . 108

---

## List of Scenarios

---

<b>Scenario 4.1.</b> What is your employee number? . . . . .	76
<b>Scenario 4.2.</b> Are you there? . . . . .	77
<b>Scenario 4.3.</b> Set it on the doorstep, thank you. . . . .	78
<b>Scenario 4.4.</b> It's for the vice-president . . . . .	79
<b>Scenario 6.1.</b> The Post-it in the transfer room . . . . .	98

