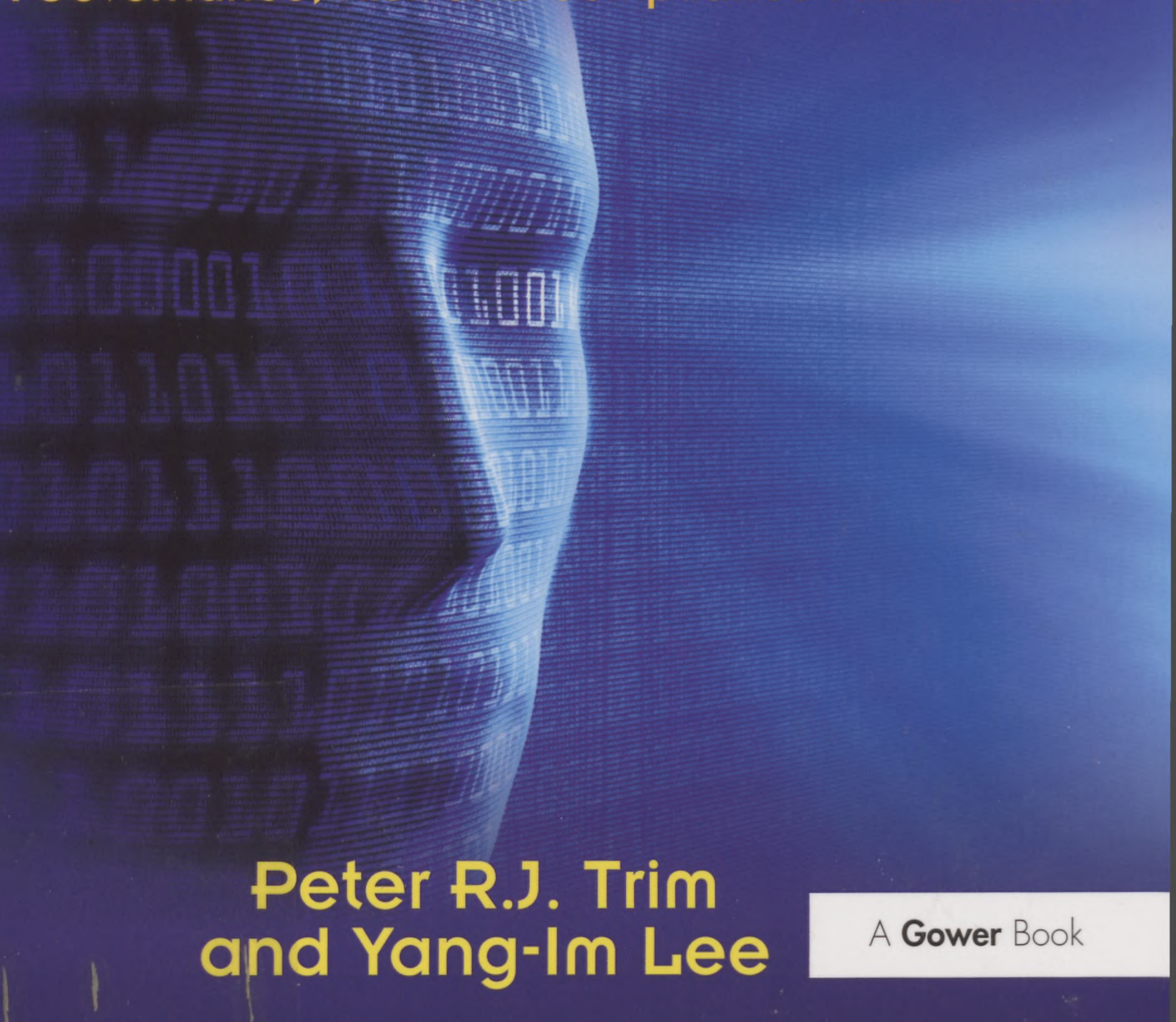
Cyber Security Management

A Governance, Risk and Compliance Framework



Peter R.J. Trim
and Yang-Im Lee

A Gower Book

Cyber Security Management

Peter Albert John Trim
With love and much gratitude

Cyber Security Management

A Governance, Risk and Compliance Framework

BIBLIOTEKA
Nr ewid. ....
Akademii Sztuki Wojennej

PETER TRIM
University of London, UK

YANG-IM LEE
University of Westminster, UK

ROUTLEDGE
Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2014 by Gower Publishing

Published 2016 by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
711 Third Avenue, New York, NY 10017, USA

Routledge is an imprint of the Taylor & Francis Group, an informa business

Copyright © Peter Trim and Yang-Im Lee 2014

Peter Trim and Yang-Im Lee have asserted their rights under the Copyright, Designs and Patents Act, 1988, to be identified as the authors of this work.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the publishers.

Notice:
Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

The Library of Congress has cataloged the printed edition as follows:
Trim, Peter R. J.
Cyber security management : a governance, risk and compliance framework / by Peter R.J. Trim and Yang-Im Lee.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4724-3209-4 (hardback) -- ISBN 978-1-4724-3210-0 (ebook) -- ISBN 978-1-4724-3211-7 (epub) 1. Business enterprises--Computer networks--Security measures. 2. Computer security. 3. Computer crimes--Prevention. 4. Corporations--Security measures. I. Lee, Yang-Im. II. Title.
HF5548.37.T74 2014
658.4'78--dc23

2014008666

ISBN 13 : 978-1-4724-3209-4 (hbk)

Contents

List of Figures and Diagrams *xi*
List of Tables *xiii*
List of Appendices *xv*
About the Authors *xvii*
Preface *xix*
Foreword by Mike Popham *xxi*

Chapter 1 **Introduction and Background to the Research** **1**
1.0 Introduction 1
1.1 Placing Cyber Threats and the Research in Context 1
1.2 Promoting a Holistic View of Security 4
1.3 Research Plan 6
1.4 Methodological Approach and Data Collection Process 7
1.5 Conclusion 8
References 9
Websites 9

Chapter 2 **Sequence-of-Events Model** **17**
2.0 Introduction 17
2.1 Cyber Security Analysis 17
2.2 Corporate Security and Corporate Intelligence 19
2.3 Cyber Security Threats 20
2.4 Issues, Developments and Considerations Needing Answers 24
2.5 Enterprise Risk Management (ERM) 27
2.6 Issues for Commerce, Industry and Government 29
2.7 Building Trust Based Relationships 31
2.8 The Protective Umbrella 32
2.9 Justifying the Approach 32
2.10 Sequence-of-Events Model 33
2.11 Conclusion 36
References 36
Television Programme 38

Chapter 3 **Organizational Strategic Governance Framework** **43**
3.0 Introduction 43
3.1 Setting the Scene 43
3.2 Inter-organizational Development 45
3.3 An Organizational Strategic Governance Framework 48

3.4 Conclusion 50
References 50

Chapter 4 Business Continuity Management Planning Framework 55
4.0 Introduction 55
4.1 Business Continuity Management 55
4.2 Dependency Modelling 57
4.3 IT and Risk Management 58
4.4 Business Continuity in the Context of IT 60
4.5 The Relevance of Strategic Purchasing 65
4.6 A Nine Stage Business Continuity Planning Process 68
4.7 Education and Training 69
4.8 A Business Continuity Management Planning Framework 70
4.9 Conclusion 73
References 73

Chapter 5 Communication Risk Management Strategy 77
5.0 Introduction 77
5.1 Culture and Communication 77
5.2 Business Continuity Management Planning Revisited 80
5.3 Communication Risk Management Strategy 81
5.4 Conclusion 81
References 82

Chapter 6 Risk Assessment Policy and its Strategic Context 85
6.0 Introduction 85
6.1 Understanding what Risk Involves 85
6.2 Defining the Term Vulnerability 86
6.3 Risk Assessment Policy 86
6.4 Strategic Management Framework 92
6.5 Cyber Security Strategy 95
6.6 Cloud Computing 95
6.7 Conclusion 97
References 98

Chapter 7 Resilience Policy and Strategy Mapping 101
7.0 Introduction 101
7.1 Risk and Resilience Defined 101
7.2 Examples Underpinning the Need for Resilience 102
7.3 Resilience Policy 108
7.4 Promoting Resilience 108
7.5 Resilience Domains and Features 110
7.6 Conclusion 112
References 112

Chapter 8 **Integrated Resilience Management Model** **115**
8.0 Introduction 115
8.1 Setting the Scene 115
8.2 Formulating a Resilience Policy 116
8.3 Security Awareness and Organizational Learning 117
8.4 Working with the Workforce 118
8.5 Conclusion 120
References 120

Chapter 9 **Integrated Management Model and System** **123**
9.0 Introduction 123
9.1 Placing the Material in a Security Context 123
9.2 Security Management 124
9.3 Conclusion 128
References 129

Chapter 10 **Integrated Governance Mechanism** **131**
10.0 Introduction 131
10.1 Placing Corporate Governance in Context 131
10.2 Harnessing Appropriate Technology 134
10.3 Organizational Commitment to Corporate Governance 136
10.4 Corporate Governance Revisited 138
10.5 Conclusion 138
References 138
Website 139

Chapter 11 **Threat Identification** **141**
11.0 Introduction 141
11.1 UK Cyber Security Strategy and Changing Threats 141
11.2 Cloud Computing: Opportunities and Threats 142
11.3 Insights into Counteracting Cyber Attacks 144
11.4 The International Context 147
11.5 Organizational Considerations 149
11.6 Conclusion 150
References 150

Chapter 12 **Competitor and Marketing Analysis** **153**
12.0 Introduction 153
12.1 Proteus's Capabilities 153
12.2 Consumerization of IT 156
12.3 Consideration of Current Cyber Security Issues and Challenges 157
12.4 Preventing Cyber Attacks 158
12.5 Mapping of Key Variables and Characteristics 159
12.6 South Korean Security Market 160
12.7 Conclusion 161
References 162

Chapter 13 Governance and Compliance Decision Making Process 173
13.0 Introduction 173
13.1 Linking Organizational Resilience with Corporate Governance 173
13.2 Organizational Decision Making Approach 175
13.3 New Business Models 175
13.4 Future Impacts 177
13.5 Information Security Governance 180
13.6 Lessons Learned 185
13.7 Conclusion 185
References 186

Chapter 14 Integrated Security Mechanism 189
14.0 Introduction 189
14.1 Security Concerns 189
14.2 Consumerization of IT 192
14.3 The Proteus Envelope 193
14.4 Integrating Security with Intelligence 195
14.5 The Benefits of Cloud Computing 196
14.6 Safeguarding Data 197
14.7 Future Working Practices 197
14.8 Issues and Concerns to be Researched 198
14.9 Issues Related to Using Cloud Computing 202
14.10 Conclusion 206
References 207
Websites 208

Chapter 15 Modified and Extended Generic Cyber Security Management Model (MEGCSMM) and Strategic Management Framework, and Project Liaison Team Management 209
15.0 Introduction 209
15.1 Strategic Security Framework 210
15.2 Impact Analysis 210
15.3 Corporate Governance 211
15.4 Modified and Extended Generic Cyber Security Management Model (MEGCSMM) and Strategic Management Framework 212
15.5 Learning Organization 216
15.6 Project Liaison Team Management 216
15.7 Conclusion 219
References 219

Chapter 16 Recommendations for Counteracting Cyber Threats 221
16.0 Introduction 221
16.1 Thinking Through the Complexities of Security and Intelligence 221

16.2 Recommendations 222
16.3 Conclusion 228
References 228

Index *231*

Cyber Security Management

Biblioteka Główna
Akademii Sztuki Wojennej
26711/III (CB)
03-026711-000-0

Czyt.
004.056

Cyber Security Management: A Go d Yang-Im Lee has been written for a wi nt in a holistic context and outlines how the strategic marketing approach can security in partnership arrangements. The book is unique because it integ highly specialized nature but which can be interpreted by those with a no the area. Indeed, those with a limited knowledge of cyber security will be able e understanding of the subject and will be guided into devising and implementing relevant policy, systems and procedures that make the organization better able to withstand the increasingly sophisticated forms of cyber attack.

The book includes a sequence-of-events model; an organizational governance framework; a business continuity management planning framework; a multi-cultural communication model; a cyber security management model and strategic management framework; an integrated governance mechanism; an integrated resilience management model; an integrated management model and system; a communication risk management strategy; and recommendations for counteracting a range of cyber threats.

Cyber Security Management: A Governance, Risk and Compliance Framework simplifies complex material and provides a multi-disciplinary perspective and an explanation and interpretation of how managers can manage cyber threats in a pro-active manner and work towards counteracting cyber threats both now and in the future.

Peter Trim is a Senior Lecturer in Management and Director of the Centre for Advanced Management and Interdisciplinary Studies at Birkbeck, University of London. He is co-author of *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training* and has published widely in the areas of strategic marketing and corporate intelligence. He has been involved in two network security projects funded by the Technology Strategy Board, one of which was also funded by SEEDA.

Yang-Im Lee is a Senior Lecturer in Marketing at Westminster Business School, University of Westminster. She has studied at several institutions including SOAS and Stirling University. She has published widely in the areas of culture, strategic marketing, and international management and has worked on two network security projects funded by the Technology Strategy Board, one of which was also funded by SEEDA.

Cover image: © Johan Swanepoel / iStock.

an **informa** business

ISBN 978-1-4724-3209-4

9 781472 43

Routledge
Taylor & Francis Group
www.routledge.com