

Crime Prevention and Security Management

Series Editor
Martin Gill
Perpetuity Research
Tunbridge Wells, Kent, UK

It is widely recognized that we live in an increasingly unsafe society, but the study of security and crime prevention has lagged behind in its importance on the political agenda and has not matched the level of public concern. This exciting new series aims to address these issues looking at topics such as crime control, policing, security, theft, workplace violence and crime, fear of crime, civil disorder, white collar crime and anti-social behaviour. International in perspective, providing critically and theoretically-informed work, and edited by a leading scholar in the field, this series will advance new understandings of crime prevention and security management.

More information about this series at
<http://www.palgrave.com/gp/series/14928>

Russell Brewer · Melissa de Vel-Palumbo ·
Alice Hutchings · Thomas Holt ·
Andrew Goldsmith · David Maimon

Cybercrime Prevention

Theory and Applications

palgrave
macmillan

Russell Brewer
School of Social Sciences
University of Adelaide
Adelaide, SA, Australia

Melissa de Vel-Palumbo
Centre for Crime Policy and Research
Flinders University
Adelaide, SA, Australia

Alice Hutchings
Department of Computer Science
and Technology
University of Cambridge
Cambridge, UK

Thomas Holt
School of Criminal Justice
Michigan State University
East Lansing, MI, USA

Andrew Goldsmith
Centre for Crime Policy and Research
Flinders University
Adelaide, SA, Australia

David Maimon
Department of Criminal Justice
and Criminology
Georgia State University
Atlanta, GA, USA

Crime Prevention and Security Management

ISBN 978-3-030-31068-4

ISBN 978-3-030-31069-1 (eBook)

<https://doi.org/10.1007/978-3-030-31069-1>

© The Editor(s) (if applicable) and The Author(s) 2019

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use. The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Cover illustration: Przemyslaw Klos/EyeEm

This Palgrave Pivot imprint is published by the registered company Springer Nature Switzerland AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

SERIES EDITOR'S PREFACE

Russell Brewer, Melissa de Vel-Palumbo, Alice Hutchings, Thomas Holt, Andrew Goldsmith, and David Maimon present a critique of seven different types of commonly deployed crime prevention interventions which they believe have the potential to be used in tackling cybercrimes (with a specific focus on cyber-dependent offences). Certainly, for this reader, these distinguished authors have fulfilled their aim 'to make a substantial original contribution' as to how their chosen crime prevention techniques can be used to tackle offending in the digital realm.

Running through their analysis are at least three issues. The first is that cyber-offending and cyber-offenders typically have different characteristics to traditional offline offenders/offences. This complicates the potential application of traditional crime prevention approaches when applied to the digital arena. Second, there is a paucity of research, and in particular evaluations of these prevention approaches in the online world. The third point is that where there is evidence, it often produces mixed results—sometimes interventions work as intended, sometimes not, sometimes their effect is neutral, and sometimes they can make things worse. This book charts a path through these issues by critiquing the available evidence in the offline world, identifying relevant overlaps with activities online, and then exploring the potential for them to be so applied—providing guidance at the same time as to how this might be undertaken most effectively.

Taking situational crime prevention as an example, and there is more research on this approach than any other they discuss, evaluations

suggest antivirus products are able at detecting and preventing malware attacks but are less positive about the effectiveness of warning messages in mitigating malicious hacking. The available evidence bars for other techniques such as firewalls, passwords, and security awareness programmes are far less developed.

Mass media messages such as awareness-raising campaigns are found wanting offline and have a limited applicability to online offending. Educational workshops may have potential although they will need a different orientation when applied in the cyber-world. Even good mentoring programmes can be thwarted by the difficulty of identifying relevant populations of both offenders and volunteers to help them. Targeted warnings and cautions by the police to warn potential offenders are deemed to have some potential where, for example, they focus on the wrongfulness of the act rather than the offender. Positive diversions that redirect offenders away from crime have some potential, for example, by transitioning malicious hackers to legitimate cybersecurity jobs. Restorative justice also has some appeal to victims and may help some offenders.

You will read more. The potential varies with offences and offenders and the context in which measures are introduced, but what is clear is that there is a need for more research. Offending has proliferated online because offences can generally be committed with more anonymity, where they have less chance of being identified, arrested, and successfully prosecuted and where victims are in plentiful supply. We know that policing generally and the security world specifically have struggled to keep up with changes, and this book suggests criminologists have too. Helpfully they outline in their final chapter ways of filling the knowledge gaps, both in terms of key issues to focus on and the positives and limitations of different evaluation methodologies.

This book is more than about cybercrime. It provides a critique and a review of crime prevention approaches and charts a way of better identifying how a much-neglected area of enquiry can be better understood, and, as importantly, how we can best target future prevention efforts. These alone make it an enticing read.

July 2019

Martin Gill

ACKNOWLEDGEMENTS

This work has its origins in a programme of research funded through the Home Office, which studied cybercrime prevention, knowledge, and practice. The book itself is an outgrowth from a symposium hosted by the University of Cambridge in late 2017, where the findings from this programme were presented by the authorship team. In bringing this research together here in this volume, we hope to contribute to the extensive work already being done by those within the cybersecurity community, law enforcement, and the criminal justice system, who contend with cybercrime and its impact every day.

The authors would like to acknowledge the contributions of several individuals, without whom this book would not have been possible. First and foremost, we would like to thank Catherine Schubert for her editorial and research support over the life of this project. Her patience, diligence, and good humour were greatly appreciated by all. We are also grateful to Ross Anderson, Alistair Beresford, Robert Clarke, Samantha Dowling, Richard Clayton, Sergio Pastrana, Daniel Thomas, and Julie-Anne Toohey for their inputs on earlier drafts of this work. In addition, we would also like to acknowledge the numerous scholars cited throughout the book, whose high-quality scholarship formed the basis of our evaluations and discussion. Finally, we would like to express our gratitude to Liam Inscoc-Jones, Josie Taylor, and the production staff at Palgrave for their dedication to bringing this book together.

In closing, the authors would like to acknowledge and thank the Home Office for funding the original programme of research, as well as the Centre for Crime Policy and Research at Flinders University for subsequent financial support in the preparation of the manuscript for this book.

CONTENTS

1	Setting the Scene	1
Part I Primary Forms of Prevention		
2	Situational Crime Prevention	17
3	Universal Communication Strategies	35
Part II Secondary Forms of Prevention		
4	Educational Workshops	51
5	Mentoring Programs	63
6	Targeted Warnings and Police Cautions	77

Part III Tertiary Forms of Prevention

7 Positive Diversions 93

8 Restorative Justice 109

Part IV New Directions

**9 Designing and Evaluating Crime Prevention Solutions
for the Digital Age 125**

Index 147

LIST OF TABLES

Table 9.1	Potential hypotheses and research designs for evaluating interventions, using the <i>Maryland Scientific Methods Scale</i>	129
Table 9.2	Measures and data sources	133