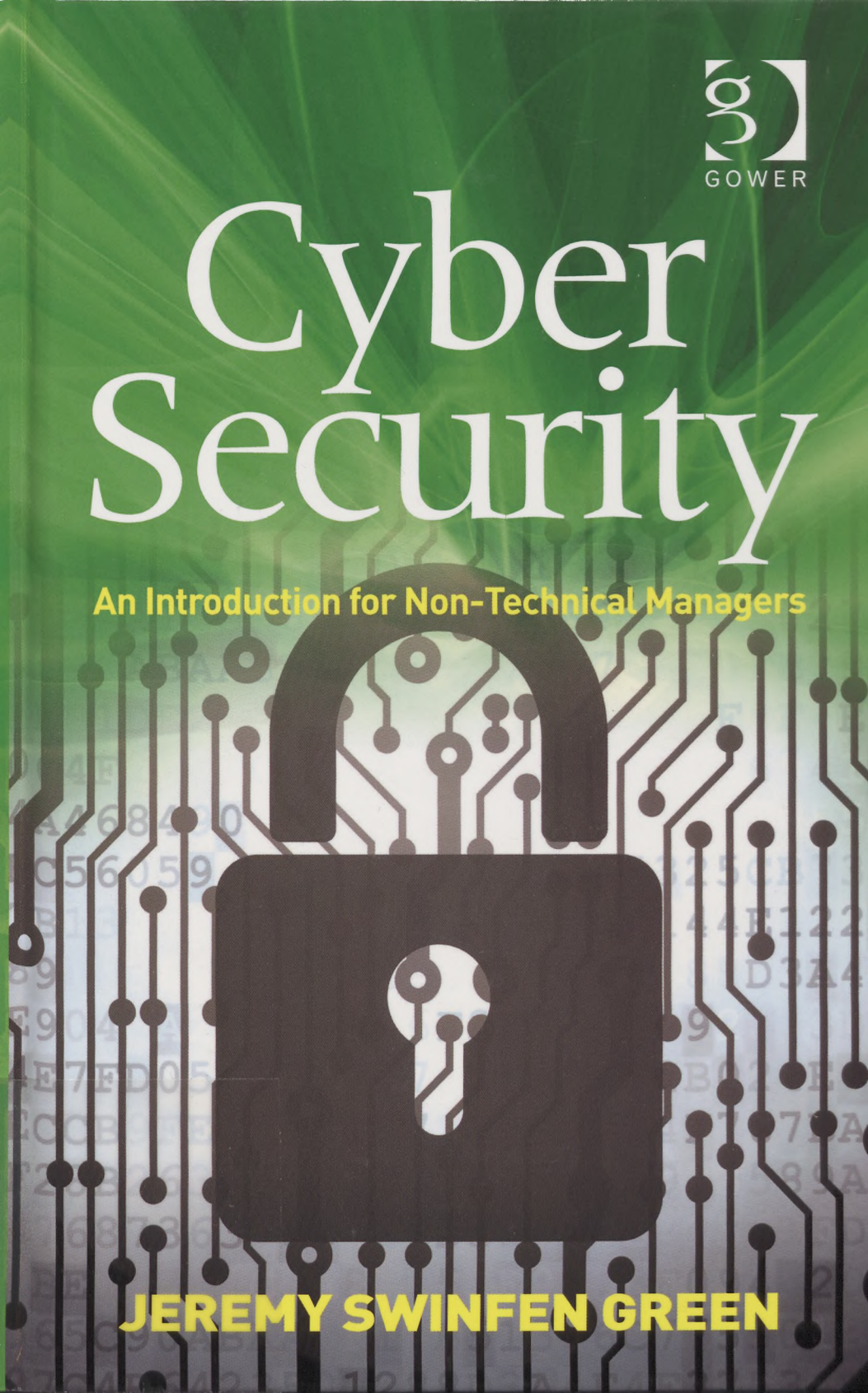
GOWER
Cyber Security
An Introduction for Non-Technical Managers
JEREMY SWINFEN GREEN

CYBER SECURITY

This publication provides a detailed analysis of some of the key cyber security risks facing business today, and provides useful guidance on how to develop an effective strategy to address them.
Andy Williams, Cyber Connect UK

Advances in technology bring enormous benefits but also pose significant risks. Managing these risks will challenge all organisations, whatever their sector or size. This book is a welcome addition to the guidance available and, importantly, emphasises the role of behavioural issues as well as technical solutions to achieve effective cyber security.
Carolyn Williams, The Institute of Risk Management

Jeremy Swinfen Green has succeeded in creating a cybersecurity book that is both well written and uses the language of business management. This is just the right reference for managers who need to understand key cybersecurity concepts and threats and how they can manage the risks.
Paul Dorey, Royal Holloway, University of London, UK;
former CISO, BP PLC

Cyber Security

An Introduction for Non-Technical Managers

Jeremy Swinfen Green
Mosoco Ltd, London, UK

BIBLIOTEKA
Nr ewid. .....
Akademii Sztuki Wojennej

GOWER

© Jeremy Swinfen Green 2015

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior permission of the publisher.

Jeremy Swinfen Green had asserted his right under the Copyright, Designs and Patents Act, 1988, to be identified as the author of this work.

Published by
Gower Publishing Limited
Wey Court East
Union Road
Farnham
Surrey GU9 7PT
England

Gower Publishing Company
110 Cherry Street
Suite 3-1
Burlington, VT 05401-3818
USA

www.gowerpublishing.com

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:
Green, Jeremy Swinfen.
Cyber security : an introduction for non-technical managers / by Jeremy Swinfen Green.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4724-6673-0 (hardback) -- ISBN 978-1-4724-6674-7 (ebook) -- ISBN 978-1-4724-6675-4 (epub) 1. Business enterprises--Computer networks--Security measures. 2. Computer security. 3. Corporations--Security measures. 4. Computer crimes--Prevention. I. Title.
HF5548.37.G737 2015
658.4'78--dc23

2015010130

ISBN 9781472466730 (hbk)
ISBN 9781472466747 (ebk – PDF)
ISBN 9781472466754 (ebk – ePUB)

Printed in the United Kingdom by Henry Ling Limited, at the Dorset Press, Dorchester, DT1 1HD

Contents

Introduction 1

PART I INTRODUCING CYBER SECURITY

1 Cyber Security and Cyber Risk 5

2 A Holistic Approach to Cyber Security 19

3 The Scope of Cyber Security 31

PART II THE MAIN THREATS TO CYBER SECURITY

4 Systems Risks 47

5 People and Networks 67

6 Cloud Computing 79

7 Bring Your Own Device 89

8 Protecting People 101

9 Keeping Data Secure outside the Office 111

10 Social Media Risk 123

11 Who is Stealing your Organisation's Identity? 141

12 Disposing of Data Safely 149

13 The Internet of Things 155

PART III MANAGING CYBER RISK

14 Developing a Cyber Security Strategy 163

15 Picking the Right Team 171

16 Getting Prepared 175

17 Developing a Risk Register 181

18 Managing the Impact of Cyber Incidents 191

19 Responding to Incidents 199

20 Digital Governance 211

Afterword: Looking from the Past to the Future *229*
Glossary *233*
Index *241*

Biblioteka Główna
Akademii Sztuki Wojennej
26712/III (CB)
03-026712-000-0

An

JEREM

Cyber security inv
organisations caus
to revenues and profits as well as indirect damage thro
lower employee morale, and reputational damage.

Czyt.
004.056

Cyber security is often thought to be the domain of the I
cyber risks are found across organisations – as well as ou
in the homes of employees or the business systems of
In order to manage these threats, organisations need to take a holistic approach, employing appropriate technology to defend IT systems, but also strengthening business processes and addressing the understanding, motivation and behaviour of employees.

Ultimately cyber security is the responsibility of every single employee in an organisation from the newest intern to the Chief Executive. Unfortunately, many managers outside IT feel they are ill-equipped to deal with cyber risks or even to question IT specialists, and for this reason the damage from cyber incidents is often worse than it needs to be. This book aims to solve that problem. As well as offering practical advice that does not rely on any understanding of computer code or technology, the author guides readers through the processes that will enable them to identify and manage such threats and help protect their organisations.

About the author

Jeremy Swinfen Green is Director of digital transformation consultancy Mosoco Ltd.

He has over 20 years' experience of digital business. He was early into the digital media space, founding digital media agency Multimedia Dimensions in 1993, advising Omnicom on one of their first digital ventures BMP interAction in 1994 and joining Aegis as digital media director in 1995. He has advised a wide variety of public and private sector organisations on their digital business strategies. In addition as leader of several digital businesses, he has had hands-on experience of the issues surrounding cyber security, data compliance and business continuity as experienced by SMEs.

He is a member of the Performance and Finance Board of TechUK (the UK's trade organisation for the Technology Industry) and a member of the Institute of Risk Management's cyber security SIG.

Cover image: © maxkabakov / iStock.

GOWER
www.gowerpublishing.com
ISBN 978-1-4724-6673-0
9 781472 466730