



M. Eric Johnson

Managing Information Risk and the Economics of Security

 Springer

Managing Information Risk and the Economics of Security

Managing Information Risk and the Economics of Security

Edited by

M. Eric Johnson
*Center for Digital Strategies
Tuck School of Business at Dartmouth
Hanover, NH, USA*

 Springer

Editor

Dr. M. Eric Johnson
Tuck School of Business Administration
Dartmouth College
Hanover, NH 03755, USA
M.Eric.Johnson@tuck.dartmouth.edu

ISBN: 978-0-387-09761-9

e-ISBN: 978-0-387-09762-6

Library of Congress Control Number: 2008936480

© Springer Science+Business Media, LLC 2009

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

springer.com

List of Contributors

Managing Information Risk and Economics of Security

M. Eric Johnson, Tuck School of Business at Dartmouth

Nonbanks and Risk in Retail Payments

Terri Bradford, Federal Reserve Bank-Kansas City

Fumiko Hayashi, Federal Reserve Bank-Kansas City

Christian Hung, Federal Reserve Bank-Kansas City

Stuart Weiner, Federal Reserve Bank-Kansas City

Zhu Wang, Federal Reserve Bank-Kansas City

Richard Sullivan, Federal Reserve Bank-Kansas City

Simonetta Rosati, European Central Bank

Security Economics and European Policy

Ross Anderson, University of Cambridge

Rainer Boehme, Dresden University of Technology

Richard Clayton, University of Cambridge

Tyler Moore, University of Cambridge

BORIS – Business-Oriented Management of Information Security

Sebastian Sowa, Ruhr-University of Bochum

Lampros Tsinas, Munich Re

Roland Gabriel, Ruhr-University of Bochum

Productivity Space of Information Security in an Extension of the
Gordon-Loeb's Investment Model

Kanta Matsuura, University of Tokyo

Communicating the Economic Value of Security Investments;

Value at Security Risk

Rolf Hulthén, TeliaSonera AB

Modelling the Human and Technological Costs and Benefits
of USB Memory Stick Security

Adam Beauteament, UCL

Robert Coles, Merrill Lynch

Jonathan Griffin, HP Labs

Christos Ioannidis, University of Bath

Brian Monahan, HP Labs

David Pym, HP Labs and University of Bath

Angela Sasse, UCL

Mike Wonham, HP Labs

The Value of Escalation and Incentives in Managing
Information Access

Xia Zhao, Tuck School of Business at Dartmouth College

M. Eric Johnson, Tuck School of Business at Dartmouth College

Reinterpreting the Disclosure Debate for Web Infections

Oliver Day, Harvard University

Rachel Greenstadt, Harvard University

Brandon Palmen, Harvard University

The Impact of Incentives on Notice and Take-down

Tyler Moore, University of Cambridge

Richard Clayton, University of Cambridge

Studying Malicious Websites and the Underground Economy
on the Chinese Web

Jianwei Zhuge, Peking University

Thorsten Holz, University of Mannheim

Chengyu Song, Peking University

Jinpeng Guo, Peking University

Xinhui Han, Peking University

Wei Zou, Peking University

Botnet Economics: Uncertainty Matters

Zhen Li, Albion College

Qi Liao, University of Notre Dame

Aaron Striegel, University of Notre Dame

Cyber Insurance as an Incentive for IT Security

Jean Bolot, Sprint

Marc Lelarge, INRIA-ENS

Conformity or Diversity: Social Implications of Transparency
in Personal Data Processing

Rainer Böhme, Technische Universität Dresden

Is Distributed Trust More Trustworthy?

Kurt Nielsen, University of Copenhagen

Preface

Security has been a human concern since the dawn of time. With the rise of the digital society, information security has rapidly grown to an area of serious study and ongoing research. While much research has focused on the technical aspects of computer security, far less attention has been given to the management issues of information risk and the economic concerns facing firms and nations. *Managing Information Risk and the Economics of Security* provides leading edge thinking on the security issues facing managers, policy makers, and individuals. Many of the chapters of this volume were presented and debated at the 2008 Workshop on the Economics of Information Security (WEIS), hosted by the Tuck School of Business at Dartmouth College. Sponsored by Tuck's Center for Digital Strategies and the Institute for Information Infrastructure Protection (I3P), the conference brought together over one hundred information security experts, researchers, academics, reporters, corporate executives, government officials, cyber crime investigators and prosecutors. The group represented the global nature of information security with participants from China, Italy, Germany, Canada, Australia, Denmark, Japan, Sweden, Switzerland, the United Kingdom and the US.

This volume would not be possible without the dedicated work Xia Zhao (of Dartmouth College and now the University of North Carolina, Greensboro) who acted as the technical editor. I am also grateful for the service of the WEIS program committee: Alessandro Acquisti (Carnegie Mellon University), Ross Anderson (Cambridge University), Jean Camp (Indiana University), Huseyin Cavusoglu (University of Texas, Dallas), Ramnath Chellappa (Emory University), Neil Gandal (Tel Aviv University), Anindya Ghose (New York University), Eric Goetz (Dartmouth College), Larry Gordon (University of Maryland), Karthik Kannan (Purdue University), Marty Loeb (University of Maryland), Tyler Moore (Cambridge University), Andrew Odlyzko (University of Minnesota), Brent Rowe (RTI), Stuart Schechter (Microsoft), Bruce Schneier (BT Counterpane), Sean Smith (Dartmouth College), Rahul Telang (Carnegie Mellon University), Catherine Tucker (MIT), and Hal Varian (University of California, Berkeley).

Many thanks also go to the individuals and the organizations that helped us organize WEIS: Hans Brechbühl, Jennifer Childs, Scott Dynes, Eric Goetz, David Kotz, Xia Zhao (all of Dartmouth), and Stuart Schechter (Microsoft), as well as the support of Tuck School of Business and Thayer School of Engineering at Dartmouth College; the Institute for Information Infrastructure Protection (I3P); the Institute for Security Technology Studies; and Microsoft. WEIS and the efforts to compile this book were partially supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) and through the Institute

for Security Technology Studies (ISTS). The I3P is managed by Dartmouth College. The views and conclusions contained in this book are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, ISTS, or Dartmouth College.

September 2008

M. Eric Johnson

Table of Contents

List of Contributors	v
Preface	vii
Managing Information Risk and the Economics of Security	1
1 Introduction	1
2 Communicating Security – The Role of Media	2
3 Investigating and Prosecuting Cybercrime	6
4 CISO Perspective – Evaluating and Communicating Information Risk	8
4.1 Ranking the Information Threats	8
4.2 Communicating the Information Risks	11
4.3 Measuring Progress	13
5 Overview of Book	14
References	15
Nonbanks and Risk in Retail Payments: EU and U.S.	17
1 Introduction	17
2 Nonbanks in Retail Payment Systems	18
2.1 Methodology	18
2.2 Definitions	19
2.3 Payment Types and Payment Activities	20
2.4 Nonbank Prevalence	21
3 Risks in Retail Payments Processing	33
3.1 Risks in Retail Payments	33
3.2 Risks along the Processing Chain	36
4 Impact of Nonbanks on Risk	42
4.1 Changing Risk Profile	42
4.2 Risk Management	45
5 Conclusions and Closing Remarks	49
Acknowledgments	51
References	51
Security Economics and European Policy	55
1 Introduction	55
1.1 Economic Barriers to Network and Information Security	57
2 Information Asymmetries	59
2.1 Security-Breach Notification	59
2.2 Further Data Sources	60
3 Externalities	63
3.1 Who Should Internalise the Costs of Malware?	63
3.2 Policy Options for Coping with Externalities	64
4 Liability Assignment	66

4.1	Software and Systems Liability Assignment.....	67
4.2	Patching.....	68
4.3	Consumer Policy.....	70
5	Dealing with the Lack of Diversity.....	73
5.1	Promoting Logical Diversity.....	73
5.2	Promoting Physical Diversity in CNI.....	74
6	Fragmentation of Legislation and Law Enforcement.....	75
7	Security Research and Legislation.....	76
8	Conclusions.....	77
	Acknowledgments.....	78
	References.....	78
BORIS –Business Oriented management of Information Security.....		81
1	Introduction.....	81
1.1	Background.....	81
1.2	Terms.....	82
1.3	Goals.....	83
2	BORIS design.....	84
2.1	Overview.....	84
2.2	Business Strategic Methods.....	84
2.3	Process Tactical Methods.....	87
2.4	Financial Tactical Methods.....	89
2.5	Operational Evaluation and Optimization Methods.....	90
2.6	Integrated Program Management.....	93
3	Evaluation.....	94
4	Conclusion and Outlook.....	95
	References.....	96
Productivity Space of Information Security in an Extension of the Gordon-Loeb’s Investment Model.....		99
1	Introduction.....	99
2	The Two Reductions.....	100
2.1	Vulnerability Reduction.....	100
2.2	Threat Reduction.....	101
3	Productivity Space of Information Security.....	102
3.1	Threat Reduction Productivity.....	102
3.2	Optimal Investment.....	103
3.3	Productivity Space.....	104
4	Implications and Limitations.....	110
4.1	Different Investment Strategies.....	110
4.2	Influence of Productivity-Assessment Failures.....	110
4.3	Upper Limit of the Optimal Investment.....	110
4.4	Influence of Countermeasure Innovation.....	111
4.5	Trade-off between Vulnerability Reduction and Threat Reduction.....	115
5	Concluding Remarks.....	116