

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

Table of Contents

V uow

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

Acknowledgments	116
References	117
Appendix	118

Communicating the Economic Value of Security Investments:

Value at Security Risk.....	121
1 Introduction and Problem Situation.....	121
2 Background and Preliminaries	123
3 Problem Formulations: Value-at-Risk.....	124
4 Value-at-Security Risk Model: Assumptions.....	124
5 Our Parametric Model	125
5.1 Some Observations on $f_c(x;t)$ and $g_c(x)$	127
5.2 A Special Case: Constant λ and v	128
6 Value-at-Security Risk Entities	129
7 Analysis of Authentic Data: Model Evaluation	131
7.1 Number of Incidents per Time Unit.....	131
7.2 Breach Loss Model	134
8 Comments and Conclusions: Present and Future Work.....	138
References	139

Modelling the Human and Technological Costs and Benefits

of USB Memory Stick Security	141
1 Introduction	141
2 The Central Bank Problem and Information Security.....	143
3 An Empirical Study	145
4 The Conceptual Model	147
5 An Executable Model	155
6 The Experimental Space.....	157
6.1 Exploratory Fit of Additional Calibration Parameters.....	158
6.2 Some Confirmation of Expected Behaviour	158
6.3 Results.....	159
6.4 A Utility Function.....	160
7 Conclusions and Directions.....	161
Acknowledgments	162
References	162

The Value of Escalation and Incentives in Managing Information Access.. 165

1 Introduction	165
2 Background and Solution Framework.....	167
2.1 Access Control Policies	167
2.2 Security and Flexibility of Access Control Policies	168
2.3 Access Governance System with Escalation	169
3 Literature Review	170
4 Economic Modeling of an Information Governance System.....	170

5	Overview of Insights and Results.....	172
5.1	Employee	173
5.2	Firm.....	174
6	Conclusion	175
	References	176

Reinterpreting the Disclosure Debate for Web Infections 179

1	Introduction	179
2	Attack Trends	181
2.1	Drive-By Downloads	183
2.2	Weaponized Exploit Packs	185
3	Market Failure: Consumer Webmasters and Mid-Tier Web Hosts.....	186
4	Vulnerability Disclosure.....	188
5	Methods for Identifying Most-Infected Web Hosts	190
6	Web Host Infection Results.....	191
6.1	The Panda in the Room.....	192
7	Recommendations	194
8	Conclusion	196
	Acknowledgments	196
	References	196

The Impact of Incentives on Notice and Take-down 199

1	Introduction	199
2	Defamation	200
3	Copyright Violations	202
4	Child Sexual Abuse Images.....	203
5	Phishing	205
5.1	Free Web-hosting.....	207
5.2	Compromised Machines	207
5.3	Rock-phish and Fast-flux Attacks.....	209
5.4	Common Features of Phishing Website Removal	210
6	Fraudulent Websites	211
6.1	Fake Escrow Agents	211
6.2	Mule-recruitment Websites.....	212
6.3	Online Pharmacies Hosted on Fast-flux Networks.....	215
7	Spam, Malware and Viruses.....	216
8	Comparing Take-down Effectiveness	217
8.1	Lifetimes of Child Sexual Abuse Image Websites	219
9	Conclusion	221
	Acknowledgments	222
	References	222

Studying Malicious Websites and the Underground Economy on the Chinese Web..... 225

1	Introduction	225
2	Related Work.....	227

3	Underground Economy Model	228
3.1	Modeling the Individual Actors	228
3.2	Market Interaction	230
3.3	Case Study: PandaWorm	232
4	Mechanisms Behind Malicious Websites on the Chinese Web	232
4.1	Overall Technical Flow	232
4.2	Web-based and Conventional Trojans	233
4.3	Vulnerabilities Used for Web-based Trojans in China	235
4.4	Strategies for Redirecting Visitors to Web-based Trojans	236
5	Measurements and Results	238
5.1	Measurements on the Underground Black Market	238
5.2	Measurements on the Public Virtual Assets Marketplace	239
5.3	Malicious Websites on the Chinese Web	240
6	Conclusions	243
	Acknowledgments	244
	References	244
	Botnet Economics: Uncertainty Matters.....	245
1	Introduction	245
2	Background and Related Work	247
3	The Benchmark Model	249
3.1	Profit-driven Cybercriminals	249
3.2	Assumptions	250
3.3	Model Without Virtual Machines	251
4	Optimization Model With Virtual Machines	253
4.1	Fixed Probability for a Rental Bot Being Virtual	253
4.2	Uncertainty for a Rental Bot Being Virtual	256
5	Further Discussion and Case Study	259
5.1	Countervirtual Strategies	259
5.2	Examples and Illustration	260
5.3	Technical Challenges	264
6	Conclusion and Future Work	266
	References	267
	Cyber Insurance as an Incentive for Internet Security	269
1	Introduction	269
2	Related Work	272
3	Insurance and Self-protection: Basic Concepts	275
3.1	Classical Models for Insurance	275
3.2	A Model for Self-protection	276
3.3	Interplay between Insurance and Self-protection	277
4	Interdependent Security and Insurance: the 2-agent Case	278
4.1	Interdependent Risks for 2 Agents	279
4.2	IDS and Mandatory Insurance	280
4.3	IDS and Full Coverage Insurance	281

5	Interdependent Security and Insurance on a Network.....	282
5.1	The Complete Graph Network.....	283
5.2	The Star-shaped Network	285
6	Discussion.....	286
7	Conclusion.....	287
	References	288

Conformity or Diversity: Social Implications of Transparency

	in Personal Data Processing	291
1	Introduction	291
1.1	From PETs to TETs	292
1.2	TETs and Individual Behaviour.....	293
2	Model.....	293
2.1	Assumptions.....	294
2.2	Problem Statement.....	295
2.3	Rationales for the Assumptions	295
2.4	Analytical Approach	297
3	Results	302
4	Discussion.....	304
5	Related Work.....	306
6	Summary and Outlook.....	307
	Acknowledgments	308
	References	308
	Appendix	311

Is Distributed Trust More Trustworthy?..... 313

1	Introduction	313
2	Threshold Trust.....	316
3	The Game-Theoretic Modeling	318
3.1	The Basic Model.....	319
3.2	The Extended Model.....	321
3.3	The Choice of N and T.....	324
3.4	The Payoff Matrix.....	326
4	Discussion and Policy Recommendation	327
4.1	NT-TTP Has a Different Cost Structure	327
4.2	Breakdown of The NT-TTP.....	327
4.3	Counteract Stable Coalitions	328
4.4	NT-TTP and Leniency Programs.....	329
5	Conclusion	330
	Acknowledgments	331
	References	331
	Index.....	333