1. Record Nr. UNINA9910437597503321

Titolo	Economics of information security and privacy III [[e-book] /] / Bruce Schneier, editor
Pubbl/distr/stampa	New York, : Springer, 2012
ISBN	1-283-64019-8 1-4614-1981-6
Descrizione fisica	1 online resource (288 p.)
Altri autori (Persone)	SchneierBruce
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	The Impact of Immediate Disclosure on Attack Diffusion and Volume -- Where Do All the Attacks Go? -- Sex, Lies and Cyber-Crime Surveys -- The Underground Economy of Fake Antivirus Software -- The Inconvenient Truth about Web Certificates -- Resilience of the Internet Interconnection Ecosystem -- Modeling Internet-Scale Policies for Cleaning up Malware -- Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security -- Are Home Internet Users Willing to Pay ISPs for Improvements in Cyber Security? -- Economic Methods and Decision Making by Security Professionals -- Real Name Verification Law on the Internet: A Poison or Cure for Privacy -- The Privacy Landscape: Product Differentiation on Data Collection.
Sommario/riassunto	The Workshop on the Economics of Information Security (WEIS) is the leading forum for interdisciplinary scholarship on information security, combining expertise from the fields of economics, social science, business, law, policy and computer science. Prior workshops have explored the role of incentives between attackers and defenders, identified market failures dogging Internet security, and assessed investments in cyber-defense. Current contributions build on past efforts using empirical and analytic tools to not only understand threats, but also strengthen security through novel evaluations of available solutions. Economics of Information Security and Privacy III addresses the following questions: how should information risk be modeled given the constraints of rare incidence and high

interdependence; how do individuals' and organizations' perceptions of privacy and security color their decision making; how can we move towards a more secure information infrastructure and code base while accounting for the incentives of stakeholders?