JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2(1), 2016, 1–2
doi: 10.1093/cybsec/tyw013
Introduction

Introduction

We are pleased to present this special issue of the *Journal of Cybersecurity*, comprising revised papers that first appeared in the 14th Annual Workshop on the Economics of Information Security (WEIS), held on the 22–23 June 2015 at the Delft University of Technology in the Netherlands. WEIS is the premier venue for presenting interdisciplinary scholarship on cybersecurity. WEIS started in 2002 at the University of California, Berkeley, organized by leading researchers from computer science and economics who recognized that information security lapses were caused by failures of incentives more so than failures of technology. Since that time, the conference has expanded to include a wide range of social science perspectives, including psychology, management science, political science, and information management. This naturally complements the *Journal of Cybersecurity's* mission to advance the interdisciplinary science of cybersecurity, so we are delighted that the WEIS steering committee has agreed to publish revised selected papers in the journal.

Papers appearing at WEIS go through a rigorous peer review process, and the papers appearing in this issue went through an additional round of peer review after authors revised their papers following the conference. The eight papers in this issue convey timely insights into cybersecurity issues.

The first three papers study data breaches. The first paper is "Hype and Heavy Tails: A Closer Look at Data Breaches," by Benjamin Edwards, Steven Hofmeyr, and Stephanie Forrest. It received the Best Paper Award, as selected by the conference attendees. The paper constructs an empirical model of data breach occurrence and size. In contrast to conventional wisdom, the authors demonstrate that neither the size (in terms of number of records lost) nor frequency of occurrence has increased over 10 years through 2015. In "Risky Business: Fine-grained Data Breach Prediction Using Business Profiles," Armin Sarabi, Parinaz Naghizadeh, Yang Liu, and Mingyan Liu construct a predictive model that can distinguish which organizations are likely to experience data breaches using features of the organization itself. As a result, the authors construct risk distributions that are tailored to particular industrial sectors and vary by threat type. Finally, in "The Economics of Mandatory Security Breach Reporting to Authorities," Stefan Laube and Rainer Böhme construct a theoretical model to examine the interactions between firms and regulators in an environment where firms are required to disclose breaches to the regulators, as is the case in the EU. The model predicts that a combination of audits and sanctions is necessary in order to incentivize firms to disclose otherwise hidden breaches to regulators.

The next two papers study the decision-making of businesses and security professionals in managing cybersecurity risk. In "Policy, Statistics, and Questions: Reflections on UK Cyber Security Disclosures," Chad Heitzenrater and Andrew Simpson perform a secondary analysis on survey responses from UK businesses about their experiences with security breaches. The authors transform the survey responses into quantitative metrics of cybersecurity investment used in the academic literature, such as expected losses and benefits. The work takes an important first step toward bridging the gap between industry surveys of cybersecurity and the methods proposed by academic researchers. Meanwhile, in 'Are Information Security Professionals Expected Value Maximisers?: An Experimental and Survey-based Test,' Konstantinos Mersinas, Bjoern Hartig, Keith M. Martin, and Andrew Seltzer survey and conduct experiments with information security professionals in order to assess their risk attitudes. They find that information security professionals are just as susceptible to behavioral heuristics and biases such as framing effects as ordinary individuals. They also find that the professionals tend to exhibit risk and ambiguity aversion.

In "Characterizing Fraud and Its Ramifications in Affiliate Marketing Networks," Peter Snyder and Chris Kanich describe an empirical investigation into the prevalence of affiliate marketing fraud, a form of online advertising abuse in which regular Internet traffic is unwittingly funneled through a third party who receives a share of any resulting sales. By examining a large amount of anonymized network traffic data from a university, the authors devise a technique to automatically detect the frauds and provide first-of-its-kind measurements on its prevalence. They also conduct a cost–benefit analysis of the fraud for affected stakeholders.

The last two papers in the issue are also empirical. Both describe experiments in which abuse data is shared with Internet operators in hopes of encouraging greater investment in security defenses and cleanup. In "Understanding the Role of Sender Reputation in Abuse Reporting and Cleanup," Orcun Cetin, Mohammad Hanif Jhaveri, Carlos Gañán, Michel van Eeten, and Tyler Moore describe an experiment in which they emailed abuse reports to the webmaster and hosting providers of compromised websites. The experiment varied the sender of the abuse reports between a university, anti-malware organization, and webmail address to test the hypothesis that the perceived reputation of the sender might influence the recipient's likelihood of taking action. The results found that the sender's email address did not in fact make any significant difference, though they did confirm earlier findings that sending notices expedites cleanup compared to a control group where no reports were sent. In "How Would Information Disclosure Influence Organizations' Outbound Spam Volume? Evidence from a Field Experiment," Shu He, Gene Moo Lee, Sukjin Han, and Andrew B. Whinston constructed

organizational reports of outbound email-spam activity levels for nearly 8000 US organizations. They then designed an experiment which found that publishing this data is associated with reductions in spam levels for the worst offenders.

We are proud of the quality of the papers appearing in this issue. We thank the reviewers, both for the original WEIS conference and the *Journal of Cybersecurity*, for their constructive feedback that has improved the papers considerably. We also thank the authors for their contributions and their willingness to take the multiple rounds of feedback on board. We hope you agree that these papers set a high bar for the quality of articles appearing in this new journal.

Tyler Moore
Editor-in-Chief

David Pym
Editor-in-Chief

Michel van Eeten
Program Chair, Workshop on the Economics of Information Security 2015