Inf Syst Front (2006) 8:335–337
DOI 10.1007/s10796-006-9010-7

Economic aspects of information security: An emerging field of research

Lawrence A. Gordon · Martin P. Loeb

Published online: 23 December 2006

Abstract This paper chronicles the development of economics of information security as an academic area of research. It also describes the contributions of the papers in the special section of this issue devoted to the topic.

Keywords Information security · Economic aspect · Security cost

1 Introduction

By the end of the 1990s, the Internet was already part of everyday life and the popular media featured stories on computer viruses and information security breaches. With this backdrop and our longstanding interests in economic modeling and analysis of managerial accounting topics such as capital budgeting and incentive compensation, we began to explore the area of information security. Our initial focus was on the following three related research questions: (1) how much should an organization spend on information security, (2) how should an organization allocate their information security budget to specific security activities, and (3) what is the economic cost of information security breaches? As we began our research related to these issues, we were surprised to find the paucity of academic literature applying or developing rigorous economic analysis to problems of information security. There was, however, an increasing realization among both computer security professionals and academicians that the provision of effective information security requires attention to economic incentives in conjunction with technical solutions (such as the improved firewalls and intrusion detection systems).

In late 2001, while our initial paper (Gordon & Loeb, 2002) addressing information security investments was under review, we became aware of a then recent conference paper by Ross Anderson, a security engineering professor at Cambridge University. That paper, by Anderson (2001), lucidly explains the crucial role economic incentives play in the computer security arena. We soon got in touch with Ross and he invited us to join himself, noted economist Hal Varian and five other distinguished scholars (L. Jean Camp, Li Gong, Andrew Odlyzko, Bruce Schneier, and Doug Tygar) to form the Program Committee organizing the first Workshop on Economics and Information Security (WEIS). Ross and Hal served as program co-chairs for that first WEIS held at Berkeley in May of 2002.[1] The Workshop, for the first time, brought together scholars and security professionals with diverse backgrounds, but with a common interest in economic aspects associated with information and computer security. Among the topics covered by

L. A. Gordon (✉) · M. P. Loeb
University of Maryland Institute for Advanced Computer Studies,
Robert H. Smith School of Business,
3351 Van Munching Hall,
University of Maryland,
College Park, MD 20742-1815, USA
e-mail: lgordon@rhsmith.umd.edu

M. P. Loeb
e-mail: mloeb@rhsmith.umd.edu

[1] The agenda for WEIS 2002 (and links to papers) can be found at: http://www.sims.berkeley.edu:8000/resources/affiliates/workshops/econsecurity/

presentations at this first workshop were liability, cyber insurance, information security investments, externalities, security metrics, free-riding, price discrimination, privacy, information sharing and incentive compatibility. In addition to presentations by the Program Committee members Anderson, Camp, Odlyzko, Schneier, and ourselves (together with Bill Lucyshyn), the program featured separate presentations by two doctoral students, Alessandro Acquisti and Stuart Schechter who would join the WEIS Program Committee in years to come.

The second WEIS was held in 2003 at the University of Maryland, and we had the pleasure to host that event. The hot topic of the time was Microsoft's trusted computing initiative, and the workshop included a presentation by a senior executive from Microsoft, as well as scholarly papers on the topic.[2] The 2004 WEIS was hosted by Andrew Odlyzko and Bruce Schneier at the University of Minnesota's Digital Technology Center.[3] The 2005 WEIS was held at Harvard's Kennedy School and hosted by L. Jean Camp[4] and the 2006 WEIS was held at Cambridge University and was hosted by Ross Anderson.[5] The 2007 WEIS is scheduled to be held at Carnegie Mellon (and hosted by Alessandro Acquisti and Rahul Telang).

In addition to the establishment and growth of WEIS, there are other indicators of the increased interest in research on economic aspects of information security. Publication of a collection of papers in book form, Camp and Lewis (2004), is another indication, as is the publication by McGraw-Hill of our own book, Gordon and Loeb (2006). Moreover, for three consecutive years, we, together with Bill Lucyshyn, have organized a one one-day forum on "Financial Information Systems and Cybersecurity: A Public Policy Perspective" that we hold at the University of Maryland. Finally, we note that the first Workshop on the Economics of Securing the Information Infrastructure (WESII) was held in Arlington, Virginia in October 2006.[6]

The three papers in this Special Section are representative of the variety of research being done in the emerging area of information security economics. The first paper in this section, Hausken (2006), uses economic modeling to assess the relation between the optimal level of information security investment and the vulnerability of an information set under differing returns scenarios. The analysis represents both a robustness check and an extension of the early Gordon and Loeb (2002) information security model.

Hausken (2006) makes the case that the probability of an information security breach, similar to various other phenomenon, is best modeled using a logistic function that exhibits increasing returns and then decreasing return to investment. With such a logistic information security breach function, the optimal investment level jumps discretely from zero at a critical vulnerability level and continues to increase in vulnerability. Hence, the investment response to increasing vulnerability of the information set, differs from the optimal response for the security breach functions studied by Gordon and Loeb (2002). Moreover, the optimal level of information security investment could well exceed the 37% (1/e) level that was found for specific classes of security breaches by Gordon and Loeb. Hausken also examine the effect of other return assumptions on the optimal information security investment level and on the relation between that level of investment and the initial vulnerability level. The paper shows how the nature of returns is a critical factor in providing guidance on information security investments.

While information security policy and investment decisions are naturally sensitive to the (marginal) benefits of these decisions, there is a paucity of available data on such benefits. The benefits of a security policy or security investment are closely tied to the reduced frequency of successful attacks resulting from such a policy or investment. In turn, the frequency of successful attacks is directly related to the frequency of total attacks. The second paper in this Special Section, Arora, Nandkumar, and Telang (2006), presents and discusses a simple economic model of attacker behavior, and then empirically examines how frequency of attacks changes in response to changes in disclosure and patching of software vulnerability. The data used for the empirical analysis comes from honeypots—computers connected to the Internet with the sole purpose of collecting information on attacks and attackers. By their very nature, the only traffic that honeypots have is illegitimate traffic. Arora et al. find that published vulnerabilities without patches get exploited more often than either secret vulnerabilities or vulnerabilities that are published with patches. Moreover, these results indicate that attackers use public patch information to devise attacks and, consequently, releasing patches may, at least in the short-run, decrease social welfare.

The final paper in this section, Poindexter, Earp, and Baumer (2006), uses experimental economics to shed light on the costs and benefits faced by consumers when they provide private information on an Internet site. The topic of privacy and identity theft has captured the attention of scholars, as well as that of the mass media and the general public. In the past, surveys have been used as the primary

[2] The agenda for WEIS 2003 (and links to the papers) can be found at: http://www.cpppe.umd.edu/rhsmith3/agenda.htm

[3] The agenda for WEIS 2004 (and links to the papers) can be found at: http://www.dtc.umn.edu/weis2004/agenda.html

[4] The agenda for WEIS 2005 (and links to the papers) can be found at http://infosecon.net/workshop/schedule.php

[5] The agenda for WEIS 2006 (and links to the papers) can be found at: http://weis2006.econinfosec.org/prog.html

[6] The agenda for WEIS 2006 (and links to the papers) can be found at: http://wesii.econinfosec.org/workshop/program.php

means of collecting data about the costs and benefits of increased privacy protection. In responding to surveys, participants do not face the type of costs and benefits that they face when making real decisions. Hence, it would not be surprising to find a survey respondent who claims that privacy is extremely important to them, while at the same time voluntarily providing extensive private information through a customer loyalty program at the grocery store in exchange for a small price discounts. Poindexter et al. describe two sets of economic experiments designed to simulate real economic decision-making. The first manually performed experiment addresses costs and benefits of proving private information in a job seeking scenario and was used to guide the development of the second web-based experimental environment. The results of the experiment show a surprising degree of sensitivity by consumers to perceived changes in risk caused either by a regulatory change in the environment or the purchase of security enhancing technology.

We believe that the three papers described above provide an important contribution to the growing body of literature that links economics to information security. Accordingly, we wish to thank R. Ramesh and H. Raghav Rao, the editors of *Information Systems Frontiers*, for giving us the opportunity to develop this Special Section of the journal.

References

Anderson, R. (2001). Why information security is hard—an economic perspective. In Proceedings of 17th Annual Computer Security Applications Conference, New Orleans, Louisiana.

Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure?—An empirical analysis. *Information Systems Frontiers, 8*(5).

Camp, L. J., & Lewis, S. (Eds.) (2004). *Economics of information security.* Boston: Klewer Academic Publishers.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457 (November).

Gordon, L. A., & Loeb, M. P. (2006). *Managing cybersecurity resources: A cost–benefit analysis*. New York: McGraw-Hill.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers, 8*(5).

Poindexter, J. C., Earp, J. B., & Baumer, D. L. (2006). An experimental economics approach toward quantifying online privacy choices. *Information Systems Frontiers, 8*(5).

Lawrence A. Gordon is the Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance at the Robert H. Smith School of Business, University of Maryland and is also an Affiliate Professor in the University of Maryland Institute for Advanced Computer Studies.

Martin P. Loeb is a Professor of Accounting and Information Assurance and a Deloitte and Touche Faculty Fellow at the Robert H. Smith School of Business, University of Maryland. He is also an Affiliate Professor in the University of Maryland Institute for Advanced Computer Studies.