Course developed January 12, 2007

The Economics of Information Security

University of Stavanger
Faculty of Social Sciences
University of Stavanger
N-4036 Stavanger, Norway
E-mail: kjell.hausken@uis.no
Internet: http://www1.uis.no/vit/oks/hausken/

Instructor: Kjell Hausken

Room To be announced
Time Z-day 12.15-16.00
Credit points: x
Admission: To be announced

Course objectives

The purpose of the course is to expose you to the broader issues relevant for understanding and appraising information security. Six main concerns are (1) the efficient use of resources, (2) internal controls, (3) information sharing, (4) technical improvements, (5) behavioral/ organizational improvements, and (6) cybersecurity insurance. The Cyber Revolution encompassing Information, Communication, and Technology (ICT) has caught our societies off guard. Benefits, costs, opportunities, threats evolve in a manner that is not understood. Multiple actors develop and apply increasingly sophisticated technology, interact and communicate strategically with each other, while information of all kinds flows in multiple directions. A main concern for all actors is resource allocation across domains and through time. From society's point of view that is challenging since the threat is continuously changing. This means that the evaluation of threats needs to be continuous in order to provide early warning of new cyber incidents. With a joint interdisciplinary focus, this course handles the challenge by focusing on research that analyzes the threat as generated by an actor equipped with objectives. The research distinguishes between random and targeted attacks through analyzing the persistence and severity of attack. This constitutes an advance beyond earlier research which often considers the threat as constant or immutable, or does not account for the objectives of the actor generating the threat, or otherwise models the threat inadequately. The course advances technical solutions that analyze anomalous behavior, but do not take the objectives and persistence of attacks into account.

Multiple attacking actors interact strategically with each other and with multiple defending actors, through time. Examples of defending actors are individuals, firms, businesses, institutions, governments, and society at large. These can also be attacking actors which may act lawfully or unlawfully. Attacking actors can also be hackers, criminal individuals, groups, and organizations, crime syndicates. Examples of strategies for defenders and attackers are security investments of multiple kinds, various forms of information sharing, hacking, penetration, intrusion prevention, etc. Behavioral modeling of cyber incidents based on the severity of threats towards various targets is well suited for understanding the need and value for protection of various assets.

Examples of attacker objectives are financial gain, political gain, a desire for challenge or status, leisure, or a desire to cause destruction. There is a need to understand the attacker's

motivation, as well as the economic and psychological makeup, so that the defender (target) may evaluate whether there is a real threat that is based on a clear objective of financial gain, destruction, espionage, etc., or whether the objective is less clear. Understanding the objective is essential for defending successfully against attacks. Today's empirics within ICT is largely generated with a technological focus, ignoring categories with a psychological and social science focus. There is a need to understand the attacking actor as an economic and psychological actor. It is clear that cyber incidents are becoming more targeted and that they are more often related to financial gain. There is also the potential for cyber terrorism affecting the critical infrastructure. This threat is intensified through the increased reliance on technology. As the world becomes increasingly digital, much profiling will take place due to security concerns. There are currently large amounts of data applicable for analyzing threats, that are not yet utilized. The profiling of cyber incidents in combination with evaluating the value of investments of various protectional efforts will serve the information security of assets well. The course has a joint theoretical and an applied focus.

The information revolution has introduced new technologies, and changed the way firms, organizations and individuals in the private and public domain interact and conduct business. Cyber security has moved to center stage. Exchange of information and economic transactions increasingly take place via digital electronic activities focused primarily on the interconnectivity obtained via the Internet. One critical part of this interconnectivity is the way organizations integrate their accounting and financial management systems with Internet based applications. Another part is how firms store and transfer information they seek to keep confidential. Organizations on the one hand seek efficient transfer of information, data, and transactions, but on the other hand seek to do this in a secure manner. Gains can be made by intruders breaking through safeguards, violating confidentiality, and unlawfully appropriating information, data, and assets. The field of information security develops at an amazing speed. The mechanisms need to be understood. Firms compete with each other and with external intruders such as hackers over their assets. In this new environment each firm needs to determine the optimal investment in security technology, and the optimal amount of information about security breaches and other events to share with other firms, and public and private information agencies of various kinds. Similarly, the objectives of the intruders need to be understood. There are income effects for intruders, and interdependence and substitution effects between firms. These phenomena can be studied from economic, political, psychological, sociological, and technological viewpoints. There is a need for theoretical development, combined with generation and application of empirics. Examples of key words are Technology, Infrastructure, Vulnerabilities, Threats, Risks, Accidental, Incidental, Computer Attack, Cyber Incident, Network Vulnerabilities, Technical Solutions, Forensics, Incident Analysis, Intelligence Analysis, Criminological Approaches, Tracing and Tracking Methodologies, Behavioral Research, Psychology Profiling, Resilience Management, Procedures, Policies, Organizational Management, Cooperation, Global Phenomenon. Examples of agencies which in recent years have improved their collection and to some extent systematic categorization of empirics, e.g. related to cyber incidents, are various statistics bureaus, CERT, CERIAS, the Centre for Information Security, the Norwegian National Authority for the Investigation and Prosecution of Economic and Environmental Crime, the Financial Supervisory Authority of Norway, the UK National Hi-Tech Crime Unit, the UK Home Office, the UK Asset Recovery Agency, the UK Serious Organised Crime Agency, the Securities and Exchange Commission, the FBI, Interpol/Europol, Symantec, various organizations (Statoil, Shell, SR-Bank, Ibas, etc.).

Course requirements

Each student will write a 3 pages double-spaced (say 600 words) essay due in class every week, starting the second week. Write concisely. I do not want to read a superfluity of sesquipedalian obfuscatory prolixity. You can take stands on the issues, but you need to justify them. You will be evaluated on your command of the material, and on the comprehension you reveal of the major factors relevant for each week's topic. Every week 2-4 of you will present your essays in class. Assignments will be arranged on the first week of class ensuring that the major viewpoints of each topic get presented. These essays to be presented are to be provided to me (or someone to be assigned the task) at 11 a.m. the day before every class. They will be copied, and can be picked up by all other students two hours later outside office C216. With less than 15 students, the course will be run as an informal lecture/discussion course. With more than 20 students, a larger auditorium will be assigned, and the course will be held in a more formal lecturing tone. Each student will write a final paper, due Thursday of exam week at 4 p.m. in my mailbox in C216. The paper should be 12-15 pages, 25-30K, and on a topic relevant for the course. Please come and see me if you want to discuss your topic, or if you want me to suggest possible topics for you. You will be evaluated 50% on your essays, 30% on your final paper, and 20% on your oral presentation including how well you withstand critique from the other students and myself. Office hours are Monday and Thursday 12.30-16.30 in C216.

Course Schedule

1. week: The nature of information security

Anderson, R., 2001. Why Information Security is Hard – An Economic Perspective. In Proceeding of 17th Annual Computer Security Applications Conference (ACSAC), December 10-14, 2001, New Orleans, Louisiana.

Anderson, R., 2003. Cryptography and Competition Policy - Issues with 'Trusted Computing'. Paper presented at WEIS2003, 2nd Annual Workshop "Economics and Information Security", May 29-30, 2003, Robert H. Smith School of Business, Center for Public Policy and Private Enterprise, University of Maryland.

Anderson, R., 2003. 'Trusted Computing' Frequently Asked Questions - TC / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA Version 1.1 (August 2003), http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

Anderson, R., Moore, T., 2006. The Economics of Information Security. Science 314 (5799), pp.610–613, October 27, 2006, http://dx.doi.org/10.1126/science.1130992.

Nagaraja, S., Anderson, R., 2005. The topology of covert conflict. Technical Report, Number 637, University of Cambridge, Computer Laboratory, UCAM-CL-TR-637, ISSN 1476-2986.

2. week: Information security investment

Gordon L.A., Loeb, M. The Economics of Information Security Investment. ACM Transactions on Information and System Security 2002: 5, 438-457.

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, 338-349.

Schechter, S.E., Smith, M.D., 2003. How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems Networks," Proceedings of the Financial Cryptography Conference, Gosier, Guadeloupe, January 27-30.

Tanaka, H., Matsuura, K., 2005. Vulnerability and Effects of Information Security Investment: A Firm Level Empirical Analysis of Japan. Paper presented at Forum on

Financial Information Systems and Cyber Security, College Park, Maryland, May 2005.

Tanaka, H., Matsuura, K., Sudoh, O., 2005. Vulnerability and information security investment: An empirical analysis of E-local government in Japan. Journal of Accounting and Public Policy 24, 37-59.

Varian, H., 2004. System Reliability and Free Riding. In Economics of Information Security, L. J. Camp, S. Lewis, eds., Kluwer Academic Publishers, vol. 12 of Advances in Information Security, pp. 1-15.

3. week: Information sharing

Gal-Or, E., 1985. Information sharing in oligopoly," Econometrica 53, 2, 329–343.

Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. Information Systems Research 16 (2), 186-208.

Ghose, A., 2006. Information Disclosure and Regulatory Compliance: Economic Issues and Research Directions. Ms, Leonard Stern School of Business, New York University.

Ghose, A., Hausken, K., 2006. A Strategic Analysis of Information Sharing Among Cyber Attackers. Ms.

Gordon, L.A., Loeb, M., Lucyshyn, W., 2003. Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy 22 (6), 461-485.

Hausken, K., 2006. Information Sharing among Firms and Cyber Attacks. Ms.

4. week: Security investment, competitor analysis, and capital budgeting

Antle, R., J. Demski, J., 1988. The Controllability Principle in Responsibility Accounting," The Accounting Review 63, 4, 700-718.

Antle, R., Fellingham, J., 1997. Models of capital investments with private information and incentives: a selective review, Journal of Business Finance and Accounting 24, 7, 8, 887-908.

Bodin, L.D., Gordon, L.A., Loeb, M., 2005. Evaluating Information Security Investments Using the Analytic Hierarchy Process. Communications of the ACM 48, 2, 79-83.

Emhjellen, M., Hausken, K., Osmundsen, P., 2006. The Choice of Strategic Core - Impact of Financial Volume. International Journal of Global Energy Issues 26, 1/2, 136-157.

Gordon, L.A., Loeb, M., 2001. Using Information Security as a Response to Competitor Analysis Systems. Communications of the ACM 44, 9, 70-75.

Gordon, L.A., Loeb, M., 2006. Budgeting Process for Information Security Expenditures. Communications of the ACM 49, 1, 121-125.

Gordon, L.A., Loeb, M., 2006. Expenditures on Competitor Analysis and Information Security: A Managerial Accounting Perspective," Chapter 5 in Management Accounting in the Digital Economy (Oxford University Press), A. Bhimini (ed), 2003, pp. 95-111.

Lambert, R., 1986. Executive Effort and Selection of Risky Projects," Rand Journal of Economics 17, 1, 77-88.

5. week: Income, interdependence, and substitution effects, and insurance

Enders, W., Sandler, T., 2003. What do we know about the substitution effect in transnational terrorism?. in A. Silke and G. Ilardi (eds) Researching Terrorism: Trends, Achievements, Failures (Frank Cass, Ilfords, UK), http://www-rcf.usc.edu/~tsandler/substitution2ms.pdf

Gordon, L.A., Loeb, M., Sohail, T., 2003. A Framework for Using Insurance for Cyber-Risk Management. Communications of the ACM 46, 3, 81-85.

Hausken, K., 2006. Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. Journal of Accounting and Public Policy 25, 6, 629-665.

Kunreuther, H., Heal, G., 2003. Interdependent security. The Journal of Risk and Uncertainty 26, 2/3, 231-249.

Lakdawalla, D., Zanjani, G., 2002. Insurance, self-protection, and the economics of terrorism. Ms., RAND and NBER Working Paper No. W9215, Federal Reserve Bank of New York.

6. week: Security investment and time

Arya, A., Glover, J., 2001. Option Value to Waiting Created by a Control Problem," Journal of Accounting Research 39, 3, pp. 405-416.

Dutta, S., Reichelstein, S., 2002. Controlling Investment Decisions: Depreciation and Capital Charges". Review of Accounting Studies 7, 253-281.

Glover, J., 2002. Discussion of: Controlling Investment decisions: Depreciation and capital charges. Review of Accounting Studies 7, 283-287

Gordon, L.A., Loeb, M., Lucyshyn, W., 2003. Information Security Expenditures and Real Options: A Wait-and-See Approach. Computer Security Journal XIX, 2, 1-7.

Rogerson, W., 1997. Inter-temporal cost allocation and managerial incentives: A theory explaining the use of economic value added as a performance measure. Journal of Political Economy 105, 770-795.

7. week: Security investment and asymmetric information

Antle, R., Eppen, G., 1985. Capital Rationing and Organizational Slack in Capital Budgeting," Management Science 31, 22, 163-174.

Dash, R., Jennings, N., Parkes, D., 2003. Computational Mechanism Design: A Call to Arms," IEEE Intelligent Systems 18, 6, 40-47.

Gordon, L.A., Loeb, M., Zhou, L., 2005. Information Security Audits and Asymmetric Information. Working paper, University of Maryland

Gordon, L.A., Loeb, M., Stark, A.W., 1990. Capital Budgeting and the Value of Information. Management Accounting Research 1, 1,21-35.

Loeb, M., Magat, W., 1978. Soviet Success Indicators and the Evaluation of Divisional Management. Journal of Accounting Research 16, 1, 103-121.

Penno, M., "Asymmetry of Pre-decision Information and Managerial Accounting," Journal of Accounting Research, Spring 1984, pp. 177-191.

8. week: Software vulnerability, IDS systems, software vendors, patching, and disclosure

Arora, A., Caukling, J., Telang, R., 2005. Sell First, Fix Later: Impact of Patching on Software Quality. Management Science, Forthcoming.

Arora, A., Krishnan, R., Telang, R., Yang, Y., 2005. Vendor Response to Software Vulnerability Disclosure: An Empirical Analysis. Working paper.

Arora, A., Telang, R., Xu, H., 2004. Optimal Time for Software Vulnerability Disclosure. Working paper

Ayres, I., Levitt, S.D., 1998. Measuring Positive Externalities from Unobervable Victim Precaution: An Empirical Analysis of Lojack, The Quarterly Journal of Economics 113(1), 43-77.

Cavusoglu, H., Birendra, M., Raghunathan, S., 2005. The Value of Intrusion Detection Systems in Information Technology Security Architecture" Information Systems Research, 16 (1), pp. 28–46

Choi, J.P., Fershtman, C., Gandal, N., 2005. Internet Security, Vulnerability Disclosure, and Software Provision", working paper.

Kannan, K., Telang, R., 2005. Market For Software Vulnerabilities? Think Again. Management Science, 51(5), 726-740.

9. week: Quality standards and liability

Backhouse, J., Hsu, W.Y., Tseng, J., Baptista, J., 2005. A Question of Trust - An economic perspective on Quality Standards in the Certification Services Market". Communications of the ACM. September, ISSN 0001-0782

Jin, G.Z., Leslie, P., 2003. The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Card. The Quarterly Journal of Economics 118, 2, 409-451.

Hotz, J., Xiao, M., 2005. The Impact of Minimum Quality Standards on Firm Entry, Exit and Product Quality: The Case of the Child Care Market. Working paper, UCLA

Ronner, U., 1991. Minimum Quality Standards, Fixed Costs, and Competition. The RAND Journal of Economics, 22 (4) , pp. 490-504.

Spence, M., 1977. Consumer Misconception, Product Failure and Product Liability, The Review of Economic Studies, 44(3), 561-572.

10. week: Secure e-commerce, peer-to-peer networks, and censorship resistance

Backhouse, J., 2001. Assessing Certification Authorities: guarding the guardians of secure e-commerce? Journal of Financial Crime 9 (3): 217-226, ISSN 1359-0790.

Danezis, G., Anderson, R., 2004. The Economics of Censorship Resistance, Paper presented at WEIS2004, 3d Annual Workshop "Economics and Information Security".

Krishnan, R., Smith, M.D., Telang, R., 2003. The Economics of Peer-to-Peer Networks. Journal of Information Technology Theory and Application 5, 3, 31-44.

Mjolsnes, S.F., Rong, C.M., 2003. On-line e-wallet system with decentralized credential keepers. Mobile Networks & Applications 8, 1, 87-99.

Yang, G., Rong, C.M., Dai, Y.P. 2004. A distributed honeypot system for grid security. LECTURE NOTES IN COMPUTER SCIENCE 3032: 1083-1086.

11. week: Information security, encryption, design, coding, decoding, and power mappings

Duursma, I., Helleseth, T., Rong, C.M., et al. 1999. Split weight enumerators for the preparata codes with applications to designs. DESIGNS CODES AND CRYPTOGRAPHY 18 (1-3): 103-124.

Helleseth, T., Rong, C.M., Sandberg, D., 1999. New families of almost perfect nonlinear power mappings IEEE TRANSACTIONS ON INFORMATION THEORY 45 (2): 475-485.

Helleseth, T., Rong, C.M., Yang, K.C., 1999. New infinite families of 3-designs from preparata codes over Z(4)(1). DISCRETE MATHEMATICS 195 (1-3): 139-156.

Helleseth, T., Rong, C.M., Yang, K.C., 2001. New 3-designs from Goethals codes over Z(4). DISCRETE MATHEMATICS 226 (1-3): 403-409.

Helleseth, T., Rong, C.M., Yang, K.C., 2001. On t-designs from codes over Z(4) DISCRETE MATHEMATICS 238 (1-3): 67-80 JUL 28.

Rong, C.M., 2003. On Probabilistic scheme for encryption using Nonlinear codes mapped from Z(4) linear codes. IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS COMMUNICATIONS AND COMPUTER SCIENCES E86A (9): 2248-2250.

Rong, C.M., Helleseth, T., Lahtonen, J. 1999. On algebraic decoding of the Z(4)-linear Calderbank-McGuire code. IEEE TRANSACTIONS ON INFORMATION THEORY 45 (5): 1423-1434.

12. week: Computer crime, profiling, and information security

Dhillon, G., Silva, L., Backhouse, J., 2004. Computer Crime at CEFORMA: A Case Study. International Journal of Information Management 24, 551-561.

Gordon, L.A., Loeb, M., Lucyshyn, W., Richardson, R., 2004. 2004 CSI/FBI Computer Crime and Security Survey. Computer Security Journal XX, 3, 33-51.

Kjaerland, M., 2005. A Classification of Computer Security Incidents Based on Reported Attack Data, Journal of Investigative Psychology and Offender Profiling, 2, 105-120, ISSN 1544-4759.

Kjaerland, M., 2005. A Differentiation between Reported Computer Security Incidents Directed towards the Bank/Finance Sector. In W. Bilsky and D. Elizur, Facet Theory: Design, Analysis & Applications (pp. 221-231). ISBN 80-86742-09-1.

Kjaerland, M., 2006. A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors, Computers & Security, 25, 7, 522-538.

Kjaerland, M., 2006. Profiling Coordinated Cyber Incidents towards the Critical Infrastructure in Norway, International Journal of Critical Infrastructures, Revise and Resubmit.

13. week: The internet, and network theory

Albert, R., Barab´asi, A.L., 2002. Statistical Mechanics of Complex Networks, Reviews of Modern Physics 74.

Albert, R., Jeong, H., Barab´asi, A.L., 2000. Error and attack tolerance of complex networks in Nature v 406, pp 387-482

Barab´asi, A.L., Albert, R., 1999. Emergence of scaling in random networks, in Science v 286, 509-512

Brandes, U., 2001. A Faster Algorithm for Betweenness Centrality, J. Math. Soc. 25(2), pp 163-177

Chaum, D., 1989. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, in Journal of Cryptology v 1, pp 65-75

Erdős, P., Renyi, A., 1959. On Random Graphs, in Publicationes Mathematicae v 6, pp 290-297

Freeman, L.C., 1977. A set of measuring centrality based on betweenness, in Sociometry v 40, 35-41

Holme, P., Kim, B.J., Yoon, C.N., Han, S.K., 2002. Attack Vulnerability of Complex Networks in Phys. Rev. E v 65 art. no. 018101.

Katz M.L., Shapiro, C., 1985. Network externalities, competition, and compatibility. The American Economic Review 75, 424-440.

Milgram, S., 1967. The Small World Problem, in Psychology Today v 2, pp 60-87

Newman, M.E.J., 2003. The structure and function of complex networks. In SIAM Review 45, 167.

Sparrow, M.K., 1990. The Application of Network Analysis to Criminal Intelligence: An assessment of the prospects, in Social Networks v 13, pp 253-274

Watts, D.J., Strogatz, S.H., 1998. Collective Dynamics of Small-World Networks, in Nature v 393, pp 440-442

Zhao, L.A., Park, K.H., Lai, Y.C., 2004. Attack vulnerability of scale-free networks due to cascading breakdown, in Physical review E v 70, 035101.

References

Adamski, A. (1999). *Crimes Related to the Computer Network. Threats and opportunities: A criminological perspective*. Retrieved January 2000, from http://www.infowar.com/new.

American Institute of Chemical Engineers (AIChE) (2002). 'Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites', August, Center for Process Safety.

Anderson, R., 2001. Why information security is hard: An economic perspective. Proceedings of 17th Annual Computer Security Applications Conference, December.

Arora, A., R. Krishnan, R. Telang, Yang, Y., 2005. An empirical analysis of vendor response to software vulnerability disclosure. Working Paper, Carnegie Mellon University, August 2005.

Arrow, K.J, Harris, T., Marschak, J., 1951. Optimal inventory policy. Econometrica 19, 250-272.

Azaiez, N., Bier, V.M., 2006. Optimal Resource Allocation for Security in Reliability Systems. European Journal of Operational Research, Forthcoming.

Bagby, J., 2005. The confluence of public policy on information security controls. Ms., Pennsylvania State University.

Beitel, G.A., Gertman, D.I. and Plum, M.M. (2004), "Balanced Scorecard Method for Predicting the Probability of a Terrorist Attack," Idaho National Engineering and Environmental Laboratory, Idaho Falls, Idaho, USA.

Bennell, C. & Canter, D. (2002). Linking commercial burglaries by modus operandi: Tests using regression and ROC analysis. *Science and Justice, 42,* 153-164.

Bier, V.M., 1995. Perfect Aggregation for a Class of General Reliability Models with Bayesian Updating. Applied Mathematics and Computation 73, 281-302.

Bier, V.M., 2004. Game-theoretic and Reliability Methods in Counter-Terrorism and Security. In Mathematical and Statistical Methods in Reliability (Wilson et al., editors), Series on Quality, Reliability and Engineering Statistics, World Scientific, Singapore, 2005, pages 17-28.

Bier, V.M., Gupta, A., 2006. Myopic Agents and Interdependent Security Risks: A Comment on 'Interdependent Security' by Kunreuther and Heal. Ms.

Bier, V.M., Abhichandani, V., 2002. Optimal Allocation of Resources for Defense of Simple Series and Parallel Systems from Determined Adversaries. Proceedings of the Engineering Foundation Conference on Risk-Based Decision Making in Water Resources X, Santa Barbara, CA: American Society of Civil Engineers.

Bier, V.M., Nagaraj, A., Abhichandani, V., 2005. Protection of Simple Series and Parallel Systems with Components of Different Values. Reliability Engineering and System Safety 87, 315-323.

Bier, V.M., Oliveros, S., Samuelson, L., 2006. Choosing What to Protect: Strategic Defense Allocation Against an Unknown Attacker. Journal of Public Economic Theory, Forthcoming.

Byres, E.J. and Lowe, J. (2004) 'The Myths and Facts behind Cyber Security Risks for Industrial Control Systems', *VDE Congress, VDE Association For Electrical, Electronic & Information Technologies,* Berlin, October, 2004.

Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. J. of Computer Security 11 (3), 431–448.

Canter, D. & Fritzon, K. (1998). Differentiating arsonists: a model of firesetting actions and characteristics. *Legal and Criminological Psychology, 3,* 73-96.

Casey, E. (2004). Reporting security breaches – a risk to be avoided or responsibility to be embraced? *Digital Investigation, 1,* 159-191.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of internet security breach announcements on shareholder wealth. International Journal of Electronic Commerce, Volume 9, Number 1, Fall 2004, pp. 69.

Cavusoglu, H., B. Mishra, B., Raghunathan, S., 2005. The value of intrusion detection systems in information technology security architecture. *Information Systems Research* 16, 1, 28-46.

Chantler, N. (1996). *Profile of a Computer Hacker*. Florida: Infowar.

Choi, J., C. Fershtman, Gandal, N., 2005. The economics of internet security. Department of Economics, Michigan State University, December 6, 2005.

Clarke R, Zeichner L. Beyond the moat: new strategies for cybersecurity, Bank systems & technology, http://www.banktech.com/showArticle.jhtml?articleID¼17501355; 2004 [2005].

Dacey RF, Hite RC. HOMELAND SECURITY: information sharing responsibilities, challenges, and key management issues. Testimony before the Committee of Government Reform House of Representatives, United States General Accounting Office. http://www.gao.gov/new.items/d03715t.pdf; 2003 [2006].

Dalvi, N., Domingos, P., Mausam, M., Sanghai, S., Verma, D., 2004. Adversarial classification. Proceedings of the 2004 ACM SIGKDD international conference on Knowledge discovery and data mining table of contents, Seattle, WA, USA, pp 99-108, ISBN:1-58113-888-9.

Dhillon, G., Silva, L., Backhouse, J., 2004. Computer crime at CEFORMA: A case study. International Journal of Information Management 24, 551-561.

Dixit, A. and Skeath, S. 1999. Games of Strategy, Norton, New York.

Dunn M. A comparative analysis of cybersecurity initiatives worldwide. The paper was prepared by Myriam Dunn, Center for Security Studies, Swiss Federal Institute of Technology (ETH Zurich) for the WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June–July 2005. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf; 2005 [2006].

Enders, W., Sandler, T., 2003. What do we know about the substitution effect in transnational terrorism?. in A. Silke and G. Ilardi (eds) Researching Terrorism: Trends, Achievements, Failures (Frank Cass, Ilfords, UK), Forthcoming, http://www-rcf.usc.edu/~tsandler/substitution2ms.pdf .

Fritzon, K., Canter, D., & Wilton, Z. (2000). The application of an action systems model to destructive behaviour: The examples or arson and terrorism. *Behavioural Science and the Law, 19,* 657-690.

Fudenberg. D. M. and Tirole, J. 1991. Game Theory, MIT Press, Cambridge.

Gal-Or, E., 1985. Information sharing in oligopoly. Econometrica 53 (2), 329–343.

Gal-Or, E., Ghose, A., 2003. The economic consequences of sharing security information. In: Proceedings of the Second Workshop on Economics and Information Security, May 29-30, University of Maryland.

Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. Information Systems Research 16 (2), 186-208.

Ghose, A. and Hausken, K. (2006a), "A Strategic Analysis of Information Sharing Among Cyber Attackers," Ms submitted to journal.

Ghose, A. and Hausken, K. (2006b), "The Dynamics of Information Sharing for Cyber Security Systems," Ms in progress.

Goetz E. (2003). *Survey and Analysis of Security Issues in the U.S. Banking and Finance Sector,* Institute for Technology Studies at Dartmouth College, Available (online): http://www.ists.dartmouth.edu/library/analysis/secfin0903.pdf. (Accessed January 2005).

Gordon, L.A., Loeb, M., 2001. Using information security as a response to competitor analysis systems. Communications of the ACM 44, 9, 70-75.

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

Gordon, L.A., Loeb, M., 2003. Expenditures on competitor analysis and information security: A managerial accounting perspective. In Bhimani, A. (ed.), Management Accounting in the New Economy, Oxford University Press, 95-111.
Gordon, L.A., Loeb, M., Lucyshyn, W., 2003. Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy 22 (6), 461-485.
Gordon, L.A., Loeb, M., Lucyshyn, W., Richardson, R., 2004. 2004 CSI/FBI computer crime and security survey. Computer Security Journal XX (3), 33-51.
Hansman S, Hunt R. A taxonomy of network and computer attacks. Computers & Security 2005;24(1):31–43.
Harsanyi, J. 1967/68. Games with Incomplete Information Played by 'Bayesian Players', I-III Management Science 14, 159-183, 320-334, 486-501.
Hausken, K., 2002. Probabilistic risk analysis and game theory. Risk Analysis 22 (1), 17-27.
Hausken, K., 2005. Production and conflict models versus rent seeking models. Public Choice 123, 59-93.
Hausken, K. (2006b), "Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment," Journal of Accounting and Public Policy 25, 6, 629-665.
Hausken, K. (2006c), "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, 338-349.
Hausken, K., (2006c), "Information sharing among firms and cyber attacks," Paper presented May 24, 2006 at the Annual Forum on "Financial Information Systems and Cyber Security: A Public Policy Perspective", Robert H. Smith School of Business, University of Maryland, Journal of Accounting and Public Policy, Revise and Resubmit.
Hausken, K. (2006d), "Protecting Complex Infrastructures Against Strategic Attackers," in Bier, V. and Azaiez, N. (eds.), Game Theory and Reliability, Springer Series on Reliability Engineering, forthcoming.
Hausken, K. (2006e), "Strategic Defense and Attack for Series and Parallel Reliability Systems," European Journal of Operational Research, Forthcoming.
Hausken, K. (2006f), "Whether to Attack a Terrorist's Resource Stock Today or Tomorrow," Games and Economic Behavior, revise and resubmit.
Hausken, K. (2007), "Strategic Defense and Attack of Systems when Agents Move Sequentially," Ms.
Hausken, K. (2007), "Strategic Defense and Attack for Reliability Systems," Ms.
Hausken, K. (2007), "Strategic Defense and Attack of Series System of Parallel Subsystems and Parallel System of Series Subsystems," Ms.
Hausken, K. (2007), "Information Sharing among Firms and Cyber Attacks," Ms.
Hausken, K. (2007), "Strategic Defense and Attack of Complex Networks," Ms.
Hausken, K. (2007), "Whether to Attack Growing Assets and Enterprises Today or Tomorrow," Ms.
Hausken, K. (2007), "Strategic Identification of Wide Intruders," Ms.
Hausken, K. and Levitin, G. (2007), "Protection and Separation of Parallel Homogeneous Elements," Ms.
Hausken, K. and Levitin, G. (2007), "Protection and Separation of Parallel Non-Homogeneous Elements," Ms.
Hausken, K. and Levitin, G. (2007), "Efficiency of Even Separation of Parallel Elements," Ms.
Hausken, K. and Levitin, G. (2007), "False Targets Efficiency in Defense Strategy," Ms.
Hausken, K. and Levitin, G. (2007), "Defense and Attack of Reliability Systems," Ms.

Hirshleifer, J., 1989. Conflict and rent-seeking success functions: Ratio vs. difference models of relative success. Public Choice 63, 101-112.
Hirshleifer, J., 1995. Anarchy and its breakdown. *Journal of Political Economy* 103(1), 26-52.
Hirshleifer, J., 2001. The Dark Side of the Force: Economic Foundations of Conflict Theory, Cambridge University Press, Cambridge.
Hollinger, R. (1988). Computer hackers follow a guttman-like progression. *Social Sciences Review, 72,* 199-200.
Howard, J., 1997. Analysis of security incidents on the Internet. Unpublished Doctoral Dissertation, Carnegie Mellon University, www.cert.org/research/JHThesis/Start.htm .
Keohane, N., Zeckhauser, R.J., 2003. The ecology of terror defense. The Journal of Risk and Uncertainty 26, 2/3, 201-229.
Kilger, M. (2004). Different perspectives on the social structure and actors within the hacker counterculture. In The Honeynet Project (Ed.), *Know your enemy: learning about security threats*. Boston: Addison-Wesley Professional.
Kirby, A., 1988. Trade associations as information exchange mechanisms. RAND Journal of Economics 29 (1), 138-146.
Kjaerland, M. (2000a). *An exploration into the culture of hackers and crackers: for the purpose of initiating the correct mode of investigation*. Unpublished report, Centre for Investigative Psychology, University of Liverpool.
Kjaerland, M. (2000b). *Electronic civil disobedience: a differentiation between 'hactivists' based on target and message of web site hacks*. MSc Thesis in Investigative Psychology, Accepted by the Department of Psychology, University of Liverpool.
Kjaerland, M. (2005a). A Classification of Computer Security Incidents Based on Reported Attack Data, Journal of Investigative Psychology and Offender Profiling, 2, 105-120, (http://www3.interscience.wiley.com:83/cgi-bin/jhome/106558626). ISSN 1544-4759.
Kjaerland, M. (2005b). A Differentiation between Reported Computer Security Incidents Directed towards the Bank/Finance Sector. In W. Bilsky and D. Elizur, Facet Theory: Design, Analysis & Applications (pp. 221-231). ISBN 80-86742-09-1.
Kjaerland, M. (2006a). (In press). A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors, Computers & Security, doi:10.1016/j.cose.2006.08.004.
Kjaerland, M. (2006b). Coordinated Cyber Incidents towards Norway in 2004. Submitted to International Journal of Critical Infrastructures, Revise and Resubmit.
Kleen, L. J. (2001). *Malicious hackers: a framework for analysis and case study*. Department of the Air Force, Ohio, Air Force Institute of Technology.
Kremen, H., 1998. Apprehending the computer hacker: The collection and use of evidence. *Computer Forensics Online.*
Kreps, D. M. and Wilson, R. 1982. Sequential Equilibria. Econometrica 50, 863-894.
Kunreuther, H., Heal, G., 2003. Interdependent security. The Journal of Risk and Uncertainty 26, 2/3, 231-249.
Lakdawalla, D., Zanjani, G., 2002. Insurance, self-protection, and the economics of terrorism. Ms., RAND and NBER, Federal Reserve Bank of New York.
Landreth, B. (1985). *Out of the inner circle*. Redmond: Microsoft Books.
Lemon, D. (2000). *Threat to computer systems & networks*. Briefing to AIA Cyber Summit attendees, Air Intelligence Center. Kelly AFB, TX.
Levitin, G., 2002. Maximizing survivability of acyclic transmission networks with multi-state retransmitters and vulnerable nodes, Reliability Engineering and System Safety 77 189-199.

Levitin, G., 2003a. Optimal multilevel protection in series-parallel systems, Reliability Engineering and System Safety 81, 93-102.
Levitin, G., 2003b. Optimal allocation of multi-state elements in linear consecutively connected systems with vulnerable nodes, European Journal of Operational Research 150, 406-419.
Levitin, G., Lisnianski, A., 2000. Survivability maximization for vulnerable multi-state systems with bridge topology, Reliability Engineering and System Safety 70, 125-140.
Levitin, G., Lisnianski, A., 2001. Optimal separation of elements in vulnerable multi-state systems, Reliability Engineering and System Safety 73, 55-66.
Levitin, G., Lisnianski, A., 2003. Optimizing survivability of vulnerable series-parallel multi-state systems, Reliability Engineering and System Safety 79, 319-331.
Levitin, G., Dai, Y., Xie, M., Poh, K.L., 2003. Optimizing survivability of multi-state systems with multi-level protection by multi-processor genetic algorithm, Reliability Engineering and System Safety 82, 93-104.
Lin. Y., 2003. The institutionalization of hacking practices. *Ubiquity.* Volume 4, Issue 4.
Martens, S., Stevens, K., 1993. Positive accounting theory and the obligation for post-retirements benefits. Critical Perspectives on Accounting 4 (3), 275-295.
Major, J., 2002. Advanced techniques for modeling terrorism risk, Journal of Risk Finance 4 (1) 15-24.
Munin Chhieng, V., Yee Loh, S., and Kong Ng, Y. (2004) 'Profiling within Information Systems Security'. *School of Information Systems, Technology & Management, The University of New South Wales*. Available at: http://www.cse.unsw.edu.au/~vanc/infs/Final.doc
Nizovtsev, D., M. Thursby. 2005. Economic analysis of incentives to disclose software Vulnerabilities. Working Paper.
Novshek, W and Sonnenschein, H., 1982. Fulfilled expectations in cournot duopoly with information acquisition and release. Bell Journal of Economics 13 (1), 214-218.
O'Hanlon, M., Orszag, P., Daalder, I., Destler, M., Gunter, D., Litan, R., Steinberg, J., 2002. Protecting the American Homeland, Brookings Institution, Washington, DC.
Parker, D. (1998). *Fighting computer crime: a new framework for protecting information*. New York: John Wiley & Sons, Inc.
Platt, C. 1996. Anarchy Online (Net Crime/Net Sex), Harper Collins, New York.
Png, I., C. Tang, Wang, Q., 2006. Information security: User precautions and hacker targeting. Working Paper, National University of Singapore.
Porter, M., 1980), Competitive strategy: Techniques for analyzing industries and their competitors, Free Press, New York, N.Y.
Post, J. (1996). *The dangerous information system insider: psychological perspectives*. Retrieved January 2003, from http://www.infowar.com
Rasmusen. E. 2001. Games and Information, Basil Blackwell, Inc., Cambridge.
Raymond, E., 2001. The cathedral and the bazaar: Musings on linux and open source by an accidental revolutionary. Revised edition. O'Reilly.
Riptech Incorporated, (2000). *Riptech Internet Security Threat Report: Attack Trends for Q1 and Q2 2002*, Volume II*,* Alexandria, VA.: July 2002.
Risan, L., 2000. Hackers produce more than software, they produce hackers. Version 2.1 http://folk.uio.no/lr isan/Linux/Identity_games/
Ritchie, C., 2000. A look at the security of the open source development model. Technical Report, Oregon State University.
Rogers, M. (1999). Psychology of *hackers: steps toward a new taxonomy*. Retrieved January 2003, from http://www.cerias.purdue.edu/homes/mkr/
Rogers, M. (2000). A new hacker taxonomy. *Telematic Journal of Clinical Criminology*. www.criminologia.org. International Crime Analysis Association. Available Retrieved

January 2003, from http://www.criminologia.org/articoli/articoli_pdf/cybercriminologia_pdf/newhacker_taxonomy.pdf

Rogers, M. (2003) 'The role of criminal profiling in the computer forensics process'. *Computers & Security,* Vol. 22, No. 14, pp. 292-298.

Salop, S.C., Scheffman, D., 1983. Raising rivals' costs. *A.E.R. Papers and Proceedings,* 73, 267-271.

Schenk, M., Schenk, M., 2002. Defining the value of strategic security. Secure Business Quarterly 1 (1), 1–6.

Schechter, S., Smith, M., 2003. How much security is enough to stop a thief?. Proceedings of the Financial Cryptography Conference, Guadeloupe, January.

Selten, R. 1975. Reexamination of the Perfectness Concept for Equilibrium Points in Extensive Games. International Journal of Game Theory 4, 25-55.

Shapiro, C., 1986. Exchange of cost information in oligopoly. Review of Economic Studies 53 (3), 433–446.

Schultz E. The human factor in security. Computers & Security 2005;24(6):425–6.

Skaperdas, S., 1991. Conflict and attitudes toward risk. American Economic Review 81, 116-120.

Skaperdas, S., 1996. Contest success functions. Economic Theory 7, 283-290.

Schultz, E.E. (2006), "The changing winds of information security," Computers & Security 25, 5, 315-316

Tanaka, H., Matsuura, K., 2005. Vulnerability and effects of information security investment: A firm level empirical analysis of Japan. Presented May 26, 2005 at the University of Maryland Forum: "Financial Information Systems and Cyber Security: A Public Policy Perspective."

Tanaka, H., Matsuura, K., Sudoh, O., 2005. Vulnerability and information security investment: An empirical analysis of E-local government in Japan. Journal of Accounting and Public Policy 24, 37-59.

Tullock, G., 1967. The welfare costs of tariffs, monopolies, and theft. *Western Economic Journal* 5, 224-232.

Tullock, G., 1980. Efficient rent seeking. In: J. Buchanan, R. Tollison and G. Tullock, (Eds.), Towards a Theory of the Rent-Seeking Society, College Station, Texas A&M University Press, pp. 97-112.

United States Secret Service and CERT®Coordination Center (2004). *Insider threat study: illicit cyber activity in the banking and finance sector*. August 2004. Retrieved January 2003, from http://www.cert.org/archive/pdf/bankfin040820.pdf

Varian, H., 2002. System reliability and free riding. In: Proceedings of the First Workshop on Economics and Information Security, May 16-17, University of California, Berkeley.

Viscusi, W. K. 2005. The Value of Life. New Palgrave Dictionary of Economics and the Law, 2nd Edition. SSRN: http://ssrn.com/abstract=827205.

Vives, X., 1990. Trade association disclosure rules, incentives to share information, and welfare. RAND J. of Economics 21 (3), 409–430.

Woo, G., 2002. Quantitative terrorism risk assessment, Journal of Risk Finance 4 (1) 7-14.

Woo, G., 2003. Insuring against Al-Qaeda, Insurance Project Workshop, National Bureau of Economic Research, Inc. (Downloadable from website http://www.nber.org/~confer/2003/insurance03/woo.pdf).

Ziv, A., 1993. Information sharing in oligopoly: The truth-telling problem. Rand Journal of Economics 24 (3), 455–465.