Cybersecurity Economics

Until ca. 2000, information security was seen as a technological discipline, based on computer science but with mathematics helping in the design of ciphers and protocols. That perspective started to change as researchers and practitioners realized the importance of economics.

Ross Anderson of Cambridge (2001), *Why Information Security is Hard: An Economic Perspective,* at Seventeenth Annual Computer Security Applications Conference.
Professor Anderson explained that a significant difficulty in the optimal development of security technology is the imperative to integrate economic implications into technical designs. But, if a security technology requires that the party with the least risk make the greatest investment, then that system will fail to be widely adopted.

The realization that incentive failures were important, and getting steadily worse, helped spark a research programme in information security economics. This paper illustrates misaligned incentives in the design and deployment of computer systems and impact of externalities: network security appears to have properties of a public good: Insecure nodes not only risk the sanity of their own systems, but also compromise the security of all users, for instance by spreading worms unintentionally and by irresponsibly tolerating distributed attacks from their computers. It also talks about asymmetric information and that insecure software dominates the market for the simple reason that most users cannot distinguish it from secure software and go for cheaper products/services.
In this paper, Professor Anderson highlights following reasons which drive away good/secure products from the market:

1. People adopt popular software products.
2. High fixed costs of products/services and low marginal costs.
3. Higher the cost of switching business, higher is the market value of the product due to lock-in.

He also elaborates how perverse incentives and corporate warfare make security engineer's life difficult.

Hal Varian, *Managing Online Security Risks*, N.Y. Times, June 1, 2000.
This paper explains tragedy of commons in simple terms using example of the antivirus software market. People did not spend as much on protecting their computers as they might have. Why not? At that time, a typical virus payload was a service-denial attack against the website of a company such as Microsoft. Although a rational consumer might well spend $20 to prevent a virus from trashing his hard disk, he might not do so just to prevent an attack on someone else. Solution suggested by Varian for this is, costs of distributed denial od services attack should fall on network operators from which flooding originates. They can then exert pressure on their users to install defensive software or supply themselves as part of subscription package.
In general terms, to counter indecisive and lenient mentalities in the security sector it is necessary to transfer responsibility to the parties that are closest to mitigating the risk. Therefore, an initial step would be to assign consequences for any losses associated with a security breach to the party in the best position to reduce the risk most easily.

Moore, Tyler & Anderson, R (2011). *Economics and Internet Security: A Survey of Recent Analytical, Empirical and Behavioral Research.* Technical report in Computer Science Group Harvard University.

This paper identifies key areas of active research in the field of cybersecurity economics. It provides analytical, empirical and behaviorial research done on each of them. The key areas are as follows:

1. Modelling attack and defense
2. Breaches of personal information

3. Malware and botnets
4. Payment system security

The research done as part of this gave rise to a focus on the development of theoretical solutions to help support the decision-making process via the use of appropriate models. This recognizes the fact that cost–benefit analyses are at the heart of such security decision making, and that (a) the threat landscape is constantly evolving and (b) resources are often limited and contested.

L. Jean Camp (2017). ***The State of Economics of Information Security*****. I/S: A Journal of Law and Policy.** This article provides an overview of findings in major areas of economics in Information Security and a snapshot of this field as it stands. It covers following topics.

1. Role of Insurance in Economics: Cyber insurance incentivizes companies to invest in security. By requiring a minimal investment, insurance can address a situation where every party's risk is a function of the lowest investment, and thus there is a clear economic argument that insurance is appropriate for security mechanisms when the reliability and robustness of those mechanisms depends upon the weakest link.
2. Construction of markets for vulnerabilities: We know that markets in vulnerabilities is quite established today, however Camp points out that nowadays it is majorly perverse incentives of security vendors who purchase vulnerabilities to illustrate value of their services. Hence, a direct participation by the government is much needed as a purchaser and distributor perhaps through an incident response team.
3. What is strategic role of security in the firm: Camp defines investment in security as a product of loss occurred as a result of security failure and probability of the failure itself. She also highlights that investing in security comes at a cost of sharing of information. While many firms would see this as a downside, Camp makes an argument that information sharing can be valuable as it helps counter downward pressure on pricing. Thereby eliminating informational asymmetry.
4. Economics of Privacy: Privacy market for example installation of software containing spyware, does not provide enough information to the customers. Thus, lack of signalling appears to be a concern in this market.
5. Economics of Digital Rights Management: Ideally meant for preventing unfair exploitation of innovation, DRM has become a cause for lock-in, since it limits user options and competition. Economics of DRM shows that its incentives maybe perverse.

H. Ogut, N. Menon, Srinivasan Raghunathan (2005). ***Cyber Insurance and IT Security Investment: Impact of Interdependence Risk.*** **Published in WEIS 2005.**

The authors of this paper investigated the impact of interdependency of security on the choices for security investments and cyber-insurance. Their findings show that the interdependence of security tends to reduce the organizations' incentive to invest in security measures and cyber-insurance.

Tony Vila, Rachel Greenstadt, David Molnar (2003). ***Why we can't be bothered to read privacy policies models of privacy economics as a lemons market.*** **Proceedings of the 5th International Conference on Electronic Commerce, ICEC 2003.**

Here, the authors use a game-theoretic model to explore privacy as a social system based on the work of (Akerlof, 1970). In their model, they express privacy akin to lemons market. Privacy policies fail to be effective signal in this market. Instead, government should provide firms with direct incentives to respect personal information. Permanent and enforced laws against certain uses of such information, or absolute reductions are the only methods now that make all consumers test and all companies respect fair information practices.

References

Anderson, R. J. 2001 Why information security is hard—an economic perspective. In Proceedings of Seventeenth Annual Computer Security Applications Conf., New Orleans, LA, 11–14 December, 2001, pages 358–365.

Varian, H. 2000 Managing online security risks. The New York Times, 1 June 2000.

Moore, T. and Anderson, R. (2011) Economics and internet security: A survey of recent analytical, empirical, and behavioral research. Technical Report TR-03-11. Harvard Computer Science Group, Cambridge, MA, USA.

Camp, L (2023). The State of Economics of Information Security.

H. Ogut, N. Menon, S. Raghunathan: Cyber insurance and IT security investment: Impact of interdependent risk. In: Proceedings of the 4th Workshop on the Economics of Information Security, 2005.

George A. Akerlof. The market for lemons: Quality uncertainty and the market mechanism. Quarterly Journal of Economics, pages 488–500, August 1970.

Vila, Tony & Greenstadt, Rachel & Molnar, David. (2003). Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. Proceedings of the 5th International Conference on Electronic Commerce, ICEC 2003, pages 403-407.

Zoom Discussion Details:

Link to the recording: https://purdue-edu.zoom.us/rec/share/i40f7CcNLPjSrjnQFkgF0tFiMHnIuabmSAtoBlxjvvfFYmkwvlECDxqmDkDqdWL4.SDA2OK2HR_oQirm1
Passcode: R9^?Sxcj

Items discussed by group members:

Akarsh Bolar

1. Cybersecurity and Economics : M. Lesk, "Cybersecurity and Economics," in IEEE Security & Privacy, vol. 9, no. 6, pp. 76-79, Nov.-Dec. 2011, doi: 10.1109/MSP.2011.160.
2. A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach : Michele Myauo, Corporate Cybersecurity Strategy to Enable Artificial Intelligence and Internet of Things, Artificial Intelligence to Solve Pervasive Internet of Things Issues, 10.1016/B978-0-12-818576-6.00015-0, (291-315), (2021).

Vignesh

1. J. E. Lerums and J. E. Dietz, "The Economics of Critical Infrastructure Controls Systems' Cyber Security," 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 2018, pp. 1-9, doi: 10.1109/THS.2018.8574159.
2. Venkatachary SK, Prasad J, Samikannu R. Economic impacts of cyber security in energy sector: A review. International Journal of Energy Economics and Policy. 2017;7(5):250-262.

Jainjie

1. Kumar, R., Baz, A., Alhakami, H., Alhakami, W., Agrawal, A., & Khan, R. A. (2021). A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application. Ain Shams Engineering Journal, 12(2), 2227-2240.
2. Davis, J. I., Libicki, M. C., Johnson, S. E., Kumar, J., Watson, M., & Karode, A. (2016). A framework for programming and budgeting for cybersecurity. RAND Corporation Santa Monica United States.

Pruthvi

1. Fouad, Noran Shafik. "The Security Economics of EdTech: Vendors' Responsibility and the Cybersecurity Challenge in the Education Sector." Digital Policy, Regulation and Governance 24.3 (2022): 259–273. Web
2. Hojda, Mihaela Hortensia. "Information Security Economics: Cyber Security Threats." Proceedings of the ... International Conference on Business Excellence 16.1 (2022): 584–592. Web

Review of the paper "Economic impacts of cyber security in energy sector: A review" presented by Vignesh in the group discussion illustrated the challenges of tackling cyber-attacks in energy sector. This helped in understanding real world scenarios of some of the approaches I learnt in my readings.