Cybersecurity Economics

Subjects: Computer Science, Interdisciplinary Applications | Economics | Computer Science, Cybernetics
Contributor: Mazaher Kianpour

Cybersecurity economics can be defined as a field of research that utilizes a socio-technical perspective to investigate economic aspects of cybersecurity such as budgeting, information asymmetry, governance, and types of goods and services, to provide sustainable policy recommendations, regulatory options, and practical solutions that can substantially improve the cybersecurity posture of the interacting agents in the open socio-technical systems.

Keywords: cybersecurity economics ; complex systems ; sustainable digital ecosystems ; information security economics

1. Cybersecurity Economics

A fundamental issue that must be addressed is what makes cybersecurity economics a single subject of investigation. Indeed, cybersecurity and economics each constitute distinct types of investigation, as reflected in the fact that they have long been studied as two separate disciplines by two large independent groups of researchers, respectively, information and computer scientists and economists. Therefore, there might be barriers to understanding how together they constitute a single field of study. It can be argued that cybersecurity economics should be understood as an interdisciplinary field of study that falls between and combines cybersecurity and economics. However, this perspective faces the problem that there is more than one conception of how different disciplines are related.

Cat [1] presented a taxonomy of possible conceptions: interdisciplinary, multidisciplinary, cross-disciplinary, and transdisciplinary. The strategy adopted by the scholars in this field is closest to the transdisciplinarity (i.e., a synthetic creation that encompasses work from different disciplines), which treats cybersecurity and economics as two different relatively independent systems of thinking that interact in a complex socio-technical system. A complex socio-technical system paradigm takes the interaction of different systems as the starting point and explains their relative interdependence regarding how they interact in social and technical settings. This paradigm enables us to capture the transformative effects that cybersecurity and economics might each have on one another[2]. To develop a more clear understanding of these effects, this section continues to elaborate on how cybersecurity started to draw from economics.

Insights in the field of cybersecurity economics empower decision-makers to make informed decisions that improve their evaluation and management of situations that may lead to catastrophic consequences and threaten the sustainability of digital ecosystems. By drawing on these insights, cybersecurity practitioners have been able to respond to many complex problems that have emerged within the context of cybersecurity over the last two decades. The academic field of cybersecurity economics is highly interdisciplinary since it combines core findings and tools from disciplines such as sociology, psychology, law, political science, and computer science.

2. History

The terms cybersecurity and information security are often used interchangeably. Solms and Niekerk argue that, despite the substantial overlap between cybersecurity and information security, the two concepts are not equal [3]. They posit that cybersecurity goes beyond traditional information security boundaries to include protecting information resources and other assets, including the human and cyber-physical systems. According to this viewpoint, which is also supported by the international standard ISO/IEC 27032:2012(E), in information security, a reference to the human factor usually relates to humans' role(s) in the security process. In cybersecurity, however, this factor has an additional dimension, namely the humans as potential targets of cyber attacks or even the humans that unknowingly participate in a cyber attack due to lack of awareness.

While ENISA concludes that there does not need to be a definition for cybersecurity [4], we provide a definition to avoid vagueness regarding what cybersecurity entails. Cybersecurity is basically the name of standard practices that involve the

people, processes, and technologies in an organization, in a group, or stand-alone environments in which the computers and cyber-physical systems with valuable data are connected to cyberspace. Cybersecurity deals with the different procedures that create a secure environment by protecting the assets. According to ISO/IEC 27002, an asset is anything that has value to an organization [5]. Assets can be categorized into different subtypes based on their convertibility (current and non-current assets), physical existence (tangible or intangible assets), and usage (operating or non-operating assets) [6]. Some assets are relation-specific. These assets are the results of one or both parties having made investments to support a particular relationship [7]. For example, people who work for a specific organization and learn skills that are valuable only for that specific organization are considered relation-specific assets. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.

Valuation of these assets and the risks of loss or damage have been controversial topics in cyber risk management and cybersecurity economics. The valuation methods vary based on cost [8], market [9], and utility [10] of the assets. With the rapid development of information technology, digital assets have been recognized as critical parts of organizations. However, cybersecurity is not limited to digital assets. In the last decade, the increasing number of cyberattacks against physical assets and critical infrastructures (e.g., Stuxnet, Industroyer, Triton, etc.) has indicated that cybersecurity can be labeled as a serious cyber and physical challenge for organizations and governments.

An accurate valuation of assets is central to efficient investment in protecting them, capital budgeting, and strategic planning. This is why this process is changed if poor decisions have been and/or are being made. Much of the published research on cybersecurity economics has been focused on the economic valuation of the assets and finding the optimal security investment level in organizations to protect those assets [11][12][13][14][15][16][17]. However, cybersecurity economics not only is concerned with whether an organization is spending enough to secure its assets and whether the security budget is spent on the right security measures and controls [18][19], but is also concerned with how a digital ecosystem and its operating agents function and behave. Cybersecurity economics covers the regulatory changes and competitive pressures (e.g., how cybersecurity can be aligned with broader business processes [20]). It studies how resource allocation by governments and businesses satisfies the requirements of creating a resilient cyber environment for themselves and other agents [21]. Furthermore, cybersecurity economics focuses on the efficiency surrounding the decisions made as a result of incentives and policies that are designed to maximize profit and trust within the environment [22].

3. Development

Currently, there is no consensus on a definition of the term cybersecurity economics. Multiple studies have created their definitions, most of which are broad. Probably the most accepted definition for cybersecurity economics is an area concerned with providing maximum protection of assets at the minimum cost [23][24]. However, Rathod and Hämäläinen adopted a wider perspective to the economics of cybersecurity based on strategic, long-term thinking incorporating economics from the outset [22]. They stated that cybersecurity economics and analysis provide benchmarks for the economic assessment of national and international cybersecurity audits and standards. It also provides policy recommendations to align policies and regulations to ensure trust within a digital environment. Additionally, Ahmed argues that cybersecurity economics addresses the issues of protection of Information and Communications Technology (ICT) applications designed to facilitate the economic activities that normally face cybercrimes that cost the companies and countries a significant amount of money and disturb the economic and financial activities around the globe, as has been indicated in ICT-based sustainable development [21].

Despite the many different definitions of cybersecurity economics, all of these studies point out that cybersecurity economic situations are characterized by direct and indirect interdependencies among the agents involved. Each agent's behavior affects the available options of other agents and even the results that they can achieve. Given a particular situation and different options, which option do agents choose and why? Does the outcome satisfy them? Does it unintentionally leave other agents worse off while it has been an optimal decision for some of them? To answer these questions, we would imply that it is crucial to be aware that cybersecurity economics covers a broader range of situations than exchanging products and services for money. Rather, this field of study includes organizations having to decide how to value their assets and scarce resources and adapt economic theories to practice in complex, uncertain environments.

Cybersecurity economics studies include forces motivating stakeholders to invest in cybersecurity provision; market structures and regulatory structures; and environmental, institutional, and distributional consequences of the social decision situation. The studies also investigate the cybercrime economics and motivation, tools, and interest of actors in today's underground marketplaces. All in all, this paper defines cybersecurity economics as a field of research that offers a socio-technical perspective on economic aspects of cybersecurity, such as budgeting, information asymmetry,

governance, and types of goods, to provide sustainable policy recommendations, regulatory options, and practical solutions that can substantially improve the cybersecurity posture of the interacting agents in the open socio-technical systems. A socio-technical perspective is essential for understanding and managing the state of cybersecurity today, as well as how to enhance it moving forward.

4. Core Issues

Kianpour et al. [25] identified seven core issues that have been subject to analysis under the field of cybersecurity economics:

- **Budgeting** is an integral part of running any business efficiently and effectively. A budget is an estimation of revenue and expenses over a specified future period of time, and it can be made for a person, a group of people, a business, or a government. The budget development process plays a vital role in setting goals, measuring outcomes, and planning for contingencies.

  – *Investment* is a part of an overall budget development and expenditure management processes. Finding optimal investment strategies to balance cybersecurity risks and spending in security measures and controls has been a topic of major importance in cybersecurity economics.
  – *Externalities* or spillover effects occur when the benefits or costs of providing cybersecurity are not fully reflected in the budget development process. Overcoming externalities, both from the public and private sectors, is important to avoid future budget deficiencies. Regulation is considered the most common solution to offset the effects of externalities [29].
  – Insurance is a contract in which an agent receives financial protection against losses from an insurance company. Insurance policies are used to hedge against cybersecurity risks and cover the business' liabilities in the event of a cyber attack. By increasing the severity of the financial consequences of cyber attacks, more businesses are turning to cybersecurity insurances. The literature on cybersecurity insurance has been focusing on determining how much cyber insurance businesses need to help insurers to understand the demand [30]. Moreover, the uncertainty of outcomes, reinsurance (i.e., insurers lay off the risk to another capital source), and scale are problems that would suggest an increase in prices, hardening risk transfer, and influx of capital.
- **Economic efficiency**, depending on the context, has various definitions in economics. For the sake of this review, we define economic efficiency as a situation in which no agent can make more profit without making at least one agent loss thereof.

  – *Misallocation of resources* indicates a state in which all resources are not allocated to serve each agent in the best way possible. The models that address this challenge are built based on the scarcity hypothesis. This hypothesis is the original source of methods such as zero-sum games, comparative advantages, marginal returns, and time discount.
  – *The type of goods* that cybersecurity would treat would significantly influence the overall structures and success of cybersecurity economic models. According to Samuelson, there are four types of economic goods: private, common, club, and public goods [31]. The controversial arguments on how cybersecurity should be treated based on Samuelson's typology started in the last two decades [32]. Any of these types raise issues that might result in reduced economic efficiency through misallocation of resources, inefficient cybersecurity provision, and potential national and international insecurity. For example, attempts at managing the free-riding problem and rent-seeking behavior is at the center of models that consider cybersecurity as a public good [33].
- **Interdependent risks** are common in today's hyper-connected world. The risks faced by anyone agent depend not only on its choices but also on those of all others with which it is directly or indirectly interacting.

  – *Network effects* are phenomena whereby increased numbers of people or participants improve the value of a good or service. Positive and negative network effects have been extensively studied within the context of software security economics [35].
  – *Lock-in effects* refer to situations in which users are dependent on a single vendor or supplier for a specific service or product and cannot move to another vendor without substantial costs. Recently, companies (e.g., Apple and Microsoft) increase their lock-in through security mechanisms. This phenomenon can be investigated in terms of control, governance, and dominance of organizations or groups such as Trusted Computing Group within the security value chain.
  – *Supply chains risks* associated with digital transformation of supply chains globally are increasingly becoming part of the enterprise risk listing and supply chain management. Modeling the target system, identifying threats, and analyzing countermeasures are three main issues that require systematic studies and socio-technical analyses to mitigate this type of risk [36].

- **Information asymmetry** deals with the situation where one party possesses more information than the other party. A lack of equal information results in adverse selection and moral hazards. All of these economic weaknesses have the potential to lead to market failure. Moral hazard is a situation where there is a tendency to take undue risks because the costs are not borne by the party taking the risk. Our tendency toward technological ubiquity, the unclear relationships between technology manufacturer and user, the inherent complexity of technology, and the network effects inherent to connected technologies are some of the factors that help this failure [26].
- **Governance** effectively coordinates the security activities of organizations and enables the flow of security information and decisions around them. Governance defines the rules and procedures for decision-making. Governance is important because it specifies the structure and distribution of rights and responsibilities among the different agents in the system.

  – *Coordination* among different agencies and stakeholders involved in performing cybersecurity functions and practices, such as response to threats or incidents and cyber crisis management, has been studied in terms of incentives, costs, and business alignment. However, there are still problems with regard to economic complexity of the coordination procedures and dependable enforcement of effective measures.
  – *Cybersecurity Policies, Regulations, and Rules (PRR)* are the areas that have involved public and private sectors in many forms of self- and co-regulations since the emergence of the internet. In this regard, the dominated notion is that cybersecurity policymaking and regulations require multifaceted strategies and recognition of the significant role that economic analysis plays to determine the actual need or effectiveness of these regulations [38].
- **Cybercrimes** are global and have strong externalities. Many academic studies and industrial documents examine the costs and losses caused by cybercrime. Some works estimate the overall costs, others evaluate the costs of individual countries, while industrial documents even measure losses of certain organizations regardless of or considering their size and technological development. For example, Reference[27] is one of the first studies measuring the costs of cybercrime. The authors continued this work seven years later to report major changes that significantly influenced the results of the original study [28].

- **Sustainability** of cybersecurity providers and services is increased by better formulation of business strategies and policies. For example, Reference[29] discusses how, to achieve sustainability of the digital ecosystems, finding a balance between the values obtained by the stakeholders is essential. If any of the stakeholders do not gain sufficient value, the entire ecosystem will collapse. Hence, promoting secure and sustainable properties is becoming a requirement in both development processes of cybersecurity products and services [30].

References

1. Cat, J. The Unity of Science. In The Stanford Encyclopedia of Philosophy; Zalta, E.N., Ed.; Metaphysics Research Lab, Stanford University: Stanford, CA, USA, 2017.
2. Von Solms, R.; Van Niekerk, J. From information security to cyber security. Comput. Secur. 2013, 38, 97–102.
3. Brookson, C.; Cadzow, S.; Eckmaier, R.; Eschweiler, J.; Gerber, B.; Guarino, A.; Rannenberg, K.; Shamah, J.; Gorniak, S. Definition of Cybersecurity-Gaps and Overlaps in Standardisation; ENISA: Heraklion, Greece, 2015.
4. ISO/IEC27002. Information Technology–Security Techniques–Code of Practice for Information Security Controls, (AS I SO/IEC 27002: 2015); International Organization for Standardization: Geneva, Switzerland, 2015.
5. Coulon, Y. Rational Investing with Ratios: Implementing Ratios with Enterprise Value and Behavioral Finance; Springer Nature: Cham, Switzerland, 2019.
6. Straub, D.; Rai, A.; Klein, R. Measuring firm performance at the network level: A nomology of the business impact of dig ital supply networks. J. Manag. Inf. Syst. 2004, 21, 83–114.
7. Moody, D.L.; Walsh, P. Measuring the Value of Information—An Asset Valuation Approach. In Proceedings of the Seven th European Conference on Information Systems (ECIS'99), Copenhagen Business School, Frederiksberg, Denmark, 2 3–25 June 1999; pp. 496–512.
8. Henderson, S.; Peirson, G.; Herbohn, K.; Howieson, B. Issues in Financial Accounting; Pearson Higher Education: Mel bourne, Australia, 2015.
9. Godfrey, J.; Hodgson, A.; Tarca, A.; Hamilton, J.; Holmes, S. Accounting Theory; Wiley and Sons: Hoboken, NJ, USA, 2 010.
10. Arora, A.; Hall, D.; Piato, C.; Ramsey, D.; Telang, R. Measuring the risk-based value of IT security solutions. IT Prof. 20 04, 6, 35–42.

11. Bistarelli, S.; Dall’Aglio, M.; Peretti, P. Strategic games on defense trees. In International Workshop on Formal Aspects i n Security and Trust; Springer: Berlin/Heidelberg, Germany, 2006; pp. 1–15.
12. Shirtz, D.; Elovici, Y. Optimizing investment decisions in selecting information security remedies. Inf. Manag. Comput. S ecur. 2011, 19, 95–112.
13. Huang, C.D.; Behara, R.S. Economics of information security investment in the case of concurrent heterogeneous attac ks with budget constraints. Int. J. Prod. Econ. 2013, 141, 255–268.
14. Ezhei, M.; Ladani, B.T. Interdependency analysis in security investment against strategic attacks. In Information Syste ms Frontiers; Springer: New York, NY, USA, 2018; pp. 1–15.
15. Li, Y.; Xu, L. Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. Int. J. Prod. Re s. 2020, 59, 1216–1238.
16. Schatz, D.; Bashroush, R. Economic valuation for information security investment: A systematic literature review. Inf. Sy st. Front. 2017, 19, 1205–1228.
17. Ekelund, S.; Iskoujina, Z. Cybersecurity economics–balancing operational security spending. Inf. Technol. People 2019, 32, 1318–1342.
18. Anderson, R.; Schneier, B. Guest Editors’ Introduction: Economics of Information Security. IEEE Secur. Priv. 2005, 3, 1 2–13.
19. Neubauer, T.; Klemen, M.; Biffl, S. Secure business process management: A roadmap. In Proceedings of the First Inter national Conference on Availability, Reliability and Security (ARES’06), Vienna, Austria, 20–22 April 2006; p. 8.
20. Ahmed, E.M. Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth. J. Knowl. Econ. 2020, 2020, 1–19.
21. Rathod, P.; Hämäläinen, T. A novel model for cybersecurity economics and analysis. In Proceedings of the 2017 IEEE I nternational Conference on Computer and Information Technology (CIT), Helsinki, Finland, 21–23 August 2017; pp. 27 4–279.
22. Gordon, L.A.; Loeb, M.P. The economics of information security investment. ACM Trans. Inf. Syst. Secur. (TISSEC) 200 2, 5, 438–457.
23. Bojanc, R.; Jerman-Blažič, B. A quantitative model for information-security risk management. Eng. Manag. J. 2013, 25, 25–37.
24. Bauer, J.M.; Van Eeten, M.J. Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommun. Poli cy 2009, 33, 706–719.
25. Marotta, A.; Martinelli, F.; Nanni, S.; Orlando, A.; Yautsiukhin, A. Cyber-insurance survey. Comput. Sci. Rev. 2017, 24, 3 5–61.
26. Samuelson, P.A. The pure theory of public expenditure. Rev. Econ. Stat. 1954, 36, 387–389.
27. Mulligan, D.K.; Schneider, F.B. Doctrine for cybersecurity. Daedalus 2011, 140, 70–92.
28. Asllani, A.; White, C.S.; Ettkin, L. Viewing cybersecurity as a public good: The role of governments, businesses, and ind ividuals. J. Leg. Ethical Regul. Issues 2013, 16, 7.
29. Rietveld, J.; Schilling, M.A. Platform competition: A systematic and interdisciplinary review of the literature. J. Manag. 2 021, 47, 0149206320969791.
30. Al Sabbagh, B.; Kowalski, S. A socio-technical framework for threat modeling a software supply chain. IEEE Secur. Pri v. 2015, 13, 30–39.
31. Vagle, J.L. Cybersecurity and Moral Hazard. Stanf. Tech. Law Rev. 2020, 23, 71.
32. Brito, J.; Watkins, T. Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy. Harard Natl. Secur. J. 2011, 3, 39.
33. Anderson, R.; Barton, C.; Bölme, R.; Clayton, R.; Ganán, C.; Grasso, T.; Levi, M.; Moore, T.; Vasek, M. Measuring the Changing Cost of Cybercrime. In Proceedings of the 18th Annual Workshop on the Economics of Information Security, Boston, MA, USA, 3–4 June 2019.
34. Kumar, R.; Baz, A.; Alhakami, H.; Alhakami, W.; Agrawal, A.; Khan, R.A. A hybrid fuzzy rule-based multi-criteria framew ork for sustainable-security assessment of web application. Ain Shams Eng. J. 2021, 12, 2227–2240.