What's New in the Economics of Cybersecurity?

Observational and Empirical Studies

Massimo Felici and Nick Wainwright | HP Labs
Fabio Bisogni and Simona Cavallini | Fondazione FORMIT

New developments are substantially increasing our dependence on technologies and services and giving rise to new risks and security challenges that require further investigation of the social, technical, and economic aspects of the cyberworld. On the one hand, efficient and effective technology benefits both consumers and providers. On the other hand, new and severe security threats and vulnerabilities might expose consumers and providers to losses and unwanted consequences.

In response to the changing cybersecurity challenges, spending on information security has grown steadily and might eventually reach a point that's inefficient and unaffordable. Furthermore, both governments and market-oriented organizations must carefully balance tradeoffs between security and privacy. A better understanding of these new socio-technical-economic complexities is urgently needed, requiring both reconsideration of traditional cybersecurity issues and investigation of new and unexplored research directions.

This special issue on observational and empirical studies—together with the forthcoming special issue on the roles of cyberactors and intermediaries—highlights research insights that guide the exploration of the economics of cybersecurity.

Looking Forward

The new style of research and development provides the foundation for what we describe as "laboratories in the economics of cybersecurity," which will explore emerging socio-technical-economic issues and challenges. These laboratories will support multidisciplinary research involving large-scale experiments in the economics of cybersecurity. A collaborative effort is necessary to address questions that tackle multifaceted cybersecurity economics issues, including the following:

 Copublished by the IEEE Computer and Reliability Societies

- How does cybersecurity economics, among other factors, affect organizational practices? Investigating the economic impact of cyberattacks that exploit vulnerabilities in complex threat scenarios provides insight that informs organizational practices as well as mechanisms, such as incentives, that mitigate risk exposure and promote security.
- Which economic tools can be adopted operationally in cybersecurity? Different approaches, both qualitative and quantitative, capture specific cybersecurity representations—for instance, metrics, models, and theories—that inform economic knowledge. Tools based on such economic knowledge, and experiences of adopting and developing them, can highlight cybersecurity's operational aspects. Economic tools link development and operation of technologies and services and inform decision-making processes.
- Which cybersecurity economic insights transfer across different areas? Experiences from different sectors and industries (for instance, critical infrastructures, information and communication technologies, and dependable systems) support economic analyses of cybersecurity that are relevant in the cyberworld. Sharing experiences and supporting cross-fertilization initiatives help us identify emerging cyberthreats and address them economically.
- Which cybersecurity economic insights shape the cybersociety? Combining social, technical, and economic aspects of cybersecurity highlights the economics that shape cyberspace. Cyberactors, including consumers and providers, have different responsibilities and exposure to emerging threats. Economic insights help us understand how actors are positioned in cyberspace.

Emerging Insights in the Economics of Cybersecurity

This special issue discusses economic aspects of cybersecurity, taking into account emergent dynamics in the cyberworld. It touches on cyberactors' changing roles and their interactions concerning cybersecurity, including economic benefits and costs as well as incentives and investment alternatives. Emerging business models, economics and opportunities in technology provision and deployment, and services across sectors and industries depend on the economics of cybersecurity including costs and benefits involved in adopting such technologies and services, potential investment alternatives and their returns, behavioral aspects of actors dealing with security and privacy issues, effects of privacy and security regulations, and economic accountability of various cyberworld actors.

The studies described in this special issue extend and advance research in the domain of economics of cybersecurity and related areas such as economics of information security.[1] Over the past decade, new technologies and services, such as cloud computing, big data, and social media, have revolutionized the cyberworld. The increased dependence on such technological developments exposes citizens, governments, and industries to new threats. Understanding the economics of cybersecurity helps us develop responses to these new threats, guide cybersecurity investment, and evaluate risks and benefits of new technologies. This special issue also aims to support cross-fertilization among research communities such as those contributing to the Workshop on the Economics of Information Security. The articles span application domains, such as information and communication technology, critical infrastructure, security, transport, healthcare, and education, and link individuals working in security research and technological operations.

This issue, which highlights observational and empirical studies, and the forthcoming companion issue, which will explore the roles of cyberactors and intermediaries in depth, builds on novel contributions of researchers, practitioners, and policymakers. The articles in these special issues exemplify the type of research needed to advance our understanding of the economics of cybersecurity.

In This Issue

The articles in this issue highlight different aspects of the economics of cybersecurity. Two principal perspectives are security and privacy, which are often depicted as competing or conflicting with one another. Understanding the economics of security and privacy highlights their interdependencies. The uneven distribution of costs and incentives of cybersecurity stress the different cyberactors' roles and economic exposures. The economics of privacy is often overlooked by users, who tend to take for granted the privacy associated with service usage. Empirical studies on the economics of security and privacy are necessary to advance the economics of cybersecurity. Observational, empirical, and behavioral models can support decision-making processes and early assessment of security policies.

The article "Economics of Fighting Botnets: Lessons from a Decade of Mitigation," by Hadi Asghari and his colleagues, focuses on the economics of security, assessing ISPs' critical role in effective mitigation. ISPs are in a more central and convenient position than end users to address vulnerabilities by implementing security policies. Security policies and economic incentives must account for how different cyberactors are positioned. This would result in alternative governance and organizational models addressing cybersecurity threats.

"The Value of Web Search Privacy," by Sören Preibusch, focuses on the economics of privacy, reporting on a laboratory experiment assessing how much individuals

value the privacy of information when performing Web searches. The study emphasizes that although individuals value privacy differently, most assume that privacy shouldn't have a cost. In this respect, individuals perceive security and privacy similarly—that is, they're assumed to be part of a service rather than an optional feature.

"Improving Security Policy Decisions with Models," by Tristan Caulfield and David Pym, addresses the economics of security policies, pointing out how models inform decision-making processes in evaluating security policies' economic operational impact. The authors emphasize the necessity of understanding other security policies and their economic implications once in operation. Economics is a distinguishing element of decision-making processes when evaluating alternative operational security policies.

The remaining two articles provide economic insights from different domains: critical infrastructure and aviation. "Assessing a Potential Cyberattack on the Italian Electric System," by Clementina Bruno and her colleagues, concerns the often underestimated cost of security attacks. Simulating potential security attacks to critical infrastructures highlights their wide impact on productive activities across targeted geographical areas as well as modern organizations' and societies' high economic interconnectivity and vulnerability. Martina De Gramatica and her colleagues' article "IT Interdependence and the Economic Fairness of Cybersecurity Regulations for Civil Aviation" concerns the fact that the cost of security regulations might impact regions and infrastructures differently, depending on their position and role in the infrastructures. These articles emphasize the importance of cross-fertilization and sharing of experiences across domains.

Focusing on the economics of security in critical infrastructures, Bruno and her colleagues discuss the economic impact of security threats on the electric grid and the surrounding geographic areas. A simulated attack's economic effect extends beyond the direct electric system to the areas affected by consequential power cuts. Economic assessment of security threats involves both direct and indirect costs, for example, those incurred by other industrial activities. However, predicting the extent of any security attack and the areas affected might be difficult. This emphasizes the complexity of security threats and attacks, whose economic impact might propagate across system and organizational boundaries.

De Gramatica and her colleagues present a study on the economic impact of security regulations across airports. Different schemes have economically supported physical security in aviation; the authors question whether similar schemes should be introduced to support the economics of cybersecurity in aviation. The results highlight how economic implication can differ

depending on the airport implementing the required cybersecurity regulations. Cybersecurity regulations must consider the economic impact for different actors affected by such regulations and responsible for implementing them. Again, the emphasis is on how to diversify the economics of cybersecurity across physical and cyberspaces and their actors.

The articles in this special issue, together with those in the companion issue, highlight the need for large, complex observational and empirical studies and represent the kind of studies that will advance our understanding of cybersecurity economics. There is a need for similar work on a larger scale and providing further foundational data for future work. We believe that the way forward is to support laboratories in the economics of cybersecurity that engage in the following:

- Observational and empirical studies involving analyses and observations of behavioral aspects of the economics of cybersecurity. These studies must consider new technological developments, such as cloud computing, big data, social networking, and the Internet of Things, and the rapidly changing industry.
- Validations that elicit detailed hypotheses characterizing the economics of cybersecurity. Often, the efficacy and effectiveness of security and privacy technologies, policies, and business models remain unsupported by detailed validation studies that would ease deployments of security and privacy technologies in the cyberworld.
- Impact and deployment assessments advancing knowledge on the economic risk associated with security threats and vulnerabilities. This knowledge supports decision-making processes and technological deployments based on the economics of cybersecurity. ■

Reference

1. R. Anderson and B. Schneier, "Guest Editors' Introduction: Economics of Information Security," *IEEE Security & Privacy*, vol. 3, no. 1, 2005, pp. 12–13.

Massimo Felici is a research engineer at HP Labs Bristol. Contact him at massimo.felici@hp.com.

Nick Wainwright is a research director at HP Labs Bristol. Contact him at nick.wainwright@hp.com.

Fabio Bisogni is a member of the board at Fondazione FORMIT. Contact him at f.bisogni@formit.org.

Simona Cavallini is head of research and innovation at Fondazione FORMIT. Contact her at s.cavallini@formit.org.