Back to the Roots: Information Sharing Economics and What We Can Learn for Security

Rainer Böhme
University of Innsbruck, Austria
rainer.boehme@uibk.ac.at

EXTENDED ABSTRACT

In a world where cybersecurity can be reduced to a race for information, defenders with different information sets can benefit from sharing what they observe and know. However, defenders supposedly share less than what is socially desirable, thereby leaving parts of society insufficiently protected. The reason for this behavior is almost certainly not a lack of technology to facilitate information exchange. Even an occasional mismatch between information needs and information supply cannot fully explain why defenders share so little information. The key obstacle is economics: defenders often have few incentives to share security information.

Back in the 1980s, economists have extensively studied general information sharing between firms, often with the involvement of intermediaries, such as trade associations. These models have been taken up in the 2000s when information security emerged as a new application domain for economic reasoning. The bottom line of most economic models is that information sharing is very fragile, which concurs with our perception of reality. As current policy initiatives seek to improve information sharing, and the topic has gained enough attention to merit a specialized workshop in its third year, I take the opportunity and revisit the "old" models, their assumptions and implications, in order to derive possible new directions for future research. After all, security information is a very special good, which might call for tailored models: maybe there are better ways to conceptualize Information Sharing Analysis Centers (ISACs) than reducing them to trade associations?

A main thread of the keynote is to systematize modeling approaches. I take Gal-Or & Ghose (GG) [1] and Gordon, Loeb & Lucyshyn (GLL) [2] as starting points. Both teams study a two-firm economy, the simplest possible model for analyzing information sharing. In this model, the firms choose independently if they share information, in anticipation of the respective other firm's choice, leading to a game-theoretic setup. Common (and limiting) assumptions are that firms pre-commit to sharing (i. e., they cannot condition the sharing decision on their observed value), firms share truthfully if they do (i. e., they cannot lie about the observed value), and attackers are outsiders (i. e., they do not see information flows). The GG and GLL models differ in the mechanisms that generate economic payoffs for the firms depending on the joint action. This is closely connected to the notion of externalities, a key concept in economics that controls how private and public benefits are aligned. I use a diagram (see Figure 1) to explain at which phases of the discrete-time game externalities emerge in different models (gray parts).

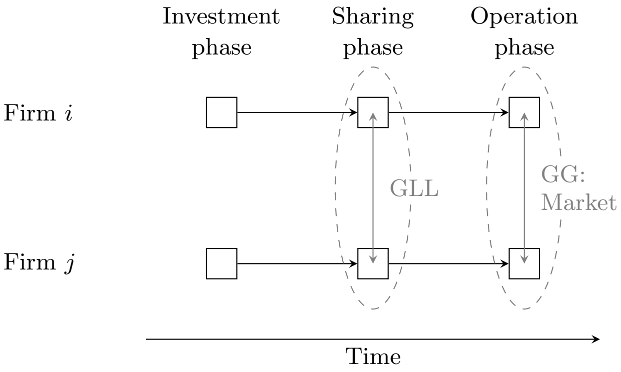

Figure 1: Illustration of the modeling space

GG follow the conventions in the economic literature and link both firms in the operation phase, where they compete on the market. Both firms anticipate this oligopolistic competition and strategically adjust their choices to the actions of the other firm. This includes, but is not limited to the decision to share information. GG assume that firms' knowledge about the information security quality of their products is the relevant item to share (or not) with their competitor before both firms commit to prices and quantities. They further assume that all customers are aware of and consider this quality in their purchase decisions, which creates the link between information security properties and demand for a product (or service, if one extends the interpretation to cloud service providers, for instance). Payoffs realize in the form of profits generated on the market.

By contrast, GLL model payoffs more directly as expected prevented losses due to security breaches. They do not require that both firms meet on a market. Consequently, their economy does not model any link between both firms unless they start to share security information. This information leverages the receiving firm's security investment. One can

WISCS '16, Vienna, Austria

ACM ISBN 978-1-4503-4565-1/16/10.
DOI: http://dx.doi.org/10.1145/2994539.2994540

think of an intrusion detection system that works best if fed with new and relevant threat signatures. As firms optimize jointly on sharing and security investment, GLL find that both choices are substitutes: more information sharing leads to lower security investment because sharing makes every unit of security investment more effective. So, firms who share need to spend less to target the same breach probability.

In both models, sharing is never a socially optimal equilibrium. To reach this desirable outcome, sharing must be mandated. This calls for additional elements in the models to justify government intervention. (Oligopolistic markets, as in the GG model, should rather curb than stimulate information sharing for anti-trust reasons.) A canonical reason for intervention are failed markets, and the presence of externalities generated by the technology itself can be a sufficient condition for market failure.

This is why in our ongoing research, we chose to introduce externalities at the investment phase of Figure 1 when studying the economics of mandatory information sharing *with authorities.* We built upon the interdependent security model introduced by Kunreuther and Heal [3]. In this model, firms anticipate that the probability of suffering a security breach depends on their own as well as others' security investment. In our information sharing model, payoffs are expected prevented losses, like in GLL, but including the cost of reputation losses if shared breach information becomes public, as provided in GG. (Another interpretation for this cost factor is privacy risk.) A positive effect of information sharing is modeled as a leverage of security investments, although this channel works indirectly in practice, with the authority serving as gatekeeper and aggregator. Another tweak to add realism is to distinguish between preventive and detective security investments [4].

Taking a broader perspective, arguably, most modern economies are in constant races for information. Financial markets have become institutions to aggregate and process this information. In the outlook of the lecture, I comment on market approaches for security information sharing. This includes not only markets where sensitive information is traded directly, which has many caveats and may raise ethical concerns if malicious parties cannot reliably be excluded from the market. Creating instruments that allow for trading on security outcomes may be a promising alternative.

To conclude, it remains difficult to specify stylized models where defenders share information voluntarily, and the situation gets worse if more realistic assumptions are introduced, such as attackers being part of the game. This reflects that security information sharing is very fragile. Its biggest obstacles are economic (dis)incentives, not a lack of technology. Regulations that aim at solving this sharing dilemma should try to fix causes, not symptoms.

Acknowledgment.

I thank Stefan Laube for very helpful comments.

References

[1] Esther Gal-Or and Anindya Ghose. "The economic incentives for sharing security information". In: *Information Systems Research* 16.2 (2005), pp. 186–208.

[2] Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn. "Sharing information on computer systems security: An economic analysis". In: *Journal of Account-ing and Public Policy* 22.6 (2003), pp. 461–485.

[3] Howard Kunreuther and Goeffrey Heal. "Interdependent security". In: *Journal of Risk and Uncertainty* 26.2/3 (2003), pp. 231–249.

[4] Stefan Laube and Rainer Böhme. "Mandatory security information sharing with authorities: Implications on investments in internal controls". In: *2nd Workshop on In-formation Sharing and Collaborative Security (WISCS).* Denver, CO, USA: ACM, 2015.