Summary

Over the last decade an increasing amount of cyber attacks threatened the functioning of the global economy. It is hard for organizations to determine their 'optimal' level of security. In order to attain this, this study advocates that information related to the nature of cyber risk and the return on investment of measures to reduce it diffuses among relevant actors, while taking into consideration the costs of doing so. Currently, there is insufficient information diffusion in cyber security. This study seeks to identify solutions for the efficient stimulation of cyber security information diffusion. The strong public good characteristics of information diffusion - the diffuser of information has little benefits from diffusing it - complicate this endeavour.

In order to fulfil this promise, *law and economics* must gain a deeper link with the *economics of cyber security*. Scholars in the economics of cyber security should benefit from the development of theory and methodology within law and economics. Scholars in law and economics should learn from the insights regarding the dynamics, empirics and microeconomic peculiarities of cyber risk of the economics of cyber security. There need to be significant efforts to link the fields because there is a large gap to be bridged.

This *law and economics of cyber security* has the task to further formulate common 'cyber security information diffusion' agenda for university, government and industry. Each party within this 'triple helix' has different roles, responsibilities and tools to stimulate information diffusion. The deployment of the individual tools of these three parties combined with their mutual cooperation will yield the most fruitful results. This study made a first modest step in doing so in its three substantive parts.

Part I epitomizes the role of university and presents a pioneering analysis that unlocks six characteristics in the literal text of 71 data protection laws. It diffuses information about the data protection law and discloses it for statistical analysis, which is beneficial to the connection of law and economics with the economics of cyber security. Hereafter, Part II exemplifies the role of government and studies the EU data breach notification law embedded in the general data protection regulation. The study revealed that the EU data breach notification law could incentivize organizations to stimulate information diffusion, provided that it wisely enforced by the national data protection authorities. I urge the data protection authorities to look at tailor made carrots and the expressive function of the law as alternative incentive schemes. Also, the threshold for notifying to individuals needs to be fairly high and clear-cut. Last, Part III focuses on industry, more specifically cyber risk insurance and pooling, which is risk shifting without the interference of an insurer. The empirical analysis on cyber insurance shows that the market for small- and medium enterprises is still in its infancy and that information diffusion between the insurer and insured is limited.

Cyber risk pooling could play an important role in situations when organizations have more or equal information about cyber risk as insurers. Cyber risk pooling can potentially move organizations to desirable (hybrid) forms of risk allocation where also individual management and cyber insurance play a role. The analysis sketches which specific conditions and design issues have taken into account regarding pooling.