LockChain technology as one source of truth for Cyber, Information Security and Privacy

Yuri Bobbert[1] and Nese Ozkanli[2]

[1] Antwerp Management School, Belgium
[2] Open University, Netherlands
yuri.bobbert@uantwerpen.be
nese.ozkanli@gmail.com

Abstract: Implementing and maintaining Information Security (IS) in a digitized ecosystem is cumbersome. Multiple complex frameworks and models are used to implement IS, but these are perceived as hard to implement and maintain in digitized dynamic value chains and platforms. Most companies still use spreadsheets to design, direct and monitor their information security function and demonstrate their compliance. Regulators too use spreadsheets for supervision. This paper reflects on longitudinal Design Science Research (DSR) on IS and describes the design and engineering of an artefact architecture, coined as LockChain, which can emancipate boards from silo-based spreadsheet management and improve their visibility, control and assurance via integrated dash-boarding and a reporting tool. LockChain is not a traditional Information Security Management System (ISMS) but is used for the design and specification of information security requirements and measures and privacy requirements. We elaborate “Why” we used Design Science Research into valorisation of the concept of LockChain, we explain “What” we have established in terms of the technology of LockChain and ”How” it is applied and the added value LockChain brings for companies on cost savings, Security and Privacy by Design engineering culture and Digital Assurance.

Keywords: Information Security Controls, Security Requirements, Security Measures, Security by Design, Privacy by Design, Digital Assurance.

This paper is accepted to publish in the Proceedings of 2020 Computing Conference in the series "Advances in Intelligent Systems and Computing". After publication, the proceedings will be submitted for indexing to ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springerlink.

The full paper will be available Q3 2020 via Springer and https://saiconference.com/Computing2020