6th International Conference on Future of
BUSINESS, MANAGEMENT & ECONOMICS

ICFBME
19 - 21 July 2024
Copenhagen, Denmark

Digital Risks and Corporate Governance: Towards Ubiquitous Cyber Risk Management in Companies' Governance

Elena F.Pérez Carrillo
University of Leon and CERGI (University of Santiago Compostela)

Abstract

The systematisation of corporate governance tools to control digital risk has advanced hand in hand with the increasing use of international standards such as ISO 27000 (and the related family). Also, under the influence of the old Network and Information Systems Security (NIS) Directive which, although superseded by a new NIS2 (in 2022), established protection schemes whose influence continues. The European corporate cybersecurity methodology is based on a combination of governance obligations, strategic obligations, implementation of management tools (continuity plans, recovery plans, etc.), and a set of notification and transparency obligations. This presentation provides an overview of the new obligations of strategic management, internal monitoring, auditing, cyber intelligence, and incident and threat reporting that are changing business management and especially corporate governance, first in strategic sectors, business sectors (such as finance), and then in all other companies. The new cybersecurity management landscape is set to modulate the demands on the care and loyalty of corporate managers, business judgement rule, and the demands on managers and executives.

Keywords: Cybersecurity, EU Regulation of Digital Risks, DORA Regulation, Networks and Systems Security, ISO 27000