Digital and Cybersecurity Governance Around the World
Other titles in Annals of Corporate Governance

*Enterprise Foundations: Law, Taxation, Governance, and Performance*
Steen Thomsen and Nikolaos Kavadis

*Beyond ESG: Reforming Capitalism and Social Democracy*
Marcel Boyer
ISBN: 978-1-68083-894-7

*The Social Purpose of the Modern Business Corporation*
Peter J. Buckley
ISBN: 978-1-68083-874-9

*Decentralized Autonomous Organizations: Internal Governance and External Legal Design*
Wulf A. Kaal
ISBN: 978-1-68083-798-8

*Decentralized Corporate Governance via Blockchain Technology*
Wulf A. Kaal
ISBN: 978-1-68083-676-9
Digital and Cybersecurity Governance Around the World

Bob Zukis
Digital Directors Network, and
USC Marshall School of Business
bob@digitaldirectors.network

Full text available at: http://dx.doi.org/10.1561/109.00000032
Annals of Corporate Governance
Volume 7, Issue 1, 2022
Editorial Board

Editors-in-Chief
Marc Goergen  Geoffrey Wood
IE Business School  Western University
Spain  Canada

Founding Editor
Douglas Cumming
Florida Atlantic University, USA

Senior Editors
Renee Adams
University of Oxford
Lucian Bebchuk
Harvard University
William Judge
Old Dominion University
Mark Roe
Harvard University
Rene Stulz
Ohio State University
James Westphal
University of Michigan

Editors
Amedeo de Cesari
Alliance Manchester Business School
Patricia Gabaldon
IE Business School
Aleksandra Gregoric
Copenhagen Business School
Anna Grosman
Loughborough University
Zulfiquer Haider
Western University
Hang Le
Nottingham Business School
Ben Sila
Edinburgh University Business School
Moshfique Uddin
Leeds University
Editorial Scope

Topics
Annals of Corporate Governance publishes articles in the following topics:

- Boards of Directors
- Ownership
- National Corporate Governance Mechanisms
- Comparative Corporate Governance Systems
- Self Governance
- Teaching Corporate Governance

Information for Librarians
Annals of Corporate Governance, 2022, Volume 7, 4 issues. ISSN paper version 2381-6724. ISSN online version 2381-6732. Also available as a combined paper and online subscription.
# Contents

1 Introduction 2

2 Digital Economies and the Case for Digital and Cybersecurity Governance 6
   2.1 The Advancement of Digital Economies 7
   2.2 Defining and Calculating the Digital Economy 11
   2.3 The Digital Value Business Case for Corporate Boards 13
   2.4 New Digital Worlds Bring New Risks 18

3 Boardroom Mechanisms for Digital and Cybersecurity Governance 23
   3.1 Digital and Cyber Governance Leading Practices 24
   3.2 Defining the Digitally Savvy Director 31
   3.3 The Technology and Cybersecurity Committee 33
   3.4 Calculating the Projected Economic Losses from Cyber Risk 35
   3.5 Governing Systemic Risk in Complex Digital Business Systems 37

4 Self-Regulation: National Codes and Other Standards 50
   4.1 Australia 52
   4.2 Japan 53
Digital and Cybersecurity Governance Around the World

Bob Zukis

Founder and CEO, Digital Directors Network, and Adjunct Professor, USC Marshall School of Business, USA; bob@digitaldirectors.network

ABSTRACT

In countries around the world, economic dependency and growth is increasingly reliant upon the modern digital systems that power and enable services, products, and markets. Implementing and protecting these digital systems requires competent and capable public and private sector leadership actively governing the opportunities and risks of the digital future. While a small assortment of private sector corporate governance policies and practices exist worldwide related to digital and cybersecurity oversight, the broad-based application of structured boardroom oversight of these issues is both underdeveloped and underapplied and significantly lags the reality of how these technologies are impacting companies and societies in the modern world. This monograph coalesces some of the scattered but representative guidelines, rules and practices that are in existence in digital and risk governance. It also documents some of the recent developments in observed practices and regulatory rulemaking to develop a framework for digital and cybersecurity governance to develop this area as a necessary component of effective corporate governance worldwide.

GDP and long-term business growth are increasingly dependent upon the complex digital systems that power and enable economies, companies, products, and services worldwide. Private enterprise is a leading part of the system that advances digital economies as businesses invest and innovate to adopt and apply Information and Communication Technologies (ICT) that create value for their investors and stakeholders.

However, many corporate boards are not actively or effectively governing digital and cyber risk as they struggle to understand and oversee the far-reaching implications of these technologies. Complex digital systems now support and directly power the operating systems that provide for many basic necessities in the modern world. The growing sophistication of cyber-attackers and their attacks threatens not just digital infrastructure, but the way of life for billions as the basic utilities that serve fundamental human needs and wants are also at risk because of digital risk.

Corporate governance practices and policies surrounding digital and cyber risk oversight are underdeveloped globally and where they do exist, they are sporadically adopted and applied. As the pace of digital change continues to accelerate, the reality of global corporate
governance practices in digital and cyber risk oversight is that they significantly lag the dependencies we have upon digital technologies and their impacts. Corporate directors worldwide have statutory and fiduciary obligations to effectively govern their organizations and the implications of these issues. Not only does digital and cyber governance immaturity threaten the digital growth and progress that has been made to date, but it jeopardizes further advancements in realizing the full potential of the digital future.

COVID-19 and war in Ukraine have also served to expose, amplify, and reinforce some of the issues facing global boardrooms on digital and cybersecurity risk oversight. In a global survey of board governance issues during COVID-19, the Singapore Institute of Directors said (Marsh and McLennan, 2021):

"Digital readiness, or the lack of it, was exposed by the rapid shift to remote business operations. During the initial lockdown, many companies scrambled to ensure business continuity and workforce productivity under work-from-home conditions. While some boards oversaw the process of getting their companies to ramp up their digital capabilities and adapt to new business models, such as boosting online presence and exploring new markets, others decided to wait out the crisis, to their cost."

As the war against Ukraine continues, experts in cybersecurity warn that “…the potential remains for dramatic cyber attacks intended to demoralize Ukraine or countries supporting Ukraine” (Accenture, 2022).

Despite this challenging and changing cyber risk landscape, the benefits to humanity of digital technologies are becoming more apparent. While there are challenges in measuring the digital economy that include the existing conceptual boundaries of GDP, the prices of new and improved digital products, and unrecorded digital sector output (International Monetary Fund, 2018), the digital economy is already a significant direct and indirect contributor to global GDP. Analysts project that over 60% of global GDP is now digitized.

Consumers and citizens are experiencing digital transformation first-hand as the adoption of modern information and communication
technologies like the smartphone have been far faster than prior advancements in similar consumer information technologies. Nevertheless, the early development of the digital economy has been uneven in emerging, developing, and developed economies worldwide. Other gaps in adoption and impact have been identified between men and women, private and public sectors, and urban and rural areas (UNCTAD, 2019).

The policies and programs that governments adopt to support and secure their ICT industry play a vital role in developing digital economies. Notwithstanding recent regulatory restraints imposed on their technology sector, China has demonstrated unprecedented momentum towards the digital future. Other countries, such as the United States, are facing risks that could slow down the progress that they have already made (Chakravorti et al., 2020).

The adoption of these technologies by the companies operating within these countries has also been as uneven as many national efforts. Corporate progress even lags government responses in many respects. Regardless of the pace of change taking place in any company’s journey to becoming a digital business, every boardroom still must understand and govern the digital and cybersecurity risks shaping the world around it. As the promise and potential of the digital future continue to work through its growing pains, its dangers are on full display. Attackers are freely exploiting weaknesses in digital systems and capitalizing on the far-reaching damages that they can inflict. Attackers are growing more sophisticated and include nation-states and well-organized, resourceful, and persistent amateur and professional groups. Industry reports pronounce that cybercrime will cost the global economy USD 10.5 trillion annually by 2025, making cybercrime the equivalent of the third-largest economy in the world, behind the U.S. and China (Morgan, 2020).

Cyber attackers are also exploiting systemic risk in new ways. Systemic risk is a dynamic new enterprise risk management challenge threatening every organization through its larger connected ecosystem. While some boardrooms are responding to these digitally driven and influenced challenges, many are not. As digital technologies and systems continue to transform economies and society, business dependence and reliance upon them will only continue to grow, as will their risks. Whether driven by a lack of understanding of the issues or uncertainty
in how to respond, corporate governance is lagging in addressing these powerful forces of digital change.

Corporate governance policy and practice needs to rapidly advance to reflect the reality of the benefits and risks impacting humanity as a result of digital technologies. This monograph is intended to establish a baseline of the emerging issues and leading digital and cybersecurity governance practices to jumpstart this development. Documenting and aligning the current fragmentary nature of digital and cyber risk practices and policies worldwide can help bring clarity to this emerging area of corporate governance. It will help establish a foundation which can then be built upon by policymakers and boardrooms to govern their economies and businesses safely and securely into the digital future.

This monograph starts by analyzing some of the work being done to study and isolate the digital aspect of economies to illustrate what is at stake. Various existing boardroom practices and policies in digital and cyber risk oversight are then identified to bring some transparency to the work already being done to improve how corporate boards govern these issues. Select national codes and standards from a diverse group of countries is then highlighted together with emerging regulatory trends to illustrate the widely acknowledged nature of this problem from practitioners and regulators.

It is intended that this monograph contributes to a structured approach to understanding these issues to create a framework for more specific solutions that can be broadly implemented to advance digital and cyber risk governance.
References


Cyentia Institute LLC (2020). *IRIS 20/20 Extreme: Analyzing the 100 Largest Cyber Loss Events of the Last Five Years*. Cyentia Institute LLC.


Ho, J. (2021). Corporate boards: Don’t underestimate your role in data security oversight. Contrary to popular belief, data security begins with the Board of Directors, not the IT Department.


Full text available at: http://dx.doi.org/10.1561/109.00000032