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
ISBN: 978-1-68083-942-5

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

now
the essence of knowledge
Boston — Delft

Annals of Corporate Governance

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

B. Zukis. *Digital and Cybersecurity Governance Around the World*. Annals of Corporate Governance, vol. 7, no. 1, pp. 1–92, 2022.

ISBN: 978-1-63828-047-7

Annals of Corporate Governance
Volume 7, Issue 1, 2022

Editorial Board

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

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.

Bob Zukis (2022), "Digital and Cybersecurity Governance Around the World", Annals of Corporate Governance: Vol. 7, No. 1, pp 1–92. DOI: 10.1561/109.00000032.

1

Introduction

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

117th Congress (2021). *S. 808 Cybersecurity Disclosure Act of 2021*. URL: https://www.congress.gov/bill/117th-congress/senate-bill/808/text.

Accenture (2022). *Global Incident Report: Russia-Ukraine Crisis | April 21*. Accenture.

Ang, C. (2021). *The Most Significant Cyber Attacks from 2006–2020, by Country*. URL: https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/.

Bayarma, A., C. Hubers, T. Schwanen, and D. E. Martin Dijst (2011). "Anything, anywhere, anytime? Developing indicators to assess the spatial and temporal fragmentation of activities (Alexander Anything Spatial and Temporal Relevance, P. 1: 1250)". *Environment and Planning*: 678–705.

BNP Media (2020). *Security*. (B. Media, Producer) Security: URL: https://www.securitymagazine.com/articles/93062-ransomware-victim-travelex-forced-into-bankruptcy.

Bordoff, J. (2021). *Foreign Policy Voice*. URL: https://foreignpolicy.com/2021/05/17/colonial-pipeline-crisis-cyberattack-ransomware-cybersecurity-energy-electicity-power-grid-russia-hackers/.

Braue, D. (2021). *ACS Information Age*. ACS Information Age: URL: https://ia.acs.org.au/article/2021/hold-company-directors-liable-for-cyber-attacks.html.

Brynjolfsson, E. and A. McAfee (2011). *Race Against the Matchine: How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Emplyoment and the Economy*. Lexington, Massachusetts, USA: Digital Frontier Press.

Chakravorti, B., R. Shankar Chaturvedi, C. Filipovic, and G. Brewer (2020). *Digital in the Time of Covid: Trust in the Digital Economy and Its Evolution Across 90 Economies As the Planet Paused for a Pandemic*. Medford, MA: The Fletcher School at Tufts Unviersity.

Chen, K. D. and A. Wu (2016). *The Structure of Board Committees*. Boston: Harvard Business School.

CMS Law (2022). *Enforcement Tracker*. GDPR Enforcement Tracker: URL: https://www.enforcementtracker.com/?insights.

CNA Financial Corporation (2021). "Form 10-Q". In: *Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934*. Chicago, IL, USA.

Commonwealth of Australia (2021). *Strengthening Australia's Cyber Security Regulations and Incentives—A Call for Views*. Commonwealth of Australia.

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

Dezan Shira & Associates (2021). *The PRC Personal Information Protection Law (Final): A Full Translation*. URL: https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/.

Digital Directors Network (2019). Systemic Digital Risk: Understanding and Overseeing Complex Digital Environments with the DiRECTOR™ and RISCX™ Frameworks.

Digital Directors Network (2021a). Boardroom Solutions: URL: https://www.digitaldirectors.network/cpages/briefings.

Digital Directors Network (2021b). *Digital Governance Maturity Model*. Los Angeles: DDN LLC.

Dittmar, J. (2011). *Information technology and economic change: The impact of the printing press*. voxeu.org: URL: https://voxeu.org/article/information-technology-and-economic-change-impact-printing-press.

Eaton, C. and D. Volz (2021). *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*. URL: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

Eddy, M. and N. Perlroth (2020). *Cyber Attack Suspected in German Woman's Death*. The New York Times: URL: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

European Commission (2020). *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission.

FASB of the Financial Accounting Foundation (2010). *FASB Exposure Draft Proposed Accounting Standards Update Contingencies (Topic 450)*. FASB.

Federal Trade Commission (2019). *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. URL: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

FedEx Corporation (2022). *FORM–10K*. Memphis: FedEx Corporation.

Ferrillo, P., B. Zukis, and C. Veltsos (2021). *The SEC's Clear Reminder About the Need for Quality Cybersecurity Disclosures*. URL: https://corpgov.law.harvard.edu/contributor/bob-zukis/.

Financial Reporting Council of Nigeria (2018). *Nigerian Code of Corporate Governance 2018*. Financial Reporting Council of Nigeria Act.

Financial Stability Board (2020). *2020 list of global systemically important banks*. URL: https://www.fsb.org/2020/11/2020-list-of-global-systemically-important-banks-g-sibs/.

Galloway, A. (2021). *'Real and Present Danger:' Government considers making company directors personally liable for cyber attacks*. The Sydney Morning Herald: URL: https://www.smh.com.au/politics/federal/real-and-present-danger-government-considers-making-company-directors-personally-liable-for-cyber-attacks-20210712-p588vz.html.

Gomez, B. (2021). Vice President, Equilar. (B. Zukis, Interviewer).

Greig, J. (2022). *Bridgestone still struggling with plant closures across North America after cyberattack*. ZD Net: URL: https://www.zdnet.com/article/bridgestone-still-struggling-with-plant-closures-after-cyberattack/.

Guaranty Trust Bank plc. (2021). *2020 Annual Report*. Lagos: Guaranty Trust Bank plc.

Hasbro, Inc. (2020). *Form 10-K*. Rhode Island: Hasbro, Inc.

Haverstock, E. (2021). *Inside The Global 2000: The Value of the World's Largest Public Companies Soars, As Sales And Profits Falter*. Forbes.Com: URL: https://www.forbes.com/sites/elizahaverstock/2021/05/13/inside-the-global-2000-the-value-of-the-worlds-largest-public-companies-soar-as-sales-and-profits-falter/?sh=1d8369aa26d4.

Hawkins, A. J. (2022). *Toyota shuts down its Japanese factories after reported cyberattack*. URL: https://www.theverge.com/2022/2/28/22954688/toyota-cyberattack-factory-shut-down-cars-output.

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.

Hope, A. (2021). *Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May Help Hackers Better Target Firm's Customers*. URL: https://www.cpomagazine.com/cyber-security/cyber-insurance-firm-suffers-sophisticated-ransomware-cyber-attack-data-obtained-may-help-hackers-better-target-firms-customers/.

Huang, K., R. Ye, and S. Madnick (2019). *Both Sides of the Coin: The Impact of Cyber Attacks on Business Value*. Cambridge: MIT Sloan School of Management.

Huawei and Oxford Economics (2017). *Digital Spillover—Measuring the True Impact of the Digital Economy*. Shenzen: Huawei Technologies Co., Ltd.

IBM Security (2021). *Cost of a Data Breach Report 2021*. IBM.

IDC (2020). *IDC FutureScape: Worldwide Digital Transformation Predictions 2021*. Framingham: IDC.

Insitute of Directors Southern Africa KING IV (2016). *Draft King IV Report—Responses to the summarised public comments 2016*. Insitute of Directors Southern Africa.

Institute of Directors In Southern Africa NPC (2016). *KING IV Report On Corporate Governanace For Southern Africa*. Johannesburg: Institute of Directors In Southern Africa NPC.

Institutional Investor (2021). *Japan's Corporate Governance Code Revised in Anticipation of "Prime Market" Segment Coming to TSE*. URL: https://www.institutionalinvestor.com/article/b1spy621t219ny/Japan-s-Corporate-Governance-Code-Revised-in-Anticipation-of-Prime-Market-Segment-Coming-to-TSE.

International Monetary Fund (2018). *Measuring The Digital Economy*. Washington, D.C.: International Monetary Fund.

International Organization Of Securities Commissions (2021). *Environmental, Social and Governance (ESG) Ratings and Data Products Providers*. Madrid: International Organization Of Securities Commissions.

International Telecommunication Union (2018). *Assessing the Economic Impact of Artificial Intelligence*. Geneva: International Telecommunication Union.

ISO/IEC (2015). *Internation Standard ISO/IEC 38500 2nd edition Information technology-Governance of IT for the organization*. Geneva: ICO/IEC.

ISO/IEC 27014 2nd edition 2020–12 (2020). *Information security, cybersecurity and privacy protection — Governance of information security (ISO_IEC_27014_2020(en). P. 1:0)*. Geneva: ISO/IEC.

ISO/IEC/IEEE 15288 (2015). *Systems and software engineering—System life cycle processes*. First edn. Geneva and New York: ISO/IEC/IEEE.

ISS (2021). *Governance QualityScore*. URL: https://www.issgovernance.com/esg/ratings/governance-qualityscore/.

Jones Day (2021). *China Finalizes Data Security Law to Strengthen Regulation on Data Protection*. URL: https://www.jdsupra.com/legalnews/china-finalizes-data-security-law-to-4249871/.

Lee, C. (2021). *Vietnam digital economy expected to contribute 20 percent of GDP by 2025*. URL: https://vietnamtimes.org.vn/vietnam-digital-economy-expected-to-contribute-20-percent-of-gdp-by-2025-21229.html.

Lewis, M. J. (2020). "Independent Directors Mitigate Legal Risk". *Private Company Director*: 56.

Malayan Banking Berhad (2020). *Corporate Governance Report*. Kuala Lumpur: Malayan Banking Berhad.

Marsh & McLennan Companies Ltd. Inc. and Global Network of Director Institutes (2021). *Global Network of Directors Institutes 2020–2021 Survey Report*. Marsh & McLennan Companies Ltd, Inc. | Global Network of Director Institutes.

Mehrotra, K. and W. Turton (2021). *CNA Paid $40 Million in Ransom After March Cyber Attack*. URL: https://www.insurancejournal.com/news/national/2021/05/21/615373.htm.

Morgan, S. (2020). *Cybercrime Magazine*. Cybercrime Magazine: URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Munter, P. (2021). *Statement on OCA's Continued Focus on High Quality Financial Reporting in a Complex Environment*. URL: https://www.sec.gov/news/statement/munter-oca-2021-12-06.

MyLogIQ (2021). *S&P 500 and R3000 Technology and Cybersecurity Oversight*. San Juan: MyLogIQ.

National Center for Incident Readiness and Strategy for Cybersecurity (2021). *Outline of Japan's Next Cybersecurity Strategy*. NISC: URL: https://www.nisc.go.jp/eng/.

National Women's Council (2021). *Increasing Gender Balance on Boards: The case for Legislative Gender Quotas in Ireland*. Dublin: National Women's Council.

Neuberger, A. (2021). *White House*. White House: URL: https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf.

New York State Department of Financial Services (2021). *Insurance Circular Letter No. 2*. URL: https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

OECD (2015). *G20/OECD Principles of Corporate Governance*. Paris: OECD Publishing.

Panettieri, J. (2021). *SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details*. URL: https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/4/.

Patterson Balknap Webb and Tyler, LLP. (2021). *SEC Signals Renewed Interest in Cybersecurity Disclosure Enforcement*. URL: https://www.jdsupra.com/legalnews/sec-signals-renewed-interest-in-6695892/.

Perez, S. (2021). *Walmart to sell it's e-commerce technologies to other retailers*. TechCrunch.com: URL: https://techcrunch.com/2021/07/28/walmart-to-sell-its-e-commerce-technologies-to-other-retailers/.

Powell, J. (2021). 60 Minutes. URL: https://www.cbsnews.com/news/jerome-powell-full-2021-60-minutes-interview-transcript/ (S. Pelley, Interviewer).

Pritchard, S. (2022). *India to introduce six-hour data breach notification rule*. URL: https://portswigger.net/daily-swig/india-to-introduce-six-hour-data-breach-notification-rule.

Reuters (2021a). *Business: AIG is reducing cyber insurance limits as cost of coverage soars*. URL: https://www.reuters.com/business/aig-is-reducing-cyber-insurance-limits-cost-coverage-soars-2021-08-06/.

Reuters (2021b). *Revisions of Japan's Corporate Governance Code and Guidelines for Investor and Company Engagement*. Tokyo: The Council of Experts Concerning the Follow-up of Japan's Stewardship Code and Japan's Corporate Governance Code.

Ross, R., M. McEvilley, and J. Carrier Oren (2016). *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. Gaithersburg: U.S. Department of Commerce/National Institute of Standards and Technology.

Securities Commission Malaysia (2021). *Malaysian Code on Corporate Governance (as at 28 April 2021)*. Kuala Lumpur: Securities Commission Malaysia.

Shoprite Holdings Ltd. (2020). *Application of the King IV Code Principles*. Johannesburg: Shoprite Holdings Ltd.

SHRM (2021). *Job Description Chief Information Officer*. URL: https://www.shrm.org/ResourcesAndTools/tools-and-samples/job-descriptions/Pages/Chief-Information-Officer.aspx.

SpencerStuart (2017). *Boardroom Best Practice: Lessons learned from board assessments across Europe*. SpencerStuart.

The Hindu (2021). *Government to unveil national cyber security strategy soon: National Cyber Security Coordinator*. URL: https://www.thehindu.com/business/government-to-unveil-national-cyber-security-strategy-soon-national-cyber-security-coordinator/article35119538.ece.

The White House (2022). *Office of the National Cyber Director*. The White House: URL: https://www.whitehouse.gov/oncd/.

Tricor Group and FT Board Director Programme (2021). *2021 Asia Pacific Board Director Barometer Report*. Hong Kong: Tricor Group.

Turton, W. and K. Mehrotra (2021). *Hackers Breached Colonial Pipeline Using Compromised Password*. URL: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

UNCTAD (2019). *Digital Economy Report 2019 Value Creation And Capture: Implications For Developing Countries*. New York: United Nations.

U.S. Bureau of Economic Analysis (2021). *Updated Digital Economy Estimates,* U.S. Bureau of Economic Analysis. Washington, D.C.: U.S. Bureau of Economic Analysis (BEA).

U.S. Securities and Exchange Commission (2021). *Cybersecurity Risk Governance*. URL: https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202104&RIN=3235-AM89.

U.S. Securities and Exchange Commission (2022a). March 9. *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*. URL: https://www.sec.gov/news/press-release/2022-39.

U.S. Securities and Exchange Commission (2022b). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure File No. S7-09-22*. Washingto, DC: Securities and Exchange Commission.

Walmart Inc. (2021). *Form 10-K*. Bentonville: Walmart Inc.

Weill, P., T. Apel, S. L. Woerner, and J. S. Banner (2019). *Assessing The Impact Of A Digitially Savvy Board On Company Performance*. Boston: MIT Management Sloan School Center For Information Systems Research (CISR).

World Economic Forum (2019). *Our Shared Digital Future Responsible Digital Transformation—Board Briefing*. Geneva: World Economic Forum.

Zukis, B. (2016). *Are Cyber Experts On Boards Inevitable?* URL: https://www.conference-board.org/blog/postdetail.cfm?post=5917.

Zukis, B. (2019). *DDN Releases DiRECTOR The Only Systemic Risk Framework Focused On Complex Digital Systems*. URL: https://www.digitaldirectors.network/blogs/ddn-releases-director-the-only-systemic-risk-framework-focused-on-complex-digital-systems.

Zukis, B. (2020). *Ransomware Has A New And Very Valuable Hostage In Sight*. URL: https://www.forbes.com/sites/bobzukis/2020/06/18/ransomware-has-a-new-and-very-valuable-hostage-in-sight/?sh=2f8ba91d170f.

Zukis, B. (2021a). *China, Fred Astaire And The Countries Dancing Towards The Digital Future*. URL: https://www.forbes.com/sites/bobzukis/2021/07/21/china-fred-astaire-and-the-countries-dancing-towards-the-digital-future/?sh=147ed10e6394.

Zukis, B. (2021b). "The Boardrooms Leading America's Digital Transformation". *NACD Directorship*: 24–30.

Zukis, B. (2022). *The SEC Is About To Force CISOs Into America's Boardrooms*. URL: https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/?sh=7e7bf1ed68a9.

Zukis, B., P. Ferrillo, and C. Veltsos (2022). *The Great Reboot—Succeeding in a Complex Digital World Under Attack From Systemic Risk*. 2nd edn. Los Angeles: DDN Press.