

OVERVIEW

CYBERSECURITY ECONOMICS FOR EMERGING MARKETS

Estefania Vergara Cobos



WORLD BANK GROUP

Overview

**CYBERSECURITY
ECONOMICS
FOR
EMERGING MARKETS**

Estefania Vergara Cobos



WORLD BANK GROUP

This booklet contains the overview and foreword from *Cybersecurity Economics for Emerging Markets*, doi:10.1596/978-1-4648-2120-2. A PDF of the final book is available at <https://openknowledge.worldbank.org/> and <http://documents.worldbank.org/>, and print copies can be ordered at www.amazon.com. Please use the final version of the book for citation, reproduction, and adaptation purposes.

© 2024 International Bank for Reconstruction and Development / The World Bank
1818 H Street NW, Washington, DC 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Some rights reserved

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, links/footnotes, and other information shown in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The citation of works authored by others does not mean The World Bank endorses the views expressed by those authors or the content of their works.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

Rights and Permissions



This work is available under the Creative Commons Attribution 3.0 IGO license (CC BY 3.0 IGO) <http://creativecommons.org/licenses/by/3.0/igo>. Under the Creative Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the following conditions:

Attribution—Please cite the work as follows: Vergara Cobos, Estefania. 2024. “Cybersecurity Economics for Emerging Markets.” Overview booklet. World Bank, Washington, DC. License: Creative Commons Attribution CC BY 3.0 IGO

Translations—If you create a translation of this work, please add the following disclaimer along with the attribution: *This translation was not created by The World Bank and should not be considered an official World Bank translation. The World Bank shall not be liable for any content or error in this translation.*

Adaptations—If you create an adaptation of this work, please add the following disclaimer along with the attribution: *This is an adaptation of an original work by The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by The World Bank.*

Third-party content—The World Bank does not necessarily own each component of the content contained within the work. The World Bank therefore does not warrant that the use of any third-party-owned individual component or part contained in the work will not infringe on the rights of those third parties. The risk of claims resulting from such infringement rests solely with you. If you wish to re-use a component of the work, it is your responsibility to determine whether permission is needed for that re-use and to obtain permission from the copyright owner. Examples of components can include, but are not limited to, tables, figures, or images.

All queries on rights and licenses should be addressed to World Bank Publications, The World Bank, 1818 H Street NW, Washington, DC 20433, USA; e-mail: pubrights@worldbank.org.

Cover design: Bill Praguski, Critical Stages, LLC

Contents

Foreword..... v

Overview 1

Introduction1

The Threat Landscape1

The Economic Costs of Cyber Incidents..... 7

The Cybersecurity Market 8

Conclusions and Policy Recommendations 10

Notes11

References 12

FIGURES

ES.1 Global evolution of disclosed cyber incidents, quarterly, 2014–25 2

ES.2 Distribution of disclosed cyber incidents, by motive and
income group, 2014–23 3

ES.3 Percentage of disclosed cyber incidents, by sector and
income group, 2014–23 4

ES.4 Cyber risk clusters according to economies’ relative
cybersecurity exposure and protection levels..... 5

ES.5 Changes in cybersecurity commitment scores and
relative exposure, 2020–24 6

ES.6 Global average cost of a data breach, 2017–24..... 8

ES.7 Cybersecurity strategies for key sectors.....11

Foreword

With approximately 5.45 billion people—about 67 percent of the global population—connected to the internet, alongside roughly 18 billion Internet of Things devices, economies, societies, businesses, and individuals have become highly dependent on the smooth operation of online systems. Although digitalization brings enormous economic and social benefits, our increasing reliance on digital technologies also introduces major risks. This is also the case in developing countries where the pace of digitalization often outstrips the necessary investments and attention required to build cyber resilience, leading to potentially debilitating consequences.

Through an innovative approach using advanced artificial intelligence tools to analyze millions of online news articles in 98 different languages, the digital research team has created a unique database of cyber incidents from the past decade, addressing a challenge to research in this field—the lack of comprehensive and publicly available data. The insights revealed an alarming reality: publicly disclosed cyber incidents are surging globally, with a 21 percent annual growth rate. This acceleration is most pronounced in Latin America and the Caribbean and across upper-middle-income countries. Moreover, this may only be the tip of the iceberg, as over 40 percent of cyber incidents are likely to remain unreported.

The economic impact of these trends in developing countries is significant. In 2022, Costa Rica experienced a massive ransomware attack that crippled over 20 government agencies, including the Ministry of Finance and Social Security. Lasting nearly two months, this incident prompted the first-ever national emergency declaration due to a cyber incident, shutting down key systems and costing the economy an estimated 2.4 percent of its annual gross domestic product (GDP). Without the financial and human resources to secure their digital environments, and lacking affordable, context-specific cybersecurity services, other developing nations risk encountering similar costly incidents in the future.

Cyber incidents are not just draining economies but also endangering human safety. Over half of developing countries experience at least one publicly disclosed cyber incident affecting critical infrastructure each year. These incidents have resulted in millions facing power outages, disruptions in medical services, fuel shortages, port shutdowns, and more. Data on publicly disclosed

cyber incidents indicate that the most impacted sectors globally are finance, health care, information and communications, and public services.

Mitigating cyber risk is essential for driving inclusive, sustainable development and economic growth. This study demonstrates that a developing country that reduces its number of major disclosed cyber incidents from the top to the bottom quartile of the distribution—reducing that number from approximately 50 to 7 during the study period—could boost GDP per capita by 1.5 percent. Equally important, a more secure cyberspace fosters trust in the digital economy and protects the most vulnerable, including those at the lower end of the income distribution and small and medium enterprises.

While we cannot eliminate cyber risk, we can try to manage and mitigate it. To do this, we must collaborate to understand and assess the threat landscape and identify efficient solutions tailored to the capacities of developed and developing nations alike. A crucial component of this effort is the routine and standardized collection of data on cyber incidents. This will be essential for informing future research and interventions, including understanding the scale of the problem, enabling the deployment of limited financial and human resources to enhance cyber resilience in ways likely to have the greatest impact, and providing a means to better evaluate the effectiveness of these interventions.

Securing our digital future hinges on our commitment to efficient cybersecurity. It is not just an option. It is a vital imperative.

Christine Zhenwei Qiang

Global Director

Digital Transformation Global Department

World Bank

Stephane Straub

Chief Economist

Infrastructure Vice Presidency

World Bank

Overview

Introduction

In an increasingly interconnected world driven by the rapid adoption of digital technologies and online systems, the critical role of cybersecurity cannot be overstated. As societies aim to harness the power of technology to boost economic growth, enhance public services, and improve quality of life, they face heightened risks associated with cyber threats. In this context, this book demonstrates that cybersecurity is essential for the socioeconomic progress of nations.

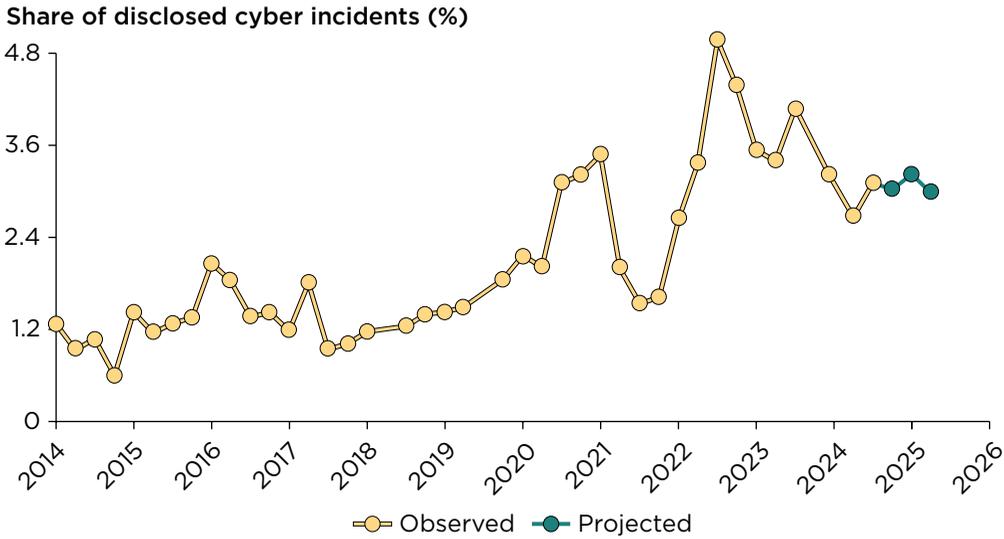
Despite increasing cybersecurity awareness, significant gaps persist. These gaps largely stem from a lack of thorough understanding of cyber incidents and their consequences. This issue poses significant obstacles in mobilizing resources for cybersecurity, particularly in developing countries with limited budgets and pressing social needs. In response to these challenges, this book offers pioneering analyses that (1) map key elements of the global cybersecurity threat landscape; (2) link these threats to the means by which economies are affected; (3) identify efficiency problems within cybersecurity markets; and (4) propose adaptive strategies, flexible policies, and decentralized governance efforts to foster innovation and sustainability amid ongoing change and uncertainty.

The Threat Landscape

Generating systemic knowledge about the cybersecurity landscape is challenging due to a global data shortage on cyber incidents, especially in developing countries. To address this gap, World Bank researchers used advanced artificial intelligence (AI) tools to analyze millions of online cybersecurity-related articles in 98 languages from the past decade, identifying over 30,000 publicly disclosed cyber incidents. Combined with data from the Center for International and Security Studies at Maryland, a comprehensive database spanning approximately 190 countries and 21 industries was produced. The findings reveal an alarming reality, unlikely to be solely explained by changes in reporting behavior.

As the digital age flourishes, the world has found itself caught in a web of cyber incidents that is increasing in both size and complexity. From 2014 to 2023, disclosed cyber incidents worldwide grew at an average annual rate of 21 percent, with upper-middle-income countries experiencing the highest surge, with a growth rate of 37 percent (figure ES.1).¹ Meanwhile, high-income countries (HICs) and lower-middle-income countries experienced growth rates

FIGURE ES.1 Global evolution of disclosed cyber incidents, quarterly, 2014–25



Source: Original figure for this book, based on data on disclosed cyber incidents from the Center for International and Security Studies at Maryland and the World Bank.

of 22 and 17 percent, respectively. The increasing trend of disclosed cyber incidents over the past decade has been fueled mainly by the COVID-19 pandemic and the Russian Federation–Ukraine war.

Digital technologies improve economic and social resilience against a wide range of threats, but societies also need to be protected from them. For example, the COVID-19 pandemic prompted a rapid shift to digital infrastructure to facilitate online health services, education, social protection, e-commerce, telecommuting, and productivity enhancements. While these technologies provided significant benefits during a critical period, they simultaneously introduced serious cybersecurity challenges. Such is the case that, from 2019 to 2020, disclosed cyber incidents worldwide increased by 62 percent, predominantly affecting the public administration, health care, and education sectors.

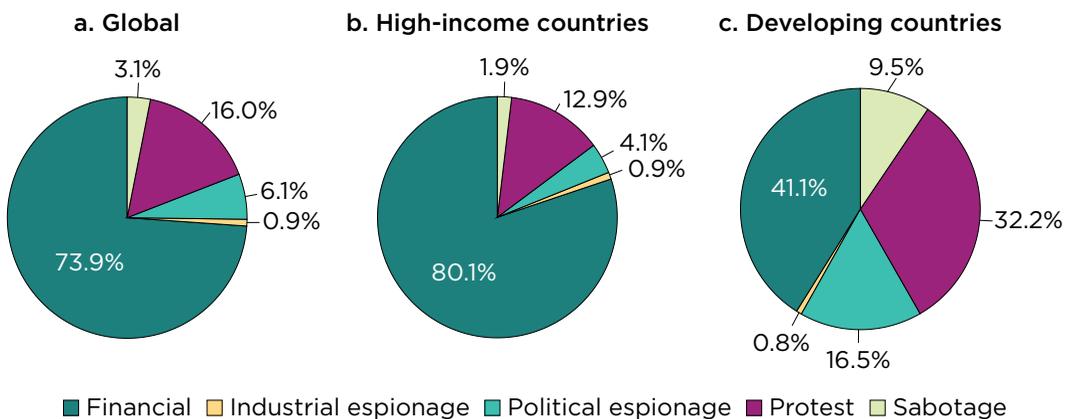
Almost two years after the start of the COVID-19 pandemic and against the backdrop of geopolitical tensions, the ground invasion of Ukraine erupted, casting a shadow over the digital realm. The postinvasion period saw an astonishing 80 percent surge in disclosed cyber incidents from 2021 to 2022, particularly affecting countries in Europe and Central Asia, such as Italy, Lithuania, and Poland, and critical sectors like utilities and information and communications. The Russia-Ukraine war illustrates how cyber incidents have become an integral part of modern conflicts, emphasizing the urgent need to design digital infrastructures that bolster resilience in times of conflict.

Developing countries account for approximately 30 percent of the world’s publicly disclosed cyber incidents.² However, the surge and impact of cyber incidents could be more severe in these countries given their rapid digitalization, lower cybersecurity commitments, and political and economic instability. Notably, Latin America and the Caribbean (LAC) is the world’s region with the fastest growth of disclosed cyber incidents, at an average annual growth rate of 25 percent from 2014 to 2023. This significant surge in LAC was associated with a 145 percent increase in Internet of Things devices, a 280 percent rise in e-commerce volume, and greater adoption of e-government tools post-COVID-19 in the region.

The global landscape of disclosed cyber incidents from the past decade reveals a complex and diverse array of incidents shaped by various interconnected factors (Harry and Gallagher 2018). Approximately 61 percent of these incidents worldwide were exploitive in nature, as were 63 percent of incidents in HICs and 49 percent in developing countries. The remaining incidents were disruptive,³ characterized by a highly stochastic trend, which adds a layer of uncertainty.

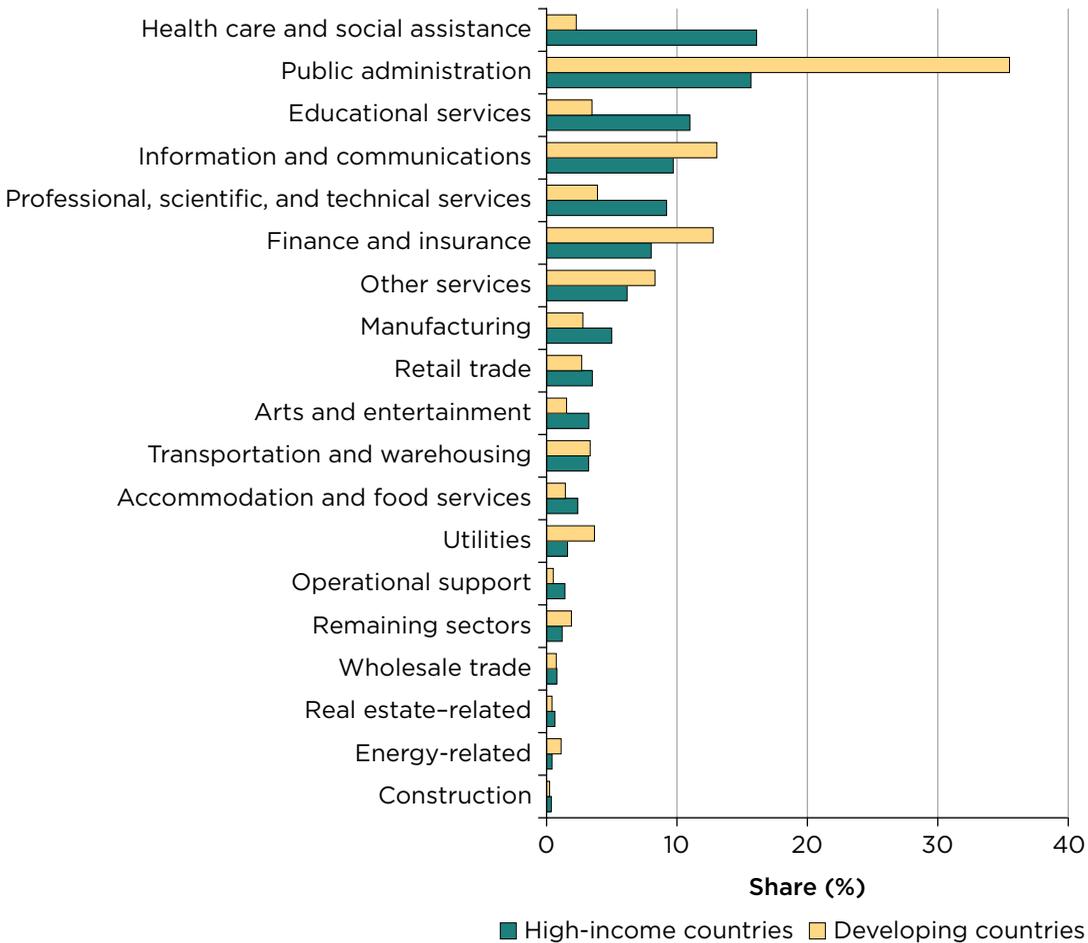
Financial motives dominate the landscape, accounting for 74 percent of disclosed cyber incidents globally and 80 percent in HICs. In stark contrast, only 41 percent of disclosed incidents in developing countries were primarily financially driven (figure ES.2). The remaining shares of disclosed cyber incidents (20 percent in HICs and 59 percent in developing countries) exhibited political motives, ranging from protests to political espionage. Across industries, these differences persist, with HICs exhibiting the largest share of disclosed

FIGURE ES.2 Distribution of disclosed cyber incidents, by motive and income group, 2014–23



Source: Original figure for this book, based on data on disclosed cyber incidents from the Center for International and Security Studies at Maryland.

FIGURE ES.3 Percentage of disclosed cyber incidents, by sector and income group, 2014–23

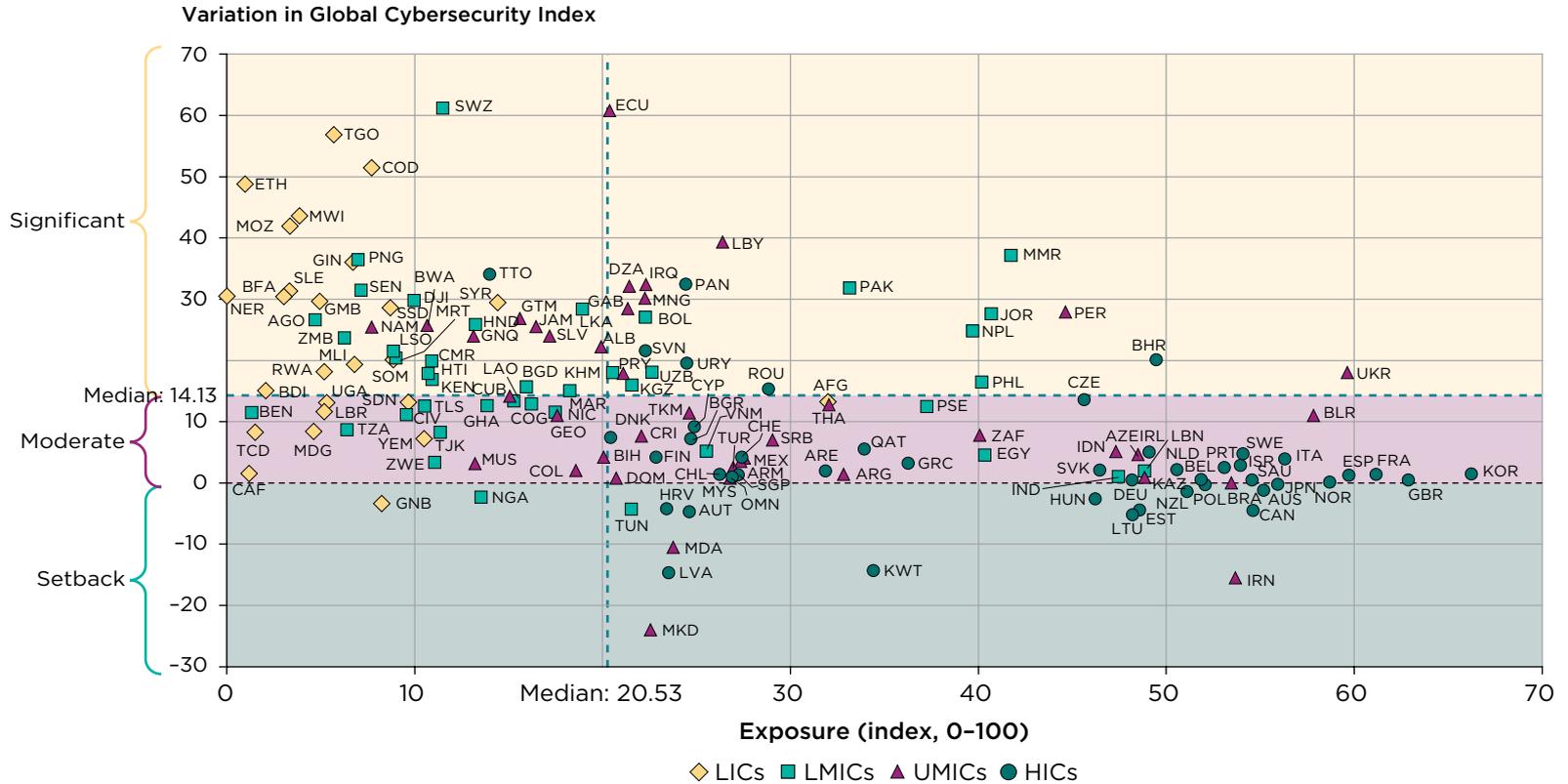


Source: Original figure for this book, based on data on disclosed cyber incidents from the Center for International and Security Studies at Maryland.

incidents in health care, and developing countries displaying a concentration of disclosed incidents of about 30 percent in public administration (figure ES.3). These findings align with the generally lower levels of political stability in developing countries. However, they also raise concerns about the lack of incident disclosure requirements for the private sector in these countries.

Worldwide, cyber risk varies significantly (figure ES.4), with countries facing different levels of exposure to cyber threats and varying degrees of cybersecurity commitments. HICs, such as the United Kingdom and the United States, have the highest exposure to cyber threats. However, various middle-income countries could be facing the highest levels of relative cyber risk due to their

FIGURE ES.5 Changes in cybersecurity commitment scores and relative exposure, 2020–24



Source: Original figure for this book, based on data from the International Telecommunication Union’s Global Cybersecurity Index (GCI).

Note: The figure excludes the outliers China, the Russian Federation, and the United States. Data for protection (y-axis) reflect the change in the GCI from 2020 to 2024; the years for the data on exposure (x-axis) vary. HICs = high-income countries; LICs = low-income countries; LMICs = lower-middle-income countries; UMICs = upper-middle-income countries. For country abbreviations, see International Organization for Standardization (ISO), <https://www.iso.org/obp/ui/#search>.

above-median exposure paired with below-median protection levels. Cybersecurity commitments, which reflect the level of protection, are crucial for risk mitigation. In fact, between 2014 and 2023, the average annual count of disclosed cyber incidents more than tripled in countries with low initial levels of cybersecurity commitments and doubled in those with high commitment levels. However, low-income countries have made the greatest improvements in cybersecurity commitments from 2020 to 2024 (figure ES.5).

The Economic Costs of Cyber Incidents

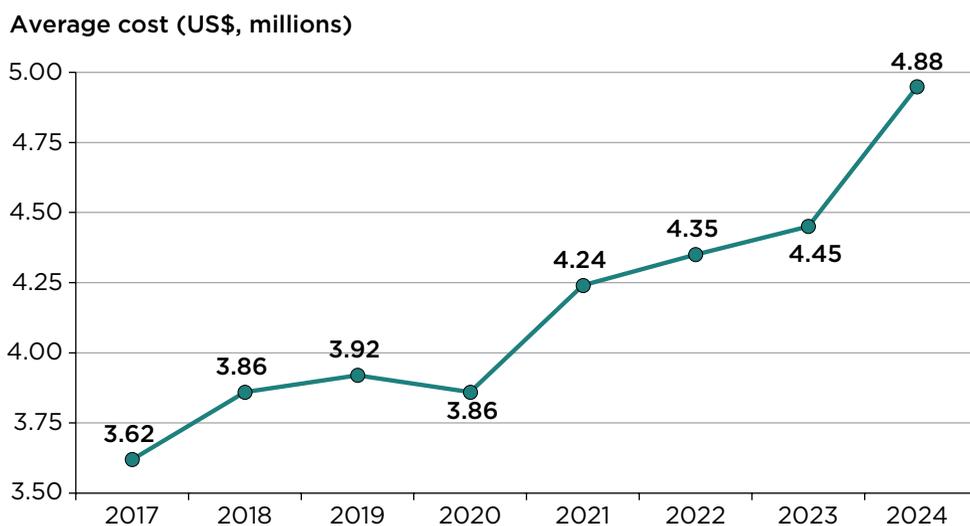
The escalating frequency and costs of cyber incidents worldwide are alarming, posing real risks to macroeconomic stability, especially for developing countries. And what we know is likely just the tip of the iceberg, as many cyber incidents remain undisclosed. The economic impact of cyber incidents is potentially more severe in developing countries, where estimates suggest that the average disclosed cyber incident has a larger impact than in HICs.

Reducing the frequency of major cyber incidents is necessary for achieving inclusive and sustainable development, as well as economic growth. Recent research by Vergara Cobos et al. (forthcoming) finds that a developing country that reduces its number of major disclosed cyber incidents from the top quartile of the distribution (around 50 disclosed cyber incidents) to the bottom quartile (around 7 disclosed cyber incidents) in a decade could see an increase in gross domestic product (GDP) per capita of approximately 1.5 percent. This exceeds the estimated productivity gains from a decade of exposure to AI (Acemoglu 2024). Likewise, stronger national cybersecurity commitments have positive economic effects, with estimates showing that more digitalized industries perform better in countries with higher levels of cybersecurity commitments than in those with lower levels, all else equal.

The onset of the COVID-19 pandemic amplified not only the frequency but also the impact of cyber incidents, with substantial increases in the average unit costs. For example, from 2022 to 2023, the average cost of a ransomware attack surged by 13 percent, and in the following year the average cost of data breaches climbed by almost 10 percent (figures ES.6). These increments disproportionately affect small and medium enterprises (SMEs) worldwide, with large businesses (with more than 10,000 employees) seeing decreases in the unit costs of data breaches (IBM 2023, 2024).

The systemic nature of cyber risk means that even a single incident can trigger widespread disruptions. Such was the case of the 2017 NotPetya cyberattack, which

FIGURE ES.6 Global average cost of a data breach, 2017–24



Source: Original figure for this book, based on data from IBM (2023, 2024).

resulted in more than US\$7.3 billion in consumer losses, a figure that is four times larger than the initial drop in profits reported by the firms that were directly hit (Crosignani, Macchiavelli, and Silva 2023). The systemic nature of cyber risk could lead to dangerous scenarios like “cyber runs”—rapid, large-scale compromises of the financial and operational stability of the banking sector, which so far have been prevented thanks to proactive measures adopted by banks and regulators.

As cyber threats grow, the consequences extend beyond mere financial losses to broader national security concerns and the protection of people’s rights, including privacy and access to essential services. This issue underscores the urgent need for efficient cybersecurity measures to safeguard economic stability and societal well-being.

The Cybersecurity Market

The cybersecurity market is experiencing remarkable growth and transformation, driven by factors such as the widespread adoption of cloud technologies and the emergence of new security challenges, such as those associated with the advancements in large language models and other AI tools. These dynamics are reshaping how organizations approach and invest in securing their digital assets and sensitive information. In 2024, global spending on information security and risk management is expected to increase by 14 percent compared to 2023 (Gartner 2024), reaching nearly 0.2 percent of the world’s GDP. This remarkably high estimated growth rate of global security

spending is nearly double that of information technology spending and almost four times higher than the projected growth of the global economy by 2024 (Gartner 2024; IMF 2024). The areas experiencing the highest growth rates include cloud security and data privacy. However, security services, such as consulting and outsourcing, continue to dominate cybersecurity spending, underscoring the critical role that expert support plays in cybersecurity.

Despite its growth, the industry faces significant hurdles, including a shortfall in research and development (R&D) investment, indispensable for facing the new and advanced threats, and a pervasive global shortage of skilled cybersecurity professionals, with more than 4 million unfilled cybersecurity positions in 2023 (ISC2 2023). The cybersecurity workforce shortage is particularly affecting nonmilitary government sectors, SMEs, and developing nations.

Moreover, varying accessibility to cybersecurity markets may be giving HICs and larger businesses comparative advantages as societies progress in the digital era. North America commands over 50 percent of the global market, with a demand that is 16 times larger than that of all the countries in LAC together. The skewed market demand is also evident at the governmental levels, with government per capita spending on cybersecurity in HICs like Canada and the United States exceeding US\$30, compared to less than US\$1 in highly targeted developing countries like India and Mexico. In the business world, large companies are leading in cybersecurity spending. Meanwhile, top cybersecurity vendors report decreasing sales to SMEs, a phenomenon primarily due to a lack of resources.

The previously mentioned challenges could be further aggravated by various sources of market inefficiency:

- *Noninternalized third-party cyber risk.* Organizations that experience a cyber incident are often exposed due to a third party. Yet, this does not lead to increased investment in extended risk management.
- *Unclear returns on investment.* Unlike other cost-saving investments, the financial benefits of cybersecurity are unclear and even impossible to quantify with the usual cost-benefit approach, obstructing efficient resource allocation.
- *Moral hazard.* The majority of compromised firms pass losses from cyber incidents on to consumers through price hikes, while shareholders suffer from declines in market value.
- *Misaligned incentives.* Undisclosed cyber incidents, coupled with low public awareness and a highly competitive technology market, result in misaligned incentives for producing resilient digital technologies.

- *Information asymmetries.* The general population lags in cybersecurity knowledge and awareness. Moreover, it is practically unfeasible to assess the level of cyber risk or the effectiveness of cybersecurity products before a cyberattack.

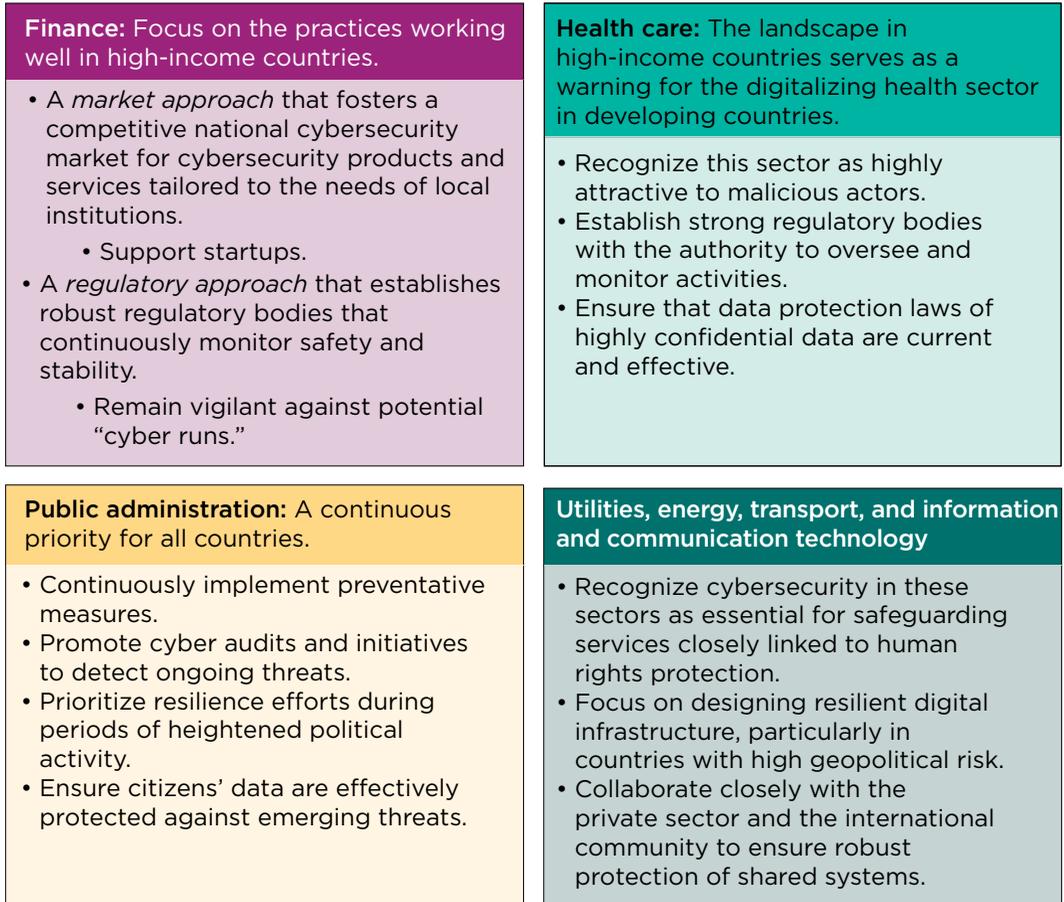
Market inefficiencies could be more pronounced in developing countries given the influence of governments in HICs on global market dynamics through their large procurements and operationalized regulations and standards. Governments could address these challenges, for example, by prioritizing awareness and training programs and coordinating an R&D plan tailored to the country's needs.

Conclusions and Policy Recommendations

Cybersecurity represents a collective responsibility that must be shared by all economic actors. This book delves into pivotal aspects of cybersecurity, including the threat landscape and its associated costs, market failures, and the critical roles of governments. By providing new evidence on the socioeconomic impact of cyber incidents, the book argues that a safe cyberspace is key for unlocking the full potential of digital technologies and paving the way for inclusive and sustainable development in the digital age.

Developing nations in particular face the dual task of fostering digitalization and safeguarding against cyber threats. Recommendations for these nations include implementing standardized and safe data collection practices to support evidence-based tailored policies; promoting the development of a national cybersecurity industry; drafting action plans that involve different sectors and stakeholders; prioritizing resilience in critical sectors; and supporting cybersecurity awareness and training programs. The policy suggestions stress the importance of protecting highly technological, operational, and financially interconnected sectors, like finance and communications, as well as highly attractive sectors, such as health care and public administration (figure ES.7). With 90 percent of global cybersecurity research centered in the US context only, the recommendations also include promoting inclusive research efforts in the realms of cybersecurity and cybersecurity economics and monitoring both the short- and long-term economic impacts of cyber incidents. Additionally, the advice emphasizes supporting a strategic and tailored R&D plan, advocating for affordable cybersecurity provisions for SMEs, creating dynamic and up-to-date regulatory frameworks, fostering international collaboration and public-private partnerships, and monitoring the development and adoption of emerging technologies such as cloud computing and advanced AI. The policy suggestions are also directed toward protecting critical infrastructure and essential services, learning from resilient sectors like the US finance sector and developing nations with strong improvements in cybersecurity commitments and results.

FIGURE ES.7 Cybersecurity strategies for key sectors



Source: Original figure for this book.

Notes

1. A *cyber incident* is an event or the end result of any single unauthorized effort taken using an information system (for example, computer technology) or a network that resulted in an actual or potential nationally relevant adverse effect on any of the three layers that constitute cyberspace—information systems, networks, and the information residing therein (Harry and Gallagher 2018; NIST, n.d.).
2. The term *developing countries* is used to refer to nations that are not classified as high-income countries (HICs).
3. The Center for International and Security Studies at Maryland defines two main types of cyber incidents: “disruptive” and “exploitive.” A *disruptive incident* impedes the target organization’s normal operations, and an *exploitive incident* illicitly accesses or exfiltrates sensitive information, such as personally identifiable information, classified information, or financial data.

References

- Acemoglu, D. 2024. "The Simple Macroeconomics of AI." Working Paper 32487, National Bureau of Economic Research, Cambridge, MA.
- Crosignani, M., M. Macchiavelli, and A. F. Silva. 2023. "Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains." *Journal of Financial Economics* 147 (2): 432–48.
- Gartner. 2024. "Planning for GenAI Initiatives Is Helping to Drive IT Spending in 2024 and Beyond." Gartner, San Francisco, CA (accessed July 21, 2024), <https://www.gartner.com/en/newsroom/press-releases/2024-04-16-gartner-forecast-worldwide-it-spending-to-grow-8-percent-in-2024#:~:text=Worldwide%20IT%20spending%20is%20expected,the%20end%20of%20the%20decade>.
- Harry, C., and N. Gallagher. 2018. "Classifying Cyber Events." *Journal of Information Warfare* 17 (3): 17–31.
- IBM. 2023. "2023 Cost of a Data Breach." IBM, Armonk, NY.
- IBM. 2024. "2024 Cost of a Data Breach." IBM, Armonk, NY.
- IS2 (International Information System Security Certification Consortium). 2023. "How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce." IS2, Alexandria, VA.
- IMF (International Monetary Fund). 2024. *Global Financial Stability Report*. Washington, DC: IMF.
- NIST (National Institute of Standards and Technology). n.d. "NIST Glossary." Definition of Cyberspace. NIST, Gaithersburg, MD. <https://csrc.nist.gov/glossary/term/cyberspace>.
- Vergara Cobos, E., S. Cakir, H. Mei-Zahav, and B. Barakcin. Forthcoming. "The Role of Cybersecurity in Economic Performance." World Bank, Washington, DC.

In our increasingly interconnected world, where digital technologies are rapidly transforming multiple aspects of daily life, the critical role of cybersecurity cannot be overstated, especially in developing nations. As these countries strive to harness the power of modern technology to drive economic growth, enhance public services, and elevate living standards, they concurrently face heightened risks associated with cyber threats. The increasing exposure of developing countries to cyber incidents is often compounded by various factors, including scarce resources, inadequate infrastructure, political unrest, inefficiencies in cybersecurity and technology markets, shortages of skilled cybersecurity professionals, legislative voids, and rapid rates of digital adoption.

Cybersecurity Economics for Emerging Markets is a pioneering research work that delves into the drivers and profound consequences of cyber incidents worldwide. From economic setbacks that can destabilize entire economies to interruptions of vital services and impediments to social and economic development, the impacts of cyber incidents are far-reaching.

This book analyzes hundreds of scholarly works and thousands of publicly disclosed cyber incidents over the past decade across some 190 countries. It sheds light on these incidents' characteristics and trends, as well as the proactive roles that private market players and governments can assume to safeguard infrastructure in cyberspace effectively. The book presents practical, evidence-based policy suggestions that include efforts to strengthen the resilience of the most essential and interconnected sectors. It advocates for bolstering the national cybersecurity industries, strategizing cybersecurity research and development, addressing market failures through cybersecurity awareness and training programs, and taking proactive steps to reduce and control contagion effects from cyber incidents.

By revealing crucial empirical and theoretical dimensions of cybersecurity economics, this book provides insights that could inform the creation of effective cybersecurity investments, with a focus on developing countries. These insights are invaluable for policy makers and stakeholders committed to fortifying the digital ecosystem against the ever-evolving landscape of cyber threats.