ISSN 1680-8754

SERIES

PRODUCTION DEVELOPMENT 225

Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean

Héctor J. Lehuedé

UNITED NATIONS

ECLAC

Thank you for your interest in this ECLAC publication

Please register if you would like to receive information on our editorial products and activities. When you register, you may specify your particular areas of interest and you will gain access to our products in other formats.

Register

UNITED NATIONS

ECLAC

www.cepal.org/en/publications

facebook.com/publicacionesdelacepal

www.cepal.org/apps

SERIES

PRODUCTION DEVELOPMENT | 225

Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean

Héctor J. Lehuedé

UNITED NATIONS

ECLAC

This document is part of a technical assistance project conducted by the Economic Commission for Latin America and the Caribbean, (ECLAC) by the Regional Telecommunications Technical Commission of Central America (COMTELCA) that groups the six countries of Central America, Mexico, the Dominican Republic and Colombia. The document was prepared by Héctor J. Lehuedé, a lawyer specialized in corporate governance, business integrity and financial affairs, under the coordination of Georgina Núñez, Economic Affairs Officer of the Division of Production, Productivity and Management of ECLAC, in charge of corporate governance, data protection and competition policy issues.

Special thanks to Wilson Perez and Fernando Rojas of ECLAC, Allan Ruiz and Jorge Torres of COMTELCA; Angeles Ayala of the Office of the Undersecretary for Communications and Technical Development of Mexico; Gastón G. González of the National Public Services Authority of Panama; Edson Alí Salguero of the Superintendency of Telecommunications of Guatemala; as well a Macarena Gatica, Emelie Kogut, Joanna Perez, Consuelo Herrera, Erick Iriarte and Pedro Huichalaf for their contributions.

United Nations publication
ISSN: 1680-8754 (electronic version)
ISSN: 1020-5179 (print version)
LC/TS.2020/103
Distribution: L

Printed at United Nations, Santiago
S. 20-00552

This publication should be cited as: H. Lehuedé, "Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean", *Production Development series*, No. 225 (LC/TS.2020/103), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2020.

Content

Tables

Figures

Abstract

This paper presents and discusses the relation between cybersecurity and corporate governance in the context of Latin America and the Caribbean. It notes that progress has been made in improving corporate cybersecurity within the region mostly from a data protection perspective, either as a result of internally driven or regulatory motivated corporate initiatives, but that not enough headway has been made regarding the cyber risks affecting critical infrastructure and essential services in the hands of private or State-owned companies. The paper describes some of the best corporate governance practices and guidance for boards of directors to address cybersecurity issues, as well as a selection of the regulatory incentives that lawmakers and regulators are deploying to incentivize boards to adopt proper cyber risk management. Three case studies are presented as examples of these types of policy interventions in the region.

Introduction

The World Wide Web has been around for merely 30 years, and only in 2018 access to it reached half of the world population, but in the last decade the number of Internet users grew yearly by 10 percent on average, to reach an estimated 4.1 billion users in 2019.[1] This broadening access to the Web, technological disruption and a move towards digital business models have made data some of the world's most valuable assets.

While not long ago most large firms were highly dependent on their control over expensive tangible assets, the corporate titans of our time are light of physical assets and heavy on intellectual assets. Microsoft, Apple, Google, Amazon and Facebook were the five largest stocks in the S&P 500 at the time of writing,[2] representing 17.5 percent of the market value of the index.[3] The value corresponding to intangibles (licenses, patents, R&D, data and the like) in the market value of US corporations has moved from less than 20 to more than 80 percent in the last four decades.[4]

Behind these intangible assets of corporations there is a wealth of data, ranging from purely commercial records to extremely sensitive personal information of clients, suppliers and employees. From sensors monitoring and predicting the behavior of a jet engine to the fitness monitor around our

---

1 See ITU (2019), Measuring Digital Development: Facts and Figures, International Telecommunication Union, 2019.

2 See 5 companies now make up 18% of the S&P 500. Is that a recipe for a crash? by Ben Carlson, Fortune, February 11, 2020.

3 In Zingales (2000) "In Search of New Foundations" The Journal of Finance Vol LV, Professor Zingales highlights how in the modern firm physical assets are less unique and easier to finance, and that as a result of better legal protection, intellectual assets are generating more value for firms. He also points the governance challenge for when the key assets of the organization cannot be owned and controlled by traditional property rights.

4 Professor Colin Mayer illustrates the point with Facebook's acquisition of WhatsApp in 2014 for USD 19 billion, despite the fact that the company was a "loss making company with no assets, no people and lots of liabilities." See Mayer, Colin (2015), "Reinventing the corporation" Sir John Cass's Foundation Lecture, March 3, 2015, Journal of the British Academy, 4, 53–51.

wrist, data are collected and processed for endless means.[5] Businesses are mining these data in ways that can boost their strategies with greater market access and scalability, offering bespoke goods and services. Yet, as we continue to process the might of data and the scope of the potential impact they can have over businesses, society and our own personal lives,[6] we are also facing the challenge of protecting them from theft and misuse in the face of sprawling cyber risks.

At the time of writing this paper, most of the world was confined to their homes because of the disruption caused by the Covid-19 pandemic, and millions of workers and students had begun to conduct their daily activities remotely through the web. Datareportal, a digital information hub, noted an enormous increase in digital activity since the beginning of 2020, especially in countries that have seen the strictest lockdowns.[7] In turn, Google reported that during the first weeks of April 2020 the volume of detected cyber threats related to Covid-19 reached 18 million malware[8] and phishing emails,[9] as well as 240 million spam messages, every day.

Those circumstances have beamed the spotlight on the crucial importance of ICT (information and communication technology) systems and connectivity, but also on the relevance of strong cybersecurity.[10] For this report, cybersecurity is understood generally as the ability to control access to networks, ICT systems and all kinds of information resources against cyberattacks or breaches of information that can affect individuals and organizations.[11]

Countless cybersecurity breaches in recent years have put numerous organizations and billions of users at risk, causing massive damage, both for those that failed to secure their corporate property, and those whose information was stolen, hijacked or corrupted. Prominent examples include the Bangladesh Bank heist,[12] the breaches at Yahoo[13] and Marriott,[14] several ransomware[15] attacks against public services and cities,[16] the Cambridge Analytica-Facebook case,[17] and the hacking of the U.S. Customs and Border Patrol Agency.[18]

---

5 The expansion of the Internet-of-Things (IoT) that will be paved by the adoption of fifth generation (5G) networks will only augment these risks. It is expected that the number of connected devices will double by 2025 to reach more than 40 billion worldwide. See International Data Corporation (IDC 2019), The Growth in Connected IoT Devices Is Expected to Generate 79.4 ZB of Data in 2025, according to a New IDC Forecast, IDC, June 18, 2019.

6 Best-selling author Yuval Noah Harari points that someone or something, an algorithm or AI for example, with unlimited access to all the data we produce would know us better than we know ourselves. He warns that this would challenge our assumption of having free will, as we would be easily manipulated by playing into our deepest desires and fears. See Yuval Noah Harari on big data, Google and the end of free will at Financial Times, August 26, 2016.

7 Datareportal, a digital information portal, notes significant increases in social media use, with video calling taking center stage, an accelerated adoption of ecommerce models for grocery shopping and others, as well as growing time spent playing video games and watching e-sports. See Datareportal 2020, Digital 2020: April Global Statshot, by Simon Kemp.

8 Malware (malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network.

9 Phishing is a fraudulent attempt to fool someone into sharing restricted information by pretending to be a trustworthy website.

10 See Google Cloud (2020), Protecting businesses against cyber threats during COVID-19 and beyond, by Neil Kumaran and Sam Lugani, April 16, 2020.

11 A more technical definition of cybersecurity is "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." For this and other useful definitions, see the U.S. National Initiative for Cybersecurity Careers and Studies (NICCS) portal's cybersecurity lexicon.

12 See The Billion-Dollar Bank Job by Joshua Hammer, The New York Times Magazine, May 3, 2018.

13 See Yahoo execs botched its response to 2014 breach, investigation finds, by Michael Kan, IDG News Service, March 2, 2017.

14 See Marriott Hacking Exposes Data of Up to 500 Million Guests by Nicole Perlroth, Amie Tsang and Adam Satariano, the New York Times, November 30, 2018.

15 Ransomware is a form of malware (abbreviation of "malicious software"; software designed to cause damage to a single computer, server, or computer network) that encrypts a victim's files. The attacker then offers a decryption key to restore the files back in exchange for a ransom payment from the victim, typically to be paid in cryptocurrency.

16 See Ransomware Hits Georgia Courts as Municipal Attacks Spread by Lily Hay Newman, Wired Magazine, May 1, 2019.

17 See Understanding the Facebook-Cambridge Analytica Story: QuickTake by Michael Riley, Sarah Frier and Stephanie Baker, The Washington Post, April 11, 2018.

18 See U.S. Customs and Border Protection says photos of travelers were taken in a data breach by Drew Harwell and Geoffrey A. Fowler, The Washington Post, June 10, 2019.

As those examples show, cybersecurity risks can affect us all. Countering them requires consistent, and ideally concerted, efforts by each link in a chain to safeguard the security of the whole.[19] From the employee that becomes victim of phishing to the weakness in the design of information systems that render restricted databases easily accessible to the public,[20] there are plenty of potentially weak points that can put ICT systems at risk, allowing hackers to gain access to our data and cause serious damage.

But even at a more macro perspective, in a world where cyber risks are ubiquitous and recognize no public/private sector distinction, nor stop at any international border, there is a significant need for collective efforts to keep us safe from threats. From multilateral agreements to company policies, there are a wide range of initiatives to curb cyber risks. They include national laws and regulations, guidelines, standards, opinions, codes of conduct, model laws and declarations, all aiming to articulate a coherent and effective cybersecurity response (see the Annex). Closer attention to them shows that they are addressing essentially three different aspects of the problem, and that only some of them target companies and more precisely the role of boards of directors and their corporate governance arrangements:

- First is prevention of cybercrime and building safety in the way ICT systems and data are protected by organizations and individuals. This is the domain of cybersecurity per se, where businesses appoint Chief Information and Security Officers (CISOs), Chief Technology Officers (CTOs) and Data Protection Officers (DPOs) to guard their data and digital assets from theft and fraud. They do this out of their own interest in most cases, as those intangibles are valuable, and their reputation is on the line. But many companies also do it because regulators have begun forcing them to have secure ICT systems to protect the personal data of their clients, consumers and other stakeholders. This data protection or privacy concern has created a direct link between corporate governance and cybersecurity, focusing mainly on potential damages, fines, corporate liability and reputation.[21]
- Then there is the domain focusing on the combat against cybercrime, concerned with the policing, investigation and prosecution of individuals and organizations that aim to use cyberspace to commit crimes. Some of them will aim to break the security of organizations included in the previous group for profit, fame or other goals, but their criminal scope is wider than just corporate assets. The focus of people working within this second community is set on catching and punishing those cyber-criminals. This is the sphere of Interpol and of Council of Europe's Budapest Convention (see the Annex). The main concerns here are enforcement, intelligence sharing, extradition and forensic international cooperation; not really on incentivizing boards of private firms to behave in any specific way, perhaps other than not becoming cyber-criminals themselves or providing cover to such criminals.
- Finally, there is the domain of cyber-defense, dealing with the preparation to defend national interests or to attack enemies in cyberspace. Here you can find both military and civil initiatives. Among the later, entities and individuals in this group are particularly

---

[19] In its 2017 Global Risk report, the World Economic Forum (WEF) argues that "greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyber-attacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways." See: World Economic Forum (2017), Global Risks Report 2017, 12th Ed., January 2017.

[20] See Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean? by AJ Dellinger, Forbes Magazine, May 26, 2019.

[21] See Lehuedé, Héctor (2019), "Corporate governance and data protection in Latin America and the Caribbean" Production Development series, No. 223 (LC/TS.2019/38), Santiago, ECLAC, 2019, for analysis of these issues from the perspective of data protection.

interested in protecting the continuity of critical infrastructure[22] and services, where cyber-attacks could cause considerable damage. Because these critical pieces of infrastructure are often controlled by private businesses or State-owned enterprises, it is again possible to find requirements for companies and their corporate governance frameworks within this community. Their focus is in making sure that the boards of relevant organizations will adopt the necessary technical measures to ensure continuity of the utilities, health, telecommunications, transportation, finance and other critical services they provide.

The communities in the three groups have different objectives with respect to cyber risk, but there is some overlap when they focus their attention towards the governance of firms, and the expectations they have for what boards of directors should do to facilitate the completion of their community's objectives. This is more evident in the cases of cybersecurity and cyber-defense. In the first case the attention is in mitigating potential damages to the company's assets and in establishing corporate liability and other incentives for firms to guard their stakeholders' personal data. In the second, it is in making sure that firms invest what is necessary to ensure that the critical services they render will not be interrupted by a cyberattack, or will be quickly recovered afterwards.

These expectations for the role of boards and corporate governance in countering cyber risks are being translated into law, regulation and policy. In the process, they are slowly shaping the agendas of boards and top managers across the globe by pushing firms to adopt whatever technical, normative and cultural means they need to keep their ICT systems safe. This paper seeks to describe and discuss those emerging cybersecurity rules and frameworks, and their relation to corporate governance, with a special interest in the situation in Latin America and the Caribbean.

Following this introductory chapter, the rest of the paper is structured as follows: chapter I portrays some of the progress made and challenges remaining for corporate cybersecurity in Latin America and the Caribbean. Chapter II presents three casea studies of sectors where cybersecurity rules are tapping the corporate governance of firms in the region to protect critical infrastructure. Chapter III outlines the conceptual rationale for the role of the board and corporate governance frameworks of firms in addressing cyber risk. Chapter IV offers some conclusions. Finally, the Annex contains a description of a selection of the relevant international frameworks and initiatives for cybersecurity, some of which include relevant corporate expectations.

[22] For this report, following the definition by the Industrial Cybersecurity Center (CCI), the term critical infrastructure is used to define facilities and systems on which essential services fall, the operation of which does not allow alternative solutions. Industrial Cybersecurity addresses the prevention, monitoring and improvement of the resilience of critical infrastructure and industrial processes, and their recovery, in the face of hostile or unexpected actions that may affect their proper functioning.

I. Cybersecurity in the region

A. Overview

In 2016 the Organization of American States (OAS) published a comprehensive report conducted together with the Inter-American Development Bank (IADB) and the Global Cyber Security Capacity Centre at the University of Oxford,[23] that presented a detailed picture of the state of cybersecurity in the region. Focusing on its risks, challenges, and opportunities, the report analyzed the state of preparedness of 32 jurisdictions based on 49 indicators developed by the Oxford researchers. To this date, it is the most complete measurement available, albeit it is already about 5 years out-of-date.

The overarching conclusion in the OAS report was that that Latin America and the Caribbean were improving their focus on cybersecurity, as data breaches and cyber-attacks were bringing it closer to the top of the social and political agendas, but that the region was much behind best practices with only a handful of jurisdiction achieving an intermediate level of preparedness. It emphasized that only one out of every five countries in the region had a cybersecurity strategy, or plans for protecting critical infrastructure, and that only one out of three had a command and control center for cybersecurity. In an editorial piece within the report, the IADB considered the region a vulnerable zone and calculated the cost of cybercrime at 90 billion USD. Some of the key conclusions offered were:

- All governments wanted their economies having access to affordable ICT services, and the rate of growth in Internet users was among the highest in the world, but on average only about half of the population had access to the Internet at the time, due to the lack of investment in broadband infrastructure.

[23] See OAS (2016) Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report, Organization of American States, 2016.

- Adopting a national cybersecurity strategy[24] was understood as indispensable for countries to reap the benefits of the digital economy, but at that time only six jurisdictions in the region had cybersecurity strategies (Brazil, Colombia, Jamaica, Panama, Trinidad and Tobago, and Uruguay) and another eleven were articulating one, many with the support of OAS' Cyber Security Program of the Inter-American Committee against Terrorism (see the Annex).
- There was a general need to increase cyber expertise[25] and also cyber-literacy among the population, and for awareness-raising initiatives to build a shared understanding of the importance of cybersecurity.
- The establishment of trusted public-private partnerships and formal information-sharing mechanisms was limited, as mistrust among stakeholders diminished collaboration.
- Only about half of countries had establish and operated a Computer Security Incident Response Team (CSIRT)[26] or a computer emergency response team to manage crisis response and reporting mechanisms,[27] which were also at early stages of development.
- Efforts to develop comprehensive cybersecurity legal frameworks were underway across the region, with improvements in enforcement and legislation, but only two jurisdictions had joined the Budapest Convention (see the Annex): the Dominican Republic and Panama. Also, that prosecution of cybercrimes was hampered by lack of reporting mechanisms, insufficient enforcement and forensics capabilities.
- Some governments were taking advantage of their Internet connectivity to promote the development of a local technology industry and encourage innovation, cybersecurity education, capacity building and jobs creation.

More recent studies and international rankings have tracked the progress of the region in advancing access to ICTs and improving cybersecurity from a global perspective. The International Telecommunication Union (ITU) tracks key ICT indicators around the globe that are useful to asses improvement of ICTs reach. Its latest time-series data for the Americas region (2019) on a selection of relevant indicators are presented in figure 1.

---

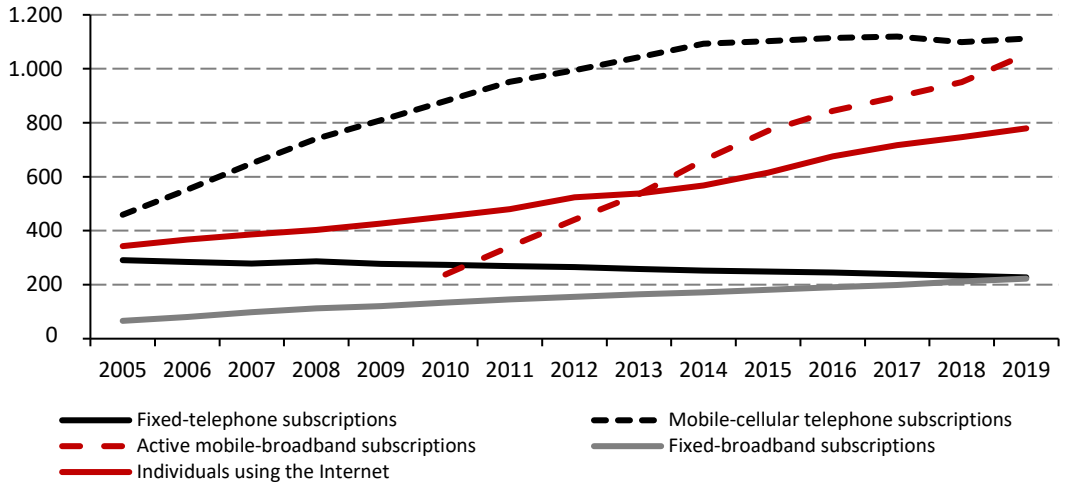
[24] National cybersecurity strategies usually include five key elements: i) A coordinating body that reports directly to the President or Prime Minister's offices to oversee implementation, coordinate agency efforts, and solve the jurisdiction and competency clashes between government bodies; ii) The allocation of responsibilities among ministries, agencies and other governmental bodies, and a mandate to coordinate and collaborate with the private sector, particularly regarding critical infrastructure; iii) Securing the availability of capable and well trained cybersecurity experts to staff critical cybersecurity functions, including a national CSIRT and cyber-police; iv) International cooperation with neighboring countries and key cybersecurity partners globally, and v) Capacity-building for the exchange of best practices and the exchange of information on threats and vulnerabilities.

[25] The report noted that initiatives to increase availability of well-trained talent in the region were underway, including Microsoft's Cybersecurity Engagement Center in Mexico and Cisco's Networking Academy.

[26] A CSIRT is defined as a team or an entity within an agency that provides services and support to a particular community in order to prevent, manage and respond to information security incidents. CSIRTs are usually comprised of multidisciplinary specialists who act according to predefined procedures and policies in order to respond quickly and effectively to security incidents and to mitigate the risk of cyberattacks. The Forum of Incident Response and Security Teams (FIRST) is a global association of incident response teams' members in over 70 countries, that enables them to respond more effectively to security incidents by providing access to best practices, organizing events and providing CSIRT education. See FIRST (2019) Computer Security Incident Response Team (CSIRT) Services Framework, Version 2.0, June 2019.

[27] The report noted that only Mexico, Peru, Colombia and Uruguay had a disclosure policy in place to mandate reporting of cyber breaches, which are essential for the authorities to have the necessary information to counter threats, reduce the damage, investigate the perpetrators and exchange intelligence with the private sector and with other countries' authorities.

Figure 1
Key ICT indicators for the Americas
(Totals in millions)



Source: ITU World Telecommunication/ICT Indicators database, updated October 2019.
Note: 2019 numbers are estimates. The Americas region in this table is based on the ITU regions, see: http://www.itu.int/en/ITU-D/Sta tisti cs/Pages /definitions/regions.aspx.

The ITU also produces a ranking of cybersecurity ordering countries based on an estimation of their commitment to reducing cyber risks, as measured for the 5 pillars of its Global Cybersecurity Agenda (see the Annex). Table 1, below, presents the results for all the available jurisdictions within the Americas. The red lines in the right column indicate if the score of each jurisdiction has increased or decreased since the first version of this index, in 2014, by noting a direction up or down from left to right. In most cases it has increased.

Table 1
ITU Global Cybersecurity Index 2018 (available jurisdictions The Americas)

Country	Regional Rank 2018	Global Rank 2018	Score 2018	Change 2014
United States of America	1	2	0,926	
Canada	2	9	0,892	
Uruguay	3	51	0,681	
Mexico	4	63	0,629	
Paraguay	5	66	0,603	
Brazil	6	70	0,577	
Colombia	7	73	0,565	
Cuba	8	81	0,481	
Chile	9	83	0,47	
Dominican Republic	10	92	0,43	
Jamaica	11	94	0,407	
Argentina	11	94	0,407	
Peru	12	95	0,401	
Panama	13	97	0,369	
Ecuador	14	98	0,367	
Venezuela (Bolivarian Republic of)	15	99	0,354	
Guatemala	16	112	0,251	
Antigua and Barbuda	17	113	0,247	
Costa Rica	18	115	0,221	
Trinidad and Tobago	19	123	0,188	
Barbados	20	127	0,173	

Country	Regional Rank 2018	Global Rank 2018	Score 2018	Change 2014
Saint Vincent and the Grenadines	21	129	0,169	
Bahamas	22	133	0,147	
Grenada	23	134	0,143	
Bolivia (Plurinational State of)	24	135	0,139	
Guyana	25	138	0,132	
Nicaragua	26	140	0,129	
Belize	26	140	0,129	
El Salvador	27	142	0,124	
Suriname	28	144	0,11	
Saint Lucia	29	149	0,096	
Saint Kitts and Nevis	30	157	0,065	
Haiti	31	164	0,046	
Honduras	32	165	0,044	
Dominica	33	172	0,019	

Source: ITU Global Cybersecurity Index (GCI) 2018 (latest available at the time of writing).
Note: The Global Cybersecurity Index (GCI) is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States cybersecurity commitment with regard to the five pillars identified by the High-Level Experts and endorsed by the Global Cybersecurity Agenda: (i Legal Measures, (ii Technical Measures, (iii Organizational Measures, (iv Capacity Building, and (v Cooperation.

Progress in the region is also visible in other aspects of the cybersecurity framework. According to data from Estonia's e-Governance Academy Foundation, the number of jurisdictions that have adopted national cybersecurity strategies has increased to include 13 in the region (from only six in 2015 according to the OAS report); the current signatories of the Budapest Convention stand at 8 within the region (instead of only two), and about 60 percent of regional jurisdictions now have an operational CSIRT (table 2).

Table 2
Cybersecurity framework features (selected jurisdictions)

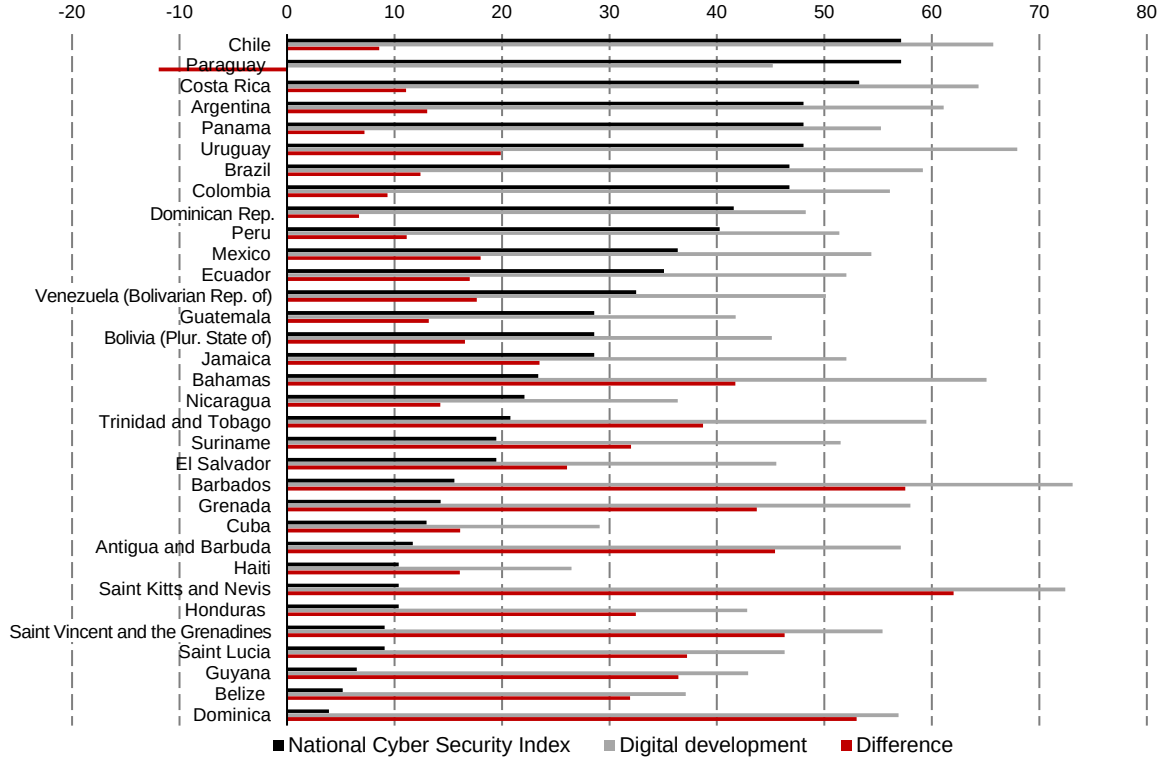
Country	National cybersecurity strategy (adoption)	Convention on cybercrime (adoption)	CSIRT unit
Antigua and Barbuda	✗	✗	✗
Argentina	✓	✓	✓
Bahamas	✓	✗	✗
Barbados	✓	✗	✗
Belize	✗	✗	✗
Bolivia (Plurinational State of)	✗	✗	✓
Brazil	✓	✗	✓
Chile	✓	✓	✓
Colombia	✓	✓	✓
Costa Rica	✓	✓	✓
Cuba	✗	✗	✓
Dominica	✗	✗	✗
Dominican Republic	✓	✓	✓
Ecuador	✗	✗	✓
El Salvador	✗	✗	✗
Grenada	✗	✗	✗
Guatemala	✓	✗	✗
Guyana	✗	✗	✓
Haiti	✗	✗	✗
Honduras	✗	✗	✗
Jamaica	✗	✗	✓
Mexico	✓	✗	✓

Country	National cybersecurity strategy (adoption)	Convention on cybercrime (adoption)	CSIRT unit
Nicaragua	✗	✗	✗
Panama	✓	✓	✓
Paraguay	✓	✓	✓
Peru	✗	✓	✓
Saint Kitts and Nevis	✗	✗	✗
Saint Lucia	✗	✗	✗
Saint Vincent and the Grenadines	✗	✗	✗
Suriname	✗	✗	✓
Trinidad and Tobago	✓	✗	✓
Uruguay	✗	✗	✓
Venezuela (Bolivarian Republic of)	✗	✗	✓

Source: Selected indicators from NSCI Index 2020, e-Governance Academy Foundation of Estonia, and Treaty Office of the Council of Europe.

Estonia's e-Governance Academy Foundation is well known for producing the National Cyber Security Index (NCSI), which measures the preparation of countries to prevent threats to cybersecurity and management of cyber incidents. Chile and Paraguay rank at the top of the region in the NCSI ranking, while Dominica closes the group with the lowest score. Figure 2, below, presents the NCSI score of available regional countries together with a Digital Development Level (DDL) and the difference between both scores. As presented in the figure, a negative difference (only happening in the case of Paraguay in this sample) shows that the country's cybersecurity development is in accordance with, or ahead of, its digital development. A positive result shows that the country's digital society is more advanced than its national cybersecurity, suggesting the size of the potential vulnerability.

Figure 2
National Cyber Security Index 2020 (available regional jurisdictions)



Source: e-Governance Academy Foundation of Estonia.
Note: The NCSI Score shows the percentage received from the maximum value of the indicators: 100 (100%). The Digital Development Level (DDL) is calculated according to the ICT Development Index (IDI) and Networked Readiness Index (NRI) as the average percentage obtained from both.

In order to produce the NCSI score, Estonia's e-Governance Academy Foundation collects a large number of indicators. This information, although only presented as a numeric grade or a binary choice, is useful to illustrate a point made in the introduction to this paper. It was suggested that, in general, the cybersecurity expectations in law and regulation for the behavior or companies stemmed mostly out of either data protection regimes or the regulation of critical infrastructure. The NCSI data on the region paints a very contrasted picture between those two areas for Latin American and the Caribbean.

Table 3, below, shows that there is a significant number of jurisdictions that have adopted data protection frameworks that score at par with those of the leading countries in the NCSI ranking (added to the table for the sake of this comparison). Although a number of regional jurisdictions have their results painted in red, indicating the lowest possible score, information collected for this paper shows that in many of them there are ongoing initiatives in the field that should improve those numbers shortly.

Table 3
NCSI indicators on data protection (selected jurisdictions)

Rank	Country	Protection of personal data	Personal data protection legislation	Personal data protection authority
1.	Greece	4	1	3
3.	Estonia	4	1	3
5.	Spain	4	1	3
15.	United States	4	1	3
39.	Chile	1	1	0
41.	Canada	4	1	3
38.	Paraguay	1	1	0
48.	Costa Rica	4	1	3
57.	Argentina	4	1	3
55.	Panama	4	1	3
58.	Uruguay	4	1	3
61.	Brazil	1	1	0
60.	Colombia	4	1	3
67.	Dominican Republic	1	1	0
70.	Peru	4	1	3
75.	Mexico	4	1	3
78.	Ecuador	0	0	0
85.	Venezuela (Bolivarian Republic of)	0	0	0
94.	Guatemala	0	0	0
95.	Bolivia (Plurinational State of)	0	0	0
96.	Jamaica	0	0	0
103.	Bahamas	4	1	3
105.	Nicaragua	4	1	3
108.	Trinidad and Tobago	1	1	0
113.	Suriname	0	0	0
111.	El Salvador	0	0	0
121.	Barbados	1	1	0
125.	Grenada	0	0	0
128.	Cuba	0	0	0
136.	Antigua and Barbuda	4	1	3
137.	Haiti	0	0	0
143.	Saint Kitts and Nevis	1	1	0
141.	Honduras	0	0	0
147.	Saint Vincent and the Grenadines	0	0	0
146.	Saint Lucia	4	1	3
149.	Guyana	0	0	0
152.	Belize	0	0	0
153.	Dominica	0	0	0

Source: Selected indicators from National Cyber Security Index 2020, e-Governance Academy Foundation of Estonia.

The results presented in table 4 for the cybersecurity of digital and essential services are significantly worse in the comparison between the region and leading jurisdictions. An almost solid block of red results populates the table for the regional jurisdictions in contrast to a green section at the top. The data in the last two columns are impressive. Not a single jurisdiction in the region has general cybersecurity requirements for operators of essential services nor conducts regular monitoring of their cybersecurity measures.

Table 4
NCSI indicators on protection of digital and essential services (selected jurisdictions)

Rank	Country	Protection of digital services	Cybersecurity responsibility for digital service providers	Protection of essential services	Operators of essential services are identified	Cybersecurity requirements for operators of essential services	Regular monitoring of security measures
1.	Greece	5	1	6	1	1	1
3.	Estonia	5	1	6	1	1	1
5.	Spain	4	1	5	1	1	0
15.	United States	1	0	6	1	1	1
39.	Chile	1	0	1	1	0	0
41.	Canada	1	0	2	1	1	1
38.	Paraguay	1	0	3	0	0	0
48.	Costa Rica	0	0	0	0	0	0
57.	Argentina	1	0	0	0	0	0
55.	Panama	3	0	0	0	0	0
58.	Uruguay	1	0	3	0	0	0
61.	Brazil	0	0	1	1	0	0
60.	Colombia	0	0	1	1	0	0
67.	Dominican Republic	0	0	0	0	0	0
70.	Peru	0	0	0	0	0	0
75.	Mexico	0	0	0	0	0	0
78.	Ecuador	1	0	0	0	0	0
85.	Venezuela (Bolivarian Republic of)	0	0	0	0	0	0
94.	Guatemala	0	0	0	0	0	0
95.	Bolivia (Plurinational State of)	0	0	0	0	0	0
96.	Jamaica	0	0	0	0	0	0
103.	Bahamas	0	0	1	1	0	0
105.	Nicaragua	0	0	0	0	0	0
108.	Trinidad and Tobago	0	0	1	1	0	0
113.	Suriname	0	0	0	0	0	0
111.	El Salvador	0	0	0	0	0	0
121.	Barbados	0	0	1	1	0	0
125.	Grenada	0	0	1	1	0	0
128.	Cuba	5	1	0	0	0	0
136.	Antigua and Barbuda	0	0	1	1	0	0
137.	Haiti	0	0	0	0	0	0
143.	Saint Kitts and Nevis	0	0	0	0	0	0
141.	Honduras	0	0	0	0	0	0
147.	Saint Vincent and the Grenadines	0	0	0	0	0	0
146.	Saint Lucia	0	0	0	0	0	0
149.	Guyana	0	0	0	0	0	0
152.	Belize	0	0	0	0	0	0
153.	Dominica	0	0	1	1	0	0

Source: Selected indicators from National Cyber Security Index 2020, e-Governance Academy Foundation of Estonia.

The information collected for the preparation of this paper generally confirms those discouraging results. With notable exceptions for certain sectors in a handful of countries, some of which will be highlighted in the following sections, there are not significant cybersecurity requirements aiming at companies, beyond those driven by data protection. As shown in table 5, below, for a selection of jurisdictions from the region, most of them have adopted data protection rules and some of them have even included key governance and accountability rules (like conducting data protection impact assessments, or DPIAs, and appointing data protection officers, or DPOs), that companies must follow to protect and secure the data of their users, tapping into the corporate governance of firms.[28]

Table 5
Key cybersecurity rules related to data protection (selected jurisdictions)

	Argentina	Bolivia (Plurination al State of)	Brazil	Chile*	Colombia	Costa Rica	Dominican Republic	Guatemala*	Mexico	Panama	Paraguay	Peru	Uruguay	Venezuela (Bolivarian Republic of)
Data protection authority	✓	×	✓	×	✓	✓	×	×	✓	✓	×	✓	✓	×
Restriction on international transfers to other jurisdictions	✓	×	✓	×	✓	×	×	×	×	×	×	×	✓	×
Restrictions on transfers to data processors	✓	×	✓	✓	✓	×	×	×	✓	×	×	✓	✓	×
Sanctions	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
Mandatory notification of breaches to authority and/or data subjects	×	×	✓	×	A	✓	×	×	✓	✓	×	×	✓	U
Mandatory DPOs	E	×	✓	×	✓	×	×	×	✓	×	×	E	✓	×
Mandatory DPIAs	✓	×	✓	×	R	×	×	×	✓	×	×	×	✓	×
Accountability	×	×	✓	×	✓	×	×	×	×	×	×	×	✓	×

Source: Author's elaboration.
Notes: (*): These jurisdictions have bills of law currently in Congress that include some of these measures; E: exceptionally; R: recommended; A: notification to the authority only; U: it is unclear who should be notified.

Beyond these rules, there is not a significant body of legislation or regulation imposing general cybersecurity requirements over companies in the region. Not even when those companies are handling critical infrastructure, holding assets or rendering services that should be guarded as part of a national cybersecurity strategy. As shown in table 4, above, the results for a large majority of regional jurisdictions are close to zero when dealing with the cybersecurity of digital services (including the imposing of cybersecurity responsibility for digital service providers) and essential services (including the identification of the operators of essential services and the establishing of cybersecurity requirements they must meet, not to mention their monitoring). This is troublesome as cyber risks do not only affect the specific companies providing those services, but all their users and the many other organizations and individuals that indirectly depend on the reliability of their functioning.

B. The cyber risk of critical infrastructure

Cyberattacks can take a multitude of forms. They can include data theft, fraud, distributed denial-of-service (DDoS), worms, ransomware, and viruses that can affect both private and public entities, as well as individuals. A 2018 report on cybercrime by the Center for Strategic and International Studies (CSIS), a think tank, and McAfee, a cybersecurity consultant, concluded that cybercrime is "relentless, undiminished, and unlikely to

[28] See Lehuedé (2019) for more information on the corporate governance implications of data protection frameworks in the region.

stop."[29] The report describes that DDoS attacks can be "outsourced" in the Dark Web[30] for about 500 USD and that passwords to corporate email inboxes are for sale for about 300 USD. Other reports show that more than 300 million new malicious viruses or malware are created every year and that the number of attacks continues to increase.[31] Accenture, a consultancy firm, assessed the value at risk globally from cybercrime at US$5.2 trillion for the period 2019-2023 (about the size of Japan's GDP),[32] while the likelihood of detection and prosecution in developed countries was assessed in 2018 to be as low as 0.05 percent.[33]

Cyber-attacks can be deployed by high-jacking control over systems and using them maliciously, not only to affect other connected systems, but also to have dangerous impacts over the physical world. The evidence shows that institutions providing essential services are increasingly being targeted by attacks that sabotage or cripple their systems and often prevent them from delivering vital public services. Attacks on critical infrastructure alone were rated the 5th highest cyber risk in 2020 by the WEF, a think tank, potentially affecting energy, healthcare, and transportation sectors, as well as entire cities.

On February of 2018, the Department of Transportation of the State of Colorado, in the U.S., was attacked by ransomware SamSam. The screens in their computer terminals went all gray and displayed the message "all your files are encrypted," demanding payment of bitcoin for the equivalent of 27,000 USD to obtain the decryption keys. The authorities refused. What followed was months of recovery efforts to salvage the 150 servers of the Department and to render operative the terminals of its 2,000 employees.[34]

On March of 2018 a prominent attack paralyzed for weeks the City of Atlanta, also in the United States.[35] The city spent over 17 million USD in incident response costs to restart its systems.[36]

The combination of high-profile targets of cybercrime, the sizeable damages caused and the rather unsuccessful prosecution of cyber criminals, have increased the attention of national authorities towards cybersecurity, particularly for critical infrastructure and essential services. At times this has been done with the urgency of a national security issue, particularly after a prominent cyber-attack linked with a hostile nation-state, but in many other cases at a much slower pace.[37]

---

29 See CSIS and McAfee (2018), Economic Impact of Cybercrime—No Slowing Down, 2018, p. 4.

30 The Dark Web is a part of the World Wide Web that is not indexed by search engines and where there is an abundance of sites that host offers for the sale or purchase of illicit material, including credit card numbers, drugs, guns, counterfeit money, stolen subscription credentials, hacked accounts, and hacking software. Its actual size is not really known, although estimates put it at about 5% of the total Internet. A 2019 study found that the number of dark web listings that offer content that could damage corporations has risen from 48% to 60% since 2016. See Into The Web of Profit, An in-depth study of cybercrime, criminals and money by Michael McGuire, Bromium, April 2018. For more information about the Dark Web see What is the dark web? How to access it and what you'll find by Darren Guccione, CSO Online, March 5, 2020.

31 See Nearly 1 million new malware threats released every day, by Harrison, Virginia and Jose Pagliery, CNN Business, April 14, 2015.

32 Accenture and the Ponemon Institute estimated the expected cost of cybercrime as a percentage of revenue for companies in a range of industries. Then they calculated the total industry revenues and multiplied those figures by the expected cost of cybercrime percentage for that industry. Finally, they analyzed how improved cybersecurity protection translates into less value at risk for business. See Accenture (2019), The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Research.

33 See Eoyang, M., et all (2018), To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors, Third Way, October 29, 2018.

34 See Colorado Department of Transportation (2018) "CDOT Cyber Incident After-Action Report" July 17, 2018.

35 See Ransomware Hits Georgia Courts as Municipal Attacks Spread by Lily Hay Newman, Wired Magazine, May 1, 2019.

36 See Deere, Stephen (2018), CONFIDENTIAL REPORT: Atlanta's Cyber Attack Could Cost Taxpayers $17 Million, The Atlanta Journal-Constitution, August 2, 2018.

37 According to the database of the United Nations Conference on Trade and Development (UNCTAD), at the beginning of 2020 135 jurisdictions around the globe had cybercrime legislation in place, 17 had it the legislative pipeline, and about 30 had not yet adopt any. See Cybercrime Legislation Worldwide (Database), United Nations Conference on Trade and Development. See also the United Nations Office on Drugs and Crime Cybercrime Repository of cybercrime laws and lessons learned.

Recent surveys show how much is still lacking within those efforts,[38] but also how crucial it is to move forward as the risks are perceived to be growing along with the increasing access to the Internet.[39] Considering the global nature of the cyber threat, cybersecurity frameworks need to be accompanied by the adoption of effective regulations, policies and institutions, ideally internationally coordinated or harmonized.[40]

The OAS General Assembly approved in 2004 the Comprehensive Inter-American Strategy to Combat Threats to Cyber Security,[41] whose objectives include establishing national CSIRTs and promotes the adoption of National Cyber Security Strategies that could manage the risks over critical infrastructure. Among those countries that have adopted such strategies, all have a section dealing with the protection of critical infrastructures. Unfortunately, many are still identifying those sectors or assets that should be included in the category, or the operators that manage them and their minimum cybersecurity requirements, so the strategies remain more theoretical than practical.

Essential services and critical infrastructure deal with public goods, even if in the hands of the private sector. Attackers target them assuming companies or public institutions will prefer to pay a ransom rather than deal with the public pressure of having their systems out of service for the long time needed to rebuild them. The State has a role in defending them, but when in private hands it is mostly for the private sector to manage cybersecurity to counter those risks. Most companies will have boards that understand these risks and will decide that it is in the interest of their company to invest in cybersecurity, to reduce their exposure, as discussed in chapter II. The crucial question is how much investment is deemed optimal in a for-profit environment when dealing with a public or national security issue.

Analyzing a similar case, Stiglitz & Wallsten describe how the economic theory predicts, and many empirical studies confirm, "that profit-maximizing firms invest less than the socially optimal level"[42] and that government intervention in some cases can help rectify this market failure, even if the design of such public policies is complex and not always successful. In the case of the cybersecurity of critical infrastructure, what is in society's best interest may not always in the best interests of the private companies handling them. Also, the risk that critical infrastructure may be subject to cyber-attacks directed by a foreign national enemy, may be deemed to escape what private sector companies consider to be part of their own level of responsibility.[43]

C. A role for regulation

As shown in the previous sections, although the region has made progress in addressing the cybersecurity requirements necessary for the protection of personal data of its citizens, it is lagging behind in regulating the cybersecurity of essential services and critical infrastructure. This is not only a problem in this region, as the

---

[38] The 2019 Internet & Jurisdiction Global Status Report offers a comprehensive mapping of internet jurisdiction related policy trends, actors and initiatives based on a survey of 150 key stakeholders (states, internet companies, technical operators, civil society, academia and international organizations). Among the key findings, it shows that "95% see cross-border legal challenges on the internet becoming increasingly acute in the next three years; only 15% believe we already have the right institutions to address these challenges; and 79% consider that there is insufficient international coordination." Internet & Jurisdiction Policy Network (2019). Internet & Jurisdiction Global Status Report 2019.

[39] Sixty nine percent of the Internet & Jurisdiction Policy Network's stakeholders surveyed 'agreed' or 'strongly agreed' that online abuses (including hate speech, harassment, hacking, privacy violations, and fraud) are increasing. Ibid.

[40] Enforcement efforts to trace or arrest the individuals responsible for cyber threats often face bureaucratic obstacles posed by the multiple jurisdictions involved. See Carter, William A. and Jennifer C. Daskal, "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge," Center for Strategic & International Studies, July 2018.

[41] See OAS (2004) Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity, Organization of American States, 2004.

[42] Stiglitz & Wallsten (1999), Public-Private Technology Partnerships: Promises and Pitfalls, American Behavioral Scientist, Vol. 43 No. 1, September 1999 52-73.

[43] See Madeline Carr (2016), Public–private partnerships in national cyber-security strategies, International Affairs 92: 1 (2016) 43–62, p.15. Carr suggests that private companies handling critical infrastructure will accept responsibility for cybersecurity "to the point that it is profitable; that is, as far as the cost of dealing with an outage promises to cost more than preventing it." Beyond that, when you are no longer dealing with low-level threats but protecting against an attack on the state (national security), the private sector has consistently argued in developed jurisdictions that it is the government who should protect assets against larger threats (organized crime, terrorists, and nation-state threats) either through law-enforcement or national defense.

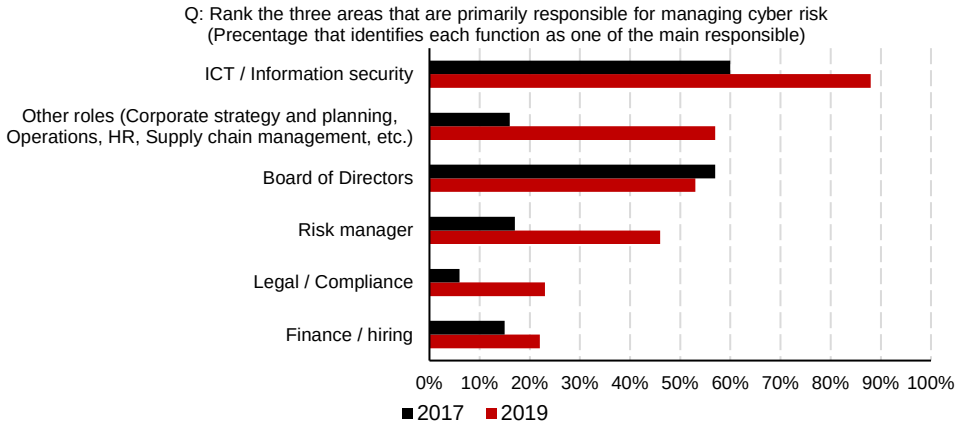
exact roles and responsibilities of companies dealing with critical assets are contested and controversial almost everywhere,[44] but that should not be a source of comfort, as the latent risks are significant. Carr suggests that the "reluctance of politicians to claim authority for the state to introduce tougher cybersecurity measures by law, coupled with the private sector's aversion to accepting responsibility or liability for national security," leaves this area of critical infrastructure "without clear lines of responsibility or accountability."[45]

This would not be such a significant issue if the level of cybersecurity preparedness of firms in the region was high already, but that is not the case. Findings for the region presented in a recent study conducted by Marsh, a risk consultant, and Microsoft, evidenced low levels of cyber preparedness.[46] The 2019 study included 531 corporate leaders from the region and showed that cyber-risk is clearly a priority on the agenda of firms in Latin America, ranking among the top five concerns for firms according to 73 percent of respondents (from 47 percent two years before). However, the results show that even if companies are adopting more rigorous and comprehensive management of cybersecurity, as compared to the previous survey in 2017, progress is still timid and slow. These were the levels of confidence of the surveyed regional leaders in critical aspects of their cyber resilience for 2019:

- understand, evaluate and quantify cyber threats (from 16 to 22 percent);
- prevent and mitigate cyber-attacks (from 12 to 20 percent), and
- manage and recover from cyber-attacks (from 7 to 18 percent).

The Marsh & Microsoft study also inquired into how firms within the region are managing cybersecurity, highlighting that many are making investments on technology protection tools (54 percent of planned investments were aimed at technology and mitigation) but may be neglecting other areas of risk management, such as risk assessment and contingency and recovery plans. Four out of five respondents on the study said that their companies have strengthened the security of ICTs since 2017, but less than a third said they had conducted cyber risk management training, or simulation of loss scenarios. The task to improve this numbers falls primary upon the ICT - information security area in 88 percent of companies (above boards of directors), but the risk management departments are growing in their role within cybersecurity (figure 3).

Figure 3
Primarily responsibility for managing cyber risk in Latin American companies



Source: Marsh & Microsoft (2019).

[44] Internet & Jurisdiction Global Status Report (2019) notes that the "increasing responsibility bestowed on private operators —through laws that make internet platforms the gatekeepers of content, as well as the voluntary assumption of responsibility— has occurred in numerous fields. This trend is particularly discernable in certain fields and has evolved particularly far in the context of terrorism, extremism and hate speech – fields in which some laws demand fast response times in content blocking." See Stanford Center for Internet and Society (2018), World Intermediary Liability Map, for information on online liability laws.

[45] See Madeline Carr (2016), p.1.

[46] See Marsh & Microsoft (2019) Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019, September 2019.

Well-run companies understand their responsibility and can see the value of investing in cybersecurity. Some others need reminding. Legal and regulatory frameworks are adding incentives to companies that do not do this simply out of their own interest, or to those that are moving too slowly. These policy interventions aim to make sure that boards and top managers pay due attention to cybersecurity, if not to prevent the damage of an attack to the company, at least to limit their own liability.

While it is common for CEOs and Chairmen to be reluctant about the prospects of new rules, often suggesting that self-regulation is a better alternative, cybersecurity seems to be the odd case where corporate leaders are looking forward for the role of regulation. In its 2018 survey on the views of boards of directors,[47] Spencer Stuart reported that board members listed cyber risk as a top concern and noted that they favor public policy interventions that could help industries move collectively towards better cybersecurity,[48] with a consensus forming about the need to have national, if not global, benchmarks.

The Marsh & Microsoft study also noted this trend, with regulators globally increasing pressure on firms to ensure that corporate leaders "are more directly responsible for effective cybersecurity, and that customer data is protected." It then asked respondents in the Latin American and Caribbean region what they thought the role of laws and regulations in cybersecurity should be. The findings show that 53 percent think that national and international legal and regulatory cybersecurity frameworks are essential for promoting the adoption of best practices within the private sector. However, 43 percent also pointed out that the definition of those best practices should be entrusted to industry standards established by recognized international organizations, such as NIST or ISO (see the Annex).

The practice by the leading jurisdictions in cybersecurity is, indeed, to move forward with regulation and legislation. They set the necessary incentives for the private sector to adopt an optimal level of cybersecurity for critical infrastructure. Lewis, writing for the IADB, notes that such jurisdictions share some common good practices, including "the adoption of appropriate laws and regulations for cybercrime, critical infrastructure, and data protection."[49] In a 2016 report reviewing the advanced experiences in cybersecurity of Estonia, Israel, South Korea, and the United States, Lewis highlights the importance of the legal and regulatory framework for cybersecurity. He describes how having a strategy and adopting the key rules and organization "are immediate requirements, and it is possible to achieve immediate results," while developing technically trained professionals, general cybersecurity education, and building a cybersecurity culture require longer and sustained efforts.

The report describes how the four advanced jurisdictions found it necessary to expand the legal and regulatory framework to deal with cybersecurity. They took immediate action rather than waiting "for the perfect strategy or the perfect law," arguing that perfection is unattainable in an environment that is rapidly evolving, where the best choice is to draw experience from best practices from other nations. A National Cybersecurity Strategy in this context may be regarded as "the initiation of a process that will lead to better cybersecurity rather than the end of the discussion." Lewis also notes that these regulatory efforts were conducted in cooperation with the private sector. Estonia, Israel, and the United States "made private sector participation a critical element of their cybersecurity efforts."

---

47 See Spencer Stuart (2018), What Directors Think, 2018.

48 The effectiveness of cybersecurity can greatly improve by the alignment of industry incentives to encourage producers to adopt safe default settings in the information technology and connected devices they market. Across the globe, legislators, regulators and associations are looking for incentives to steer the corporate sector towards better practices that would put safer products in the hands of users, creating a virtuous circle of cyber security involving individual consumers and other organizations.

49 James A. Lewis (2016), Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States, Inter-American Development Bank, 2016, p.10.

II. Case studies

The next sections discuss three examples of how some national laws and regulations in Latin America and the Caribbean are incentivizing firms to increase their levels of cybersecurity for essential services and critical infrastructure, paying particular attention into what kind of demands they have for the corporate governance of firms. The cases have been selected considering how developed are the cybersecurity regulations or guidance in the region, as well as the relevance of the sectors, as in the case of State-owned enterprises.

A. Cybersecurity expectations at SOEs (in Chile)

State-owned enterprises (SOEs) stand at the border between the private and public sectors and are often trusted to handle essential services and critical infrastructure, frequently in a monopolistic setting. Cyber risks in this context are particularly crucial.

A 2017 report by the OECD on the size and distribution of SOEs describes the importance of these entities in the national economies of several of its member jurisdictions. The report describes that they frequently operate in sectors with high levels of linkage to essential goods and services for the operation and competitiveness of national industries, like transportation, public utilities and finance.SOEs also represent a sizeable portion of national assets and employment in some jurisdictions, with a total valuation estimated by the OECD in 2017 at over USD 2.4 trillion and 9.2 million people employed.

The International Finance Corporation (IFC) has slightly addressed the cybersecurity expectations for SOEs as part of its 2019 Corporate Governance Progression Matrix for State-Owned Enterprises,[50] which is aimed at helping these entities better integrate ESG (environmental, social, and governance) issues in their corporate governance practices. The IFC guidance calls for specialized committees with independent members to oversee conflicts of interest and technical topics, including cybersecurity, if applicable. It also

[50] IFC (2019) Corporate Governance Progression Matrix for State-Owned Enterprises.

describes that best practices for internal control at SOEs will require the adoption of international standards, including ISO 31000, ISO 19600 and ISO 27001 on information security management systems (See Annex).

Although more specific guidance on how to address cybersecurity within SOEs is not readily available, perhaps because there are no significant technical differences from how private companies should handle these issues, it is important to notice that SOEs face a somewhat different incentive setting. As mentioned, when deciding the optimal level of investment on cybersecurity, what is in society's best interest may not always in the best interests of the companies handling them. Now, if those companies are run by the State, ensuring the public interest is more likely to fall within the mandate of boards and management, as well as to be backed by effective accountability. We would expect, then, to find the State leading with the example, with a more robust cybersecurity framework than average in SOEs dealing with critical infrastructure.

Chile offers a good example. Most of the State-owned enterprises (SOEs) in Chile are managed by a central public agency called Sistema de Empresas Públicas (SEP).[51] SEP's portfolio includes 20 strategic companies, holding assets for 12 billion USD and employing more than 12,000 workers in fields such as ports, transportation and the postal service. Among the policies adopted by the SEP is a Code[52] that contains ethical principles and corporate governance practices, as well as regulations and management policies that define the expectation for the behavior of those in leadership and management positions at all the companies in its portfolio.

Chapter 9 of the SEP Code deals with cybersecurity (information security in the language of the document). It was drafted using ISO 31.000 (2009) and ISO 27.001 (2005) standards, as well as COSO's integrated framework, as a reference (see the Annex). The cybersecurity expectations set in the Code ask for the protection of the SOE's information through policies, organizational structures, procedures, and adequate allocation of resources for information security within the organization.

Among the three key considerations listed for the design of such framework, the first is the commitment by the Board and management, which is expected to include engagement and regular reviews of the overall status of the information security program and the provision of direction, whenever needed. The second key element is implementation, where the Code suggests that information security is a continuous process, involving technological and human resources issues, for which comprehensive solutions are required in three stages (diagnosis, planning, and implementation). The last key element is a set principles that and should be reflected throughout the information security system: integrity, accuracy, confidentiality and availability.

The structure of the information security of all SOEs dependent on the SEP should be structured around an information security policy, a Security Committee, the appointment of a Security Officer, a business continuity management system and a compliance program, among others:

- The information security policy should reflect the expectations of the organization and provide support to the established principles, by providing for the adoption of a General Information Security Policy and specific rules or procedures, such as Access Control, Operational Continuity, and Physical Security;
- The Security Committee, composed of board members and senior management, is responsible for defining and establishing general security guidelines, publishing and approving policies, standards and other definitions;
- The Security Officer is in charge of ensuring the functioning of the framework, including responsibility for defining and implementing the annual dissemination plan, ensuring compliance with defined security norms, procedures and standards, reporting to the Security Committee on incidents and risks, and ensuring that contingency plans remain updated and tested for operational continuity;

---

[51] See the webpage of the SEP: http://www.sepchile.cl.

[52] See SEP (2017), Nuevo Código SEP, Sistema de Empresas Públicas, 2017.

Management of operational continuity for information security must be adopted, to face interruptions in institutional activities and protect critical processes from the effects of major failures or disasters in information systems, ensuring timely recovery, and

A compliance program should include routine audit procedures to avoid breaches of any law, statute, regulation or legal contractual obligation and of any security requirement to which the design, operation, use and management of information systems may be subject.

B. Cybersecurity in the financial sector (several jurisdictions)

One of the essential services sector that has made more progress in addressing cyber threats in the region is the financial sector, and banking in particular. It was one of the first sectors that embraced the opportunities of the digitalization of the economy and electronic banking has proved a suitable solution in the region, particularly due to the penetration of the Internet through mobile devices. Naturally, the risks came along with the opportunities, and hacks and online fraud have become part of the daily concerns of banks and their users alike.

Banks were targets of cyber-attacks already in the 1990s, mostly benefiting from the lack of awareness among banking users and the unsophisticated nature of the hardware for securing communications and passwords. In the 2000s risks multiplied, with online fraud becoming commonplace. In many jurisdictions the amounts stolen were still rather small and banks covered them as a cost of doing business, so regulators were not yet involved. This started happening only in the 2010s when information security teams started forming in larger banks,[53] information encryption tools became available and regulators decided that the risks were too high to keep unaddressed. Slowly, regulation from banking authorities in a number of jurisdictions explicitly demanded higher cybersecurity systems and reporting, as well as introduced some form of accountability from boards and management over the security of the essential banking systems.

In Bolivia, where data protection is still not well developed, the main cybersecurity obligations for companies can be found in the financial sector. Pursuant to the Financial Services Law N° 393 of 2013,[54] and Resolution N° 596/2019 of the Authority for the Supervision of the Financial System,[55] financial intermediaries are required to adopt a number of cybersecurity controls and policies to prevent data breaches. The assessment of the information security systems and the cybersecurity policies must be reported regularly to management, approved by the Board, and operate within a framework of accountability where responsibility for all the relevant actors is defined.[56]

---

53 See Santiago F. Rodríguez V., Felaban: Cybersecurity In Latin American And Caribbean Banking, at Chapter 3.4 of OAS (2018), State of Cybersecurity in the Banking Sector in Latin America and the Caribbean, Organization of American States.

54 See the Financial Services Law N° 393, of 21 August 2013, available at: https://www.bcb.gob.bo/webdocs/sistema_pagos/2013 - LEY 0393 - Servicios Financieros.pdf.

55 See Resolution N° 596/2019 of the Authority for the Supervision of the Financial System, available at: http://servdmzw.asfi.gob.bo/circular/circulares/ASFI_596.pdf.

56 Among other, the Bolivian framework requires: i) That companies that manage electronic cards must have security systems aimed at preventing fraud capable of generating operational failure reports that have to be forwarded to the Financial System Supervisory Authority – ASFI (Article 361 of the Financial Services Law); ii) That mobile payment service companies adopt at all times effective security mechanisms of technological platforms for the provision of mobile payment services, including the adoption of plans for the continuity of the service, guaranteeing the confidentiality and protection of operations. This responsibility is extended to entities that directly provide mobile payment services, and must adopt the operational measures and procedures that guarantee the operations and proper functioning of the service (Articles 375 and 376 of the Financial Services Law), and iii) That operations carried out through electronic means must comply with the security measures that guarantee integrity, confidentiality, authentication and non-repudiation. For that, the ASFI and the Central Bank of Bolivia have the authority to issue regulations that establish the procedures and safety regulations for operations, as well as the minimum requirements that entities must meet to carry out electronic banking activities, banking by telephone and by mobile devices, as well as regulatory compliance with mandatory compliance by financial institutions that provide the service (Article 124 of the Financial Services Law).

A similar case can be found in Guatemala, where in the absence of a functioning data protection regime (a number of bills of law are currently being discussed in Congress),[57] some corporate cybersecurity obligations can be found in Decree 19-2002, the Law of Banks and Financial Groups,[58] which establishes the confidentiality of the operations and information of bank customers.

In Chile, where a bill of law aiming to revamp outdated data protection rules adopted in the 1990s[59] has been in discussion for years, and there is still no national data protection or cybersecurity authority, the financial sector is also ahead of the rest. This is so evident that a former banking commissioner was the latest national cybersecurity coordinator, high-level position created as a Presidential advisor that has seen great turnover and large periods of vacancy.

Although there is no general cybersecurity breach notification requirement in Chile, for banks and financial institutions any cybersecurity incidents must be reported to the Banking supervisory authorities when it may put their business continuity at risk, endanger their or their clients' resources, the quality of their service or the entity's image. Notification of any cybersecurity incident must be made within 30 minutes from the moment it takes place, including as much information as possible. Once the incident is controlled, a report is required including an extended set of information listed in the regulation.[60] Clients and users must be informed and kept up to date, but only if the incident affects the continuity or quality of service, or is of public knowledge.

The Chilean cybersecurity regulations for financial institutions contains a non-exhaustive list of possible incidents, which includes "technology issues affecting information security" and "loss of information of the bank or its clients," among others. Entities are required to appoint an officer as contact point and define a clear communication channel with the authority. Banks and insurance companies have additional requirements that involve a risk management approach to cybersecurity.

A recent update of Chapter 20-10 of the Chilean banking regulation61 that was published in July 2020, and which will enter into force in December 2020, reinforces the link between cybersecurity expectations for critical infrastructure and corporate governance of firms in the financial sector.[62] In the new rules, the regulator states that the board plays a fundamental role by setting the institutional strategy and budget for cybersecurity. It is the board's responsibility "to ensure that the entity maintains a management system for information security and cybersecurity, which contemplates the specific administration of these risks in consideration of existing international best practices, which must be consistent with the volume and complexity of the entity's operations." Among other requirements, the rules ask the board to:

---

57 See: Iniciativa 4054 – "Ley Contra el Cibercrimen" (18/Aug/2009) available at: https://www.congreso.gob.gt/detalle_pdf/iniciativas/2227; Iniciativa 4094 – "Ley de Protección de Datos Personales" (20/Aug/2009) available at: https://www.congreso.gob.gt/detalle_pdf /iniciativas/1353; Iniciativa 5254 – "Ley Contra la Ciberdelincuencia" (09/Mar/2017) available at: https://www.congreso.gob.gt/detalle_ pdf/iniciativas/4266, and Iniciativa 5601 – "Ley de Prevención y Protección Contra la Ciberdelincuencia" (17/Sep/2019) available at: https://www.congreso.gob.gt/detalle_pdf/iniciativas/5614.

58 Decree 19-2002: Law of Banks and Financial Groups, available at: https://www.banguat.gob.gt/leyes/2013/ley_bancos_y_grupos_ financieros.pdf.

59 Law 19.628 of 1999, the Personal Data Protection Law. See the full text of the Law at: www.leychile.cl/Navegar?idNorma=141599

60 See Chapter 20-8 of the Updated Compilation of Rules issued by the Chilean Commission for the Financial Market, available at: https://www.sbif.cl/sbifweb3/internet/archivos/norma_10696_1.pdf.

61 See the July 2020 update of Chapter 20-10 of the Updated Compilation of Rules issued by the Chilean Commission for the Financial Market, available at: http://www.cmfchile.cl/portal/principal/605/articles-29310_doc_pdf.pdf.

62 The banking regulator states that the financial industry and the payment system are a relevant component of the country's critical infrastructure, as defined by the National Cybersecurity Policy to include "includes facilities, networks, services and physical and information technology equipment whose affectation, degradation, interruption or destruction can have a significant impact on the safety, health, well-being of citizens and the effective functioning of the State and the private sector." It then adds that for this reason financial institutions must have policies and procedures for the identification of those critical assets and for the adequate exchange of technical information on incidents that affect or could affect the entity's cybersecurity, with other members who are part of this critical infrastructure, always taking care to comply with the legal requirements of secrecy and legal reserve, and of confidentiality of customers' personal information. In order to detect and manage threats and vulnerabilities that could affect the operation of the system as a whole, the regulator encourages all financial entities to carry out joint tests of risk scenarios.

- Define an organizational structure with specialized and dedicated personnel and collegiate bodies at a high hierarchical level, with the powers and competencies necessary to manage information security and cybersecurity;
- Establish a risk function, independent of the risk-generating areas, responsible for the design and maintenance of an adequate system for the identification, monitoring, control and mitigation of information security and cybersecurity risks;
- Create a high-level structure for crisis management, with real administrative powers, legally delegated by the board to know and manage high-impact security and cybersecurity incidents that affect or could affect its own or its clients' information assets;
- Approve, disseminate, reviewed and revise at least annually the necessary policies for the management of information security and cybersecurity risks that define at least the scope and objectives of the entity regarding these matters; the specific risk tolerance level for each of them; a clear definition of the information assets to protect; criteria for classifying information and the existence of a permanently updated inventory of information assets, consistent with the entity's process map, and
- Ensure that it is regularly and adequately informed about the risks to which the entity is exposed in terms of information security and cybersecurity, as well as compliance with its policies and incidents of information security and cybersecurity, in order to improve its management and prevention.

In Panama, which is a regional financial hub, cybersecurity obligations for companies can be found in the data protection regime,[63] but also in abundant regulation for consumer credit reporting agencies[64] and in the financial sector. The banking regulator has adopted two rulings that set guidelines for the management of information technology risks (Agreement No. 003-2012 of May 22, 2012)[65] and on electronic banking and the management of related risk (Agreement No. 006-2011 of December 6, 2011).[66] Both include requirements on business continuity management systems and information security management systems. The second one also addresses disaster recovery and the obligation for all banks to develop a comprehensive plan for both business continuity and disaster recovery.

Data breaches are also subject to notification requirements in the financial sector of Panama, where financial institutions must report to the Superintendency of Banks any event or attempted fraud of electronic banking services. Some accountability and governance rules can also be found in Panama, requiring that banks must have an information security unit within their organizational structure, reporting to an official of high hierarchy and independence.

All these national efforts are contributing to enhancing the cybersecurity of the financial sector in the region. The OAS conducted in 2018 a regional survey of cybersecurity in the banking sector in particular.[67] Its key findings present a picture of persistent risks, with at least 9 out of 10 banks having suffered cyber incidents during the last year, 37 percent of them having been successful, and 39 percent of the incidents not having been reported (in the case of the largest banking entities, this number goes down to 19 percent). But in the report there is also evidence of progress in cybersecurity, which albeit uneven and sometimes slow-moving, is advancing on the financial sector throughout the region.

---

63 Law No. 81 of 2019, Law on Protection of Personal Data, available at: https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf.

64 Law No. 24 of 2004 that regulates the information service on credit history, available at: https://www.superbancos.gob.pa/superbancos/documentos/leyes_y_regulaciones/leyes/Ley_24-2002.pdf.

65 See Agreement No. 003-2012 of May 22, 2012, available at: https://www.superbancos.gob.pa/superbancos/documentos/leyes_y_regulaciones/acuerdos/2012/Acuerdo_3-2012.pdf.

66 See Agreement No. 006-2011 of December 6, 2011, available at:https://www.superbancos.gob.pa/superbancos/documentos/leyes_y_regulaciones/acuerdos/2011/Acuerdo_6-2011.pdf.

67 See OAS (2018), State of Cybersecurity in the Banking Sector in Latin America and the Caribbean, Organization of American States.

The report describes how boards and top managers at banks are increasing their attention to cybersecurity. This is reflected in the narrowing distance between the head of cybersecurity and the CEO, which currently stands at two hierarchical levels on average, and in that 72 percent of the boards within regional banks receive periodic cybersecurity reports, directly or through a specialized board committee.[68] Commitment to cybersecurity within banks is also reflected in their support to risk management, with 65 percent of them making the adoption of good cybersecurity practices a corporate objective, 63 percent promoting training and awareness, and 60 percent sponsoring digital security plans. The report also describes the extended adoption of ISO 27001 and COBIT standards (see Annex) within the banking sector in the region.

One aspects where support from the top is still deemed insufficient, as shown in the OAS report, is budget. Sixty percent of surveyed entities reported difficulties securing funding for cybersecurity, which currently stands, on average, at less than 1 percent of EBITDA of the previous fiscal year for about 60 percent of banks. In about a third of banks it rises to between 1 and 5 percent, and only in one out of twenty it is greater than 5 percent of EBITDA of the previous fiscal year. This, despite that the estimated return on investment in cybersecurity is set at approximately 24 percent, and with three fourths of the experts surveyed for the report indicating that the total cost of responding to, and recovering from, a cybersecurity incident is on average 1.5 percent of EBITDA of the preceding year (about two million USD per incident on average, totaling approximately 809 million USD for the region in 2017).

The OAS report makes an important policy point in calling for harmonization of cybersecurity, data privacy and ICT frameworks, as critical components for the development of the financial sector in the region going forward.

C. Cybersecurity in the electricity sector (based on regional study)

The energy sector is part of any definition of critical infrastructure and another example of a sector where digitization has been widely adopted, exposing it to cyber-attacks and a likely target for cyber war.[69] The December 2015 attack on the Ukrainian power grid, considered to be the first cyberattack of its kind, is a good example of the scope of cyber risks in the sector. Then, unidentified hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine, temporarily disrupting the electricity supply to hundreds of thousands of people, from 1 to 6 hours, in the middle of winter.[70]

As various actors intervene in a power grid, from power generation to transmission to the end customers, including power generators, energy providers, transmission service providers, and consumers, the risks are multiple. Unlike other types of interconnected systems where the fall of a node does not imply the fall of the system, in a power network the failure of any node changes the flow of energy and leads to a redistribution of loads across the network, which may lead to blackouts due to overload. This makes the electricity grid particularly susceptible to threats that can affect the availability of the service.

A recent study of the electrical systems in Latin America by Barrero, writing for the IADB, shows how knowledge about cybersecurity has begun to develop in the region.[71] The 2020 study, conducted via a digital survey aimed at CISOs and Senior Control Engineers throughout the electricity supply chain, was responded by 43 companies in the region (including companies with a main business in generation, transmission, distribution and national operators of electrical systems). The results of the report show that up to 68 percent of firms see a high probability of being victims of cyberattacks, including malware, ransomware and sabotage to IoT devices.

---

[68] According to the OAS report, digital security management (information security, cybersecurity and fraud prevention in digital media) is overseen by the Risk Committee in 39% of banking entities in the Latin America and the Caribbean region. The Security Committees (23%) and Technical or Technology Committees (21%) are also involved.

[69] See https://en.wikipedia.org/wiki/Industroyer for a description of the malware (Industroyer or Crashoverride) considered to have been used in the cyberattack on the Ukrainian power grid in 2016, and https://en.wikipedia.org/wiki/Stuxnet for a description of the malware (Stuxnet) allegedly used to cripple the Iranian nuclear program in 2010, both believed to have been developed by national intelligence services.

[70] See How an Entire Nation Became Russia's Test Lab for Cyberwar, by Andy Greenberg, June 20, 2017, WIRED magazine.

[71] See Barrero, Vladimir (2020), Estado de preparación en ciberseguridad del sector eléctrico en América Latina, Monografía del BID; 802, Vladimir Barrero, Oscar Bou; editores, Juan Roberto Paredes, Miguel Porrúa.

Despite the awareness of the cyber risks faced, 16 percent of respondents described that while having support from management and the board, they lack a dedicated cybersecurity budget. Likewise, 20 percent of companies have not yet adopted a cybersecurity policy and only 13 percent have adopted a robust policy. A majority of those that have a policy, do not conduct regular updates on it and less than half communicate and train their employees and stakeholders on the policy through formal or informal mechanisms. Likewise, in two out of five companies in the survey, the role of the CISO is not part of the internal organization, and in a third of them it is a part-time assignment, shared with other roles.

The IADB report points out the lack of meaningful commitment in some firms, and concludes with a set of policy recommendations, calling for a harmonized framework within the region that is built upon some key considerations:

- States must develop their National Cybersecurity Strategies, following the roadmap set by the OAS, setting their definition and classification of critical infrastructure, and identifying their operators. Whether public or private, those operators should be required to adopt cybersecurity protection plans, identifying threats and vulnerabilities to their infrastructure, which should be reviewed by the relevant authorities.
- States must develop a security strategy for the energy sector and promote regulatory development via frameworks, guidelines and recommendations to encourage more robust and mature cybersecurity in the sector, built around risk assessment, cyber resilience strategies and continuity of service plans.
- National and international cooperation is needed as grids begun to interconnect across the region, requiring communication and cooperation mechanisms for the prevention, identification, response and recovery of cybersecurity incidents in the network or within electric operators.
- Coordination among CSIRTs and the development of a common framework for cooperation and exchange of information between the parties involved and the public authorities, which could facilitate the detection and management of an incident as soon as possible, thus reducing its impact and scope. This may require the design of training, qualification and certification programs of the specific capacities required for the identification, prevention, detection, response and recovery of cyber incidents.
- The formalization of a roadmap with the participation of the private sector, but also of independent experts, that allows progress in the above listed objectives considering the concerns and economic relevance of the grid, as well as the role of policymakers and their responsibility before citizens for the risks affecting the functioning of the sector.

These recommendations are well aligned with those contained in a 2019 European Commission Recommendation[72] that proposes a series of actions to reinforce cybersecurity in the energy sector in Europe. Among them, the Commission urges relevant agents, such as energy network operators, technology providers and especially essential service operators, to adopt standards such as ISO / IEC 27001/27019, IEC62443, IEC62351 and ISO / IEC31000 (see the Annex).

As an example of what jurisdictions in the region are doing, the Chilean National Coordinator for the Electric Sector, an autonomous public law and not-for-profit corporation, launched in September 2019 an initiative leading to the adoption of a Cybersecurity Plan for the national electric sector.[73] This follows a request from the Chilean Ministry of the Interior for the establishment of a CSIRT for the sector, and a

[72] See EC (2019) Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector, SWD (2019) 1240 final, European Commission, available at: https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf.

[73] See a 2019 presentation of Pan de Ciberseguridad by Coordinador Eléctrico Nacional of Chile at: https://www.coordinador.cl/wp-content/uploads/2019/09/20190927-Plan-Ciberseguridad.pdf.

request from the Superintendency of Electricity and Fuels for the Coordinator to: i) collect information of cybersecurity practices among companies (for which the authority was planning the launch of a survey); ii) define minimum requirements for safeguarding cybersecurity within the electricity sector, understanding that a cyber-attack will not qualify as *force majeure*, and iii) instruct immediate measures for the implementation of such minimum standards.

As described in the information publicly available at the time of writing this report, the Coordinator has requested companies within the sector to self-assess the risks and risk management practices they currently have. This includes their adoption of information security measures, event registration and permanent monitoring, their implementation of controls and formalized related procedures, as well as the definition and execution of business continuity plans and disaster recovery plans. Next steps will include the creation of a Security Committee (including representatives of the Ministry, the Superintendency and the Coordinator), the implementation of "urgent" minimum requirements and, looking at the medium term, to work in the adoption of an industry standard: NERC-CIP / ISO 27002 (see the Annex).

The presentation of the Cybersecurity Plan by the Coordinator concludes with some high-level messages. Among them are that "it is urgent to establish a culture of safety, so that risk mitigation measures are valued even when they generate effort or discomfort"; that "security measures must be promoted by the top management of the organizations and complied with by all without exceptions," and that "cybersecurity is a permanent task that requires constant revision." [74]

[74] See Ibid, p. 10.

III. Corporate governance implications

Companies contribute a fair share to the creation of cyber risk. The ICT systems they build and the digital assets they use to sell their products or render their services, in their move towards an ever more digital economy, are attractive targets for cybercriminals. That is also the case for the databases with personal data of stakeholders they collect and process, which could be misused for fraud and espionage. They also handle critical parts of the infrastructure of countries, which have become heavily dependent on ICT systems and IoT devices, and shoulder a responsibility to ensure continuity of their services. Companies have thus a primary responsibility to also adopt the internal measures needed to mitigate the cyber risks they help create.

This chapter aims to describe how the management of cyber risk is viewed from a corporate governance perspective. It presents the expectation for the board of directors in cybersecurity, through the adoption of safe business models and corporate practices that can improve data security and guard its privacy.

A. The scope of cyber risk for companies

In line with good corporate governance practices, the board is expected to identify and deal with risky issues and oversee management, to ensure that they are mitigated in a way that can ensure the sustainability of the company. The board has to exercise control, oversight and set the risk appetite[75] and tolerance for the organization, in-line with the mission, vision, values and the strategic plan it has set for the business.[76]

Cyber risks have moved up in the agenda of boards to reach a prominent position at the top. The scope of corporate cyber risk is extremely wide, and it will likely continue to increase as more people acquire better

[75] The risk appetite is the amount of quantifiable risk an organization is willing to accept in pursuit of its strategy. A board should define at what level of measured risk the company should deploy the appropriate controls and mitigating actions needed bring risk back to acceptable levels. The risk appetite should be communicated to inform decisions across the enterprise and influence the corporate culture. For more on risk appetite see PwC (2014), Board oversight of risk: Defining risk appetite in plain English.

[76] The G20/OECD Principles of Corporate Governance establish that boards are expected to have oversight "of the accountabilities and responsibilities for managing risks, specifying the types and degree of risk that a company is willing to accept in pursuit of its goals, and how it will manage the risks it creates through its operations and relationships. It is thus a crucial guideline for management that must manage risks to meet the company's desired risk profile." See OECD (2015), G20/OECD Principles of Corporate Governance, OECD Publishing, Paris.

access to the Internet and companies advance their digital strategies. Data breaches and malware attacks, among other cybersecurity risks, could thus have significant impacts over companies and their customers, employees and their supply chains. A 2018 survey by Kaspersky Lab,[77] a technological consultant firm, collected responses from almost 6,000 businesses across 29 countries, showing that 46 percent of small and medium-sized companies, and 42 percent of large enterprises, have suffered at least one data breach at some point in their history.

A 2019 study by the Ponemon Institute and IBM Security, analyzing over 500 companies from around the globe, concluded that the average organizational cost of a data breach in 2019 was $3.92 million USD. It is even higher in some countries, like in the U.S., where it reaches $8.19 million USD on average.[78] Class-action lawsuits add to these costs in some jurisdictions, with settlements reaching over $100 million USD.[79] But disruption is not only financial, nor paid as direct out-of-pocket expenses or fines following a cybersecurity failure. On average, stocks of affected companies decline in price about 5 percent following the disclosure of such events.[80] The Ponemon Institute and IBM Security study also found that loss of customer trust had a large impact. Organizations suffering a data breach in 2019 reported an average cost of lost business for of USD 1.42 million (36 percent of the total average cost). About a third of companies that experienced a breach included in the Kaspersky Lab survey, mentioned above, said they had to also lay off staff as a consequence.

The U.S. National Association of Corporate Directors (NACD) conducted a survey of listed companies over 2018–2019, finding that directors selected the threat of cyberbreach as the third most likely to have the greatest impact on their companies in the coming 12 months.[81] Aligned with this, the WEF's 2019 Risk Report[82] pointed that data fraud and cyber-attacks were high in the concerns of corporate leaders. The 2020 version goes even further, and ranks cyberattacks as the seventh most likely and eighth most impactful risk, and the second most concerning risk for doing business globally over the next 10 years.[83]

B. The responsibility of the board over cybersecurity

Cyber risk raises serious management challenges, both from financial and reputational perspectives, and can expose the company and its leaders to material consequences. This is why cybersecurity is on the agenda of most board meetings these days, both to prevent future incidents as well as to deal with the consequences of those that already took place.

Corporate leaders are increasing their attention to cybersecurity, often becoming reluctant participants in what appears as a complex and sometimes technically incomprehensible processes of protecting the firm's systems, processes and data. However, board are recognizing that cybersecurity is an indispensable requirement for their companies being able to advance in their digital transformation, create long-term value and sustain trust with its online customers and other key stakeholders.[84] Directors are understanding that it is their duty and in the interest of their companies, to ensure that internal processes and policies are in place to address potential cyber risks, and to oversee an effective implementation of cybersecurity and privacy frameworks.

Cybersecurity and data protection rules in some jurisdictions are increasing these stakes by making board members and top managers personally responsible for cybersecurity-related risks. As suggested by insurance experts,[85] boards' failure to comply may be viewed as a breach of their own duties to exercise due

---

77 See Kaspersky Lab (2018), From data boom to data doom: the risks and rewards of protecting personal data.
78 See Ponemon Institute and IBM Security (2019), Cost of Data Breach report 2019.
79 See Southwell, Alexander H. et al (2017), Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy, The CLS Blue Sky Blog (Columbia Law School), February 3, 2017.
80 See: Ponemon Institute (2017), The Impact of Data Breaches on Reputation and Share Value, May 2017.
81 See NACD (2018), 2018–2019 Public Company Governance Survey, 2018, National Association of Corporate Directors.
82 See WEF (2019), Global Risks Report 2019, World Economic Forum.
83 See WEF (2020), Global Risks Report 2020, World Economic Forum.
84 See NACD (2020), Director's Handbook on Cyber-Risk Oversight, National Association of Corporate Directors, January 2020.
85 See Directors Beware: The EU's General Data Protection Regulation Is Upon Us!, blog post by Kevin LaCroix, December 20, 2017.

care, skill and diligence. Thus, they may be exposed to damages and termination, or even disqualification, in a way that not even their cyber[86] and "directors and officers" (D&O) insurance may be able to shield them from.

Some of the more recent surveys are however showing signs of progress, with boards beginning to feel more comfortable with their role on cybersecurity.[87,88] According to a NACD 2019-2020 survey of listed companies,[89] even if only half of directors think that their own understanding of cybersecurity is strong enough to provide effective oversight, almost 80 percent of boards declare having significantly improved their understanding of cyber risk compared to two years ago. Two thirds of boards now express confidence their companies can effectively respond to a materially significant cybersecurity breach.

C. Board oversight of cyber risks in practice

Numerous organizations offer advice as how boards can oversee these risks, some of them offer technical frameworks as discussed in the Annex, and others have elaborated guides and handbooks, some of which have been cited already. The EY Center for Board Matters[90] suggest some of the main objectives that boards need to consider to effectively oversee the management of cybersecurity:

- Understanding the cyber risks facing the organization and how they may affect the business;
- Challenging the effectiveness of the organization's cybersecurity risk management program, and supporting the continued evolution of the program;
- Gaining confidence in the adequacy of the program; and
- Having assurance in the information they receive.

The first step to any attempt by the board to tackle cyber risks is to understand how they apply to their firm. As each firm is different, there is no simple model or foolproof guidance to accomplish this, other than resorting to best practices, standards and committing to the hard work it entails.

In the U.S., the third edition of the NACD Cybersecurity Handbook of 2020[91] offers 5 principles that help to summarize what boards should consider assessing their exposure to these risks:

- Directors need to understand and approach cybersecurity as a strategic, enterprise risk, not just an ICT risk.
- Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
- Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on board meeting agendas.
- Directors should set the expectation that management will establish an enterprise-wide, cyber risk management framework with adequate staffing and budget.

---

86 In some developing countries, cybersecurity insurance itself is not widely available. New startups and companies linked to large cybersecurity providers, like Symantec-backed CyberCube, are offering risk-modeling platforms to insurers in order form them to process the mighty data that are necessary to calculate the risk of the potential clients. Microsoft for Startups is also investing in these models.

87 A 2018 survey by the NACD found that in the U.S. 97 percent of directors of listed companies and 94 percent of directors in private companies were looking to improve cybersecurity oversight in 2019. See NACD (2018).

88 A survey by PWC pointed that a majority of corporate directors had allocated more resources or budget to cybersecurity in 2018. See PwC's (2018), 2018 Annual Corporate Directors Survey, PricewaterhouseCoopers LLP, 2018.

89 See NACD (2019), 2019–2020 Public Company Governance Survey, National Association of Corporate Directors, 2019.

90 See EY (2017), The evolving role of the board in cybersecurity risk oversight, EY Center for Board Matters, July 2017.

91 See NACD (2020).

Board-management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.

In 2019, the Organization of American States and The Internet Security Alliance issued a regional adaptation of the NACD Handbook, aiming to interpret these principles within the needs of companies in the region. The document, titled Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas, was launched in September 2019 and is available in English, Spanish and Portuguese.[92]

1. Implementing a framework

Having a clear understanding of the status quo, is essential for boards to be able to move ahead into the adoption the technical and policy measures necessary to increase security. From a technical standpoint, there are a multitude of approaches for developing safeguards around ICT systems, security, encryption, backups and control of data and information.

Boards are obviously not expected to implement them. That is a task for management and external experts that the company may need to engage, but the board has to understand, approve and oversee what they do, as it is ultimately responsible for the appropriate integration of cybersecurity in the strategy and business plans of the company.

Deloitte UK suggests a number of questions[93] that boards could use to address their responsibilities towards cybersecurity:

- Do we demonstrate due diligence, ownership, and effective management of cyber risk?
- Do we have the right leader and organizational talent?
- Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?
- Are we focused on, and investing in, the right things? And, if so, how do we evaluate and measure the results of our decisions?
- How do our cyber risk program and capabilities align to industry standards and peer organizations?
- Do we have a cyber-focused mindset and cyber-conscious culture organization-wide?
- What have we done to protect the organization against third-party cyber risks?
- Can we rapidly contain damages and mobilize response resources when a cyber incident occurs?
- How do we evaluate the effectiveness of our organization's cyber risk program? and
- Are we a strong and secure link in the highly connected ecosystems in which we operate?

All this entails making sure that the technical solutions appropriately fit the company, that the budgets and other resources for their proper implementation are available, and that the necessary actions are implemented through the firm to embrace the new security and privacy features.

This demands a long-term approach, looking to make incremental improvements in security by changing the organizational culture. Different departments within the firm need to be incentivized to work in tackling cyber risks together, with ICT collaborating with human resources (HR), compliance and legal to develop procedures and guidance that can foster such a culture. Employees need to adopt safe cyber practices and follow security protocols as part of their daily routines. Recent studies show that only one in two

---

92 See OAS & ISA (2019), Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas, Organization of American States, September 2019.

93 See Deloitte (2017a) Assessing cyber risk: Critical questions for the board and the C-suite, Deloitte, 2017.

companies have employee security awareness training programs, even if employees are regarded as the top source of cyber risk.[94]

Firms need also to prepare for the event of a breach, which is not something that could be completely avoided. Using scenarios and a clear definition of roles for the contingency, firms can prepare to react as best as possible to a breach to cybersecurity. If the risk is ever materialized, the company will be able to execute the plans it has prepared to ensure that the incident is contained while the business continues to operate. A well-prepared board would, in such a case, make sure it is quickly briefed about the scale of the attack and the information that has been compromised, to oversee the adoption of the necessary actions, including notifying the authorities and/or the affected parties, as applicable.

2. Three Lines of Defense Model

The three lines of defense is popular conceptual model for managing cyber risk across an organization, involving the different parts that need to own specific activities and be accountable for them. Originally developed for the financial sector,[95] it has been adapted as a cross-functional, multi-stakeholder management framework to address cyber risk. The model is based on three layers that manage risks throughout the company, with different responsibilities and oversight:

- First line, management control. The first line encompasses the information security department as well as various business units that operate the business, own their cyber risks, and implement risk management by executing risk and control procedures. These include handling risk events, updating key risk indicators, and deploying and managing controls that affect people, processes and technology within organizationally acceptable tolerances. Each business line defines the cyber risk they face and adopts controls and self-assessment into risk, fraud, crisis management and recovery.
- Line 2, established as a separate independent function, the second line looks at cybersecurity control frameworks, defines key risk indicators and metrics, creates assessments and reviews performance by tracking the first line's effectiveness in mitigating cyber risks. This function is often performed under an umbrella of senior management (may include compliance, legal, quality control and financial control) and a board-level committee (frequently the audit or risk committee). This independence is necessary in order to be able to provide a credible challenge to the first line and communicate their assessment of aggregate risks, at an enterprise level, to the board, to be used in the setting of risk appetite.
- Line 3, commonly internal audit (but may include input from external auditors and regulators) is responsible for rendering an independent, objective assessment of company processes and controls across the other lines, with a focus on operational effectiveness and efficiency. It ensures that the organization's internal control framework is adequate and provides checks regarding the adequacy of the controls in place. This function usually reports directly to the board or the audit committee.

3. Disclosure of cyber risk

Disclosure of risks and risk mitigation strategies is yet another important element in the role of the board towards cybersecurity. Providing shareholders and other stakeholders with appropriate disclosures of the material cyber risks the company is exposed, is essential for the market to be able to assess the value of the company and, also, a way for board members to reduce their personal exposure. Considering the frequency, magnitude and cost of cybersecurity incidents, these risks could be material in many sectors and investors are increasingly demanding firms for more and better disclosure.

---

[94] See, Loop, Paula et all, PricewaterhouseCoopers LLP, Blog for the Harvard Law School Forum on Corporate Governance and Financial Regulation, "Overseeing Cyber Risk," February 18, 2018.

[95] In the wake of the financial crisis, the Institute of Internal Auditors suggested the '3 Lines of Defense' as a model for better risk management and for allowing regulators to better assess the risks in the financial industry, as it was mainly designed for the financial sector. See IIA (2013) Position Paper: The Three Lines of Defense in Effective Risk Management and Control, January 2013.

In the U.S., the U.S. Securities and Exchange Commission (S.E.C.) has had cybersecurity disclosure guidance since 2011, adopted by the Corporate Finance Section of the authority, that focus how listed companies report their management of the cyber risks they face. In February of 2018 these rules where revamped and the Commissioners themselves got involved in a new version of the Guidance.[96] In it, they argue that "given the frequency, magnitude and cost of cybersecurity incidents," the Commission "believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion." Then they add that the Commission also believes that "the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face."

This puts a high level of responsibility for cybersecurity over the corporate governance of the firm as such disclosures "allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area." The guidance focuses on the following core areas:

- Pre-incident disclosure: The SEC calls for transparency around the quick identification and management of cyber incidents that have a material impact on the business across the organization.
- Board oversight: The SEC advises boards to disclose, as part of their proxy statement, the way in which they discharge their duties regarding cybersecurity and their engagement in understanding, quantifying and overseeing cyber risk.
- Incident disclosure: The SEC requires companies to adopt mechanisms to identify and quantify cyber risk exposure and breaches, allowing them to determine whether they were material and providing transparency to customers, investors and other shareholders.
- Controls and procedures: The SEC expects companies to assess the resilience of their company's enterprise-wide risk management.
- Insider trading: The SEC also reminds companies that knowledge of a cyber vulnerability or breach is privileged information until made public, thus potentially putting directors, managers and other insiders at risk of insider trading if they trade before such a breach or vulnerability is divulged.

The stock exchanges add disclosures in their own listing rules, which apply to cybersecurity risks when they are material. The New York Stock Exchange (NYSE), for example, requires listed companies to "release quickly to the public any news or information which might reasonably be expected to materially affect the market for its securities."[97] NASDAQ also requires listed companies to "make prompt disclosure to the public of any material information that would reasonably be expected to affect the value of its securities or influence investors' decisions."[98]

Deloitte has suggested seven principles for boards to be able to improve cyber risk disclosures:[99]

- Think carefully if cyber is not identified as a principal risk for your company;
- The damage that cyber risk can cause if so high that a detailed disclosure is worthwhile to highlight the risks to shareholders and let them know the company is taking them seriously;

---

96 See the U.S. S.E.C.'s Commission Statement and Guidance on Public Company Cybersecurity Disclosures of February 2018.

97 See NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments.

98 See Nasdaq Listing Rule 5250(b)(1).

99 See Deloitte (2017b), Just 5% of FTSE 100 companies disclose having a board member with specialist technology or cyber experience, Press Release, February 6, 2017.

- The better disclosures are company-specific, year-specific and provide sufficient detail to give meaningful information to investors and other stakeholders;
- Boards and committees should educate themselves about the cyber-threat and challenge management on how they are dealing with cyber risk;
- Companies should take credit for what they are doing, including describing who has executive responsibility, board level responsibilities, the policy framework, internal controls, and disaster recovery plans;
- Boards should think about what could be missing from their disclosures, for example a clear indication of the main threats facing the company, who poses those threats, the likelihood, possible impact and detail about what the company – and the board – is doing to manage or mitigate those particular risks; and
- Finally, if the company's disclosure does not look strong enough after taking credit for what the company is doing already, the board should ask itself whether it is actually doing enough.

4. Monitoring

Once a cybersecurity framework is in place, the board needs to ensure it remains up-to-date and functioning effectively. This may be as difficult as designing the system itself, since it involves looking for technical but also human failures. A state-of-the-art system will not be safe if any of the individuals that has access to the data can create a vulnerability by falling for a phishing scam, for example. Sound oversight is, thus, both technically complex and time consuming. Boards need to ensure that management is active in compliance.

A board's guidance should inform the company's policies and procedures, and management should adopt appropriate steps for their effective implementation throughout the company. This has to permeate into its culture, including from a compliance, human capital and information technology perspective, as well as involving all other relevant departments, such as marketing, sales and customer support. The task for a board is to become conversant in the technical solutions and options available to identify, monitor and improve any gaps in the cyber risk management. It has to consider scenarios and develop mitigation plans or contingency measures, working closely with the technical people and keeping up with new risks and the expectations of investors.

In the U.S., the Council of Institutional Investors (CII) published a list of questions for investors to pose to boards in an effort to understand how they are prioritizing cybersecurity. The questions suggested by the CII are:

- How are the company's cyber risks communicated to the board, by whom, and with what frequency?
- Has the board evaluated and approved the company's cybersecurity strategy?
- How does the board ensure that the company is organized appropriately to address cybersecurity risks? Does management have the skill sets it needs?
- How does the board evaluate the effectiveness of the company's cybersecurity efforts? and
- When did the board last discuss whether the company's disclosure of cyber risk and cyber incidents is consistent with legal and regulatory requirements?

D. Cyber skills at the Board

A number of cited surveys and cases of cybercrime show that even the most sophisticated companies are susceptible to attacks or cyber failures. One of the factors at play in this is a disconnect between the technical people responsible for cybersecurity and those who sit at the board. Directors with skills and experience

involving technology or science are currently a minority at boardrooms, reflecting in part that their area of expertise has become more relevant for the average firm only in recent years.

A well-organized board of directors involves people with complementary skills and experiences who can collectively address challenging issues. The majority of the directors of today have nevertheless backgrounds in finance, law and business, not science or technology. This poses the risk that in the absence of the necessary minimum cyber skills in the room, the board may act simply as a passive consumer of metrics and information prepared by management.

A number of studies have picked this as a problem, encouraging firms to add enough expertise among their board members so that they can exercise ownership for these issues. They show that cyber skills at the board are scarce even for leading firms in developed markets. This gap in boards' composition has been detected even in sectors that are particularly exposed to cyber risks, such as banking and finance. Accenture, a consultancy firm, reviewed in 2017 the professional experience in boardrooms of 109 of the largest banks around the world,[100] concluding that: i) only 6 percent of board members and 3 percent of CEOs had technology professional backgrounds; and ii) 43 percent of banks did not have any board members with a professional technology background, while 30 percent had only one such person. Several other sources report similar findings in most developed markets.[101] [102]

Recruiting a director with cyber skills to the board in not the only way to address this potential gap, as it is also possible to improve the skills of those already at the board or to complement it with experts made available from within management. In the first case, the obvious tool is training, yet only a few companies are providing cyber risk training to their boards. According to a 2018 UK Government's survey[103] of FTSE 350 companies, while 57 percent of respondents reported they have clear understanding of the potential impact of loss of or disruption to key information or data assets, 68 percent said they have not received any training on how to deal with a cybersecurity incident.

Looking into the availability of external cyber expertise to boards, the evidence is not encouraging. A 2018 survey of CISOs by Gartner,[104] a research and advisory company, showed that 35 percent of firms declare not having cyber-security experts in their management and that they are unsure how to protect their organizations' sensitive information, communications or data. This, despite the fact that 91 percent of CISOs declared that they expect cyber-threats to increase over the next three years.

Increasing the quality of reporting to the board is also an effective measure. Surveys in the U.S. note that a large majority of directors agree that the quality of cyber risk information provided by management has improved,[105] that the amount of cybersecurity reporting has increased, and that many boards are using external advisors to enhance reporting.[106]

---

[100] See Accenture (2016), Bridging the technology gap in financial services boardrooms, by Richard Lumb et al., Accenture, 2016.

[101] A 2016 report by Russell Reynolds, a consultant firm, analyzed the backgrounds of board members of 300 large companies (Fortune 100 companies in the U.S. as well as Fortune 100-equivalent companies in Europe and Asia/Pacific), looking for the presence of non-executive board members with significant digital experience. Their conclusion was that they account for less than 5 percent of total board seats, even if this was an improvement from 2014's results. See Russel Reynolds (2016), Digital Directors 2016: Diverse Perspectives in the Boardroom, 2016.

[102] A 2017 Deloitte review of the annual returns and board member biographies of FTSE 100 companies showed that while 87 percent of companies identified cyber as a principal risk, only 5 percent of them had any cybersecurity experience in their board. See Only 5% of FTSE companies have cyber-security expertise on the board, by Tom Reeve, SC Media, February 6, 2017.

[103] See the UK Government (2017), FTSE 350 Cyber Governance Health Check Report, July 2017.

[104] See Gartner (2018), The 2018 CIO Agenda, by Kasey Panetta, October 27, 2017.

[105] See NACD (2018).

[106] See PwC's (2018).

E. Cybersecurity Committees

Board committees are also an effective way to help boards to deal with particularly complex issues. They allow the board to have a smaller group of members, sometimes with the help of external experts, spending sufficient time on such issues to prepare the discussion at the board level, where they subsequently report.

Across all industries, boards generally rely on three committees that are the most commonly required by laws and regulations: audit, compensation, and nomination/governance.[107] This means that cybersecurity issues have to either be discussed at the full board level or assigned to one of these three committees. Many firms assign cybersecurity issues to the audit committee, where they have to compete for attention with a number of other important priorities and risks.

Cybersecurity committees, where they exist, can take primary responsibility for all cyber risk matters, even if the board still remains responsible overall. Their objective is often to identify, evaluate and monitor all cybersecurity activities within the firm and to determine how they align with the overall corporate risk profile. For this, they take a wide-angle view of the cybersecurity risks, considering all aspects within the firm, but then zoom-in on specific threats, often using scenarios and simulations, and checking how well prepared the company is to prevent them, to mitigate the damage they may cause, and to recover the essential functionalities that may have been affected. By doing this, they digest these complex issues and distill the essential information the board needs to know to make informed decisions, identifying issues that deserve a high priority and helping the board to prioritize them in their oversight.

[107] In a 2018 survey that tracked board structures in S&P 500 companies, EY concluded that board committee structures have stayed largely the same over the past six years. Since 2013 only a few companies have created committees that focus on compliance (16 percent), risk (11 percent) and technology (7 percent). Further, only 10 percent of companies included in the sample assigned responsibility for cybersecurity, digital transformation and information technology to a specific committee, often technology, risk or compliance committees. See Klemash, Steve W. et al. (2018), EY Center for Board Matters, A Fresh Look at Board Committees, at Harvard Law School Forum on Corporate Governance and Financial Regulation, July 10, 2018.

IV. Conclusions

From the outset of research for this paper there was the assumption that it would be possible to find a significant body of laws and regulation, throughout Latin America and the Caribbean, setting the social expectations for the minimum cybersecurity standards that private firms must comply with, and the role of the board of directors in ensuring them. This had been the case for a 2019 paper by the author researching the links between data protection and corporate governance in the region. Of course, these would most likely be just minimum standards, as many firms are addressing cyber risks on a daily basis out of their own accord, understanding that it makes business sense to do that for too many reasons that chapter III addresses in more detail. Also, it was predictable that such rules may not be found across all sectors of the economy, nor for all sizes of companies, but at least for some of the largest and for those dealing with essential services and critical infrastructure in relevant sectors of the economy. Therefore, the search targeted at any such legislation, regulation or at least guidance.

As shown in chapter I, the findings of the research within the region were slight. Even if it is the best practice of those jurisdictions that are recognized as leaders in cybersecurity, and a recommendation included in almost any report on the subject, both from technical experts and international organizations, the findings of the research offered just a few instances of cybersecurity regulation beyond data protection regimes. Those few regulatory cases, many of them currently in the making, are present only for a fraction of the companies handling critical infrastructure, holding assets or rendering services that should be guarded as part of a national cybersecurity strategy. This, despite the fact that cyber-attacks on critical infrastructure were rated the fifth highest cyber risk globally in 2020 by the WEF.

Already in 2004, the OAS General Assembly approved a Comprehensive Inter-American Strategy to Combat Threats to Cyber Security, encouraging the adoption of National Cyber Security Strategies that could manage risks over critical infrastructure. More than a dozen jurisdictions in the region have adopted such strategies, all of them including a section dedicated to the protection of critical infrastructures. The combination of being high-profile targets for cybercrime, the sizeable damages potentially caused and the rather unsuccessful prosecution rate of cyber criminals, have increased the attention of national authorities towards the cybersecurity of these critical pieces of infrastructure in many jurisdictions, including in the region.

But the results of the research were surprising, as little has been done to move from high-level strategies to their implementation. Most countries have not identified precisely the pieces of infrastructure that should be regarded as critical, the entities controlling them, the cybersecurity standards they need to deploy to protect them, and the monitoring and accountability rules that will make sure those standards are implemented. In this sense, many national strategies remain more theoretical than practical, offering perhaps a notional sense of security that is definitely not real.

Essential services and critical infrastructure deal with public goods, even when in the hands of the private sector, so there is a clear role for the State to regulate. Those companies that do not have the fortune of having boards and managers that understand these risks, and are willing to decisively address them, need to be incentivized to make the socially optimal level of investment in cybersecurity. Yet, many of the reports cited in this paper show that current levels of cybersecurity in the region remain low. Corporate leaders have cyber-risk as a top 5 priority on their agenda, but progress is often slow, which is reflected in the modest levels of confidence those leaders have on their company's cyber resilience.

As in many other fields, well-run companies do not need reminding of their responsibility and can see the value of investing in cybersecurity by themselves. Others need legal and regulatory frameworks to push their boards and top managers to pay due attention to cybersecurity. Some of the surveys cited in this paper show that many corporate leaders agree that the harmonization of regulation and the adoption of minimum standards or benchmarks, ideally developed by technical organizations, is in the interest of all market participants. They see clearly that this could help industries move collectively towards better cybersecurity. As the case studies in chapter II show, policy interventions can take different forms and styles, but all point in the direction of better engagement and incentives for boards and top managers to integrate the corporate governance of firms behind the objective of enhanced cybersecurity.

If firms are collecting information about almost everything we do, intangibles represent 80 percent of the value of the largest listed companies, and a piece of malware can put an entire region into a blackout, the stakes are high for cybersecurity. The forced lockdown that many of us have suffered due to the Covid-19 pandemic, and the enduring impact it will have in the way in which we will work and study from now on, has made this an even more pressing issue. The crucial importance of ICT systems and connectivity, and the impact that security breaches can cause, demand a more active role not only of the companies operating them and their boards of directors, but also from regulators and lawmakers in the region.

The blueprints for action can be found with a simple Google search. The willingness not. That will demand consistent, and ideally concerted, efforts by each link in the chain to safeguard the security of the whole. Part of the equation will require focusing attention to the governance of firms, setting the expectations for what boards should do to facilitate the implementation of robust cybersecurity, and the liability they will incur if they neglect their duties. Some jurisdictions have done it for data protection, and in some sectors, they have also done it for critical infrastructure. The sharing of these experiences and the drawing of good practices, in collaboration with the private sector, may be all it takes to move forward.

Ideally, future research on this topic will find multiple examples of national cybersecurity strategies that tap on the role of the board to ensure adequate private-public cooperation, fully implemented to properly address the risks of essential services and critical infrastructure, and conducted in coordination within regional frameworks that could promote harmonization and international cooperation.

Bibliography

Accenture (2016), Bridging the technology gap in financial services boardrooms, by Richard Lumb, Mauro Macchi and Juan Pedro Moreno, 2016, available at: www.accenture.com/t20160118T152822__w__/us-en/_acnmedia/PDF-4/Accenture-Strategy-Financial-Services-Technology-Boardroom.pdf.

Accenture (2019), The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Research, available at: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

AICPA (2017), AICPA Unveils Cybersecurity Risk Management Reporting Framework, April 26, 2017, available at: www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html.

Barlow, J.P. (1996), A declaration of the independence of cyberspace, Electronic Frontier Foundation, February 8, 1996, available at https://www.eff.org/cyberspace-independence.

Barrero, Vladimir (2020), Estado de preparación en ciberseguridad del sector eléctrico en América Latina, Monografía del BID; 802, Vladimir Barrero, Oscar Bou; editores, Juan Roberto Paredes, Miguel Porrúa, available at: https://publications.iadb.org/publications/spanish/document/Estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-America-Latina.pdf.

Carter, William A. and Jennifer C. Daskal (2018), "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge," Center for Strategic & International Studies, July 2018, available at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdpoRspiGYNGcGKTUjrGY3rN.

CEPAL eLAC (2018), Declaración de Cartagena de Indias, available at: https://conferenciaelac.cepal.org/6/sites/elac2020/files/cmsi.6_declaracion_de_cartagena.pdf.

Colorado Department of Transportation (2018) "CDOT Cyber Incident After-Action Report" July 17, 2018, available at: https://www.colorado.gov/pacific/dhsem/atom/129636.

Commonwealth Model Law on Computer and Computer Related Crime https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf.

Council of Europe, Chart of signatures and ratifications of Treaty 185- Convention on Cybercrime, Status as of 20/04/2020, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dcrCEZ9F.

Council of Europe, Convention on Cybercrime of the Council of Europe (CETS No.185), available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

CSIS and McAfee (2018), Economic Impact of Cybercrime—No Slowing Down, 2018, p. 4, available at: https://www.csis.org/analysis/economic-impact-cybercrime.

Cybercrime Legislation Worldwide (Database), United Nations Conference on Trade and Development, available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

Cyberspace Solarium Commission (2020), Final Report, March 11, 2020, available at: https://www.solarium.gov/report.

Datareportal 2020, Digital 2020: April Global Statshot, by Simon Kemp, available at: https://datareportal.com/reports/digital-2020-april-global-statshot.

Deere, Stephen (2018), CONFIDENTIAL REPORT: Atlanta's Cyber Attack Could Cost Taxpayers $17 Million, The Atlanta Journal-Constitution, August 2, 2018, available at: https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/.

Deloitte (2017a), Assessing cyber risk: Critical questions for the board and the C-suite, available at: www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ra-assessing-cyber-risk.pdf.

Deloitte (2017b), Just 5% of FTSE 100 companies disclose having a board member with specialist technology or cyber experience, Press Release, February 6, 2017, available at: www2.deloitte.com/uk/en/pages/press-releases/articles/just-5-of-ftse-100-companies-disclose.html#.

Directors Beware: The EU's General Data Protection Regulation Is Upon Us!, blog post by Kevin LaCroix, December 20, 2017, available at: www.dandodiary.com/2017/12/articles/uncategorized/guest-post-directors-beware-eus-general-data-protection-regulation-upon-us/.

Eoyang, M., et all (2018), To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors, Third Way, October 29, 2018, available at: https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

EC (2019) Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector, SWD (2019) 1240 final, European Commission, available at:https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf.

_____1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

_____(2016), Directive 2016/680 of the European Parliament and of the Council of 27 April 2016, available at:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC.

_____(2016), Guidelines on Data Protection Officers ('DPOs'), December 13, 2016, available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

_____(2016), Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679.

EY Center for Board Matters (2017), The evolving role of the board in cybersecurity risk oversight, (July 2017), available at: www.ey.com/us/en/issues/governance-and-reporting/ey-the-evolving-role-of-the-board-in-cybersecurity.

FIRST (2019) Computer Security Incident Response Team (CSIRT) Services Framework, Version 2.0, June 2019, available at: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.0.pdf.

Gartner (2018), The 2018 CIO Agenda, by Kasey Panetta, October 27, 2017, available at: www.gartner.com/smarterwithgartner/the-2018-cio-agenda-infographic/.

Ghosh, Dipayan, What You Need to Know About California's New Data Privacy Law, July 11, 2018, Harvard Business Review, available at: https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

Google Cloud (2020), Protecting businesses against cyber threats during COVID-19 and beyond, by Neil Kumaran and Sam Lugani, April 16, 2020, available at: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond.

IFC (2019) Corporate Governance Progression Matrix for State-Owned Enterprises, available at: https://www.ifc.org/wps/wcm/connect/39fd3481-018c-4cc2-8075-0cd5936f8050/IFC_Progression_Matrix_Fund _Governance_ 043019.pdf?MOD=AJPERES&CVID=mGdwMuT.

IIA (2013) Position Paper: The Three Lines of Defense in Effective Risk Management and Control, January 2013, available at: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines % 20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf.

Inter-American Convention on Mutual Assistance in Criminal Matters https://www.oas.org/juridico/english/treaties/a-55.html.

International Data Corporation (IDC 2019), The Growth in Connected IoT Devices Is Expected to Generate 79.4 ZB of Data in 2025, according to a New IDC Forecast, IDC, June 18 2019, available at: https://www.idc.com/getdoc.jsp?containerId=prUS4521321917.

Internet & Jurisdiction Policy Network (2019), Internet & Jurisdiction Global Status Report 2019, available at: https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf.

ITU (2019), Measuring Digital Development: Facts and Figures 2019, International Telecommunication Union, available at https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

James A. Lewis (2016) Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States, Inter-American Development Bank, 2016, available at: https://publications.iadb.org/publications/english/document/Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United-States.pdf.

Kaspersky Lab (2018), From data boom to data doom: the risks and rewards of protecting personal data, available at: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Lab_Business%20in%20a%20data%20boom.pdf.

Klemash, Steve W. et al. (2018), EY Center for Board Matters, A Fresh Look at Board Committees, at Harvard Law School Forum on Corporate Governance and Financial Regulation, July 10, 2018, available at: https://corpgov.law.harvard.edu/2018/07/10/a-fresh-look-at-board-committees/#1.

Lehuedé, Héctor (2019) "Corporate governance and data protection in Latin America and the Caribbean," Production Development series, No. 223 (LC/TS.2019/38), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2019, available at https://repositorio.cepal.org/handle/11362/44629.

Loop, Paula et all (2018), PricewaterhouseCoopers LLP, Blog for the Harvard Law School Forum on Corporate Governance and Financial Regulation, "Overseeing Cyber Risk," February 18, 2018, available at: https://corpgov.law.harvard.edu/2018/02/18/overseeing-cyber-risk/.

Madeline Carr (2016), Public–private partnerships in national cyber-security strategies, International Affairs 92: 1 (2016) 43–62, available at: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf.

Marsh & Microsoft (2019) Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019, September 2019, available at: https://www.marsh.com/uy/es/insights/research/marsh-microsoft-encuesta-percepcion-riesgo-cibernetico-2019.html.

Mayer, Colin (2015), "Reinventing the corporation" Sir John Cass's Foundation Lecture, March 3, 2015, Journal of the British Academy, 4, 53–51, available at https://www.thebritishacademy.ac.uk/publications/reinventing-corporation.

McKinsey Global Institute (2016), Digital Globalization: The New Era of Global Flows, March 2016, available at: http://ma.mckinsey.com/practicecrm/MGI/MGI_Digital_globalization_Full_report_March_2016.pdf.

NACD (2017), Director's Handbook on Cyber-Risk Oversight (January 2017), available at: www.nacdonline.org/insights/publications.cfm?ItemNumber=10687.

_____(2018), 2018–2019 Public Company Governance Survey, available at: https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63764&aitrk=nacd-gs.

_____(2019), 2019–2020 Public Company Governance Survey, available at: https://www.nacdonline.org/analytics/survey.cfm?ItemNumber=66753.

_____(2020), Director's Handbook on Cyber-Risk Oversight (January 2020), available at: https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298.

Nasdaq Listing Rule 5250(b)(1), available at: http://nasdaq.cchwallstreet.com/nasdaq/main/nasdaq-equityrules/chp_1_1/chp_1_1_4/chp_1_1_4_4/chp_1_1_4_4_4/chp_1_1_4_4_4_10/default.asp.

NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments, available at: http://wallstreet.cch.com/LCMTools/PlatformViewer.asp?selectednode=chp%5F1%5F3&manual=%2Flcm%2Fsections%2Flcm%2Dsections%2F.

OAS (2004) Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity, Organization of American States, 2004, available at: http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

_____(2009), Consolidated List of Confidence and Security Building Measures, Organization of American States, 2009, available at: https://www.oas.org/csh/english/csbmlist.asp.

_____(2016), Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report, available at: https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.

_____(2018), State of Cybersecurity in the Banking Sector in Latin America and the Caribbean, Organization of American States, available at: https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf.

OAS & ISA (2019), Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas, September 2019, available at: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-070/19.

OECD (2015), G20/OECD Principles of Corporate Governance, available at: http://dx.doi.org/10.1787/9789 264236882-en.

Office of Civil and Criminal Justice Reform of the Commonwealth (2017), Model Law on Computer and Computer Related Crime, Commonwealth Secretariat, available at: https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf.

Ponemon Institute (2017), The Impact of Data Breaches on Reputation and Share Value, May 2017, available at: www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf.

Ponemon Institute and IBM Security (2017), Cost of Data Breach Study: Global Overview, June 2017, available at: www.ibm.com/downloads/cas/ZYKLN2E3.

_____(2019), Cost of Data Breach report 2019, available at: https://www.ibm.com/security/data-breach.

PwC (2014), Board oversight of risk: Defining risk appetite in plain English, available at: http://www.ceolearning network.com/_assets/library/2014/08/Defining-Risk-Appetite.pdf.

PwC's (2018), 2018 Annual Corporate Directors Survey, available at: https://www.pwc.com/us/en/governance-insights-center/annual-corporate-directors-survey/assets/pwc-annual-corporate-directors-survey-2018.pdf.

Russel Reynolds (2016), Digital Directors 2016: Diverse Perspectives in the Boardroom, 2016, available at: www.russellreynolds.com/en/Insights/thought-leadership/Documents/2016%20Digital%20Directors%20FINAL.PDF.

Santiago F. Rodríguez V., Felaban: Cybersecurity in Latin American And Caribbean Banking, at Chapter 3.4 of OAS (2018), State of Cybersecurity in the Banking Sector in Latin America and the Caribbean, Organization of American States, available at: https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf.

SEP (2017), Nuevo Código SEP, Sistema de Empresas Públicas, 2017, available at: http://www.sepchile.cl/fileadmin/ArchivosPortal/CodigoSep/GobiernoCorporativo/CODIGO_SEP_V2.pdf.

Southwell, Alexander H. et al, Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy, The CLS Blue Sky Blog (Columbia Law School), February 3, 2017, available at: http://clsbluesky.law.columbia.edu/2017/02/03/gibson-dunn-reviews-u-s-cybersecurity-and-data-privacy/.

Spencer Stuart (2018), What Directors Think, 2018, available at: www.spencerstuart.com/-/media/2018/april/what-directors-think-2018.pdf.

Stanford University Draft International Convention To Enhance Protection from Cyber Crime and Terrorism https://law.stanford.edu/publications/draft-international-convention-to-enhance-protection-from-cyber-crime -and-terrorism/.

Stiglitz & Wallsten (1999), Public-Private Technology Partnerships: Promises and Pitfalls, American Behavioral Scientist, Vol. 43 No. 1, September 1999 52-73, available at: https://www8.gsb.columbia.edu/faculty/jstiglitz/sites/jstiglitz/files/Public%20Private%20Technology%20Partnerships.pdf.

U.S. Securities and Exchange Commission (2018), Commission Statement and Guidance on Public Company Cybersecurity Disclosures of February 2018, available at: www.sec.gov/rules/interp/2018/33-10459.pdf.

UK Government (2017), FTSE 350 Cyber Governance Health Check Report, July 2017, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635605/tracker-report-2017_v6.pdf.

WEF (2017) World Economic Forum, Global Risks Report 2017, 12th Ed., January 2017, available at: www.weforum.org/reports/the-global-risks-report-2017.

_____(2019) World Economic Forum, Global Risks Report 2019, available at: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

_____(2020) World Economic Forum, Global Risks Report 2020, available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

Zingales (2000) "In Search of New Foundations" The Journal of Finance Vol LV, available at http://faculty.chicagobooth.edu/luigi.zingales/papers/research/search.pdf.

List of used acronyms

AICPA	American Institute of CPAs
CEO	Chief Executive Officer
CII	Council of Institutional Investors
CIS	Center for Information Security
CISO	Chief Information and Security Officer
COBIT	Control Objectives for Information and Related Technology
CSIRT	Computer Security Incident Response Team
CTO	Chief Technology Officer
D&O	Directors' and officers' insurance
DDL	Digital Development Level
DDoS	Denial-of-service attacks
DPIA	Data protection impact assessment
DPO	Data Protection Officer
EBITDA	Earnings before interest, taxes, depreciation, and amortization
EC	European Commission
ECLAC	United Nations Economic Commission for Latin America and the Caribbean
EU	European Union
GCA	Global Cybersecurity Agenda
GCI	Global Cybersecurity Index
GDP	Gross domestic product
GDPR	General Data Protection Regulation
ICT	Information and communication technology
IADB	Inter-American Development Bank
IFC	International Finance Corporation
IoT	Internet-of-things
ITU	International Telecommunication Union
NACD	National Association of Corporate Directors
NCSI	National Cyber Security Index
NIST	National Institute of Standards Technology
OAS	Organization of American States
OECD	Organization for Economic Co-operation and Development
R&D	Research and development
SEP	Sistema de Empresas Públicas
SOE	State-owned enterprise
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
USD	United States Dollars
WEF	World Economic Forum

Annex

Annex 1
Cybersecurity frameworks

The following sections highlights some of the international cybersecurity frameworks and initiatives that foster a coordinated approach with or within the private sector. Where present, corporate governance incentives aimed at the board or senior management of private sector firms are highlighted. These frameworks include international treaties and supranational rules, but also sectorial initiatives and national rules, which are briefly described in this Annex to inform the discussion in the rest of the paper.

International cooperation initiatives

UN's Cybersecurity framework

UN's Group of Government Experts

The United Nations' Group of Governmental Experts (GGE) "on Advancing responsible State behavior in cyberspace in the context of international security" is an UN-mandated working group in the field of information security that has been working since 2004. Six different groups of experts have been created since then[108] and they have been one of the most influential forces for the setting of the global cybersecurity agenda. It was one of these groups (the third, in 2013), that convinced the UN's General Assembly to recognize that national sovereignty, the UN Charter, and international law apply to cyberspace.[109] This constituted a groundbreaking success that redefined the politics of the Internet and its governance.

The current GGE comprises experts from 25 states working in their personal capacity and is chaired by the Ambassador of Brazil. Their objective is to submit a report to the General Assembly in 2021, after consultation with several regional organizations, including the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations.

ITU Global Cybersecurity Agenda

The International Telecommunication Union (ITU)[110] is the United Nations' specialized agency for ICTs, founded in 1865 to facilitate international connectivity in communications networks worldwide. In 2007, the ITU launched a Global Cybersecurity Agenda (GCA)[111] as framework for international cooperation aimed at enhancing confidence and security in the information society. The 2019 session of ITU's Council instructed the drafting of guidelines developed for utilization of the GCA. At the time of writing this paper, work on these guidelines was ongoing.

The GCA is comprised of five Pillars or Work Areas: i) Legal measures; ii) Technical and procedural measures; iii) Organizational structures; iv) Capacity building, and v) International cooperation. The GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts.

Economic Commission for Latin America and the Caribbean's eLAC

The Economic Commission for Latin America and the Caribbean (ECLAC) has developed a dialogue that sees the use of digital technologies as instruments of sustainable development for the region. The dialogue promotes the advancement of the digital ecosystem in the region "through a process of regional integration

---

[108] See more about the UN's Group of Governmental Experts at: https://www.un.org/disarmament/group-of-governmental-experts/

[109] Until then there were many prominent voices defending the Independence of the Internet from any national or supranational jurisdiction (some of they still exist). In a famous article published online in 1996, John Perry Barlow, a founder of the Electronic Frontier Foundation, argued for the independence of cyberspace saying that "the only law that all our constituent cultures would generally recognize is the Golden Rule." See Barlow, J.P. (1996), A declaration of the independence of cyberspace, Electronic Frontier Foundation, February 8, 1996.

[110] See ITU's website: https://www.itu.int/en/about/Pages/default.aspx.

[111] See the Global Cybersecurity Agenda (GCA) website: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

and cooperation, strengthening digital policies that promote knowledge, inclusion and equity, innovation and environmental sustainability."[112]

The initiative traces back to regional dialogue on the information and knowledge society that started in the year 2000, with the Declaration of Florianópolis and the commitment to design and implement programs for the access and use of information technologies and communications. During its Sixth Ministerial Conference, which took place in April 2018, eLAC approved the Cartagena Declaration[113] and the Digital Agenda for Latin America and the Caribbean (eLAC2020).[114] Colombia chairs eLAC's 2020 Digital Agenda and ECLAC provides technical secretariat.

The eLAC 2020 Digital Agenda includes 7 action areas and 30 objectives. One of the seven pillars deals with governance for the information society. There, one of the lines of work is to "prevent and combat cybercrime through public policies and digital security strategies."

OAS' Inter-American Integral Strategy to Combat Threats to Cybersecurity

The Organization of American States has been engaged with cybersecurity and cybercrime for many years promoting capacity building among its member states. In 2004 its members adopted the Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity,[115] calling for a coordinated, multi-stakeholder effort to improve cybersecurity in the region via a common framework and cooperation.

Within the OAS, the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE)[116] has led the work on cybersecurity. As described in its website, its work is centered in assisting member states in developing national cybersecurity strategies, providing training to CSIRTs, facilitating crisis management exercises and emergency response assessments, and engaging civil society and the private sector to foster awareness raising about cybersecurity.

OAS's Committee on Hemispheric Security released in 2009 a "Consolidated List of Confidence and Security Building Measures"[117] that includes voluntary exchanges of information on government cybersecurity entities, cooperation on policy and research, as well as the establishment of national points of contact regarding the protection of critical infrastructure.

As mentioned in chapter III, in 2019 the OAS and The Internet Security Alliance issued a regional adaptation of the NACD Handbook, titled Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas, addressing the corporate governance expectations for the handling of cybersecurity in the private sector.[118]

COE's Budapest Convention against cybercrime

The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, is the first international treaty addressing cybercrime and was adopted by the Committee of Ministers of the Council of Europe on November 8, 2001, and entered into force on July 1, 2004. It was negotiated by Council members and observer states Canada, Japan, Philippines, South Africa and the United States, with the aim of promoting the harmonization of national laws, enhancing enforcement and investigative techniques, as well as promoting international cooperation against cybercrime.

The Convention focuses on crimes committed via the Internet and other computer networks, and has special provisions for infringements of copyright, computer-related fraud, exploitation of images of child

---

[112] See more on these dialogues at: https://www.cepal.org/en/events/dialogue-series-latin-american-and-caribbean-region.
[113] See eLAC (2018), Declaración de Cartagena de Indias.
[114] See the webpage for eLAC 2020 Agenda digital para América Latina y el Caribe, available at: www.cepal.org/es/proyectos/elac2020.
[115] See OAS (2004) Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity, Organization of American States, 2004.
[116] See the website of the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) at: http://www.oas.org/es/sms/cicte/default.asp.
[117] See OAS (2009), Consolidated List of Confidence and Security Building Measures, Organization of American States, 2009.
[118] See OAS & ISA (2019), Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas, September 2019.

sexual abuse, hate crimes, and violations of network security, among others.[119] It encourages member states to criminalize domestically those offences and have the ability to facilitate an effective regime of international cooperation that could benefit from mutual access to powers and procedures, such as the search of computer networks and lawful interception.[120]

At the time of writing this paper, the Convention had 65 ratified member states and 3 states that had signed the convention but not yet ratified it. From Latin America and the Caribbean, the Dominican Republic was the first jurisdiction to request accession to the Convention in 2006. Since then, Argentina, Chile, Colombia, Costa Rica, Panama, Paraguay and Peru have joined the Dominican Republic as members to the Budapest Convention.[121]

Article 12 of the Convention, on corporate liability, is particularly relevant for this paper as it requires that member states adopt legislative and other measures necessary to ensure that legal persons can be held liable for cybercriminal offences when committed for their benefit. The objective is to impose liability on corporations, among other legal entities, for (i the criminal actions undertaken for the benefit of the company by anyone within a leadership position, and (ii the failure of such leaders to supervise or control an employee or an agent of the company in a way that facilitates the commission, by that employee or agent, of one of the cybercrimes established in the Convention.

In the first case there are four elements that can configure cybercrime liability for the company:

- one of the offences described in the Convention must have been committed;
- the offence must have been committed for the benefit of the company;
- a person who has a leading position must have committed the offence (including aiding and abetting); and
- the leader must have acted on the basis of a power of representation or an authority to take decisions or to exercise control. This is necessary to demonstrate that the person did not overstepped his or her authority.

In the second case, the liability of the corporation is triggered when:

- one of the offences described in the Convention has been committed;
- the offence has been committed by an employee or agent of the company,
- the offence has been committed for the benefit of the company;
- the commission of the offence has been made possible by the leadership of the company having failed to supervise the employee or agent. Such failure is assessed by comparing to a reasonable standard of supervision including adequate measures, determined by factors such as the type of business, its size, its resources and the like.

For both cases, members states are expected to adopt criminal, civil or administrative liability for the legal entities found guilty, provided that the punishment meets the criteria of Article 13, paragraph 2, demanding for it to be "effective, proportionate and dissuasive." Furthermore, paragraph 4 of Article 12 expressly states that corporate liability does not exclude individual liability.

---

[119] The Convention defines and invites members states to criminalize the following offences: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to the exploitation of images of child sexual abuse, and offences related to copyright and neighboring rights.

[120] The Convention includes rules regarding procedural law, including expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data.

[121] See Council of Europe, Chart of signatures and ratifications of Treaty 185- Convention on Cybercrime, Status as of 20/04/2020.

Commonwealth Model Law on Cybercrime

The Commonwealth of Nations (the Commonwealth) is a political association of 54 member states, nearly all former territories of the British Empire, organized by the Commonwealth Secretariat which focuses on intergovernmental cooperation.[122] The Commonwealth's Law Ministers adopted an initiative for the creation of a Model Law on Computer and Computer-Related Crime in 1999, to be used by those Commonwealth member countries seeking assistance in the development of an appropriate legislative framework. The work was commissioned to a group of experts with a mandate to follow the (at the time) draft Council of Europe Convention on Cybercrime. The final document was submitted by the experts to Commonwealth Law Ministers in November 2002. At its adoption, Law Ministers mandated to keep the Model Law under review, to ensure it is kept up to date.[123]

The EU Data protection framework

In April of 2016 the European Union adopted Directive (EU) 2016/680[124] and Regulation (EU) 2016/679[125] of the European Parliament and of the Council, the General Data Protection Regulation (the GDPR). Generally regarded as the most advanced data protection framework in place, the GDPR has set a new international benchmark on data protection and has raised the bar for cybersecurity not only in Europe.

Aimed to harmonize data protection laws across Europe as well as to give greater protection and rights to individuals, the new legislation entered into force on 25 May 2018, with its new rules affecting individuals, companies and other organizations that are regarded to be either data controllers (those that determine how data are processed) and data processors (their subcontractors) of personal data and sensitive personal data of EU citizens.

Among the 99 articles of the GDPR, the EU set out the rights of individuals and the obligations placed on organizations dealing with their personal data. These rules apply to all companies processing personal data of data subjects residing in the EU, regardless of their location. Pursuant to the regulation, non-EU businesses processing data of EU citizens have to appoint a representative in the EU and are subject to the reinforced penalty systems it created. Breaches[126] of the GDPR can be fined up to the greater of 4 percent of the annual global turnover of the organization or €20 million, for the most serious infringements. Lower level offenses can result in fines of 2 percent of the annual global turnover of the organization.

From a corporate governance perspective, data controllers and data processors are also subject to new accountability and compliance obligations under the GDPR. They aim to make their handling of people's personal data more responsible, including the adoption of data protection policies, the use of data protection impact assessments (DPIAs), and the appointment of data protection officers (DPOs), among others.

In particular, the GDPR sets out that data controllers must "implement appropriate technical and organizational measures" to protect personal data in a way that ensures "the ongoing confidentiality, integrity, availability and resilience of systems." This creates an expectation that board of directors and senior managers

---

[122] See https://thecommonwealth.org.

[123] See Office of Civil and Criminal Justice Reform of the Commonwealth (2017), Model Law on Computer and Computer Related Crime, Commonwealth Secretariat.

[124] See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC.

[125] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[126] Under the GDPR the destruction, loss, alteration, unauthorized disclosure of, or access to personal data has to be reported to the relevant data protection authorities (DPAs) within 72 hours. These are the authorities of all jurisdictions where data subjects may experience financial loss, confidentiality breaches as well as damage to their reputation as a consequence of the breach.

will have to get personally involved in the design, implementation and monitoring of their organizations' data protection and information security frameworks.[127]

Technical standards

A number of organizations have created technical frameworks and methodologies to help firms evaluate and report on their cybersecurity programs. Guidance from these professional and international bodies offers companies advice to direct their efforts in an area that may not be familiar to many of its members. It can also give them a measure by which to compare their firms risk management efforts with those of their peers.

ISO standards

ISO is an international, non-governmental and independent organization with a membership of 164 national standards bodies that bring together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards. It has adopted five standards that promote cybersecurity and have relevant corporate governance elements: ISO 27001 and ISO 27002 on information security management systems, ISO 27014 and 38500 on governance of ICTs and information security, and ISO 22301 on business continuity management systems, which is applied by critical cyber-infrastructure management.

ISO 27001

ISO 27001[128] offers a standard for managing information security management systems over the basis of risk-based processes, which require businesses to put in place measures for detecting security threats that impact their information systems. To address identified threats, it recommends 114 controls to mitigate security cyber risks that an organization should select over the basis of best fit and availability of resources. The standard is structured around 7 blocks: context of the organization, leadership, planning, support, operation, performance evaluation and improvement.

The standard lists the requirements for establishing, implementing, maintaining and continually improving an information security management system. It notes that adoption of such a system is a strategic decision for an organization, as it will be part of, and integrated with, some of the most crucial processes of the organization, affecting how information is used within the organization. The key objective of the system is to apply effective risk management processes to guard the confidentiality, integrity and availability of information, and offer assurances to the relevant stakeholders.

The standard sets out the expectation that an information security management system implementation will be shaped and scaled in accordance with the context of the organization. This context includes the organization's needs and objectives, its size and structure, security requirements and organizational processes, as well as its evolution overtime. Defining the context requires organizations to determine two important elements that are also crucial for a sound corporate governance framework:[129]

- The external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcomes of its information security management system.
- The interested parties that are relevant to the information security management system; and the requirements of these interested parties relevant to information security.

---

[127] Among other highlights, the GDPR introduces into the legal framework the concept of "privacy by design," which calls for the inclusion of data protection considerations from the early stages of building data processing systems. Article 23 calls for data controllers to hold and process only the data absolutely necessary for the completion of their duties. Companies with more than 250 employees are also required to map and document the justification for storing and processing personal data, including how long it's being kept in the databases. Furthermore, companies that have "regular and systematic monitoring" of individuals at a large scale or process significant amounts of sensitive personal data, have to employ a data protection officer (DPO). The DPO position has to be independent and must report directly to the highest level of management about compliance with the GDPR, it is also a point of contact for employees and customers.

[128] See more information about the standard at: https://www.iso.org/isoiec-27001-information-security.html.

[129] See sections 4.1 and 4.2 of the standard, ISO iec 27001-2013, p.7.

Next the standard sets the expectations for the leadership of the organization. Here again the corporate governance references are evident. The standard calls upon top management to demonstrate leadership and commitment with respect to the information security management system by:

- Establishing a policy and objectives that are aligned with the strategy;
- Ensuring that the system requirements are integrated with the organization's processes;
- Allocating necessary budget and resources;
- Setting the tone from the top on supporting the system requirements;
- Monitoring performance;
- Incentivizing compliance;
- Promoting continual improvement; and
- Supporting other relevant managers to contribute to the overall functioning of the system.

The information security policy is a key element within the system, and the standard sets on the organization's leadership the expectation that it will: i) be aligned with the mission of the organization; ii) include objectives (or a framework for setting them), a commitment to comply with applicable requirements and for continual improvement; and iii) be available as documented information, communicated within the organization, and available to interested parties, as appropriate.

Finally, the standard sets expectations for organizational roles, responsibilities and authorities regarding information security, including for ensuring compliance with the standard itself, and reporting on the performance of the system to the board.

ISO 27002

ISO 27002[130] offers a standard of controls to manage the cybersecurity risks of information systems, designed for use alongside ISO 27001. It includes policies for enhancing information security, controls such as asset inventory for managing ICT assets, access controls for various business requirements and for managing user access, and operations security controls.

ISO 27014

ISO 27014[131] standard offers guidelines, concepts and principles for the governance of information security, by which organizations can evaluate, direct, monitor, and communicate information security-related activities within the organization.

The standard endorses corporate governance best practices and highlights that information security has become a key issue for organizations, not only for regulatory reasons but also due to the potential impact on their reputation. Accordingly, it calls upon boards and senior managers to oversee information security to ensure the strategic objectives of the organization are achieved. For that, it expects the leadership to issue a clear mandate for driving information security initiatives throughout the organization and demand relevant reporting about related activities, to inform timely decision-making.

The standard lists three as the main objectives for the governance of information security: i) achieving strategic alignment, ii) value creation; and iii) accountability for the managing of information risk. Six action-oriented principles are suggested as means to achieve these objectives:[132]

---

[130] See more information about the standard at: https://www.iso.org/standard/54534.html.
[131] See more information about the standard at: https://www.iso.org/standard/62816.html.
[132] See section 5 of the standard.

- Establish an organization-wide information security. Information security should be handled at an organizational level with decision-making taking into account business, information security, and all other relevant aspects. Activities concerning physical and logical security should be closely coordinated.
- Adopt a risk-based approach. Determining how much security is acceptable should be based upon the risk appetite of an organization, including loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial loss.
- Set the direction of investment decisions. An information security investment strategy should be established over the basis of the business outcomes achieved, resulting in harmonization between business and information security requirements, both in short and long term, to meet the evolving needs of stakeholders.
- Ensure conformance with internal and external requirements. Information security policies and practices should ensure compliance with relevant mandatory legislation and regulations, as well as committed business or contractual requirements and other external or internal requirements.
- Foster a security-positive environment. Human behavior is one the largest sources of risk, and the governance framework should require, promote and support coordination of stakeholder activities, and the delivery of security education, training and awareness programs.
- Review performance in relation to business outcomes. The information security approach should fit the organization, providing agreed levels of information security, as required by current and future business requirements. Performance should be assessed against its business impact, not just effectiveness and efficiency of security controls.

Structure-wise, the standard suggests that the board should govern information security by conducting four processes distilled into: evaluation, direction, monitoring and communication. In addition, a compliance function should provide an independent and objective opinion about the governance of information security and the level attained.

The standard contends that a corporate framework for information security that meats these objectives, adopts the principles and structure recommended, would allow a board to effectively monitor risks, be able to act swiftly when needed, make efficient and effective investments on information security, and comply with external requirements (legal, regulatory or contractual).

ISO 38500

ISO 38500[133] standard offers principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring the use of ICTs in their organizations.

The standard explains that nowadays ICT systems are essential for the functioning of almost all organizations, which spend large budgets in it not always obtaining the desired return and at times exposing the organization to adverse events. The standard argues that this adverse events are caused by a lack of a whole-of-enterprise approach on how to govern ICTs. The ICT model suggested is presented as part of the corporate governance of firms and aligned with mainstream corporate governance definitions.

As in the case of ISO 27014, this standard offers 6 principles for building the governance of ITCs, suggesting how to structure decision-making: i) Responsibility, ii) Strategy; iii) Acquisition; iv) Performance; v) Conformance, and vi) Human behavior. Each of these principles should be applied in a structure that follows a model similar to that described in ISO 27014: evaluate, direct and monitor.

[133] See more information about the standard at: https://www.iso.org/standard/43754.html.

ISO 22301

ISO 22301 standard specifies requirements for setting up and managing an effective business continuity management system (BCMS). A BCMS ultimately seeks to help organizations becoming capable of managing disruptive incidents ("to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise")[134] through the adoption of policies, objectives and controls, as well as monitoring and reviewing the performance and effectiveness of the system.

The standard sets out from the outset that the final shape of a BCMS will be determined by an organization's needs and stakeholders' expectations, its size and structure, its sector, and the legal, regulatory, organizational and industry requirements applicable to the products and services it makes, and the processes employed. For this, the standard recommends to first identify the organizations':[135]

- Activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact of a disruptive incident over them;
- Links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy; and
- Risk appetite.

Like ISO 27001, this standard also has expectations regarding the role of leadership and their commitment with respect to the BCMS, which translate in some of the same corporate governance related tasks and requirements described for ISO 27001.

NIST standards

The U.S. National Institute of Standards Technology (NIST) Framework for Improving Critical Infrastructure Security[136] is a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines, and practices. It is widely used beyond the U.S. and by non-critical infrastructure organizations as well.

NIST SP 800-39

NIST SP 800-39 on Information Security Risk Management, is a standard aiming to provide guidance for an integrated organization-wide program to manage information security risk for operations (i.e. mission, functions, image and reputation), assets and individuals. It provides a structured but flexible approach to managing information security risk that is intentionally broad-based, with specific details of risk assessment, response and monitoring on an ongoing basis, provided by other supporting NIST security standards and guidelines. The information security guidance contained in this standard is complementary and can be used as part of a more comprehensive business risk management (ERM) program.

NIST SP 800-53

NIST SP 800-53, on Security and privacy controls for organizations and information systems is a standard that provides a set of controls for protection against various threats, including hostile attacks, natural disasters, structural failures, human error and privacy risks.

---

134 See p.11.
135 See p.19.
136 See https://www.nist.gov/cyberframework.

Other technical frameworks

CIS

The Center for Information Security (CIS) framework[137] was designed by a coalition of volunteer experts to help companies improve cybersecurity. It uses 20 controls and the three-fold process starting with the basic elements, then moving into foundational aspects and finishing at the organizational level. This approach suits companies ranging from those that have limited cybersecurity expertise and resources, to companies with vast cybersecurity expertise and resources, allowing companies to create budget-friendly and focused cybersecurity programs.

COBIT

Control Objectives for Information and Related Technology (COBIT)[138] is a framework for the identification and mitigation of cyber risk, originally developed for ICT governance professionals to reduce technical risk, but that has evolved into a standard to align ICT with business goals. What it lacks is informative practical advice. While it's not as widely followed as others, COBIT is mostly used within the finance industry to comply with standards such as Sarbanes-Oxley.

AICPA

The American Institute of CPAs (AICPA) offers a framework[139] and guidance for evaluating and reporting on an organization's cybersecurity risk management program and underlying controls. Its use is entirely voluntary and offers tools that can be used to identify gaps and design remediation activities to fill those gaps.

Industry and sectorial initiatives

- The Council to Secure the Digital Economy (CSDE),[140] launched in 2018 by international Internet service providers, aims at securing digital infrastructure. CSDE released an International Anti-Botnet Guide in 2018.
- The Cyber Threat Alliance[141] has industry members who share threat intelligence to improve cybersecurity and resilience.
- Cybersecurity Tech Accord[142] has over 100 industry members seeking to share cybersecurity capacities.
- World Economic Forum Centre for Cybersecurity.[143]
- The global Forum of Incident Response and Security Teams (FIRST)[144] with 400 members from Africa, the Americas, Asia, Europe and Oceania.
- The Anti-Phishing Working Group[145] engages law enforcement, industry, NGOs and governments to under-take data exchange, research and public awareness in order to respond to cybercrime.
- The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)[146] has industry members working together to combat cyber-crime.

---

137 See more information about the standard at: https://www.cisecurity.org/controls/.
138 See COBIT's webpage: https://www.isaca.org/resources/cobit.
139 See AICPA (2017), AICPA Unveils Cybersecurity Risk Management Reporting Framework, April 26, 2017, available at: www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html.
140 See Council to Secure the Digital Economy website: https://securingdigitaleconomy.org/.
141 See Cyber Threat Alliance website: https://www.cyberthreatalliance.org.
142 See Cybersecurity Tech Accord webpage: https://cybertechaccord.org/accord/.
143 See World Economic Forum, Centre for Cybersecurity, webpage: https://www.weforum.org/centre-for-cybersecurity.
144 See Forum of Incident Response and Security Teams webpage: https://www.first.org.
145 See Anti-Phishing Working Group webpage: https://apwg.org.
146 See Messaging, Malware and Mobile Anti-Abuse Working Group webpage: https://www.m3aawg.org.

UNITED NATIONS

ECLAC Series

Production Development

Issues published

A complete list as well as pdf files are available at
www.eclac.org/publicaciones

225. Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean, Héctor J. Lehuedé, (LC/TS.2020/103), 2020.
224. Institutional change and political conflict in a structuralist model, Gabriel Porcile and Diego Sanchez-Ancochea (LC/TS.2020/55), 2020.
223. Corporate governance and data protection in Latin America and the Caribbean, Héctor J. Lehuedé (LC/TS.2019/38), 2019.
222. El financiamiento de la bioeconomía en países seleccionados de Europa, Asia y África: experiencias relevantes para América Latina y el Caribe. Adrián G. Rodríguez, Rafael H. Aramendis y Andrés O. Mondaini (LC/TS.2018/101) 2018.
221. The long-run effects of portfolio capital inflow booms in developing countries: permanent structural hangovers after short-term financial euphoria, Alberto Botta (LC/TS.2018/96) 2018.
220. Agencias regulatorias del Estado, aprendizaje y desarrollo de capacidades tecnológicas internas: los casos del Servicio Nacional de Pesca y Acuicultura y el Servicio Nacional de Geología y Minería de Chile, Rodrigo Cáceres, Marco Dini y Jorge Katz (LC/TS.2018/40) 2018.
219. Capital humano para la transformación digital en América Latina, Raúl L. Katz (LC/TS.2018/25), 2018.
218. Políticas de fomento productivo para el desarrollo de sectores intensivos en recursos naturales. La experiencia del Programa Nacional de Minería "Alta Ley", Jonathan Castillo, Felipe Correa, Marco Dini y Jorge Katz (LC/TS.2018/16), 2018.
217. El estado de la manufactura avanzada: competencia entre las plataformas de Internet industrial, Mario Castillo (LC/TS.2017/123), 2017.
216. Políticas para la atracción de inversión extranjera directa como impulsora de la creación de capacidades locales y del cambio estructural: el caso de México, Luz María de la Mora Sánchez (LC/TS.2017/122), 2017.

PRODUCTION DEVELOPMENT

Issues published:

225. Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean
Héctor J. Lehuedé

224. Institutional change and political conflict in a structuralist model
Gabriel Porcile
Diego Sanchez-Ancochea

223. Corporate governance and data protection in Latin America and the Caribbean
Héctor J. Lehuedé

222. El financiamiento de la bioeconomía en países seleccionados de Europa, Asia y África
Experiencias relevantes para América Latina y el Caribe
Adrián G. Rodríguez
Rafael H. Aramendis
Andrés O. Mondaini

ECLAC
Economic Commission for Latin America and the Caribbean (ECLAC)
Comisión Económica para América Latina y el Caribe (CEPAL)
www.eclac.org

LC/TS.2020/103