Cybersecurity Economics for Latin America and the Caribbean[1]

Preliminary Version

May 2nd, 2024

Abstract

Fueled by the rapid proliferation of connectivity, IoT devices, e-commerce, e-government tools, and low levels of cybersecurity commitments, LAC ranks as the world's region with the highest growth rate of disclosed cyber incidents, particularly since the onset of the COVID-19 pandemic. Additionally, it is the second most affected developing region in terms of frequency of cyber incidents. Notable cases of cyber incidents in LAC have resulted in significant economic losses for countries, infringements upon citizens' basic rights such as the right to privacy and vote, and disruptions to essential services.

Despite the escalating cyber threats in the region and the demonstrated potential harm of cyber incidents, there has been minimal research efforts to facilitate informed cybersecurity decisions by stakeholders. This work aims to contribute to closing such a knowledge gap by offering a comprehensive data-based analysis of the region's threat landscape, identifying the determinants, motives, types, targets, and, where possible, the effects of disclosed cyber incidents in the region.

In this sense, this paper sheds light on the region's escalating cyber risks, propelled by the swift digitization of nations, alongside inadequate cybersecurity commitments, competing social needs, and unclear rates of return. Complemented by case studies and an industry analysis, it also presents practical policy recommendations to bolster cybersecurity in LAC.

Keywords: Cybersecurity, cybercrime, cyber incidents, economic growth, productivity.

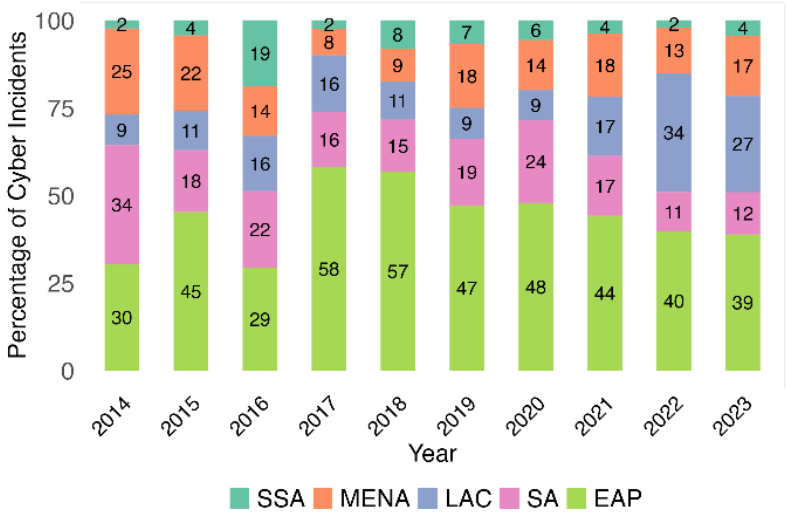
JEL codes: L1, G1, O3, Z01.

[1] This note is a product of LCRVP and INFCE, produced by Hualong Diao (STC) and Estefania Vergara Cobos (Economist) under the support of Luis Alberto Andres and Stephane Straub. This work is a ramification of the "Cybersecurity Economics for Emerging Economies" report. The authors may be contacted at evergaracobos@worldbank.org.

1. Introduction

In 2022, a ransomware attack infiltrated approximately 26 government entities in Costa Rica, including critical institutions like the Ministry of Finance and the Ministry of Labor and Social Security. This cyber incident lasted for roughly 56 days, resulting in economic losses equivalent to about 2.4% of the nation's annual GDP.[2] Around the same time, Telecom Argentina, a major telecommunications provider in the South American country, grappled with the aftermath of a ransomware attack that translated into a long-lasting drop in its share price, while the Mexican banking system experienced a major cyber-attack to the interbank electronic payment system. Although a cyber-run[3] was avoided, the incident left significant losses for banks and delays in users' payments.[4] However, going beyond just economic considerations, perhaps the most alarming cyber incidents in LAC in the last years are those that have compromised the human right to privacy of countries' entire populations. This occurred in 2019 and 2022, when all citizens from Ecuador and Argentina, respectively, witnessed their confidential data being breached and sold in illegal markets, including banking details, addresses, contact information, and other sensitive data. These cases coincided with two politically motivated cyber incidents during regional and national elections in Brazil and Ecuador, respectively. In the latter, a significant portion of expatriates found themselves deprived from their right to vote due to a disruption in the online electoral system.

Figure 1: Distribution of cyber incidents across developing region (2014 to 2023).



Source: Vergara Cobos (forthcoming) based on CISS and WB cyber incidents databases.[5]

[2] According to Datta and Acton (2022), the 2022 Costa Rican ransomware attack lasted 56 days, from April 17, 2022 to June 11, 2022. The local economy is estimated to have lost about USD 30m per day.

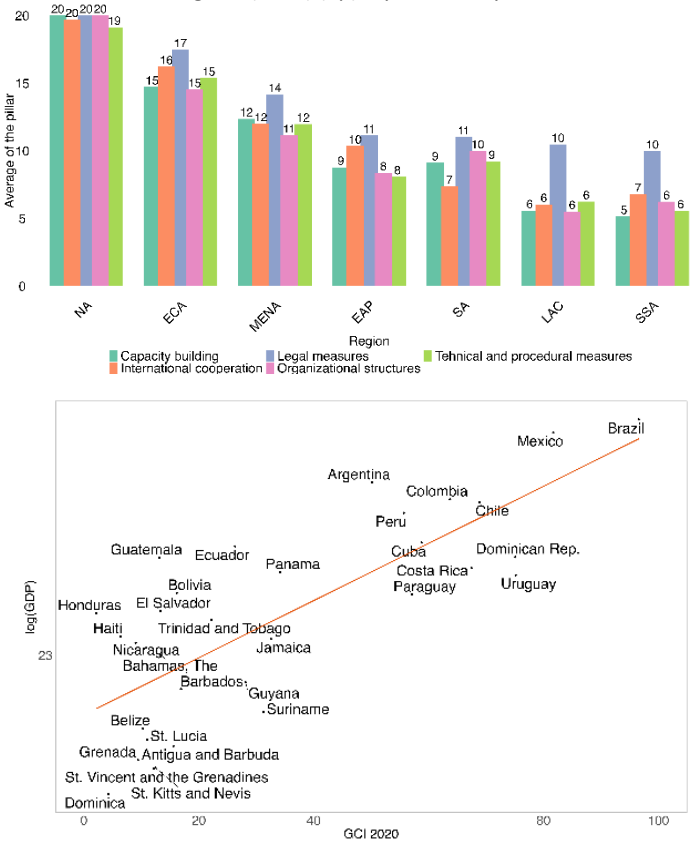
[3] A cyber run is a systemic cyber incident in the financial sector.

[4] https://www.bbc.com/mundo/noticias-america-latina-44130887

[5] The sample of disclosed cyber incidents is collected in two databases, built scraping data from publicly available sources (e.g., news outlets). The Cyber Incidents Database collected by the Center of International and Security Studies (CISS) at the University of Maryland which covers about 11,000 cyber incidents from 2014 to 2023 in 156 countries, and the Media-Disclosed Cyber Incidents database built by the authors of this book, which covers approximately 27,000 cyber incidents from 2017 to 2022 in 179 countries. The open sources used to gather data on disclosed cyber incidents included media outlets in 98 different languages. The final analysis covers 451 cyber incidents in the LAC region from 2014 to 2023, with November and December data in 2023 imputed with November and December data in 2022.

Amid the COVID-19 pandemic, LAC has emerged as the world's fastest-growing region for cyber incidents, and the second developing region in terms of number of disclosed cyber incidents.[6] This alarming trend stems largely from cybersecurity commitments that have failed to keep pace with the region's digital advancements. For example, despite the significant growth in internet adoption, from 48% to 76% of the population connected to the internet between 2014 and 2021, LAC ranks second to last in terms of legislative, technical, cooperation, and capacity building cybersecurity measures, only after SSA.[7] The biggest gap in the region lies on capacity building measures such as those related to the development of a national cybersecurity industry and investment in R&D, both crucial factors to achieve efficient market allocations. At the country level, although Brazil and Mexico show the highest scores (with GCI scores of 96.6 and 81.7, respectively) in terms of cybersecurity commitments,[8] they remain as the most attacked countries in the region, a situation that showcases that further commitment measures could be needed for highly attacked countries.

Figure 2: Cybersecurity commitments across regions (2020) (up). Cybersecurity commitments versus GDP in LAC (2020) (down).



Source: Authors' elaboration based on GCI 20201 and WDI database.

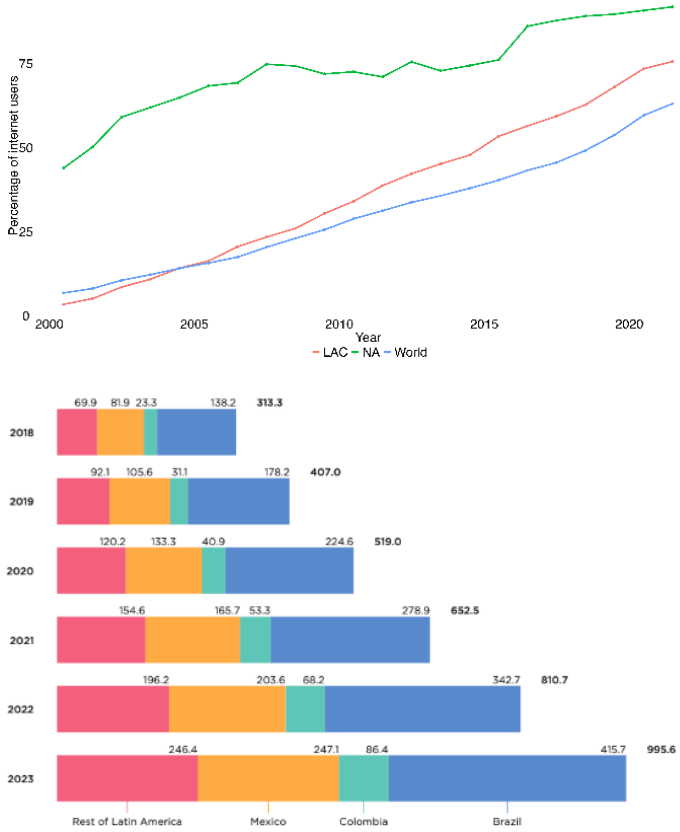
[6] Vergara, E., forthcoming.

[7] ITU online statistics and GCI (2020).

[8] The cybersecurity commitments are measured by Global Cybersecurity Index (GCI 2020). The ITU's Global Cybersecurity Index (GCI) assesses the commitment of countries to cybersecurity at a global level using five pillars - (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation - and generates an aggregate score per country ranging from 0-100.

Additionally, the region has seen a notable increase in the number of Internet of Things (IoT) devices, rising from 407 million units in 2019 to 997 million in 2023, and projected to increase by 141% from 2023 to 2030.[9] With more connected devices and population's internet adoption, the possible entry points for malicious actors increases. This phenomenon is referred to as the *expanding cyber-attack surface*.

Figure 3: Percentage of internet users in LAC versus NA and world, from 2000 to 2021 (up). Number of IoT Devices in LAC, from 2018 to 2023 in millions (down).



Source: Author's elaboration based on The World Bank data[10] and IDB (2019).

The issue of the region's *expanding cyber-attack surface* has also been fueled by the boom in e-commerce volume, soaring from 176 billion to 509 billion between 2019 and 2023,[11] and the COVID-19 pandemic push of daily activities toward remote work, telehealth, and remote learning. Moreover, governments in the region have leveraged digital tools to enhance transparency and efficiency of public services,[12] while more infrastructure sectors have adopted online systems and software-based controls.[13] These and other connectivity factors, combined with nations' low cybersecurity commitments and pressing social needs, have translated into an alarming cybersecurity challenge for most countries in the region. **However, the expansion of the *cyber-attack surface* goes beyond connectivity and commitment**

[9] Source: https://explodingtopics.com/blog/number-of-iot-devices.
[10] Source: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZJ.
[11] Source: https://explodingtopics.com/blog/number-of-iot-devices.
[12] OECD, 2023.
[13] IDB, 2020.

factors, as the development of cyberspace itself is intrinsically vulnerable. With nearly 6 million developers worldwide writing code at every moment in time, and rarely initiating projects entirely from scratch, secure software development poses one of the most significant challenges in the digital age, as the norm is to build vulnerabilities on top of vulnerabilities.[14]

Although disclosed cyber incidents are mostly centered in HICs and in the biggest economies, the growth and severity of incidents across LAC is non-negligible, especially in the near future **as 24% of the LAC's population have yet to be connected, and thus, countries have yet to see the full extent of the connectivity effects on cybersecurity.**

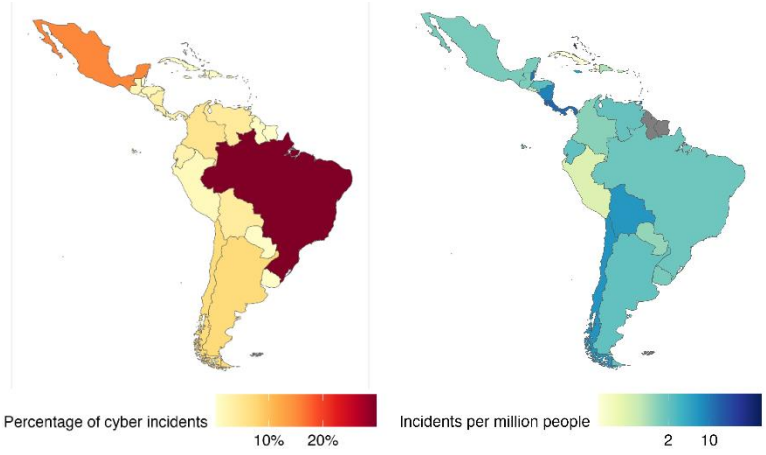
Figure 4: Global distribution of disclosed cyber incidents from 2014 to 2023

Source: Vergara Cobos (forthcoming). Note: This map is based on two data samples of disclosed cyber incidents identified from scraping millions of media outlets in various languages, built by Harry & Gallagher (2018) and the WB team.

The nature of disclosed cyber incidents varies greatly between countries, highlighting the need for data-driven approaches that allow for tailored and efficient policy recommendations. Cyber incidents are influenced by three primary factors: the attractiveness of the victim to malicious actors, the potential gains involved, and the target's cybersecurity maturity. Approximately **58% of cyber incidents in LAC have a financial motivation.** However, in countries with political stability challenges, such as Venezuela, the top motivation is political including political espionage, protest, and sabotage. Likewise, there is a vast difference at the country and sectorial levels, with the frequency of cyber incidents reflecting the level of digitization of countries' economies. For example, Brazil, a country with a dynamic digital economy, presents incidents in over 10 sectors, with the majority centering in the public administration, finance, and information and communications. On the other hand, more concentrated economies such as Panama and the Caribbean countries of Jamaica and Cayman Islands, mostly see cyber incidents targeting a handful of sectors. However, in general, **the sectors that standout in LAC as the most targeted by malicious actors are the public administration and finance**. Moreover, amid the COVID-19 pandemic, incidents targeting the professional services sector have increased significantly, reflecting the threats of hybrid work.

[14] Vergara, E., forthcoming.

Figure 5: Distribution of cyber incidents in LAC (left), Distribution of cyber incidents per million people in LAC (right) (Jan 2014 to Jun 2023).



Source: Authors' elaboration based on Maryland CISSM Cyber Attacks Database and the Media-Disclosed Cyber Events (MDCE) Database.[15]

The rest of this paper further elaborates on the nature and determinants of cyber incidents in the region, showing the threat landscape. It also discusses the levels of relative cyber risk across countries, that signal Peru, Venezuela, Panama, and Argentina as the ones with the highest risk. The analysis also dives deep into an exploration of the determinants of cybercrime in LAC, identifying key socioeconomic, political, and digital factors that contribute to the region's vulnerability. Finally, this paper presents a couple of case studies revealing the diverse strengths and weaknesses in different aspects of cybersecurity commitments, and a brief description of the industry in the region, which serves in the analysis of market failures and policy recommendations.

The paper is developed in the following sections: Section 2 provides a literature review about LAC and global studies on the economics of cybersecurity. Section 3 presents the cybersecurity landscape in LAC, including a discussion about cybersecurity commitments, determinants, vulnerabilities, and cross-country cyber risks. Section 4 studies the policy framework, opportunities, and challenges of cybersecurity for Brazil and Mexico. Section 5 presents the status quo of the cybersecurity market in LAC and possible sources of market failures. Finally, section 6 discusses the main conclusions and policy implications from the analysis.

2. Literature review

LAC studies

According to the literature, the rising trend of cyber incidents since the COVID-19 pandemic observed in LAC has been mainly driven by the shift towards a digital lifestyle and the adoption of new

[15] The Media-Disclosed Cyber Events Database (2017-2022) follows a seven-step data mining process based on the GDELT media reports, which is described in Vergara et al. (forthcoming). The graph of cyber incidents per million people only includes the countries with population over 200 thousand excluding Guyana and Suriname.

technologies,[16] with studies identifying the surge in internet users[17] and the expanding use of AI as two key drivers. This has consequently underscored the need for stricter data protection regulations across the region.[18] Moreover, studies have also highlighted the existing **security gap in critical infrastructure**, especially infrastructure used in the provision of essential services, evidenced by a low adoption of advanced cybersecurity systems across organizations, and a relative low degree of critical infrastructure protection across countries in the region.[19]

Financial, technical, and staff shortages also appear in the literature as limitations for achieving appropriate levels of cybersecurity in the region.[20] However, these are not the only restrictions, the region also requires updated cybersecurity legislations and regulations,[21] increased cybersecurity awareness, strengthened regional and international cooperation, and an overall control of organized crime.[22] For example, in Brazil, a country were cybersecurity policies and infrastructure expansion (e.g., 5G development) have been developed almost in parallel,[23] top cybersecurity challenges include those related to the operability of legislation and scarcity of law enforcement resources, as well as the rapidly expanding demand for cybersecurity professionals. Strengthening existing cybersecurity measures could involve updating the national cybersecurity strategy and enhancing privacy protections such as the LGPD (*Lei Geral de Proteção de Dados*, General Data Protection Law), Brazil's 2020 data protection law with penalties enforced since 2021.[24]

On the other hand, facing various security issues such as organized crime and drug trafficking, Mexico's cybersecurity challenges stem from outdated legislations, low cybersecurity awareness, and organized crime.[25] Works like Martinez et al. (2017) highlight the importance of working jointly on data protection measures and users' awareness to minimize the cyber risk of Mexicans, especially in online registration forms and social network sites. In terms of organized crime, Kobek (2017, 2018)[26] emphasizes on the need for continuously updated legislation, backed up by stronger public-private collaborations, and international cooperation.

Across the region, the literature on governance of cyberspace in LAC has increasingly adopted a militaristic approach,[27] which highlights the threats of cybersecurity issues to democratic processes in the region.[28] Mainly, Solar (2020) identifies a regional trend where armed forces in countries such as Argentina, Colombia, Chile, Mexico, and Venezuela have taken on roles in cyberspace protection, following the example of Brazil's Cyber Defense Command. Although necessary, these cybersecurity

[16] Izycki (2018); Buzzio-Garcia et al., 2021; Flor-Unda et al., 2023; Saavedra, 2023.
[17] Buzzio-Garcia et al., 2021.
[18] Kobek and Caldera, 2016; Rendon, 2022.
[19] Flor-Unda et al., 2023.
[20] Kshetri and DeFranco, 2020; Martinez et al., 2017.
[21] Carapeto and Calil, 2020; Arellano, 2016; Kobek and Caldera, 2016; Rendon, 2022, Solar, 2020; 2023.
[22] Kobek, 2017 & 2018; Izycki, 2018; Torres, 2018.
[23] Source: Carapeto and Calil (2020). They focus on Brazil's cybersecurity regulation with comparing it with policies in Argentina, Chile, Colombia, and Mexico. They find that other LAC countries also share the challenges of confronting infrastructure expansion and regulation commitment.
[24] Kshetri and DeFranco (2020).
[25] Arellano, 2016; Kobek 2017, 2018.
[26] He provides overview of Mexican cybersecurity environments and national cybersecurity strategy.
[27] The military computer network operation units increase by 116% from 2000 to 2017 among the 95 countries listed as victims in the Council on Foreign Relations' cyber operation tracker. (Source: https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities.)
[28] Solar, 2020 and 2023.

militarization processes in the region need to be transparent, interactive, and collaborative not to deter broader stakeholder participation in cyberspace protection.

Global studies on the economics of cybersecurity

Research on the economics of cybersecurity as a tool to justify investments is scarce and highly focused in developed countries, mainly due to the issue of data availability elsewhere. However, a new study[29] shows that there is a statistically significant negative correlation between the frequency of cyber incidents and economic performance in developing countries. Mainly, Vergara et al. (forthcoming) show that a cyber incident in non-HICs is associated to average decreases in GDP per capita between USD 2.4 and USD 2.7, with higher losses associated to cyber incidents in the financial, information and communications, and public sectors. Moreover, this research also finds that cybersecurity commitments could help alleviate such economic losses, by showing that digitized industries in highly committed countries grew faster between 2014 and 2022 than those in low committed countries, holding everything else constant and controlling for cofounding factors.

Besides the associated economic losses of cyber incidents, there is a challenge on the increasing unit cost of incidents.[30] Mainly, research shows **an increasing trend in the total cost of cyber incidents, driven by a rise in the number of incidents and the growing unit cost, particularly in the healthcare sector and from data breaches.** For example, according to IBM (2023) the global average cost of a data breach went from USD 3.62 million to USD 4.45 million from 2017 to 2023. In Latin America, this figure increased by a third, going from USD 2.8 million to USD 3.69 million between 2017 and 2023.[31] Such an increasing trend is observed across various sectors but mainly those highly financially and operationally interconnected, such as finance, and information and communications. With higher cost increases amongst incidents targeting small businesses, the situation could be worse for small and medium-sized enterprises (SMEs) in LAC.

However, not all cyber incidents matter or lead to important economic or social consequences. According to the literature, the most dangerous and costly cyber incidents have been those that have led to second, third, and even fourth rounds of effects. Like for example, the 2017 NotPetya attack that resulted in the inoperability of thousands of organizations worldwide, including hospitals and transnational corporations, leading to economic losses of over USD 7.3 billion from the consumers of the attacked firms, a figure equal to 4 times the revenue losses faced by the directly hit firms.[32]

According to the literature, different factors affect the proliferation of cyber incidents within a country, including political, socio-economic, technical, and digital considerations. For example, **recent research[33] shows that countries with higher unemployment rates, high connectivity, corruption, and an unstable political environment are more likely to face cyber incidents than their counterparts,** an alarming finding for countries in LAC.

[29] Vergara et al., forthcoming.
[30] IBM (2023), Vergara Cobos (forthcoming).
[31] IBM, 2023.
[32] Vergara Cobos, forthcoming.
[33] Kumar and Carley (2016), Mezzour et al. (2014), Kigerl (2012), Asal (2016), Chen et al. (2023).

3. The cybersecurity landscape in LAC

From 2015 to 2022, LAC shifted from being the fourth to the second most attacked developing region only after EAP. Accounting for approximately 10% of global cyberattacks and 5% of cyber incidents worldwide, LAC faces a significant rise in cyber threats, particularly accentuated by the COVID-19 pandemic.[34] Several factors fuel this increase, including historically low levels of cybersecurity commitments in the region, heightened connectivity among the population, and the rapid proliferation of interconnected IoT devices. Additionally, the region's unstable political landscapes and challenging economic conditions have translated into cyber threats, with Venezuela leading in politically motivated incidents and Brazil in financially motivated ones.

The frequency of incidents in the region correlates with the size of the economy, with the top 5 most attacked countries being Brazil, Mexico, Argentina, Chile, and Colombia, collectively accounting for nearly 65% of total cyber incidents. However, at the per capita level, Barbados, Bahamas, Costa Rica, Panama, and Trinidad and Tobago stand out at the highest targeted countries.[35]

Despite the frequency and sheer numbers, cyber incidents in the region have led to severe and diverse consequences, including privacy breaches, critical system shutdowns, and substantial financial losses. Notable incidents include the 2018 attack on Mexico's interbank transfer system, which posed a threat to the sector's stability by attempting to steal from banks between USD 17.7 million to USD 23.6 million.[36] Subsequently, in 2021, an attack on Brazil's health ministry websites resulted in computer system shutdowns and the exposure of millions of citizens' COVID-19 vaccination details. This, however, has been just one of the many concerning confidential data breaches in the region, with Argentina and Ecuador having suffered data breaches of their entire population. Mainly, the entire national ID database of Argentina's population (45 million) was compromised and offered for sale on the dark web following a hack of the National Registry of Persons in 2021. The same occurred in Ecuador in 2019, after an incident to a third-party vendor led to the breach of confidential data of about 20 million citizens, including the entire alive population plus 4 million deceased. Cyber incidents have also led to the disruption of essential services. For example, in 2019, Mexican petroleum company Pemex received a ransomware attack by Sodinokibi, leading to disruptions in 5% of equipment, and an estimated cleanup cost of USD 71 million.[37] Lastly, perhaps the severer cyber incident in the region was Costa Rica's 2022 ransomware attack to government computer systems that resulted to the shutdown of public services such as tax declarations and customs, for approximately 60 days.

Based on a comprehensive consideration of almost 30 determinants of cyber incidents, research suggests that countries like **Peru, Venezuela, Panama, and Argentina could be facing the highest relative**

[34] Fortinet (2023), IARI (2023). Source: a) https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent; b) https://iari.site/2023/10/05/current-panorama-of-cyber-security-in-latin-america-threats-and-possibilities/#:~:text=According%20to%20Fortinet%20statistics%2C%20cyberattacks,finally%20Peru%20(15%20billion.

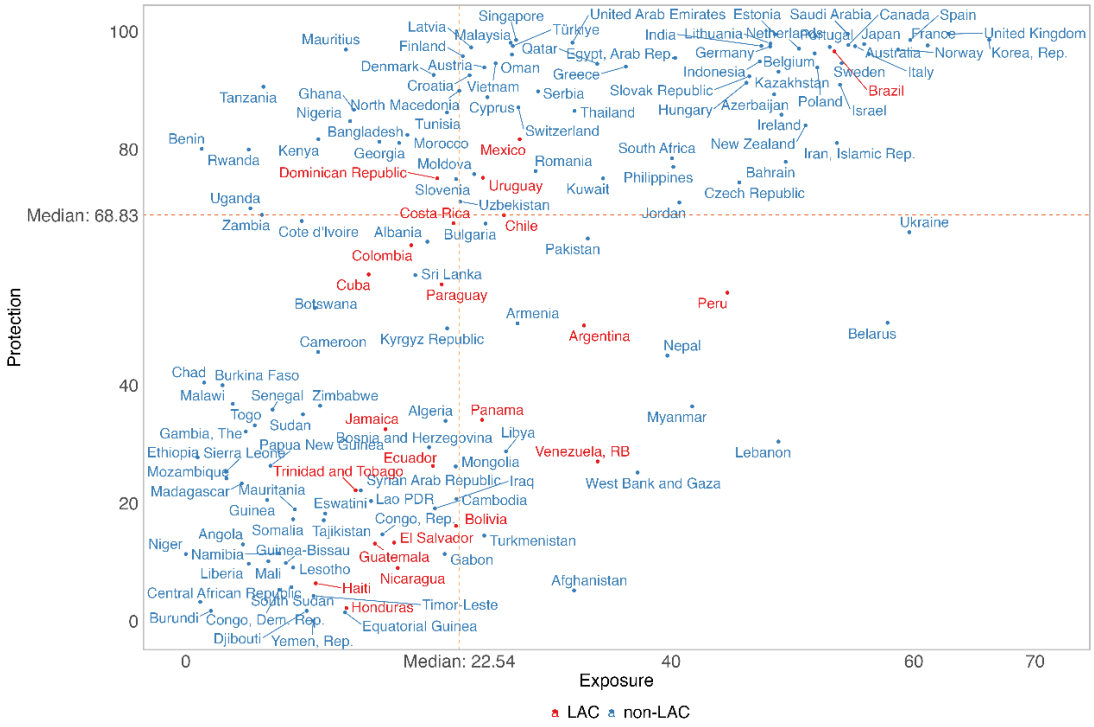
[35] The number of cyber incidents per million people only includes the countries with population over 200 thousand excluding Guyana and Suriname.

[36] Although the exact status of attacks is not certain, it is said that the authorities have confirmed that no one was affected. (Source: https://www.welivesecurity.com/2018/05/24/mexico-cybercriminals-steal-400-million/)

[37] Source: a) Mariano, Diaz (2021). https://repositorio.cepal.org/server/api/core/bitstreams/8baec4f7-bd99-47b2-bd53-f6e01f4c3a1b/content. b) https://www.cdw.com/content/cdw/en/articles/security/ransomware-attacks-energy-industry.html. Note: The attackers demand $50 million ransom which was not paid by the company in the end.

risk in the region with exposure levels in between 32.8 and 44.6 out of 100 and protection levels in between 27.1 and 55.7 out of 100.[38] Like other countries in the region, these countries present gaps in capacity building, organizational structures, technical measures, international cooperation, and even legislation, with for example, gaps in national cybersecurity strategies, critical infrastructure protection, cybercrime legislation, and updated and operationalized data protection laws. The third quadrant in Figure 6 represents countries with low cybersecurity exposure and low protection levels, including 13 countries in LAC, like Jamaica, Ecuador, and Colombia. Countries in this quadrant indicate **a uniform cyber risk profile in the region that warrants attention for improved cybersecurity as digitization rises.**

Figure 6: Protection and exposure levels in LAC.



Source: Authors' elaboration based on ITU and WB Cybersecurity Readiness Index.

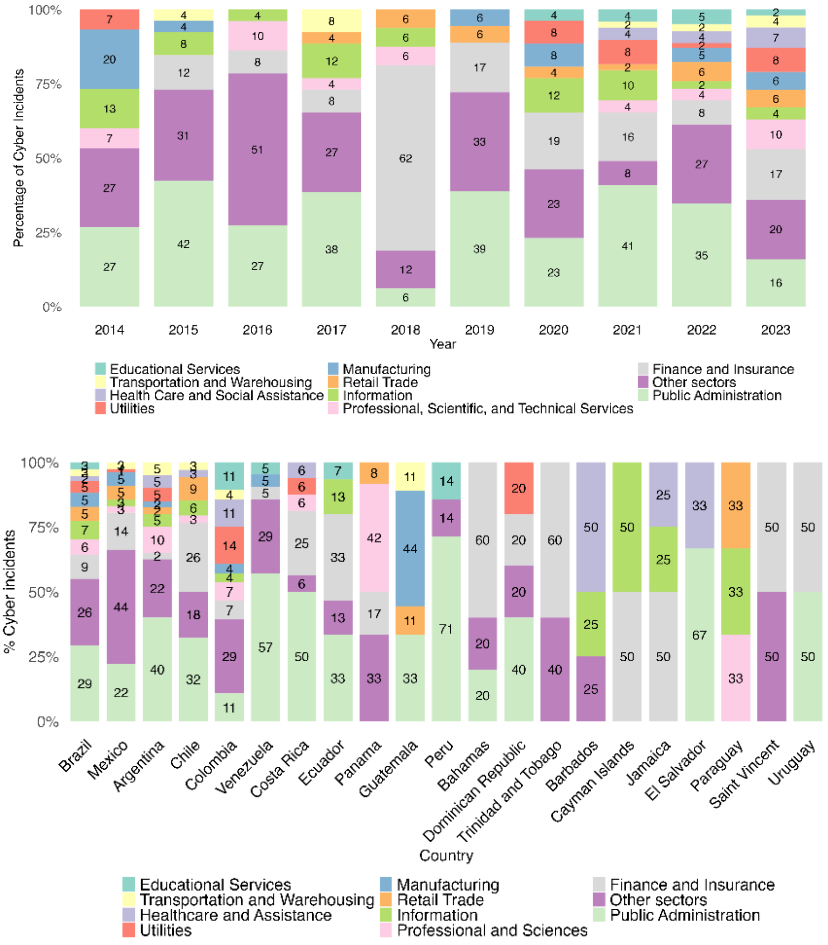
Threat landscape

The public administration ranks as the most attacked sector in LAC based on the number of disclosed cyber incidents, followed by finance, and information and communications. Notably, cyber incidents have been spreading across the newly digitized industries throughout the last decade, and especially, since the COVID-19 pandemic. However, the sectorial distribution of cyber incidents varies greatly across countries, showing the diversification of the economy, and the digitization and cyber maturity of the sector. For example, the region's biggest economy, Brazil, has observed cyber incidents directed at over 10 different sectors, whereas other countries like Panama and the Caribbean countries

[38] Vergara Cobos, forthcoming.

mainly experience incidents targeting the financial and information and communications sectors. However, the public administration represents an important share of cyber incidents amongst most countries in the region, with some of the most significant cases being those that aimed to disrupt or influence elections, like it occurred in Brazil's 2020 regional and Ecuador's 2023 national elections that disrupted the vote counting system and prevented expats from their right to vote, respectively.[39]

Figure 7: Evolution of cyber incidents by sector in LAC (up) and by countries (down) (2014 to 2023)



Source: Authors' elaboration based on Maryland CISSM Cyber Attacks Database.

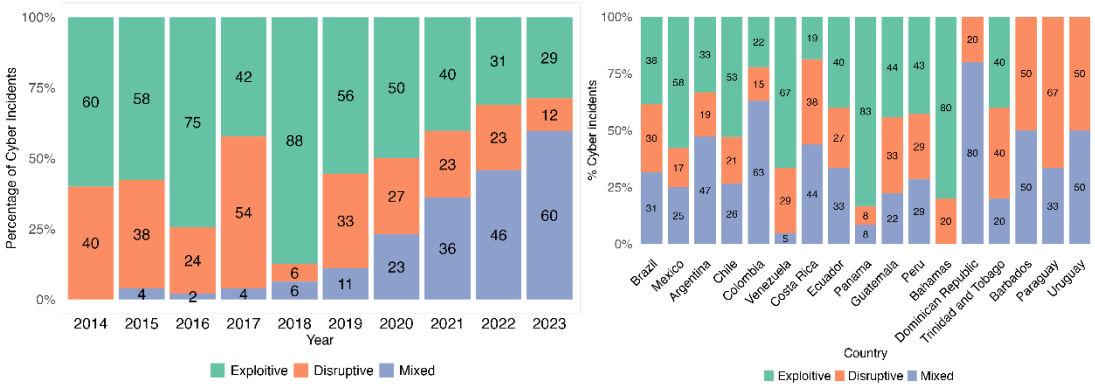
In terms of the type of incident, in the last decade the region has mainly experienced exploitive incidents or those aiming to steal information mostly for financial purposes. However, this has been changing since the COVID-19 pandemic, with a growing number of incidents of both an exploitive and a disruptive type (mixed), with disruptive being those that impede the normal operations of the victims.[40] However, the type of incident varies among countries, with for example, Panama and the Bahamas experiencing over 70% of exploitive cyber incidents, and Paraguay and Uruguay over 50% of disruptive

[39] Source: https://www.cbsnews.com/news/ecuador-presidential-election-polls-candidates-cyber-attacks/.

[40] The disruptive incidents impede the normal operations of the targeted organizations. The exploitative incidents aim to access or steal sensitive information such as personal identifiable information, classified information, or financial data. The mixed type incidents contain cyber incidents incorporating both disruptive and exploitative elements, such as ransomware attacks. (Source: https://gotech.umd.edu/cyber-events-database.)

incidents. Mixed type incidents occur in a variety of settings such as when the attacker aims to both steal information and disrupt systems, usually for financial reasons. Alarmingly, mixed types are associated with the disruption of critical services like healthcare, financial, and essential services, making their increase one of high concern for governments, due to the criticality of the services disrupted and the associated financial losses. For instance, the Brazilian electric power distributor Light Energia S.A. felt victim of a ransomware attack in 2020 that resulted in the block of server access with a demanded ransom of USD 14 million.[41]

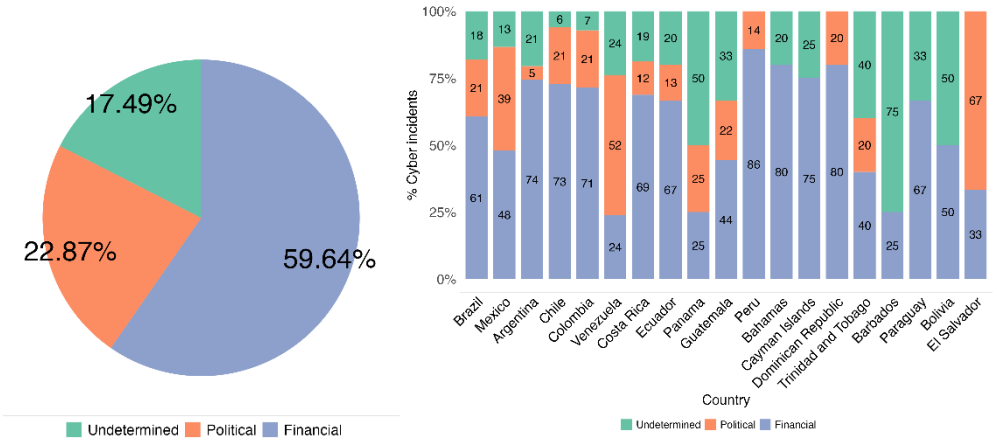
Figure 8: Evolution of cyber incidents by type of incidents (From 2014 to 2023).



Source: Authors' elaboration based on Maryland CISSM Cyber Attacks Database.

Cyber incidents in LAC are predominantly financially motivated, with the rest serving as tools for political reasons such as protest, sabotage, and espionage. However, with over 40% of incidents having a political motivation, Venezuela and Mexico are two outliers in the region.

Figure 9: Distribution of cyber incidents by motives in LAC (From Jan 2014 to Dec 2023).



Source: Authors' elaboration based on Maryland CISSM Cyber Attacks Database.

Critical infrastructures (CI) are increasingly targeted in the region through the employment of ransomware and malware to disrupt essential services. Across the world, key vulnerabilities lie within

[41] Source: https://repositorio.cepal.org/server/api/core/bitstreams/8baec4f7-bd99-47b2-bd53-f6e01f4c3a1b/content (Mariano Diaz, 2021).

the security of Data Acquisition, Supervision, and Control (SCADA) system and Industrial Control Systems (ICS), crucial for operating utilities and public services.[42] Specifically, it is estimated that, in 2021, industrial control systems receive about 1.15 cyberattacks per hour and more than 10,000 attacks in LAC.[43] Despite this, only 22% of LAC countries have critical infrastructure plans to defense against cyberattacks, leaving vital systems at high risk of cyber incidents.[44] Currently, countries experiencing the most frequent cyber incidents to CI include Brazil, Colombia, Argentina, Costa Rica, Mexico, and Dominican Republic, most of them having experienced incidents to energy suppliers.

Determinants of cyber incidents in LAC

Cybercrime is a lucrative business, thus, all else equal, the wealthier and more digitized countries, and targets, see, on average, more cyber incidents.[45] This is validated by the fact that across HICs, the top targeted sector is healthcare, as the unit cost of an attack is priced based on the confidentiality of the data compromised and the criticality of the services disrupted. In LAC, the healthcare sector is less digitized than in HICs, therefore, less vulnerable, and targeted. However, the financial sector in the region occupies the second place in terms of incidents, showing a sector vulnerability and attraction not observed across HICs, where the financial sector has achieved the highest levels of cybersecurity maturity (measured in terms of disclosed cyber incidents and successful responses to attacks). Mainly, across HICs, the financial sector appears as the sixth in terms of frequency of disclosed cyber incidents despite the high attractiveness of the sector to malicious actors.

In addition, unemployment and other unmet social needs can further exacerbate cybercrime. This is mostly a problem for countries with a surplus of computer skilled labor force, that given a lack of legitimate employment might employ their expertise in malicious cyber activities.[38] Therefore, countries must aim to combine computer education programs with subsequent matching of participants in the labor market.

Beyond connectivity and cybersecurity variables, **other technical and digital factors are also contributors to cybercrime, and cyber incidents in general.** This includes the emergence and adoption of new technologies such as cloud computing that allow data to be accessed across various locations, and artificial intelligence (AI), that is seen as a double-edged sword in cybersecurity. Therefore, countries in the region must address governance challenges of generative and other types of AI.

Cyber incidents are also a political tool used to influence political outcomes and agendas. Worldwide, it is estimated that approximately 25% of national elections held in 2023 faced a cyber-attack. This implies the urgency to prioritize cybersecurity measures during times of high political activity. Moreover, research shows that when governments are weak and corruption is rampant, cybercriminals often operate with impunity, exploiting the lack of law enforcement. While most countries in LAC have

[42] Saavedra, 2023.
[43] Source: Kaspersky (2021) and https://www.bnamericas.com/en/news/industrial-system-cyberattacks-in-latam-running-at-more-than-one-an-hour.
[44] Source: https://www.csoonline.com/article/574875/latin-american-companies-governments-need-more-focus-on-cybersecurity.html.
[45] Kumar and Carley, 2016; Kshetri, 2010; Overvest and Straathof, 2015; Kigerl, 2012.

cybercrime legislations,[46] **the overwhelming focus on traditional crime has led to inadequate cybercrime enforcement**. This enforcement gap helps cybercrime to thrive.[47] This could be the case especially for the so called "tax heaven" countries in the region.[48] Additionally, as governments increasingly use surveillance technologies for diverse purposes,[49] it is important to maintain updated systems to avoid compromises to the governmental databases.[50]

Finally, the cybersecurity workforce gap[51] and skills gap can further exacerbate the cyber risk of countries. The cybersecurity skill shortage indicates that the critical IT positions for security are not filled, leading to insufficient preventive and defensive actions, thus increasing the cyber risk of victims. In LAC, the cybersecurity workforce gap remains but with a closing trend. Mainly, by 2023 the skills gap is estimated to be of around 348 thousand professionals, a figured that decreased by 32.5% between 2022 and 2023. The efforts to bridge the skills gap are mainly driven by the largest economies, Mexico and Brazil, that have closed the gap by 42.7% and 25.9% between 2022 and 2023, respectively.[52] However, at the same time, Brazil and Mexico are the countries with the most layoffs in cybersecurity, a phenomenon that could be reflecting the need to increase skilled cybersecurity workforce, and not just any technical level of cybersecurity labor supply.

4. Case studies

4.1 Brazil

Brazil stands out in the region as a focal point for cyberattacks, attributed to its significant digital economic growth. With internet penetration expected to rise from 81.8% in 2023 to 98% by 2029[53] and a high e-government development index placing it third in the region, Brazil's digital landscape is expanding rapidly. This growth, however, enlarges the available cyberattack surface, making the country increasingly susceptible to cyber incidents. Notably, Brazil was the target of 10.6% of global ransomware attacks in 2019 and ranked as the second most vulnerable country worldwide to cyber threats in the first half of 2023, only surpassed by the United States.[54]

The economic costs from cyber incidents in Brazil is substantial, with businesses incurring billions in losses each year. Direct costs, such as recovery and mitigation expenses, are compounded by

[46] 85% of the LAC countries have cybercrime legislation, 3% of them have draft legislation, and 12% of them are without legislation (UNCTAD, 2021).
[47] Kshetri, 2013.
[48] For instance, the GhostMarket Forum—an online marketplace for malware and illegal information—operated its financial transactions through a Costa Rican bank, exploiting the country's banking privacy (Malik, 2011; Kshetri, 2013)
[49] Source: https://www.americasquarterly.org/article/surveillance-technology-is-on-the-rise-in-latin-america/.
[50] For example, the 2022 data breach of Peru's National Directorate of Intelligence (DIGIMIN) by the Conti group reflected an arbitrary government surveillance. The hackers downloaded confidential documents, which can post risks to national security once being disclosed and found no data encryption in DIGIMIN's network. (Source: https://www.eff.org/deeplinks/2022/12/hacking-governments-and-government-hacking-latin-america-2022-year-review)
[51] It calculates the difference between the number of cybersecurity professionals that organizations require to properly secure themselves and the number of professionals available for hire (ISC2).
[52] ISC2, 2023.
[53] Statista, 2024.
[54] The risk is based on the number of risk events, malware detection, and malicious URL access detected via Trend Micro Attack Surface Risk Management system (Source: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/stepping-ahead-of-risk-trend-micro-2023-midyear-cybersecurity-threat-report).

indirect costs, including reputational damage and lost business opportunities. McAfee estimated the annual cost of cybercrime in Brazil to be at around USD 10 billion, or 0.5% of the Brazilian GDP in 2018,[55] while Symantec reported that cyberattacks affected approximately 62 million Brazilians with more than 30 hours recovery time, causing over USD 22 billion in losses.[56] By 2018, Brazil ranked second globally in terms of cyberattack-related economic losses, with the average annual cost from cyber incidents faced by a Brazilian company reaching over USD 7.24 million.[57]

This challenging situation occurs even though Brazil leads in cybersecurity measures with a score on cybersecurity commitments of 96.6 out of 100.[58] Mainly, the country has implemented significant strategies and frameworks to bolster its cybersecurity defense, including:

- A 2020 National Cybersecurity Strategy to guide its overarching cyber defense efforts.
- The establishment of specialized agencies such as the Cyber Defense Center and the Brazilian National Computer Emergency Response Team (CERT.br) to coordinate cybersecurity initiatives and respond to incidents.
- The creation of the Cyber Defense Command (CDCiber) within the army in 2012, a key component of Brazil's National Defense Strategy, with an investment of about USD 104 million,[59] focusing on cyber defense operations.[60]
- A defined critical infrastructures list covering 7 priority areas and 13 sectors.[61] In 2022, Brazil published the National Plan for the Safety of Critical Infrastructure (PLANSIC) to establish the collaborative mechanisms for efficient management across public and private sectors.
- Engagement in numerous bilateral and multilateral collaborations, involving partnerships with over 10 countries to enhance cybersecurity efforts.[62]

Despite the strengths in cybersecurity protection, Brazil still faces challenges in defending cyberspace including weak law enforcement and high-skilled cybersecurity workforce shortage. One significant institutional challenge is the country's law enforcement system, with insufficient resources allocated to cybercrime due to the overwhelming traditional crime, managing to solve only 5-8% of physical crimes.[63] This inefficiency results in limited attention to cybercrime, elevating the risk of cyberattacks. Additionally, Brazil faces a critical shortage of skilled cybersecurity professionals, a talent gap that further compromises its defensive capabilities against cyber incidents. It is reported that Brazil had a cybersecurity workforce shortfall of nearly 313 thousand individuals in 2022, underscoring the urgent need for skilled professionals to enhance Brazil's cyber defenses.[64]

---

[55] Machado, 2018.
[56] Symantec, 2018.
[57] Kshetri and DeFranco, 2020.
[58] Kshetri and DeFranco, 2020.
[59] This investment reflects 0.03% of Brazilian government spending in 2022. (Source: https://www.theglobaleconomy.com/Brazil/government_spending_dollars/.)
[60] Solar, 2023.
[61] The priority areas are waters, energy, transport, communications, finance, biosafety and bio-protection, and defense. The sectors include dams, urban water supply, electrical energy, peganbio, terrestrial, aerial, waterway, telecommunications, broadcasting, postal services, finance, biosafety and bio-protection, and defense. (Source: https://interlira-reports.com/featured/the-protection-of-critical-infrastructures-in-brazil/10/04/2023/.)
[62] Source: https://cyberpolicyportal.org/states/brazil.
[63] Kshetri and DeFranco, 2020, and https://www.huffpost.com/entry/brazil-most-violent-country-murders_n_3618704.
[64] ISC2, 2022.

4.2 Mexico

As the second largest economy in LAC, Mexico leads on e-commerce, with an e-commerce market value representing 1.8% of the country's GDP in 2022. Mexico has ranked in the top 5 countries with the biggest e-commerce growth worldwide from 2020 to 2023, with an expected increase of 26.8% in 2024.[65] However, Mexico also ranks as the second most attacked country in the region,[66] with 90% of the cyber fraud in the country being related to e-commerce.[67]

The growing digital economy not only exacerbates the threats but also results in substantial economic losses from cyber incidents. It has been reported that the cost of cybercrime and cyber fraud to the Mexican economy can be as high as USD 7.7 billion (0.6% of Mexican GDP in 2018) annually in 2018.[68] Moreover, the average financial loss for a Mexican victim due to a scam is estimated at around USD 262,[69] an amount equal to almost one month's salary at the minimum wage.[70] Besides the direct financial losses, the indirect costs from the aftermath defense such as the duration to deal with the consequences of cybercrime is non-trivial. In fact, on average, in Mexico it takes more than twice the amount of time (55 hours) to deal with the cybercrime aftermath than in the rest of the world.[71]

Mexico is the region's second-best country in terms of cybersecurity commitments, especially in capacity building and multilateral cooperation. However, in certain areas, Mexico presents relative weakness, such as in legal measures. For example, Mexico can improve legal measures by implementing substantive law on unauthorized online behaviors and online safety. Moreover, for a better capacity development, Mexico can develop and support more educational programs and academic curricula in cybersecurity. Amongst the commitments that Mexico has put in place to defend cyberspace are:

- Mexico's 2017 National Cybersecurity Strategy (NCS), aiming to identify and establish cybersecurity actions in social, economic, and political areas to safely use ICT for all organizations.
- CERT-MX to manage cyber incident response, maintain and monitor public internet networks.
- Legislations to protect personal data such as the Federal Law of the Protection of Personal Data Held by Private Parties 2010 and the General Law on the Protection of Personal Data in the Possession of Obliged Subjects 2017.
- Article 211 of the Penal Code that aims to deal with cybercrime but without a dedicated cybercrime law.[72]
- Sector-wise regulations in the finance and health sectors, but cybersecurity infrastructure and practice gaps necessary to secure the ICT sector.[73]

[65] ITA, 2023; ECDB, 2023.
[66] Source: https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment.
[67] CSIS, 2021.
[68] CSIS, 2021; Norton, 2018.
[69] Norton, 2023.
[70] The minimum wage of 2023 in Mexico is around USD 12.5 per day.
[71] Norton, 2018.
[72] OEA, 2020.
[73] CSIS, 2021.

5. The cybersecurity market in LAC

The cybersecurity market in LAC is boosting as digitization increases. Mainly, the region's cybersecurity market measured in total sales of digital security products is projected at USD 8.92 billion in 2024 (4.9% of the global market), with a CAGR of 6.95% from 2024 to 2029, reaching USD 12.48 billion by 2029.[74] Key suppliers with some of the largest market shares in the region include AVG Technologies, Check Point Software Technologies Ltd, Cisco Systems Inc, Cyber Ark Software Ltd, and Dell Technologies Inc.[75] On the other hand, the cybersecurity demand in the region mainly consists of 1) business needs for information security monitoring, and 2) the increasing individual needs for application security using mobile payments.

In LAC and worldwide, the cybersecurity market is filled with sources of market failures. In cyberspace, overall security depends on the most vulnerable components due to the interdependency of resilience of digital assets. Thus, the most efficient allocation can be achieved only when no alternative allocations can improve resilience without making anyone worse off.[76] Mainly, in cybersecurity there are four types of market failures leading to inefficient allocation: failure to internalize systematic risk, underinvestment in Research and Development, asymmetric information, and vendor risk exposure and misaligned incentives to produce digital products.

Cyber incidents can have contagion effects, leading to the amplification of losses. Such as phenomenon is referred to as the systemic risk. Failure to internalize systemic risk by the market players results in underinvestment in cybersecurity. Although the region has yet to observe major cases of systemic disruptions, such as a cyber run, stakeholders must assess and plan for the possibility of such cases, especially in highly interconnected sectors. For example, in the U.S., a possible case of cyber-run was successfully prevented thanks to proactive financial and cybersecurity measures taken by the second-round affected banks and the central regulator.

Market players often don't see immediate benefits from investing in cybersecurity, leaving systems exposed to more advanced and sophisticated cyber-attacks. LAC has the lowest GCI pillar score in terms of R&D programs, reflecting a potential to enhance capacity development. Mainly, within the region, only 6 out of 33 countries have established R&D programs[77] at the national level across both public and private sectors. This situation is further exacerbated by the centralization of cybersecurity research in HICs, especially, in the U.S., which compromises informed policymaking decisions.

Market players' reticence of information leads to information asymmetries, affecting efficiency in cybersecurity investments. It is well-known that the potential damages to the victim's reputation and customer relationships heightens reticence in information sharing.[78] This results in unreliable information about the cybersecurity landscape within a sector and a country. Furthermore, this could lead to inefficient investment levels as market participants cannot assess the threats and manage cyber risk

[74] Source: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market and https://www.mordorintelligence.com/industry-reports/cyber-security-market.
[75] Source: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market.
[76] Vergara Cobos, forthcoming
[77] The results come from GCI2020 pillar scores for research and development programs under capacity development group. The 6 countries ranked by their scores are: Brazil, Uruguay, Mexico, Cuba, Colombia and Paraguay.
[78] Moore, 2010; Kopp et al., 2017.

effectively. In the region, only about 60% of countries have an operational CSIRT unit,[79] a component considered as a good practice for information sharing. Moreover, worldwide, cybersecurity is considered a credence-good market, or one in which the seller has more information than the buyer, which without efficient liability or labelling measures, could further complicate the cyber risk of users relying on third-party products.

Increasing cybersecurity awareness can alleviate the degree of information asymmetry, however, for both businesses and individuals in LAC, awareness remains to be improved. For example, only 37% of LAC companies cited increased security concerns as a driving factor for higher IT budgets in 2022,[80] while in 2021 about 56% of LAC internet users claimed to be "very worried" about online identity theft.[81]

Moreover, vendors often face a tradeoff between cybersecurity robustness and profits. Such a tradeoff represents a misaligned incentive, exacerbated by 1) the unclear returns on investments in increasing the robustness of digital products; 2) the stochastic nature in the frequency and costs of cyber incidents; and 3) producers' preferences over proprietary and less transparent production processes to lock consumers, rather than complying with valid standard processes.[82]

6. Conclusions and policy recommendations

The accelerated proliferation of disclosed cyber incidents in the region, and the devastating consequences of some of the main incidents in the last years, show that LAC is unprepared to respond to the increasing cybersecurity challenges of the digital era. Facing the world's highest growth rate of disclosed cyber incidents, second to last ranking in terms of cybersecurity commitments, and a highly accelerated digitization process, LAC is vulnerable to financial and political cyber incidents, especially across the public administration, and the financial and information and communications technologies. Moreover, as digitization in other sectors increases, the region could also face cyber incidents compromising critical services such as those provided by the healthcare sector and critical infrastructures. This note proves that there are various reasons leading to the challenging cybersecurity situation seen in LAC, including the socio-economic, political, technical, and digital landscapes, such as unemployment, political instability, legislative gaps, enforcement gaps, inefficient cybersecurity markets, corruption, amongst others.

Cybersecurity is a shared responsibility; thus, governments and other stakeholders must aim to understand the cybersecurity threats and market failures in the region to help provide a safe cyberspace. Particularly, and according to the analysis presented in this paper, stakeholders could aim to:

1. Prioritize cybersecurity measures in public administration, finance, and information and communications.
2. Operationalize data protection regulations, and other cybersecurity legislations, to secure the fast-evolving digital environment, especially in the realm of e-commerce.

[79] UNECLAC (2021).
[80] SWZD, 2022.
[81] The 2021 World Risk poll.
[82] Vergara Cobos, forthcoming.

3. Place preventive cybersecurity measures in electoral institutions and during times of high political activity.
4. Foster the development of a regional cybersecurity industry, tailored to the threat landscape of the region.
5. Foster the demand for cybersecurity through awareness and education programs, especially across SMEs.
6. Invest in R&D programs to keep pace with the rapid adoption of advanced technologies like cloud computing and AI.
7. Promote and invest in data collection efforts that could help assess the threat landscape across countries in the region and be used as tools for informed policymaking decisions.
8. Enhanced regional and international cooperation through, for example, the collaboration across CERTs.

Considering the scarcity of empirical data in cybersecurity, this paper offers an extensive descriptive examination of the cyber threat environment in LAC, establishing a basis for future research that could guide effective and customized cybersecurity strategies for the region. Safeguarding against cyber threats in LAC is crucial not only for preserving economic prosperity but also for upholding civil liberties, ensuring access to vital services, and safeguarding democratic processes. The escalating trajectory of cybersecurity issues in the region is projected to persist, underscoring the urgent need for stakeholders to redouble their endeavors in fortifying cyberspace and mitigating the setbacks associated with digital advancement.

Reference

Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. (2021) 'Hacking corporate reputations', Rotman School of Management Working Paper, (3143740).

Americas Market Intelligence (2022). 6 TRENDS IN THE USE OF TECHNOLOGIES AT INNOVATIVE COMPANIES IN LATIN AMERICA. Available at: https://americasmi.com/insights/trends-use-of-technologies-innovative-companies-latin-america-innovation/.

Americas Quarterly (2023). Surveillance Technology Is on the Rise in Latin America. Available at: https://www.americasquarterly.org/article/surveillance-technology-is-on-the-rise-in-latin-america/.

Amir, E., Levi, S., & Livne, T. (2018) 'Do firms underreport information on cyber-attacks? Evidence from capital markets', Review of Accounting Studies, 23, pp. 1177-1206.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J., Levi, M., Moore, T. and Savage, S., 2013. Measuring the cost of cybercrime. The economics of information security and privacy, pp.265-300. Springer.

Apau, R. and Koranteng, F.N., 2019. Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. International Journal of Cyber Criminology, 13(2).

Argüelles Arellano, M.D.C. (2016) 'Challenges of cyber law in Mexico', Computación y Sistemas, 20(4), pp. 827-831.

Austin, G. and Withers, G., 2020. Creating social cyber value as the broader goal. In Cyber Security Education (pp. 99-118). Routledge.

Azzolini, C.M. (2017) 'Ciberseguridad en la República Argentina y su perspectiva futura' [Trabajo Final Integrador]. Instituto de Inteligencia de las Fuerzas Armadas.

Bnamericas (2021). Industrial system cyberattacks in LatAm running at more than one an hour. Available at: https://www.bnamericas.com/en/news/industrial-system-cyberattacks-in-latam-running-at-more-than-one-an-hour.

Bolgov, R., 2020, April. The UN and cybersecurity policy of Latin American countries. In 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 259-263). IEEE.

Buzzio-Garcia, J., Salazar-Vilchez, V., Moreno-Torres, J. and Leon-Estofanero, O., 2021, October. Review of Cybersecurity in LatinAmerica during the Covid-19 Pandemic. A brief Overview. In 2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM) (pp. 1-5). IEEE.

Carapeto, R. and Calil, A.L., 2022. Cybersecurity regulation in Brazil and Latin America: an overview. International Cybersecurity Law Review, 3(2), pp.385-410.

Catota, F.E., Morgan, M.G. and Sicker, D.C., 2018. Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4(1), p.tyy002.

Catota, F.E., Morgan, M.G. and Sicker, D.C., 2019. Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), p.tyz001.

Corbet, S. and Gurdgiev, C., 2019. What the hack: Systematic risk contagion from cyber events. International Review of Financial Analysis, 65, p.101386.

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023) 'Pirates without borders: The propagation of cyberattacks through firms' supply chains', Journal of Financial Economics, 147(2), pp. 432-448.

CSIS (2021). The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment. Available at: https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment.

CSO (2023). Latin American companies, governments need more focus on cybersecurity. Available at: https://www.csoonline.com/article/574875/latin-american-companies-governments-need-more-focus-on-cybersecurity.html.

Cyber Policy Portal (2023). Brazil.

Datareportal (2023). Digital 2023: Argentina. Available at: https://datareportal.com/reports/digital-2023-argentina#:~:text=Argentina's%20internet%20penetration%20rate%20stood,at%20the%20start%20of%202023.

Datta, P.M. and Acton, T., 2022. Ransomware and Costa Rica's national emergency: A defense framework and teaching case. Journal of Information Technology Teaching Cases, p.20438869221149042.

Electronic Frontier Foundation (2022). Hacking Governments and Government Hacking in Latin America: 2022 in Review. Available at: https://www.eff.org/deeplinks/2022/12/hacking-governments-and-government-hacking-latin-america-2022-year-review.

Exploding Topics (2024). Number of IoT Devices (2024). Available at: https://explodingtopics.com/blog/number-of-iot-devices.

Flor, O., 2023. A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America.

Földvári, A., Biczók, G., Kocsis, I., Gönczy, L., & Pataricza, A., 2021. Impact Assessment of IT Security Breaches in Cyber-Physical Systems: Short paper. 2021 Latin American Dependable Computing Conference (LADC), pp.1-4.

Fortinet (2023). Fortinet reports that Latin America was the target of more than 360 billion cyberattack attempts in 2022. Available at: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent.

Gallup (2021). World Risk Poll 2021: A Changed World?

Harry, C., & Gallagher, N. (2018). Classifying Cyber Events. Journal of Information Warfare, 17(3), 17-31.

Hurel, L., 2024. Mapping Cyber Policy in Latin America: The Brazilian Case.

IARI (2023). CURRENT PANORAMA OF CYBER SECURITY IN LATIN AMERICA: THREATS AND POSSIBILITIES. Available at: https://iari.site/2023/10/05/current-panorama-of-cyber-security-in-latin-america-threats-and-possibilities/#google_vignette.

ISC2 (2022). Cybersecurity Workforce Study.

ITA (2023). Panama Country Commercial Guide --- Cybersecurity. Available at: https://www.trade.gov/country-commercial-guides/panama-cybersecurity.

ITU (2021). World Telecommunication/ICT Indicators Database: Individuals using the Internet (% of population) – Latin America & Caribbean.

Izycki, E. (2018) 'National cyber security strategies in Latin America: Opportunities for convergence of interests and consensus building', RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 15(1), pp. 39-52.

Jamilov, R., Rey, H. and Tahoun, A., 2021. The anatomy of cyber risk (No. w28906). National Bureau of Economic Research.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021) 'Risk management, firm reputation, and the impact of successful cyberattacks on target firms', Journal of Financial Economics, 139(3), pp. 719-749.

Kennedys (2023). Identifiable trends in LAC data protection legislation. Available at: https://kennedyslaw.com/en/thought-leadership/article/2023/identifiable-trends-in-lac-data-protection-legislation/.

Kobek, L.P. (2017) 'The State of Cybersecurity in Mexico: An Overview', Wilson Center Mexico Institute.

Kobek, L.P. (2018) 'Quo vadis? Mexico's National Cybersecurity Strategy', Wilson Center Mexico Institute.

Kobek, L.P., 2017. The state of cybersecurity in Mexico: An overview. Wilson Centre’s Mex. Institute, Jan.

Kosevich, E., 2024. Cybersecurity, cyberspace and cyberthreats at the beginning of the 21st century: a Latin America typology and review. Area Development and Policy, 9(1), pp.86-107.

Kshetri, N. (2013) 'Cybercrime and Cybersecurity in Latin American and Caribbean Economies', in Cybercrime and Cybersecurity in the Global South. London: Palgrave Macmillan, pp. 135-151.

Kshetri, N. and DeFranco, J.F., 2020. The economics of cyberattacks on brazil. Computer, 53(9), pp.85-90.

Kshetri, N., 2013. Cybercrime and cybersecurity in the global south. Springer.

Lending, C., Minnick, K., & Schorno, P. J. (2018) 'Corporate governance, social responsibility, and data breaches', Financial Review, 53(2), pp. 413-455.

Lin, Z., Sapp, T. R., Ulmer, J. R., & Parsa, R. (2020). Insider trading ahead of cyber breach announcements. Journal of Financial Markets, 50, 100527.

Martinez, F.R.C., Candelaria, A.D.H., Lozano, M.A.R., Zuñiga, A.R.R., Pelaez, R.M. and Michel, J.R.P. (2017) 'After click the submit button control over personal information and privacy is lost: A case study in Mexico', RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 21(1), pp. 115-128.

Mexico Business News (2024). Battling Cyber Threats in Latin America's Payment Landscape. Available at: https://mexicobusiness.news/entrepreneurs/news/battling-cyber-threats-latin-americas-payment-landscape.

Mordor Intelligence (2024). Latin America Cyber Security Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029) Available at: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market.

OneTrust DataGuidance (2023). Argentina: Cybersecurity incidents landscape. Available at: https://www.dataguidance.com/opinion/argentina-cybersecurity-incidents-landscape.

Parraguez Kobek, L. and Caldera, E., 2016. Cyber Security and Habeas Data: The Latin American response to information security and data protection.

Piccotti, L. R., & Wang, H. (2022) 'Informed trading in the options market surrounding data breaches', Global Finance Journal, 100774.

Saavedra, B. 2023. Cybersecurity in Latin America: Challenges, Concerns and Opportunities.

Setiawan, N., Tarigan, V.E., Sari, P.B., Rossanty, Y., Nasution, M.D.T.P. and Siregar, I., 2018. Impact of cybercrime in e-business and trust. Int. J. Civ. Eng. Technol, 9(7), pp.652-656.

SWZD (2022). The 2022 State of IT in Latin America. Available at: https://swzd.com/blogs/the-2022-state-of-it-in-latin-america/#:~:text=Key%20findings%20from%20the%202022%20State%20of%20IT%20in%20LATAM&text=The%20average%20YoY%20budget%20increase,NA%2C%20Europe%2C%20and%20APAC..

The Guardian (2016). What are the Panama Papers? A guide to history's biggest data leak. Available at: https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers.

Toapanta, S.M.T., Jaramillo, J.M.E. and Gallegos, L.E.M., 2019, December. Cybersecurity analysis to determine the impact on the social area in Latin America and the caribbean. In Proceedings of the 2019 2nd International Conference on Education Technology Management (pp. 73-78).

Toapanta, S.M.T., Peñafiel, L.B. and Gallegos, L.E.M., 2019, December. Prototype to mitigate the risks of the integrity of cyberattack information in electoral processes in Latin America. In Proceedings of the 2019 2nd International Conference on Education Technology Management (pp. 111-118).

Toapanta, S.M.T., Pesantes, R.P.R. and Gallegos, L.E.M., 2020, July. Impact of cybersecurity applied to IoT in public organizations in Latin America. In 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4) (pp. 154-161). IEEE.

Torres, D. (2018) 'Cyber security and cyber defense for Venezuela: an approach from the Soft Systems Methodology', Complex Intelligent Systems, 4, pp. 213-226.

Tosun, O. K. (2021) 'Cyber-attacks and stock market activity', International Review of Financial Analysis, 76, 101795.

Trend Micro (2023). Midyear Cybersecurity Threat Report. Available at: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/stepping-ahead-of-risk-trend-micro-2023-midyear-cybersecurity-threat-report.

UMD Center for Governance of Technology and Systems (2024). Cyber Events Database. Available at: https://gotech.umd.edu/cyber-events-database.

UNECLAC (2021). State of Cybersecurity in Logistics in Latin America and the Caribbean.

UNCTAD (2021). Cybercrime Legislation Worldwide.

Vantiva (2024). Digital Transformation in Latin America: 5 trends to know.

Vergara Cobos (forthcoming). Cybersecurity Economics for Emerging Economies.

Vergara, Cakir, and Barakcin. The role of cybersecurity in economic performance. World Bank Working Paper. Forthcoming.

Weikert Bicalho, F., 2020. The resilience of infrastructure services in Latin America and the Caribbean: a first approach.