SPC2: Special Conference on Labor in the 21st Century

Student Officer: Mehmet Alp Ünal

Issue: Combatting cybersecurity threats in the workplace

TIMUN '24

Turkish International Model United Nations

THIMUN Affiliated Conference

Committee:	Special Conference on Labor in the 21st Century (SPC2)
Issue:	Combatting cybersecurity threats in the workplace
Student Officer:	Mehmet Alp Ünal - Vice President

I. Introduction

Cybersecurity is the general term that is used for the digital platforms being secure such as computers and phones and the actions that are taken in order to maintain the security in these digital platforms. In the modern world, thanks to the digitalization and technology age, people are able to perform many activities with ease. However, as there are people with evil intentions in real life, there are also these kinds of people in cyberspace. These people are the ones who cause cybersecurity threats. There are so many ways of cybersecurity threats and these threats are present in multiple areas. For example areas like military, infrastructure, workplace, diplomacy, trade, etc. The one common thing of the areas is that regardless of the area, similar risks are present and almost the same types of threats are present in all of the aforementioned areas. The threats can be listed as but not limited to: Cyber blackmailing, Ransomwares, Computer viruses, Malwares, Phishing attacks, Trojan viruses, etc. Throughout the report the detailed approach to the areas that these malicious software are seen and how to be prepared for them is discussed.

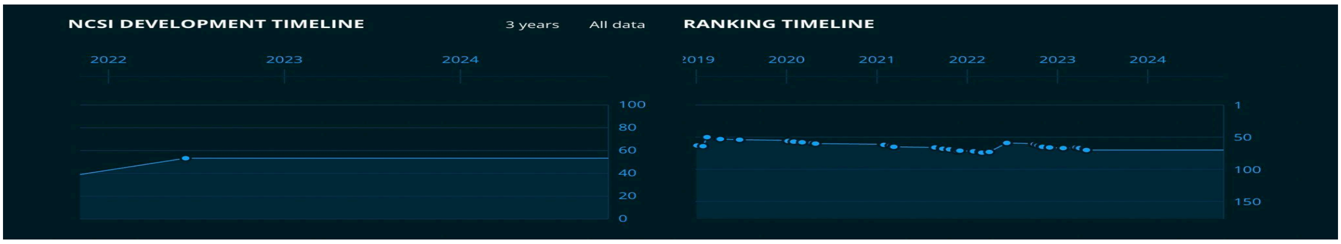
II. Involved Countries and Organizations

Panama

Panama is a country located in the Latin American region, along with many other nations discussed in this section. While Panama has established a framework for the "development of a digital government," its cyber systems are still in the early stages of development. Despite this, Panama is committed to advancing efforts to prevent cyberattacks. In 2019, Panama passed Law No. 81 of 2019 on Personal Data Protection, which regulates the collection, storage, and use of personal data which has a goal to enhance the protection of individuals' personal information, particularly in the context of digital activities, marking a significant step toward addressing cybersecurity challenges and safeguarding data privacy.

Colombia

According to the data provided by the National Cyber Security Index, Colombia is the 69th country among 96 countries receiving a score of 53.25 out of 100. As can be seen below, their cybersecurity level is constant without necessary changes throughout the years there are no improvements or losses. In 2023, Colombia faced a huge cyberattack in which their government web was targeted. One of the major communication centers named "IFX network" was targeted. It was stated that the type of the attack was ransomware. After the attack, the government of Colombia immediately tried to take countermeasures and did the aftermath by "a command post-PMU Ciber". Colombia tried to take action after the attack but this huge-sized attack shows that they are not ready for a possible cyber attack. However, by the command post they have posted, they want a solution to the issue to no longer be affected by the cyber threats.



(NCSI Development Timeline)

Costa Rica

Costa Rica is a highly committed country that is aware of the vitality of the topic. Nearly half of their exports are related to digitalization. Costa Rica also took part in one of the resolutions to solve the issue in III. section of this report. Costa Rica works in a way that is in favor of the OAS Cyber Security Program. In 2022, Costa Rica faced a severe cyber attack and after that incident, the government set up cybersecurity as a must. This cyber attack is the Conti attack and as it is stated its type is ransomware. Costa Rica is a signatory of the Budapest Convention and their frameworks regarding cyber threats are well prepared.

Chile

As a country that implemented a cybersecurity policy statement in 2017, Chile has efforts for this issue. "The policy is also aiming at reducing the risks associated with cyberspace and at improving areas like awareness, training, and a culture of cybersecurity among the citizens. (European Council)" Chile has a separate constitution named the "Supreme Decree No. 1299 Programme" to deal with Information and Communication Technology (ICT) systems. Another constitutional law that Chile has is Law number 21.459/2022 which is about cybersecurity crimes.

Dominican Republic

The Dominican Republic is in the 21st place in the National Cybersecurity Index out of 96 countries and it has a score of 71.67 out of 100. The government has "adopted in 2018 a National Cybersecurity strategy 2018-2021. (Council of Europe)". The strategy consists of 4 main areas which are: infrastructure-related protection nationally, that aims to prevent any detrimental effects on the information technology systems that are caused by cyber-attacks. The second plan is to fully secure educational sites and areas for cyber threats. Additionally, the strategy targets secure "international alliances". In order to maintain the strategy that is adopted two organizations are produced: "The National Centre of Cybersecurity, a Cybersecurity Strategies Coordination Team (ECEC), and a Computer Security Incident Response Team (CSIRT-RD)(Council of Europe)." The Dominican Republic can be shown as a committed country that tries to prevent the issue and it can be seen that it has done coordination with the Council of Europe for this specific case.

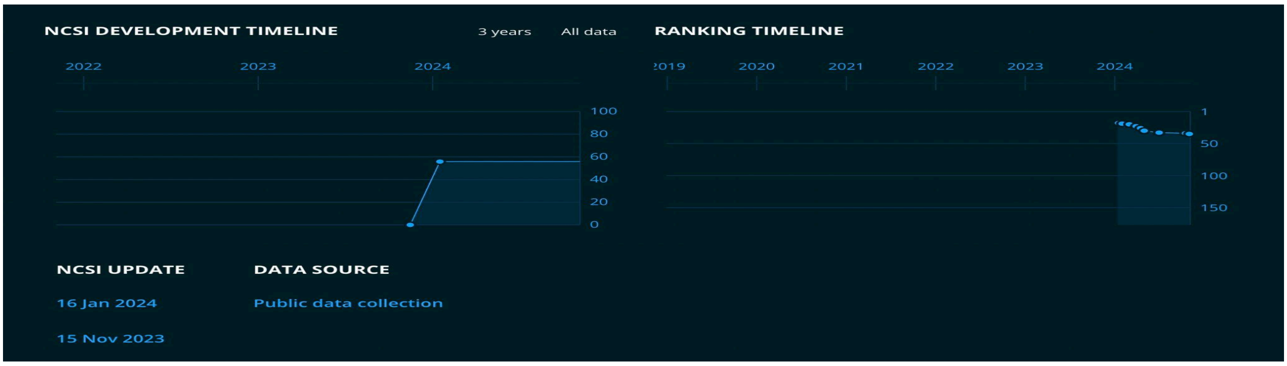
Peru

Peru is remarkable in the case of its internet penetration rate, which is a rate that if it is high the internet is not so secure. The data collected from ITU (International Telecommunication Union) suggests that the mentioned rate is %71.1. Another point where Peru is weak is the internet network coverage. The country does not have full access to the internet. The coverage is near to non-existent in the rural side of the city. Even though Peru does not have sufficient requirements in the case of a network, they are working on a solution to this issue. The laws they regulate about the topic of cyberspace are an example. "Cyber Defense Act" is another vital point for Peru.

This act establishes a legal framework for coordinating government, military, and private sectors to prevent and respond to cyberattacks. The law reflects Peru's commitment to enhancing national security and resilience in the digital space.

III. Focused Overview of the Issue

When the Latin America region searched for cybersecurity in the region it is possible to say that generally, there is not a solid prevention system that protects the continent in a robust way. For example, the Conti ransomware attack, in which the target country was Costa Rica, had effects on neighboring countries. Similarly, the attack that is explained in the aforementioned section is another example of this situation. As the Interactive Financial Exchange (IFX) network of Columbia was damaged through a similar ransomware attack, due to the fact that the network was infected, 17 countries were also affected in the region. An additional point is to keep in mind that networks and network security concepts have a huge vitality and can be considered as the backbone of the issue. As explained in the keywords section, when a network is affected and if this network is a huge IFX network as in this example. Hackers can use the infected network to filtrate into other computers and even to other countries that communicate through the same network.



NCSI UPDATE

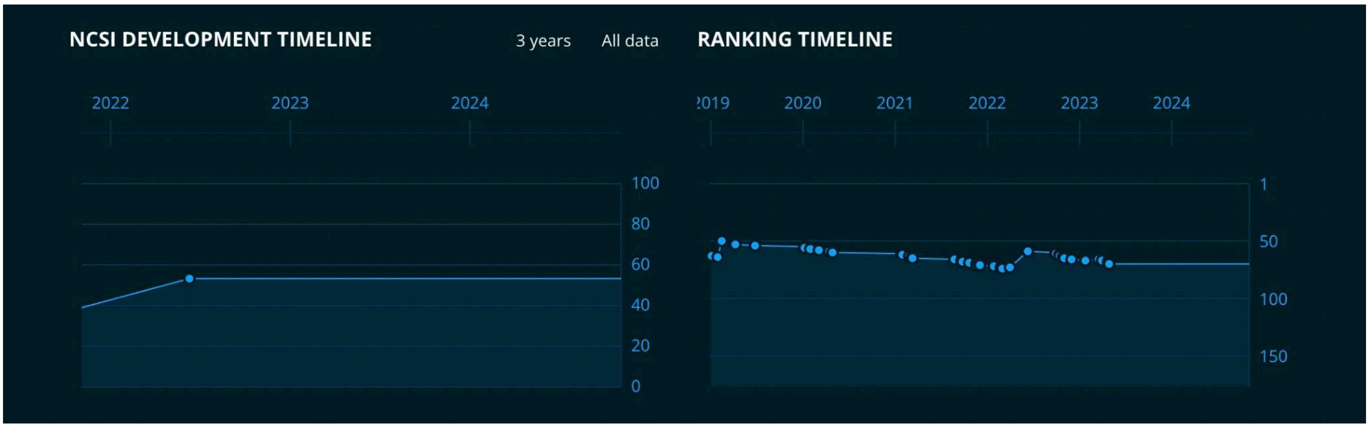
16 Jan 2024

15 Nov 2023

DATA SOURCE

Public data collection

NCSI (Data for Panama)



(NCSI Data for Colombia)

When the data for Colombia is observed it is more possible to say that in the case of the cybersecurity index, there is little to no development and this can be understood by looking at the first graph's 2022-2024 interval. Similarly, Colombia's ranking is constant on average with some shifts over time. These are the two specific examples from the countries in the region and these development graphs show that the region countries are not ready for a cyber threat even though they are committed to development and improvement. The inference that can be made is that the reason why the region is overwhelmed by a ransomware attack is because of the lack of development and modernization. These features are also important for any future malware that the countries might encounter.

In the paragraphs above more of the regional and international approach is taken. However, for the workplaces, both a national measure for the countries and company-wise precautions can be helpful. IFX networks and other open networks are a huge risk for these kinds of cyber attacks. In a workplace, the risks are nearly the same and similarly, the things that are explained and the governments face in the issue can apply to the workplaces. When the Latin American region is considered as a macrostructure in these kinds of cybersecurity threats, the workplaces and other organs of the Latin American countries are micro organs that are bound to the mentioned macro organs. It is vital for the region to work collaboratively and in diplomatic behavior. Because a possible cyber threat in the region might affect the surrounding countries as seen in the Ransomware attack that happened to Colombia.

Internet penetration is another concerning topic. In countries such as Peru, the high penetration rate is concerning because of the fact that the internet is not controlled in a meticulous way and leaks or other data breaches are easier. These rates should be lowered in urgent behavior for the sake of stability in the region regarding the cybersecurity and cyberspace-related prosperity.

To sum up, it is essential to work collaboratively in the region to overcome cyber threats. The networks play a crucial role and the security of the networks should be maintained. It is seen that the only threat is not the hackers but also some intelligence agencies of other governments as seen in the timeline section. Governments should be aware of these threats and take precautions in order to avoid problems regarding the issue.

IV. Key Vocabulary

Cybersecurity: Cybersecurity is the general term that is used for the digital platforms being secure such as computers and phones and the actions that are taken in order to maintain the security in these digital platforms.

Malware: A detrimental software or a program that is used by hackers or other vicious people that disrupts how the system works. Malware can also be used for hijacking information.

Ransomwares: Ransomware is a type of malware. The purpose of the person who uses ransomware is to block the connection to a site or program temporarily so that the hacked party will pay an amount of money to use the system again. If the money is not paid the program can be permanently blocked.

Computer Viruses: There can be various types of viruses that are programmed for different purposes but basically, they are malware that aims to infect the computer and make the files and the system useless.

Phishing: Phishing or “fishing” attacks are the general name that is given for the links, emails, and other things that trick the person to which the message is sent, and when they click the message a program is activated which is for data stealing.

Trojan: A type of malware that shows itself as an application or an innocent program and when installed infects the computer. It gets its name from the “Trojan War” and refers to the “Trojan horse”.

Computer Network: A computer network can be defined as a group of different computers in the same network. Even though these computers are different, they are registered to the same system, which is essential because if one of these systems is hacked the hacker can filter to the network and infect the whole computer network.

Cyber Blackmail: Similar to regular blackmail, the aim is to threaten people to get what is wanted. However these actions take place in cyberspace and the cyber threat is done through digital media organs or similar platforms.

Cyberspace: The general network between all of the computers regardless of the place where the computers are located. Furthermore, it is regarded as an existing location.

V. Important Events & Chronology

Date (Day/Month/Year)	Event
The early 1970s	The first computer virus “The Creeper” was seen in the United States military computer database. This virus has affected other computers on the network and displayed the message: “I’M THE CREEPER: CATCH ME IF YOU CAN.”
1971	Around the year 1971, the idea of antivirus came to people’s minds and the first antivirus idea “Reaper” was programmed. Reaper is another computer virus that has the goal to eliminate “The Creeper” virus in case it is detected in the system.
1976-2006	A former worker in the Boeing aviation firm was detected leaking information from the company to China in return for payment. This situation was considered a vital insider attack at that time and after the person named Greg Chung was detected he was sentenced to prison.
June 2013	A former CIA personnel named Edward Snowden did one of the most vital leaks of the time. He has leaked confidential CIA documents and caused turmoil in the trust of US citizens in their government.
2013-2014	Hackers got information from the users of the internet browser, Yahoo. Their personal information was gathered and when Yahoo noticed this, it was a year later.
September 2023	A huge ransomware attack took place in the Latin American Region, this huge ransomware attack affected 17 countries and caused a huge amount of damage to the IFX networks.

	The details about this attack are also explained in the Involved Countries section under Colombia.
May 2024	Chinese hackers tried to infiltrate the work device of one of Canada's parliament members. According to the source, this attack by the hacker was fortunately not successful.

VI. Past Resolutions and Treaties

- Security Council, 79th year: 9662nd meeting, Thursday, 20 June 2024, New York

- OEA/Ser.L/X.2.17 http://scm.oas.org
- CICTE/RES. 1/17 http://scm.oas.org
- Convention 108 (https://www.coe.int/en/web/data-protection/convention108-and-protocol)
- Budapest Convention, ETS No. 185 (https://www.coe.int/en/web/cybercrime/the-budapest-convention)
- CAMP (a cybersecurity alliance: https://www.cybersec-alliance.org/camp/about.do)

VII. Failed Solution Attempts

Governments are mostly trying to resolve the issue through the resolutions that are mentioned in the previous section. Also, conferences like the Budapest Convention and other actions regarding the issue are tried. There are no explicit failures due to the fact that cybersecurity is a cumulative concept where as long as the system is stronger there can be a stronger malware. In cyberspace, there are no such things as 0 risk. The risk can be minimized however it can not be eliminated in a total way. However, the reason that can be shown for the failed solution attempts can be the countries' weak frameworks and regulations about the topic itself. For example, some of the governments that are listed in the related parties section, do not have any improvements in their cyber systems with a lack of action plans in case a cyber attack occurs. Additionally, for a failed solution attempt the near-today data breaches can be given as an example. Even though the mentioned data breaches were present in different companies, the idea of having a data breach shows that all of the well-known companies are not fully immune to a cyberattack. Between the years 2013 and 2014 a data breach to the web browser Yahoo occurred. Afterward, the breach in 2015 to the US OPM organization occurred. Another attack took place in 2017 when NotPetya faced ransomware violence which affected the microsoft systems. The consistent attacks that were successful by the hackers on the different companies and networks can be concluded that the precautions the companies took were not efficient which makes it a failed solution attempt. A global solution for the issue might be regional frameworks and regulations as it is stated in numerous parts throughout the report.

VIII. Possible Solutions

Especially in the region of Latin America, it can be seen that the malware type Ransomwares are a huge threat to people and the workplaces in which people work. In order to avoid the threats that Ransomwares causes, leaving a budget for cybersecurity and malware prevention in the region is essential. Another point is that when the region is beholden in general it can be seen that most of the regions' governments do not have a meticulous regulation or a policy and they are not ready for a possible cyber danger. A regulation or a policy statement can be stated or determined in order to decide the action plan that will be taken when malwares are active (a). Additionally, one solution to avoid cyber threats in the workplace can be implemented via raising awareness in the workplace. For example, the employees should be aware of the fact that in case their computer is hacked or attacked, by using the modem network other users can also be affected. It is important to make them knowledgeable about spam mail links, phishing attacks, and other cyber threats that they may face and can affect the other members of the workplace. VPNs and other Antivirus programs are other steps that can be taken to combat viruses and malwares. Even though experienced hackers and strong malwares can bypass these programs, it is a step that complicates the job of the attacker and can be seen as a way to combat cyber threats. Also think if the system is attacked and the data are lost or ransomware has infected the computer, in this case, it is essential to pre-back up the data in secondary disks that are stored in a separate system from the modem network and the computer. In this way even if the data are stolen, the data will not be lost and the malware will not reach it because of its separate network feature. These are some of the features that can solve the issue and by doing these the detrimental effects of cyber attacks can be minimized.

IX. Useful Links

https://www.cyberdb.co/cybersecurity-games-for-students/

https://www.youtube.com/watch?v=A4hHWDcPHqE(?)

https://www.cisa.gov/topics/cyber-threats-and-advisories

https://www.cybersec-alliance.org/camp/about.do

https://ncsi.ega.ee/

X. Works Cited

Buckbee, Michael. “8 Events That Changed Cybersecurity Forever.” *Varonis*, Varonis, 7 July 2023, www.varonis.com/blog/events-that-changed-cybersecurity.

“Building a Skilled Cyber Security Workforce in Latin America.” *OECD*, 22 Sept. 2023, www.oecd.org/en/publications/building-a-skilled-cyber-security-workforce-in-latin-america_9400ab5c-en.html.

“Chile - Octopus Cybercrime Community - .” *Octopus Cybercrime Community (Council of Europe)*, 7 Oct. 2023, www.coe.int/en/web/octopus/-/chile.

“Colombia.” *NCSI*, ncsi.ega.ee/country/co_2022/. Accessed Nov. 2024.

“Convention on Cybercrime (ETS No. 185).” *European Parliament*, www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf. Accessed Nov. 2024.

“Costa Rica :: Eu Cyber Direct.” *EU Cyber Direct*, eucyberdirect.eu/atlas/country/costa-rica. Accessed Nov. 2024.

CSIS, csis-website-prod.s3.amazonaws.com/s3fs-public/2024-10/241007_Significant_Cyber_Events.pdf?VersionId=qn46PstY2SYKbsaXoE5F572aXHzv2E8r. Accessed Nov. 2024.

Cybersecurity Incident & Vulnerability Response Playbooks, www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf. Accessed Nov. 2024.

“Dominican Republic.” *NCSI*, ncsi.ega.ee/country/do/. Accessed Nov. 2024.

Dragilev, Dmitry. “Council Post: How Your Employees Can Prevent and Detect Cybersecurity Threats.” *Forbes*, Forbes Magazine, 12 Aug. 2024, www.forbes.com/councils/forbestechcouncil/2022/01/06/how-your-employees-can-prevent-and-detect-cybersecurity-threats/.

Google Search, Google, www.google.com/search?q=Combatting%2Bcybersecurity%2Bthreats%2Bin%2Bthe%2Bworkplace%2Bdone%2Bevents%2Btimeline&oq=Combatting%2Bcybersecurity%2Bthreats%2Bin%2Bthe%2Bworkplace%2Bdone%2Bevents%2Btimeline&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDkzMDhqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8. Accessed Nov. 2024.

Google Search, Google, www.google.com/search?q=Combatting%2Bcybersecurity%2Bthreats%2Bin%2Bthe%2Bworkplace%2Bdone%2Bevents%2Btimeline&oq=Combatting%2Bcybersecurity%2Bthreats%2Bin%2Bthe%2Bworkplace%2Bdone%2Bevents%2Btimeline&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDkzMDhqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8. Accessed Nov. 2024.

Greenwald, Glenn, et al. “Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations.” *The Guardian*, Guardian News and Media, 11 June 2013, www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

“Guides: International and Foreign Cyberspace Law Research Guide: Treaties & International Agreements.” *Treaties & International Agreements - International and Foreign Cyberspace Law Research Guide - Guides at Georgetown Law Library*, Georgetown Library, guides.ll.georgetown.edu/cyberspace/cyber-crime-treaties. Accessed Nov. 2024.

“History of Antivirus.” *Antivirussupport.Ca*, 12 July 2023, antivirussupport.ca/history-of-antivirus/#page-content.

“Know the Types of Cyber Threats.” *Mass.Gov*, www.mass.gov/info-details/know-the-types-of-cyber-threats. Accessed Nov. 2024.

“Measures Taken Following the Unprecedented Cyber-Attack on the ICC.” *International Criminal Court*, www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc. Accessed Nov. 2024.

Muncaster, Phil. “2022 Özeti: Yılın En Büyük 10 Siber Saldırısı.” *ESET*, 27 Dec. 2022, www.eset.com/tr/blog/2022-ozeti-yilin-en-buyuk-10-siber-saldirisi/.

“New Report Highlights Need for Investment to Reduce Systemic Risks of Ransomware in Latin America.” *Center for Cybersecurity Policy and Law*, www.centerforcybersecuritypolicy.org/insights-and-research/new-report-highlights-need-for-investment-to-reduce-systemic-risks-of-ransomware-in-latin-america. Accessed Nov. 2024.

OECD. “Building a Skilled Cyber Security Workforce in Latin America.” *OECD*, www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/building-a-skilled-cyber-security-workforce-in-latin-america_6210dead/9400ab5c-en.pdf. Accessed Nov. 2024.

“Panama - Cybersecurity.” *International Trade Administration | Trade.Gov*, www.trade.gov/country-commercial-guides/panama-cybersecurity. Accessed Nov. 2024.

“Panama.” *NCSI*, ncsi.ega.ee/country/pa/. Accessed Nov. 2024.

“Peru :: Eu Cyber Direct.” *EU Cyber Direct*, eucyberdirect.eu/atlas/country/peru. Accessed Nov. 2024.

“Protecting Your Business and Employees.” *Protecting Your Business and Employees | Cyber.Gov.Au*, www.cyber.gov.au/resources-business-and-government/essential-cyber-security/protecting-your-business-and-employees. Accessed Nov. 2024.

Ritchey, Diane. “Mitigating the Insider Threat: Boeing’s Successful Approach.” *Security Magazine RSS*, Security Magazine, 5 Feb. 2018, www.securitymagazine.com/articles/88654-mitigating-the-insider-threat-boeings-successful-approach.

Times, The Brussels. “Massive Cyber Attack Cripples Colombian Government Sites.” *The Brussels Times*, www.brusselstimes.com/693227/massive-cyber-attack-cripples-colombian-government-sites. Accessed Nov. 2024.

"What Latin America Can Teach Us on Resilient Cybersecurity." *World Economic Forum*, www.weforum.org/agenda/2024/05/latin-america-cybersecurity-report-ransomware-attacks/. Accessed Nov. 2024.