The Economics of Cyberattacks on Brazil

By: Nir Kshetri and Joanna F. DeFranco

Kshetri, Nir and J. DeFranco (2020). "The Economics of Cyberattacks on Brazil" IEEE Computer vol. 53 (9) pp. 85-90. https://doi.org/10.1109/MC.2020.2997322

Abstract:

Cyberattacks have significant economic, political, and privacy-related impacts in Brazil. Regulatory and enforcement measures have been insufficient to prevent these attacks. The authors analyze these trends and assess some recent measures to address these issues.

Keywords: data privacy | Brazil | cyberattacks | computer crime | economics | government | companies | computer hacking

Article:

Cyberattacks are a serious problem in Brazil.[1] It was reported that, in October 2019, the personal information of 92 million Brazilians was auctioned off in an underground forum. The culprits were suspected to have illegally accessed the data from a stolen government database.[2] According to Symantec, in 2017, more than 60% of Brazilian Internet users (some 62 million people) were victimized by cybercriminals leading to a loss of US$22 billion.[3] In 2018, such attacks affected more than 70 million citizens.[4] The cybersecurity firm Trend Micro's study indicated that Brazil was the world's second largest victim of ransomware attacks in the first quarter of 2019. Brazil's ransomware attacks account for 10.64% of the global ransomware attacks.[5] A 2019 report of the International Telecommunication Union noted that Brazil's cyberattack-related economic losses were second highest in the world.[6]

In 2018, Brazilian companies lost more than US$20 billion to cyberattacks.[4] The average annual cost of cybercrime for a Brazilian company was estimated at US$7.24 million in 2018.[7] Unfortunately, cybersecurity initiatives have not been well developed in Brazil to deal with these growing threats. While Brazil has developed guidelines and best practices to deal with cyberthreats, prevention measures and a national security strategy is lacking,[8,9]

On the privacy front, the Brazilian General Data Protection Law [Lei Geral de Proteção de Dados (LGPD)] was ratified in the congress in mid-2018, which was scheduled to into effect on 15 August 2020. The LGPD is inspired by and modeled after the European Union's General Data Protection Regulation (GDPR).[10] However, Brazil lacks a national data protection authority to enforce basic provisions of the LGPD. The country's congress had passed the creation of a

federal agency, the National Data Protection Authority, or Autoridade Nacional de Proteção de Dados, to enforce data protection rules.[11] Nonetheless, then-President Michel Temer vetoed the legislation, arguing that such initiatives should be undertaken by the executive branch rather than the congress. Before leaving office, his government had formed an interim agency with a two-year mandate. However, after the current president Jair Bolsonaro took office in January 2019, the ability of the new agency to impose penalties for the violation of the LGPD has been restricted.[11]

Cyberthreats Facing Brazil

Brazil has earned its reputation as the "king of the banking Trojan."[12] A Trojan can identify the Internet Protocol address of a user of an infected web page, which enables it to perform targeted attacks.[13] The Brazilian financial system faces about 15,500 cyberattacks and 500 new malware threats daily.[14] Bancos, a well-known password-stealing Trojan, which is designed to steal banking information mainly from Latin American consumers, is believed to have originated in Brazil. Other well-known banking Trojans, such as ZeuS, SpyEye, and CARBERP, are also reported to be increasingly common in Brazil.[15]

Brazil's cybercrime setting presents a security professional with a significantly more challenging landscape. One of the reasons is that antivirus/malware products used are locally developed.[1] Unlike their Eastern European counterparts, Brazilian cybercrime groups have not realized the need to internationalize their operations due to Brazil's well-developed financial sector.[12] The Brazilian hackers mainly target Brazilians.[16]

Table 1. Real and perceived cyberthreats facing Brazil: Some examples.

	Internal	**External**
Political	• June 2011: The hacking group LulzSec shut down the website of Petrobras with a DDoS attack for part of a day. • 2013: Anonymous Brazil defaced the website of the Brazilian Air Force.[17] • 2014: Anonymous Brazil's attack (publishing stolen usernames and passwords) on Brazilian government websites to protest against the 2014 FIFA World Cup. • 2018: Anonymous group's Twitter campaign to interfere with the Brazilian election #OpEleiçãoContraOFascismo.	• Feb. 2011: A Brazilian power plant was infected by Conficker worm, which caused its management systems to freeze up and not display data.[18] • 2018: Russian hackers' interference in the presidential elections using social media.
Economic	• 2014: Cyberattack on Boleto Bancário system (a Brazilian payment method). • February 2012: a coordinated attack that coincided with quarterly earnings reports and victimized most major Brazilian banks.[19]	• The NSA's alleged industrial espionage on the oil giant Petrobras. • OGlobo: Canadian spy agencies tracked the Brazil's Mines and Energy Ministry emails and phone calls as well as communications to other countries. • 2012: a cyber espionage campaign targeted high-profile oil companies, including those of Brazil, according to Dell Secure Work CTU.

Recent measures have further increased Brazil's vulnerability. In April 2019, in an attempt to improve efficiency in the financial system, the central bank (Banco Central do Brasil) published new guidelines that require financial institutions to share customer data with third parties (such

as financial technology companies), product aggregators, and nonfinancial companies (such as Uber and Google[14]). These third parties may not have the same level of security as banks and thus may be more vulnerable to attack. Table 1 presents additional internal economic examples of real and perceived cyberthreats facing Brazil.

In a high-profile cyberattack reported in mid-2014, Brazil's popular payment method, Boleto Bancário, was targeted. Criminals attempted to steal US$3.75 billion. Researchers from the Internet security company RSA traced the crime to a gang in Brazil.[20] A report from the Igarape Institute noted that a few cybercriminals who had been caught fit a profile: "well-educated, upper-middle-class males from 25 to 35 years old."[21]

Brazil also faces politically motivated internal and external cyberthreats, such as distributed denial of service (DDoS) attacks and the Conficker Worm (a virus that disables security features and backup settings as well as creates a path for communication from remote systems) (Table 1). In 2011, LulzSecBrazil, a Brazilian component of the hacker group LulzSec (Lulz Security), released personal information including identification numbers and bank details of the employees of energy producer Petrobras.[22]

Websites have also been attacked to interfere with elections and protests. For instance, the websites of Brazilian government agencies have been attacked frequently by Anonymous (a secret group of online hackers) and other hacking groups.[23] In June 2014, as a protest against the 2014 FIFA World Cup, the hacker group Anonymous Brazil defaced a number of Brazilian government websites. The Foreign Ministry's server and FIFA partner sites were attacked, which compromised emails and attachments. An alleged Anonymous hacker emailed Reuters news organization the following threat: "Companies and institutions that work with a government that denies the basic rights of its people to promote a private, exclusive, and corrupt sports event will be targeted."[24]

Brazil is also reported to be among the top countries in terms of the government's actions to control and monitor citizens' activities online. For instance, around the time of the 2013 antigovernment protests, the country's intelligence agencies allegedly compiled a list of 700 topics that they considered potential security threats. As a result, an operation code-named *Mosaico* was launched that actively trawled through social media websites such as Facebook, Twitter, WhatsApp, and Instagram.[25]

A report of the IT security company Imperva noted that "strong government or corporate resentment in a population is a key factor" behind the escalation of cyberattacks in Brazil.[21] Thus, Brazilians perceived that many of their targets deserved attack by the hacktivists. Imperva notes, "In the minds of many Brazilians, the cyber mayhem was no crime."[26] This was a crucial factor in increasing hacking and cyberattacks in Brazil.

There are also external threats. Russian hackers reportedly tried to interfere with the country's 2018 presidential elections using social media.[27] For instance, according to the cybersecurity firm FireEye, the hackers used bots to increase the distribution of posts that criticized the Brazilian democratic model and questioned the legitimacy of the election. The Brazilian branch

of the Anonymous group (@anonopsbrazil) had also started a Twitter campaign #OpEleiçãoContraOFascismo (Operation Against Fascism).

A turning point for Brazil was when U.S. National Security Agency (NSA) whistleblower Edward Snowden revealed the NSA's alleged industrial espionage on the oil giant Petrobras, Latin America's largest energy producer. The United States has denied spying for commercial advantage; many Brazilians do not seem to be convinced. President Dilma Rousseff argued that if the allegation of the NSA's breaking into Petrobras computers is true, then gathering economic information would be the motive.[28] The networks of Ministry of Mines and Energy were also hacked, which, together with Petrobras, was involved in the auction of oil fields.[29] Specifically, Brazilians think that the company's data on Brazil's offshore oil reserves and plans for allocating licenses for exploration to foreign companies were the intended targets.[1]

In 2012, the Dell SecureWorks Counter Threat Unit (CTU) research team tracked a cyberespionage campaign that targeted high-profile oil companies in a number of countries, including those in Brazil.[30] Likewise, according to Brazilian television OGlobo, Canadian spy agencies tracked the Brazil's Mines and Energy Ministry emails and phone calls as well as communications to other countries, including the Ecuador-based Latin American Energy Organization.[31]

Cyberthreat Mitigation Challenges

Brazil has faced many challenges in dealing with the cyberthreats, as there is severe congestion in the law enforcement system—only 5–8% of crimes are solved in Brazil.[32] This remarkable situation is a direct consequence of the scarcity of law enforcement resources. A prevailing culture of violence takes most of the available law enforcement resources with little law enforcement left to address cybercrimes. There is also a cybersecurity skill shortage. In a global survey conducted by Sophos in 13 of the major world economies in 2019, 83% of Brazilian respondents reported that they face challenges in recruiting people with cybersecurity skills.[33]

Recent Initiatives and Actions to Strengthen Security and Privacy

Security

In terms of strategic planning to deal with cyberthreats, Brazil has lagged behind other regional economies, such as Argentina, Chile, and Mexico. For instance, in 2017, Chile and Mexico published their Cybersecurity Strategies, which outlined what, how, and when to address various types and categories of cybersecurity risks. Mexico's focus has been to boost its economy and innovation, strengthen civil society and public institutions, and improve public and national security. Chile's cybersecurity strategy aims to improve its digital infrastructure and people's rights in cyberspace, develop a cybersecurity culture, and promote the growth if its cybersecurity industry. Likewise, Argentina's Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad seeks to improve the regulatory framework for identifying and protecting its digital infrastructures.[34] Brazil has realized the urgency of addressing the cybersecurity threats. The Institutional Security Cabinet, which is an executive cabinet office of the country's federal government, has been working to develop a national cybersecurity strategy.[9] In November 2019,

the Brazilian government announced the creation of a network of eight R&D labs.[35] One of them will focus on the use of artificial intelligence technology in cybersecurity, which will involve the Brazilian Army.[36] Nonetheless, the Brazilian cybersecurity strategy has much to learn from other countries in the region.

Privacy

Currently, Brazil has more than 40 legal norms at the federal level that directly and indirectly deal with the protection of privacy and personal data. These norms often function in a sector-based system and sometimes are conflictive. The lack of clear legal rules has hindered legal certainty and predictability, which has reduced the country's competitiveness.[37] The LGPD is expected to address these concerns.[38]

The LGPD is described as Brazil's first significant attempt to deal with digital privacy.[39] Whereas the existing laws are primarily directed toward regulating Internet service providers and requiring them to store and make data available for law enforcement and government agencies, the LGPD addresses Brazilian citizens' right to data privacy and security. It will replace the existing patchwork of legislation governing cybersecurity issues, such as the Civil Rights Framework for the Internet (Internet Act), the Civil Code, and the Consumer Protection Code.

As is the case of GDPR, the LGPD has outlined new rules regarding how personal data can be collected, used, processed, and stored.[40] The LGPD will affect all industries and economic sectors. For instance, Article 18 of the LGPD gives consumers rights for their personal data. Organizations are required to ensure personal data are "anonymized, redacted, or eliminated."[41] The country has also created the Brazilian National Data Protection Authority to enforce the LGPD.[40]

The LGPD applies to domestic as well as foreign entities that collect or process personal data in Brazil or provide goods or services to individuals in Brazil. For instance, a business that collects or processes personal data of individuals in Brazil is required to follow the LGPD even if it does not have a physical presence in Brazil. The fines of violating the LGPD can be up to 2% of the company's gross revenues derived from Brazil, or 50 million reals (about US$13 million).[40]

Brazil's social, economic, political, and cultural characteristics provide insights into the key drivers of cybercrimes and the nature of cybersecurity measures. This country has been exposed to significant cyberthreats due to the country's financially motivated cybercriminal gangs. The detection of threats are difficult since many of the domestically originated attacks do not pursue foreign targets and hence are unknown to international security researchers.

Finally, there is an underlying and subtle warning here. Countries that do not treat cybersecurity as a national security threat incur enormous economic risks to their citizens, corporations, and democratic elections.

Acknowledgment

We thank Jeffrey Voas (editor in chief, *Computer*) for his many rewrites and suggestions on this article.

References

1. N. Kshetri, *The Quest to Cyber Superiority: Cybersecurity Regulations Frameworks, and Strategies of Major Economies*. New York: Springer-Verlag, 2016.
2. B. Barth, "Data on 92M Brazilians found for sale on underground forums," *SCMedia*, Oct., 2019. [Online]. Available: https://www.scmagazine.com/home/security-news/data-breach/data-on-92m-brazilians-found-for-sale-on-underground-forums/
3. A. Mari, "More than half of connected Brazilians suffered cyberattacks," *ZD Net*, Jan., 2018. [Online]. Available: https://www.zdnet.com/article/more-than-half-of-connected-brazilians-suffered-cyberattacks/
4. "*Brazil watch: Cable costs, cyber losses*," BNamericas, Newark, DE, Sept., 2019. [Online]. Available: https://www.bnamericas.com/en/news/brazil-watch-cable-costs-cyber-losses
5. A. Mari, "Brazil leads in ransomware attacks," *ZD Net*, June, 2019. [Online]. Available: https://www.zdnet.com/article/brazil-leads-in-ransomware-attacks/
6. "*Why is Brazil so vulnerable to cyber attacks?*" BNamericas, Newark, DE, Jan., 2020. [Online]. Available: https://www.bnamericas.com/en/features/why-is-brazil-so-vulnerable-to-cyber-attacks
7. "*The cost of cybercrime*," Accenture Security, Dublin, Ireland, 2019. [Online]. Available: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
8. "*Brazil's critical infrastructure faces a growing risk of cyberattacks*," Net Politics, Apr., 2018. [Online]. Available: https://www.cfr.org/blog/brazils-critical-infrastructure-faces-growing-risk-cyberattacks
9. L. Belli, "From BRICS to CyberBRICS: New cybersecurity cooperation," *China Today*, Nov., 2018. [Online]. Available: http://www.chinatoday.com.cn/ctenglish/2018/tpxw/201911/t20191113_800184922.html
10. M. Filho, V. Filho MarreyJr., and Q. Advogados, "*Data protection and privacy in Brazil*," Lexology, Aug., 2019. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=980b7a87-a569-499d-b631-88595d8c1927
11. "*Brazil's data protection paradox*," Council on Foreign Relations, Dec., 2019. [Online]. Available: https://www.cfr.org/blog/brazils-data-protection-paradox
12. C. Theriault, "*Brazil's cybercrime evolution: It doesn't look pretty*," Sophos, Abingdon, U.K., Oct., 2011. [Online]. Available: http://nakedsecurity.sophos.com/2011/10/05/brazils-cybercrime-evolution-it-doesnt-look-pretty/

13. D. Bestuzhev, "*Brazil: A country rich in banking Trojans*," Kaspersky Lab, Woburn, MA, 2012. [Online].
Available: http://www.securelist.com/en/analysis/204792084/Brazil_a_country_rich_in_banking_Trojans?print_mode=1

14. D. Feliba, "*Cybersecurity concerns mount over Brazil's open-banking pursuit*," S&P Global, July, 2019. [Online]. Available: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/52581872

15. J. Robertson, "Why are hackers flooding into Brazil," *Bloomberg*, Sept., 2013. [Online].
Available: http://www.bloomberg.com/news/2013-09-13/why-are-hackers-flooding-into-brazil-.html

16. Insikt Group, "*Pirates of Brazil: Integrating the strengths of Russian and Chinese hacking communities*," Recorded Future, Somerville, MA, Apr., 2019. [Online].
Available: https://www.recordedfuture.com/brazilian-hacking-communities/

17. E. Kovacs, "*Brazilian Air Force website hacked and defaced by Anonymous*," Softpedia, 2013a. [Online]. Available: http://tinyurl.com/o8kuan5

18. R. McMillan, "A power plant hack that anybody could use," *IDG News Service*, 2011. [Online].
Available: https://www.pcworld.com/article/237347/a_power_plant_hack_that_anybody_could_use.html

19. C. Lincoln, "What security managers can learn from Brazil: Frontline in the global cyber wars," *Professional Security Magazine*, 2013. [Online].
Available: https://www.professionalsecurity.co.uk/news/interviews/learn-from-brazil/

20. N. Perlroth, "Cybercrime scheme uncovered in Brazil," *NY Times*, July, 2014. [Online].
Available: https://www.nytimes.com/2014/07/03/technology/cybercrime-scheme-aims-at-payments-in-brazil.html

21. L. Garcia-Navarro, "Brazil's cybercrime free-for-all: Many scams and little punishment," *NPR*, 2015. [Online].
Available: http://www.npr.org/sections/parallels/2015/06/15/414622197/brazils-cybercrime-free-for-all-many-scams-and-little-punishment

22. "*UPDATE 3-Hackers target Brazilian statistics agency*," Reuters, London, June, 2011. [Online]. Available: https://www.reuters.com/article/cybersecurity-brazil-hackers/update-3-hackers-target-brazilian-statistics-agency-idUSN1E75N0IK20110624

23. "*Spy vs Spy: Cyber Crime, surveillance on rise in Latin America*," Southern Pulse, InSight Crime, Washington, D.C., Aug., 2011. [Online]. Available: http://insightcrime.org/insight-latest-news/item/1478-spy-vs-spy-cyber-crime-surveillance-on-rise-in-latin-america

24. H. Gaskell, "*Hackers bring down World Cup websites*," ITP Media Group, Dubai, United Arab Emirates, 2014. [Online]. Available: http://www.itp.net/598576-hackers-bring-down-world-cup-websites

25. M. Spektor, "*Five goals for Brazil's new foreign policy*," Americas Quarterly, 2016. [Online]. Available: http://americasquarterly.org/content/five-goals-brazils-new-foreign-policy

26. "*Imperva's hacker intelligence summary report: The anatomy of an anonymous attack*," Imperva, Redwood Shores, CA, 2012. [Online]. Available: http://www.imperva.com/docs/hii_the_anatomy_of_an_anonymous_attack.pdf

27. B. Benevides, "*Russian hackers are trying to interfere in Brazilian elections, cybersecurity firm says*," Folha De S.Paulo, Oct., 2018. [Online]. Available: https://www1.folha.uol.com.br/internacional/en/world/2018/10/russian-hackers-are-trying-to-interfere-in-brazilian-elections-cybersecurity-firm-says.shtml

28. "*China suspends cooperation in joint task force over cyberspying charges*," Democracyastray, May, 2014. [Online]. Available: http://democracyastray.blogspot.com/2014/05/china-suspends-cooperation-in-joint.html

29. P. Purkayastha and R. Bailey, "U.S. control of the internet: Problems facing the movement to international governance," *Mon. Rev., Indep. Soc. Mag.*, vol. 66, no. 3, pp. 103–127, 2014. doi: 10.14452/MR-066-03-2014-07_7.

30. S. Cutler, "*The Mirage campaign*," SecureWorks, Inc, Atlanta, GASept., 2012. [Online]. Available: http://www.secureworks.com/cyber-threat-intelligence/threats/the-mirage-campaign/

31. C. Jasasmie, "*Canada spied on Brazil's Mines and Energy Ministry: Snowden*," Glacier Media, Vancouver, Canada, Oct., 2013. [Online]. Available: https://www.mining.com/canada-spied-on-brazils-mines-and-energy-ministry-snowden-23584/6240/

32. A. Presse, "Brazil, 7th most violent country in the world, had 1.1 Million murders between 1980 and 2011," *Huffington Post*, Dec., 2017. [Online]. Available: http://www.huffingtonpost.com/2013/07/19/brazil-most-violent-country-murders_n_3618704.html

33. "*The impossible puzzle of cybersecurity*," Sophos, Abingdon, U.K., June2019. [Online]. Available: https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

34. C. Schreiber, "*Cybersecurity challenges for Latin America*," Global Strategy, Sept., 2018. [Online]. Available: https://www.seguridadinternacional.es/?q=es/content/cybersecurity-challenges-latin-america

35. A. Mari, "Brazilian government announces creation of AI lab network," *ZD Net*, Nov., 2019. [Online]. Available: https://www.zdnet.com/article/brazilian-government-announces-creation-of-ai-lab-network/

36. B. Henriques, "*Brazil is emerging as a world-class AI innovation hub*," VentureBeat, San Francisco, CA, Jan., 2020. [Online]. Available: https://venturebeat.com/2020/01/12/brazil-is-emerging-as-a-world-class-ai-innovation-hub/

37. "*Proteção de dados a legislação vigente no Brasil*," Baptista Luz, Sao Paulo, Brazil. White Paper, Nov., 2017. [Online]. Available: http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf

38. R. Monteiro, "*The new Brazilian General Data Protection Law: A detailed analysis*," International Association of Privacy Professionals, Portsmouth, NH, Aug., 2018; [Online]. Available: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/

39. D. Woods, "Brazil's new president and the changing cyber risk landscape," *Forbes*, Nov., 2018. [Online]. Available: https://www.forbes.com/sites/riskmap/2018/11/27/brazils-new-president-and-the-changing-cyber-risk-landscape/#59f548e05453

40. S. Blickensderfer, J. Swanson, and A. RegoJr., "*Brazil's new data protection law: An overview and four key takeaways for U.S. Companies*," The National Law Review, May, 2019. [Online]. Available: https://www.natlawreview.com/article/brazil-s-new-data-protection-law-overview-and-four-key-takeaways-us-companies

41. S. Ikeda, "Citizen data of 92 Million Brazilians offered for sale on underground forum," *CPO Magazine*, Oct., 2019. [Online]. Available: https://www.cpomagazine.com/cyber-security/citizen-data-of-92-million-brazilians-offered-for-sale-on-underground-forum/

Nir Kshetri is a professor of management in the Bryan School of Business and Economics at the University of North Carolina at Greensboro and the "Computing's Economics" column editor for *Computer*. Contact him at nbkshetr@uncg.edu.

Joanna F. Defranco is an associate professor of software engineering at Penn State Great Valley School of Graduate Professional Studies. Contact her at jfd104@psu.edu.