Cybersecurity

Capacity Review

Federative Republic of Brazil

Global Cyber Security Capacity Centre
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD
GSI-PR
GREAT for PARTNERSHIP
OAS More rights for more people

Cybersecurity

Capacity Review

Federative Republic of Brazil

Acknowledgments

This publication has been possible thanks to the collaboration of many people and institutions. Therefore, the Secretariat of the Inter-American Committee against Terrorism of the Organization of American States, the Center for Global Cybersecurity Capacity of the University of Oxford, the Department of Information Security - DSI of the Office of Institutional Security of the Presidency of the Republic of Brazil, and the Government of the United Kingdom would like to thank the following institutions for having participated in the process of preparing and launching this report.

Ministry of Defense

Brazilian Intelligence Agency (Abin)

Cyber Defense Center (CDCIBER)

Brazilian Army (CIE)

Federal Police of Brazil

Federal Public Ministry

High Court of Justice

Ministry of Justice

Ministry of Science and Technology

National Telecommunications Agency (ANATEL)

Ministry of Foreign Affairs

Ministry of Education

Ministry of Labor and Employment

Ministry of Planning, Budget and Management

Ministry of Finance

Ministry of Health

Ministry of Transport

Ministry of Mines and Energy

Federal Internal Affairs Office (CGU)

Federal Audit Court (TCU)

Brazilian Central Bank

Ministry of Industry, Foreign Trade and Services

Ponto BR Information and Coordination Center (NIC.BR)

Government Cyber Treatment and Response Center (CTIR.BR)

Internet Security Incident Response Group in Brazil (CERT.Br)

National Incident and Research Network Security Incident Response Center (CAIS / RNP)

Brazilian Army Network Incident Coordination Center (CCTIR / EB)

Brazilian Air Force Network Incident Handling Center (CTIR.FAB)

Security Incident Response Groups on CAIXA Computers (CSIRT / CAIXA)

Computer Security Incident Response Team of the Bank of Brazil (CSIRT / BB)

SERPRO Attack Response Group (GRA / SERPRO)

Chamber of Deputies Computer Security Incident Response Group (GRIS/CD)

Rio-Computer Network (CEO / Rio Network)

Abril Group Security Incident Response Group (GRIS ABRIL)

Banco Caixa Geral

Bank of Brazil

Brazilian Telecommunications (Telebras)

Table of Contents

7 Document Administration

8 List of Abbreviations

10 Executive Summary

25 Introduction

27 Dimensions of Cybersecurity Capacity

29 Stages of Cybersecurity Capacity Maturity

30 Methodology – Measuring Maturity

33 Cybersecurity Context in Brazil

35 Review Report

36 Overview

37 Dimension 1
Cybersecurity Strategy and Policy

38 D 1.1 - National Cybersecurity Strategy

41 D 1.2 - Incident Response

44 D 1.3 - Critical Infrastructure (CI) Protection

46 D 1.4 - Crisis Management

48 D 1.5 - Cyber Defence

49 D 1.6 - Communications Redundancy

50 Recommendations

54 Dimension 2
Cybersecurity Culture And Society

55 D 2.1 - Cybersecurity Mind-set

57 D 2.2 - Trust and Confidence on the Internet

59 D 2.3 - User Understanding of Personal Information Protection Online

60 D 2.4 - Reporting Mechanisms

61 D 2.5 - Media and Social Media

62 Recommendations

64 Dimension 3
Cybersecurity Education, Training, and Skills

64 D 3.1 - Awareness Raising

67 D 3.2 - Framework for Education

68 D 3.3 - Framework for Professional Training

70 Recommendations

74 Dimension 4
Legal and Regulatory Frameworks

75 D 4.1 - Legal Frameworks

80 D 4.2 - Criminal Justice System

83 D 4.3 - Formal and Informal Cooperation Frameworks to Combat Cybercrime

85 Recommendations

89 Dimension 5
Standards, Organizations, and Technologies

89 D 5.1 - Adherence to Standards

91 D 5.2 - Internet Infrastructure Resilience

92 D 5.3 - Software Quality

93 D 5.4 - Technical Security Controls

94 D 5.5 - Cryptographic Controls

95 D 5.6 - Cybersecurity Marketplace

96 D 5.7 - Responsible Disclosure

97 Recommendations

101 Additional Reflections

103 References

DOCUMENT ADMINISTRATION

Lead researchers (2018):
Dr Ioannis Agrafiotis, Dr Eva Nagyfejeo, Dr Maria Bada

Lead researchers (2019):
Dr Andraz Kastelic

Reviewed by:
Professor William Dutton, Professor Michael Goldsmith, Professor Basie von Solms

Approved by:
Professor Michael Goldsmith

Version	Date	Notes
1	3 August 2018	First draft to Technical Board
2	16 August 2018	Second Draft reviewed by Technical Board
3	11 September 2018	Third Draft reviewed by OAS
4	3 July 2019	First revised draft following the validation workshop
5	21 April 2020	Second revised draft submitted to OAS after the validation workshop
6	18 May 2020	Third version submitted to OAS
7	5 June 2020	Final version submitted to OAS

LIST OF ABBREVIATIONS

ABIN
Agência Brasileira de Inteligência (Brazilian Intelligence Agency)

ANATEL
Agência Nacional de Telecomunicações (National Telecommunications Agency)

CA
Certification Authority

CEPESC
Center for Research and Development of Secure Communications

CERT
Computer Emergency Response Team

CGSIC
Comitê Gestor de Segurança da Informação e Comunicação (Committee on Information Security and Communications)

CI
Critical Infrastructure

CICTE
Inter-American Committee against Terrorism

CISM
Certified Information Security Manager

CISSP
Certified Information Systems Security Professional

CMM
Cybersecurity Capacity Maturity Model for Nations

CMU CERT
Carnegie Mellon University Computer Emergency Response Team

CNPJ
Cadastro Nacional da Pessoa Jurídica (Identification number issued to Brazilian companies)

CoE
Council of Europe

CPF
Cadastro de Pessoas Físicas (Brazilian individual taxpayer registry identification)

C-PROC
Cybercrime Programme Office of the Council of Europe

CSIRT
Computer Security Incident Response Team

CTIR gov
Brazilian Government Response Team for Computer Security Incidents

DDOS
Distributed Denial of Service

ECA
Estatuto da Criança e do Adolescente (Child and Adolescent Statute)

FIRST
Forum of Incident Response and Security Teams

FPA
Federal Public Administration

GCSCC
Global Cyber Security Capacity Centre

GSI
Gabinete de Segurança Institucional da Presidência da República (Institutional Security Cabinet of the Presidency)

ICT
Information and Communication Technologies

IDS
Intrusion Detection Systems

ISP
Internet Service Provider

KPIs
Key Performance Indicators

LACNIC
Latin American and Caribbean Internet Addresses Registry

NGO
Non-Governmental Organisation

NIST
National Institute of Standards and Technology

OAS
Organization of American States

RNP
Rede Nacional de Ensino e Pesquisa (Brazilian National Research and Educational Network)

SENAC
Serviço Nacional de Aprendizagem Comercial (National Service for Commercial Education)

SERPRO
Serviço Federal de Processamento de Dados (Federal Data Processing Service)

SIAFI
Sistema Integrado de Administração Financeira do Governo Federal (Integrated System of Financial Administration of the Federal Government)

SIEM
Security Information and Event Management

SME
Small and medium-sized enterprises

SPED
Sistema Público de Escrituração Digital (Public System of Digital Bookkeeping)

SSH
Secure Shell

STIX
Structured Threat Information eXpression

TCU
Tribunal de Contas da União (Federal Court of Accounts)

TLP
Traffic Light Protocols

URCC
Unidade de Repressão a Crimes Cibernéticos (Federal Police Unit for Combating Cybercrime)

Executive Summary

The Global Cyber Security Capacity Centre (GCSCC or 'the Centre') undertook a review of the maturity of cybersecurity capacity in Brazil at the invitation of, and in collaboration with, the Secretariat of the Inter-American Committee against Terrorism (CICTE), through its cybersecurity programme, of the Organization of American States (OAS). The objective of this review was to enable the Government to gain an understanding of its cybersecurity capacity, in order to strategically prioritise investment in cybersecurity capacities.

Over the period 19–20 March 2018, the following stakeholders participated in roundtable consultations: criminal justice, law enforcement, the defence community, information-technology officers and representatives from public-sector entities, critical infrastructure owners, policy makers, computer emergency response teams, information-technology officers from the private sector (including financial institutions), telecommunications companies, the banking sector and international partners.

The GCSCC researchers visited Brasilia once again a year later to validate the 2018 results and to update the draft of the Cybersecurity Capacity Review report accordingly. The data-collection methodology used in March 2019 was similar to the methodology used the year before. Stakeholders participating in the focus-group interviews included representatives from academia, critical national infrastructure operators, telecommunication providers and other private sector entities, government ministries, the judiciary, law enforcement, the defence community, the financial sector, computer emergency response teams (CERTs), the media, the private sector and civil society.

Both in 2018 and 2019, the consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five dimensions of cybersecurity capacity:

- Cybersecurity Policy and Strategy
- Cyber Culture and Society
- Cybersecurity Education, Training and Skills
- Legal and Regulatory Frameworks
- Standards, Organisations and Technologies

Each dimension is made up of a number of factors which describe what it means to possess cybersecurity capacity. Each factor presents a number of aspects and for each aspect there are indicators, which describe steps and actions that, once observed, define the state of maturity of that aspect. There are five stages of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. More details on the definitions of each stage across all dimensions are provided in the CMM document.[1]

Figure 1 (below) provides an overall representation of the cybersecurity capacity in Brazil and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

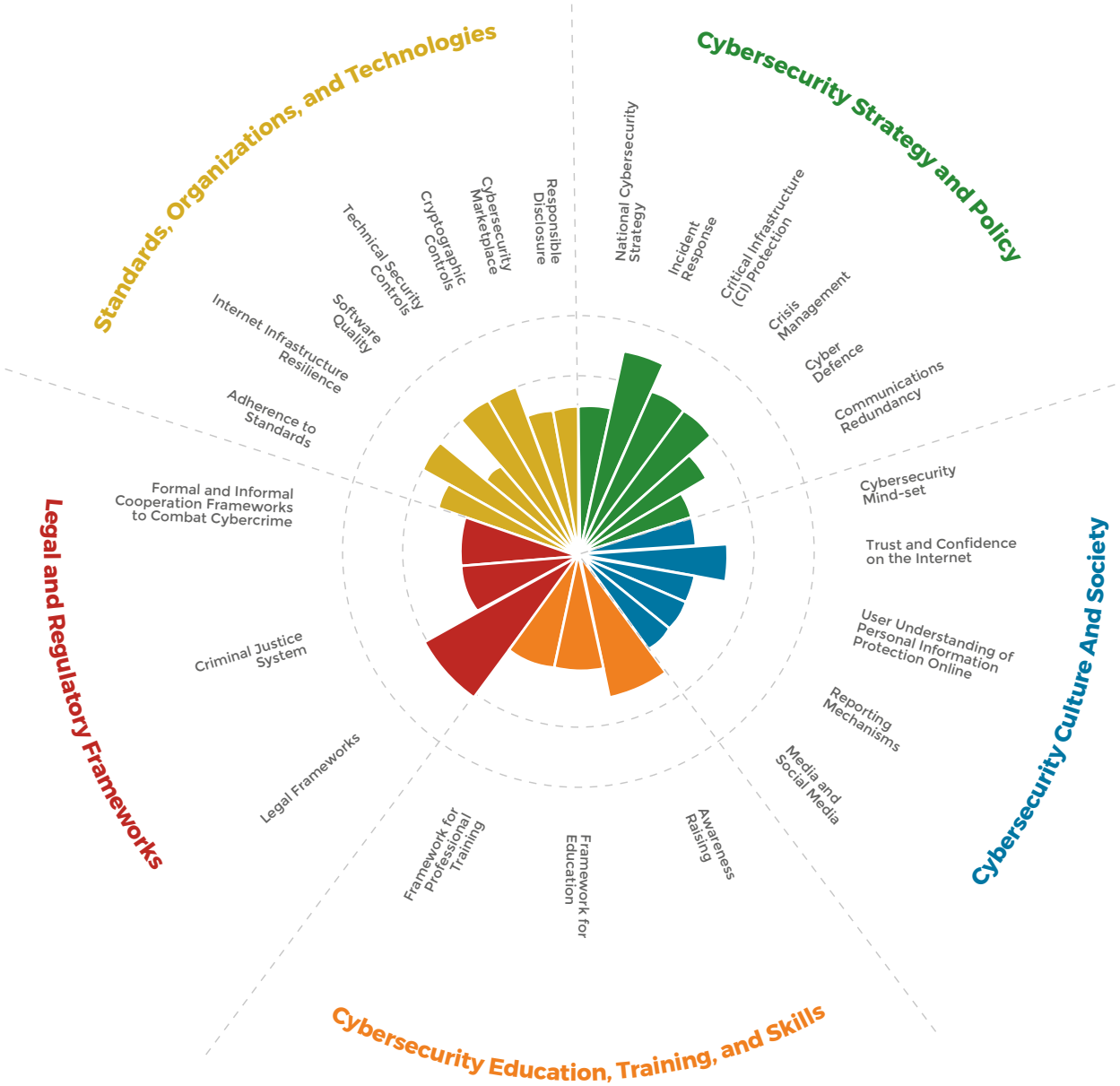


Figure 1: *Overall representation of the cybersecurity capacity in Brazil*

Cybersecurity Policy and Strategy

At the time of the review in March 2018, there was no official national cybersecurity document detailing how to establish co-ordination between key cybersecurity governmental and non-governmental actors. The lack of collaboration between governmental institutions and the private sector, and the "fragmentation of responses" were potentially addressed with the Estrategia (2015–2018).[2] The aim of the Estrategia was to detail the strategic guidelines for information and communications security and to co-ordinate these efforts between the various actors involved in order to mitigate risks to which organisations and society are exposed. The strategy focused on the FPA with critics highlighting the absence of a central authority to implement such a systematic and multi-stakeholder approach, as well as the absence of civil-society organisations, Internet-stakeholders and the general public from the design of the strategy. Regarding the organisation of the cybersecurity programme, participants expressed their preference for a decentralised model, where commercial sectors would be overseen by existing regulatory agencies, with a newly established national agency to co-ordinate efforts.

Following the validation of the focus-group interviews conducted in March 2019, it was confirmed that the National Cybersecurity Strategy (Federal Decree No. 10.222) was finally adopted in February 2020.[3] According to government sources it focuses on ten strategic actions that should guide the FPA to devise its own actions towards cyber security.

Focusing on incident response, there are many Computer Security Incident Response Teams (CSIRTs),[4] ranging from government entities to private sector and academic facilities. Depending on the role of a CERT, these entities may be involved exclusively in managing the security of systems, enforce cybersecurity guidelines or be responsible for co-ordinating efforts between national authorities and local levels. The national CERT (CERT.br) is a body certified by the Forum of Incident Response and Security Teams (FIRST) and responsible for handling incident reports for the private sector.[5] The Brazilian Government Response Team for Computer Security Incidents (CTIR Gov) provides incident response for the FPA while CERTs are dedicated to specific sectors and critical infrastructure (CI) stakeholders. Also, there is a military CERT that protects military networks. All these institutions have clear guidelines and roles regarding incident response; CERT.br holds the register for national incidents and publishes statistical data of threats and incidents on an annual basis. All CERTs provide reports through official channels to the CERT.br. Automated systems following international standards, such as Structured Threat Information eXpression (STIX) and Traffic Light Protocols (TLP) ensure that threat intelligence is shared to CERTs that collaborate with the CERT.br. Current legal efforts focus on streamlining the sharing of threat intelligence between all CERTs, since not every private CI stakeholder is entitled to receive threat intelligence. As the range of CI stakeholders is expanding, there is a need for greater participation by research institutions.

The maturity of Brazil's capacity to protect critical infrastructure varies between public and private CI operators. All federal institutions are required to conduct cyber-risk assessments, which are updated annually

based on lessons learnt from major events. Public CI stakeholders comprise telecommunication companies, transport, energy and financial institutions, all of which co-operate and co-ordinate through formal channels of communication with the Ministry of Defence. There are clearly defined policies and procedures in place for all public institutions to follow based on information provided by CERT.br's situational awareness tool. Access to such protocols is provided to the Federal Police and to intelligence services to increase co-operation among CI stakeholders. The private sector is not currently considered to be part of the country's CI. Since Brazil has endorsed privatisation in critical sectors such as finance, it is imperative that the list of CI stakeholders is revisited, to consider private institutions. Private institutions do not have any obligations to inform the Government of a major incident, are restricted from obtaining access to threat intelligence and are oblivious to risk assessments and processes that the Government has in place for public CI operators. Therefore, private institutions need to develop their own internal risk assessments and security policies, the effectiveness of which will depend on the degree of their maturity. The majority of the participants urged the Government to create a mechanism to identify the level of maturity in IT governance both in the public and private sectors, a protocol of communication to distribute alerts across public and private sectors, and an initiative to evaluate the norms and the standards applied by private and public organisations.

Over the last decade, Brazil has hosted a series of important events and, as expected, the country has experienced a series of cyber-attacks during these events. The incident-handling processes during these events demonstrated that critical organisations for cyber-defence are capable of collaborating and effectively mitigating the impact of these attacks. Organisations that participated in crisis management had clear roles, there were transparent protocols on how to disseminate information and escalate incidents, and specific guidance on how to protect systems. However, crisis management processes were tailored to these specific events. The experience and lessons learnt from these events should underpin current efforts in crisis management. Crisis-management protocols should be designed, and a network of public and private organisations should be created to handle crises. Training and exercises on simulated crisis events were suggested as the optimal way to validate communication protocols, increase cybersecurity awareness and to test incident-handling processes. Towards that end, participants mentioned the Cyber Guardian exercise, which uses high-level planning to devise scenarios and simulation platforms for cyber operations that can emulate critical systems from the finance, nuclear and public sectors.

Regarding cybersecurity governance, the Brazilian Government has assigned the political and strategic level to the Gabinete de Segurança Institucional da Presidência da República (GSI) and the strategic, operational procedures and cyber defence to the Ministry of Defence. During recent years, the military has been restructured to fit the needs of an evolving democratic system, with focus on emerging cross-border threats and internal security events. There is an official cyber-defence document, published in 2012, and guidelines on cybersecurity policies. The military operates a CERT and provides training regarding risk management and incident response. Participants suggested that the military possesses both offensive and defensive capabilities and focuses on the enhancement of defensive measures. They indicated that the military deploys systems that provide situational awareness and proactively defend against Distributed Denial of Service (DDoS) attacks or web defacement. There are laboratories to analyse malicious software, and a significant number of personnel being trained to execute these tasks.

It was not possible to obtain a comprehensive view regarding communications redundancy in the course of the CMM review. Participants suggested that the public sector has emergency-response assets hardwired into the national strategy and its emergency communication network, with appropriate resources to evaluate the current protocols in place for redundancy, evaluate the redundant systems, execute exercises and perform communication drills. There are multiple crisis centres designated in dispersed geographical locations to ensure participation of all stakeholders in the event of an emergency. In stark contrast, the private sector is neglected and is excluded from these plans, with the exception of private CERTs.

Cybersecurity Culture And Society

Regarding the cybersecurity culture and society dimension, the Government has recognised the need to prioritise cybersecurity across its institutions. Also, aspects of governmental processes and institutional structures have been designed in response to risks to cybersecurity, but initiatives are to be found primarily within leading agencies. Overall, participants noted that the security culture in Brazil varies across different parts of the country and different sectors of government and the economy. A concern noted by participants is that governmental structures are very complex. Therefore, if the maturity of the public sector is being assessed, varying stages can be identified within different departments. Another concern raised by participants is the lack of a co-ordinating mechanism to identify the level of maturity within and across government.

Leading firms within the private sector have begun to place greater priority on a cybersecurity mind-set by identifying high-risk practices. The finance and IT sectors are more advanced in cybersecurity; as they are more frequent targets, they are investing more in cybersecurity. Participants informed us that since national banks have begun to take proactive security measures, criminals have increasingly focused on regional banks and small and medium-sized enterprises (SMEs). A limited but growing proportion of Brazil's Internet users have begun to place greater priority on cybersecurity; for example, as by identifying risks and threats. Society as a whole still lacks a cybersecurity mind-set; users may be aware of cybersecurity risks but they often fail to act accordingly in their everyday practices. It was mentioned that it is common even for IT experts, who are aware of risks, to nevertheless click on phishing emails, or to share sensitive information on social media sites such as Facebook.

Overall, participating stakeholders believe that only a small proportion of Internet users critically assess what they see or receive online. Similarly, few believe that end users have the skills to use the Internet safely and to protect themselves online.

Overall, there is a general encouragement for companies to provide online services. E-commerce service provision is growing and has increased since 2017. In 2017, Brazil (the Brazilian Federal Police) and Europol signed a strategic agreement to increase co-operation to combat cross-border criminal activities, which could be considered to be a formal co-operation. A growing proportion of users trust in the secure use of e-commerce services. The Ministry of Justice has a secretariat that focuses on consumer rights and e-commerce.

E-government services have also been developing and a growing proportion of users trust in the secure use of these services. Services such as those for sending Statements of Income Tax and providing information about Social Security and Government procurement have been available via the Internet since 1998.

A growing number of users and stakeholders within the public and private sectors are perceived to have general knowledge about how personal information is handled online and to employ good (proactive) cybersecurity practices to protect their personal information online. Personal data regulations that are being discussed in the EU are not in line with those being discussed in Brazil. Discussions have begun regarding Brazil's approach to the protection of personal information and about the balance between security and privacy, but this has not yet resulted in concrete actions or policies.

In Brazil, both the public and private sectors provide some channels for reporting online incidents but these channels are not well co-ordinated and are generally used in an ad-hoc manner. Reporting mechanisms have been established for users to report Internet-related crime, and these are frequently used. SaferNet Brazil provides information on Internet safety and the means to register complaints via its website. SaferNet Brazil[6] is a non-profit organisation that was created in 2005. Also, the Federal Police[7] has a dedicated page where denunciations can be registered on its website, and these can also be sent to a dedicated email address. Online illegal content can be reported to the child and adolescent pornography[8] helpline set up by the Government.

All incidents can be reported to the police, while those that are not clearly classified are sent to the governmental CTIR Gov and are then categorised before being forwarded to the appropriate institutions. Overall, participants indicated that citizens in Brazil do not have a culture of reporting. Moreover, it was not possible to identify how often or routinely existing reporting mechanisms established by the public and private sectors are used.

There is ad-hoc media coverage of cybersecurity in Brazil, with limited information provided and infrequent reporting on specific issues that individuals face online, such as online child pornography or cyber-bullying. In addition, participants mentioned that there is limited discussion about cybersecurity on social media. Generally, the media ignores the technical details of cybersecurity incidents and has frequently provided arguably incorrect guidance and advice about safe online behaviour.

Cybersecurity Education, Training, and Skills

A national programme for raising awareness about cybersecurity, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established.
Due to the lack of civil society participants, it was not possible to obtain a clear picture of existing initiatives aimed at raising cybersecurity awareness.

During the review, the most important awareness-raising body recognised by the participants was SaferNet Brazil, which is an NGO created in 2005.[9] It has unique partnerships with the Ministry of Justice, the Federal Police and the Human Rights Secretariat at the Office of the President of the Republic and exists to "protect human rights and serve as a Hotline, Helpline and Awareness node in Brazil."[10]

The Internet Steering Committee in Brazil (www.cgi.br) – a multi-stakeholder council created by Interministerial Ordinance 147 of 31 May 1995 – is the main institution in charge of promoting Information and Communication Technologies (ICT) security standards and Internet best practices[11] and it conducts its activities via the Brazilian Network Information Centre (NIC.br) (http://nic.br/quem-somos/).[12] Based on desk research, NIC.br implements several initiatives such as Antispam.br[13] (http://www.antispam.br/) and InternetSegura.br[14] (https://www.Internetsegura.br/), two portals that are aimed at raising awareness in children and parents about spam and which disseminate materials about Internet safety.

Regarding raising cybersecurity awareness for executives, participants acknowledged that levels are often low among senior business management members and that they need to be educated about how cybersecurity risks affect the organisation. Also, there is no obligation for executives to attend cybersecurity training, although it is considered to be best practice.

Due to the lack of participation by academia, it was not possible to obtain a clear picture about cybersecurity education in Brazil. Therefore, the information provided is based on desk research.
The need for enhancing cybersecurity education in schools and universities has been identified by leading government and industry stakeholders.

The Ministry of Education sets the national curriculum on cybersecurity-related courses and requirements and standards but the level of development is left to the universities to decide. It is not regulated by a central agency. The review did not inform if there is any distinct national budget set aside for cybersecurity education. Similarly, it was not clear from the focus-group discussions to what extent co-operation exists between the private sector and universities.

Qualifications for and the supply of cybersecurity educators are readily available. In Brazil, specialised courses in computer science are offered at university level.

The need for training professionals in cybersecurity has been recognised by the Government. Based on desk research, the Brazilian Internet Steering Committee (CGI.br) (see D 3.1) co-ordinates training efforts via CERT.br, the Best Practices Portal (BCP.nic.br) and CGSIC. Participants stated that most of the professionals within the public sector obtain IT professional qualifications from overseas and receive ICT certificates such as the Certified Information Systems Security Professional (CISSP), and Certified Information Security Manager (CISM) authorised by international institutions (International Information System Certification Consortium (ISC)2 and ISACA ®).

The Control Objectives for Information and Related Technologies (COBIT) network has been accepted as "a de facto standard for good practices throughout Brazil, in private, public and government organizations."[15]

Legal and Regulatory Frameworks

Brazil does not have an all-encompassing regulatory framework that deals explicitly with cybersecurity. Despite the efforts to introduce regulation through a binding legislative framework, cybersecurity legislation in Brazil remains under development. However, several official guidelines or "soft laws" have been adopted that concern cybersecurity issues.

The Cyber Crimes Act (Law No. 12.737/2012),[16] also known as the "Carolina Dieckmann Law", and the Brazilian Civil Rights Framework for the Internet (Law No. 12.965/2014)[17] are considered to be the most relevant and substantive pieces of legislation in place and seek to formally handle cybercrime offences and provide procedural powers when handling electronic evidence.

The Brazilian Civil Rights Framework for the Internet (Law No. 12.965/2014) (Marco Civil da Internet) was developed via a multi-stakeholder consultation process in order to regulate the use of the Internet in Brazil by establishing principles, guarantees, rights and duties for Internet users.

At the time of the reviews, in March 2018 and March 2019, Brazil did not have a specific data protection or privacy law but relied on various provisions stated in the Federal Constitution,[18] the Brazilian Penal Code,[19] the Consumer Protection Code[20] and the Brazilian Civil Rights Framework for protecting privacy on the Internet.

Comprehensive legislation for the protection of children online has been adopted and enforced. Article 241-D of the Statute of the Child and Adolescent (ECA) defines online grooming and sets a penalty of one to three years of imprisonment.[21] Some participants criticised this penalty as being too lenient and raised concern about the lack of comparable legislation to criminalise cyber-bullying, sexting and accessing or downloading images child-pornography.

At present, Brazil also lacks legislation that deals explicitly with cyber threats to intellectual property (IP). An exception is the Law on Copyright (Law No. 9.610/1998),[22] which guarantees the protection of any type of intellectual product, irrespective of its being registered or published.[23]

In December 2019, Brazil started its accession process to the Budapest Convention, as an observer.[24]

The regulatory authority for cybercrime is the Ministry of Justice and Public Security.[25] According to Article 10, Item V of the Law No. 13.844/2019, the Institutional Security Office of the Presidency of the Republic is responsible for other cybersecurity matters.[26]

The Federal Police's Unit for Combating Cybercrime (URCC), based in Brasilia, is the main law-enforcement actor in charge of fighting cybercrime, and therefore plays a critical operational role in pursuing cybercriminals both within and beyond Brazil's borders.[27]

Based on follow-up interviews, the capacity of prosecutors and judges to handle cybercrime cases and cases involving digital evidence was considered by the participants to be too ad-hoc and un-institutionalised. For example, there are no special courts for handling cybercrime cases, nor specialised training for judges on cybercrime. However, judges receive training as part of the training held for federal prosecutors.

The authorities in Brazil have recognised the need to improve informal and formal co-operation mechanisms, both domestically and across borders, but these mechanisms remain ad-hoc. In particular, the interviewees mentioned that co-operation in the fight against cybercrime is an area with many difficulties, especially at international level.

Among the various international co-operation channels available, the engagement with INTERPOL, Ameripol and Europol were described as the most important channels to facilitate cross-border co-operation and sharing of information.

Standards, Organizations, and Technologies

The design, adoption and audit of cybersecurity standards varies significantly across the public and private sectors. Regarding the public sector, there are strict rules that have been converted to standards since 2001 and apply to Federal Administration. There is a system in place for auditing and all federal agencies are required to designate a unit to perform auditing. Furthermore, there is a general controls office that is tasked with designing standards and monitor the progress of all departments in their implementation of these standards. Focusing on the private sector, participants said that the rate of adoption varies between sectors, with finance and electronic communication companies being pioneers in this area. Certain sectors, such as electronic communications and finance, have some mandatory security requirements; however, in the majority of the cases, the driving force for adherence to standards is market demand and business needs. ISO 27001 is the most frequently adopted framework, with the National Institute of Standards and Technology (NIST) cybersecurity framework being considered as well. Focusing on standards in software development and procurement, there are specific guidelines in place for the public sector but the extent to which these guidelines are related to cybersecurity is not clear. Participants acknowledged the need for a security-related authority to set standards across all sectors (not only in the Federal Administration) and to promote adherence to these standards.

Review participants suggested that the Internet infrastructure in Brazil is very resilient. There is a wide range of public and private internet service providers (ISPs) in Brazil, with varying degrees of quality, services and pricing. There are regulations imposed by Brazilian Internet Association (Abranet) but we were unable to interview people from the telecommunications sector in our review. Based on our desktop research, there exist more than 25 Internet eXchange Points (IXPs), which are maintained by an overarching project called IX.br. The number of IXPs ensures an appealing environment for innovation and Internet connectivity, while it increases the resilience of the Internet infrastructure.

Software quality varies significantly in the public sector depending on whether organisations are part of the Federal Administration or not. There is an inventory of secure software for the Federal Administration and networks are monitored for malware. Patching of outdated software is achieved automatically and there are Key Performance Indicators (KPIs) in place to evaluate the effectiveness of the patching mechanisms. State Governments do not have a catalogue of secure software, and patching is not implemented consistently. Regarding the private sector, software quality depends on the size of the organisation, with corporations in the financial and telecommunication sectors being more mature.

The adoption of technical security controls in Brazil varies across sectors and organisations. Participants suggested that the adoption and implementation of controls in government bodies is very advanced within the Federal Administration but elementary and inconsistently promoted in State Governments due to financial restrictions, limitations in human resources and a lack of appropriate organisational structure. There is a strategy for the implementation of controls in the Federal Government which includes a detailed model for assessing the maturity of organisations, but the Federal Government has no control over the states and municipalities. In the private sector, there is an understanding that organisations which are well established adopt adequate technical controls tailored to their networks. Network-segmentation controls and monitoring tools are evident in this sector, as well as the use of Intrusion Detection Systems (IDS) and other Security Information and Event Management (SIEM) tools. Specific organisations have established a CERT to monitor their networks. Of particular concern, however, is the fact that organisations in the private sector are not required to share information about incidents with CERT.br and may not receive threat intelligence.

Brazil has established technical standards for the accreditation of certification authorities (CAs) and registration authorities (RAs), and provides audits for Root CA and its service providers. Participants noted that there are very strict requirements both for Root CAs (Level 5) and CAs who handle Public Key Infrastructure (PKI). In the Federal Government, the Agência Brasileira de Inteligência (ABIN) is the accreditation centre for encryption and provides specific rules on how classified information should be transmitted, the protocol communication for sensitive information (PGP) is used and how data should be stored and handled. Regarding the private sector, similar observations can be made. Encryption is mainly considered for critical systems, both for data in transit and data at rest. We were not able to obtain a clear picture of whether web service providers offer Secure Shell (SSH) connections between servers and web browsers.

There is a wide range of cybersecurity software products developed in-house by the public sector as well as by private companies, which even export these technologies to other countries. Similarly, there is less dependence on foreign cybersecurity technologies. According to participants, the prevalence of hackers in Brazil has resulted in an ever-increasing demand for cybersecurity products. To meet this demand, local companies develop and offer solutions and national security software. An important factor for the established domestic market is the lack of legislation to protect IP; the threat of IP theft makes foreign organisations reluctant to sell their software solutions. The cyber-insurance market offers a range of policies and the demand for these from organisations is increasing. Usually policies detail situations under which the insurance is valid and, on a positive note, specify policies that organisations must adhere to in order to be insurable.

A vulnerability-disclosure framework is in place for the Federal Government. Organisations have established formal processes to disseminate information automatically and the CERT.br receives this information and provides comprehensive reports on how to address incidents. Conversely, private organisations are excluded from the Government's threat-intelligence sharing. Moreover, they are not obliged to report incidents so they tend to conceal any issues that they detect. Considering the fact that Brazil has started to privatise critical parts of the national infrastructure, participants urged the Government to acknowledge the important role played by private organisations in the national cybersecurity strategy, and to grant them access to threat intelligence. There are various means for citizens to report incidents, either via State Police or via websites. Regarding the financial sector, banks in particular provide dedicated channels of communication for customers to report online fraud.

Additional Reflections

This was the 23rd country review, supported directly by the Global Cyber Security Capacity Centre (GCSCC) at Oxford. This review is intended to assist the Government of Brazil to gain insights into the breadth and depth of the country's cybersecurity capacity. This report suggests a number of specific steps by which Brazil's cybersecurity capacity might achieve greater levels of maturity and which might contribute to fostering collaboration between private-owned and state-owned organisations that are part of the CI.

Cybersecurity

Capacity Review

Federative Republic of Brazil

Introduction

At the invitation of OAS, the GCSCC has conducted a review of cybersecurity capacity of Brazil. The objective of this review was to enable Brazil to determine areas of capacity in which the Government might strategically invest, in order to improve its national cybersecurity posture.

Over the period 19–20 March 2018, stakeholders from the different sectors participated in a three-day consultation process. Additionally, we conducted virtual interviews at a later stage. Data collected in 2018 was validated through a similar process in March 2019.

- **Public sector entities**

  - Institutional Security Cabinet of the Presidency (GSI)

  - Computer Security and Incident Response Team of Government Networks (CTIR Gov)

  - Ministry of Defence

  - Brazilian Intelligence Agency (ABIN)

  - National Telecommunications Agency (ANATEL)

  - Ministry of Transport, Ports and Civil Aviation

  - Ministry of Finance

  - Federal Data Processing Service (SERPRO)

  - Social Security Information Technology Company (DATAPREV)
  - Cyber Defence Centre (CDCiber)

  - Brazilian Navy

  - Brazilian National Research and Education Network (RNP)

- **Criminal justice sector**

  - Federal Police

  - Public Prosecutor's Office

- **Finance sector**

  - Caixa Econômica Federal

  - Critical infrastructure owners

  - National Confederation of Industry (CNI)

  - Brazilian Association of Information Technology and Communications Companies

- **Private Sector**

  - Opice Blum Advogados Associados (law firm)

  - Bialer Falsetti Associados (law firm)

  - IBM

  - Concordia Public Affairs Strategies

  - Apura Cybersecurity Intelligence

Dimensions of Cybersecurity Capacity

Consultations were based on the GCSCC Cybersecurity Capacity Maturity Model (CMM),[28] which is composed of five distinct *dimensions* of cybersecurity capacity.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity of each factor. The table below shows the five dimensions, together with the factors of which they are comprised:

Dimension 1 **Cybersecurity Policy and Strategy** (devising cybersecurity strategy and resilience)	**D1.1** National Cybersecurity Strategy **D1.2** Incident Response **D1.3** Critical Infrastructure (CI) Protection **D1.4** Crisis Management **D1.5** Cyberdefense **D1.6** Communications Redundancy

Dimension 2 **Cyberculture and Society**	**D2.1** Cybersecurity Mind-set **D2.2** Trust and Confidence on the Internet **D2.3** User Understanding of Personal Information Protection Online **D2.4** Reporting Mechanisms **D2.5** Media and Social Media
Dimension 3 **Cybersecurity Education, Training, and Skills**	**D3.1** Awareness Raising **D3.2** Framework for Education **D3.3** Framework for Professional Training
Dimension 4 **Legal and Regulatory Frameworks**	**D4.1** Legal Frameworks **D4.2** Criminal Justice System **D4.3** Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 **Standards, Organizations, and Technologies**	**D5.1** Adherence to Standards **D5.2** Internet Infrastructure Resilience **D5.3** Software Quality **D5.4** Technical Security Controls **D5.5** Cryptographic Controls **D5.6** Cybersecurity Marketplace **D5.7** Responsible Disclosure

Stages of Cybersecurity Capacity Maturity

Each dimension is composed of a number of factors, which describe what it means to possess cybersecurity capacity. Each factor presents a number of aspects and for each aspect there are indicators, which describe steps and actions that, once observed, define this specific aspect's state of maturity. There are five stages of maturity, ranging from the *start-up* stage to the dynamic stage. The *start-up* stage implies an ad-hoc approach to capacity, whereas the *dynamic stage* represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **Start-up:** at this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage;

- **Formative:** some aspects have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined – or simply new However, evidence of this aspect can be clearly demonstrated;

- **Established:** the indicators of the aspect are in place, and functioning. However, there is no well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined;

- **Strategic:** at this stage, choices have been made about which indicators of the aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the state's or organisation's particular circumstances; and

- **Dynamic:** at this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances, such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies mid-stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out below, this report presents results of the cybersecurity capacity review of Brazil and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

Methodology – Measuring Maturity

During the in-country review, specific dimensions are discussed with relevant groups of stakeholders. Each stakeholder cluster is expected to respond to one or two dimensions of the CMM, depending on their expertise. For example, academia, civil society and internet governance groups would all be invited to discuss both Dimension 2 and Dimension 3 of the CMM.

In order to determine the level of maturity, each aspect gathers a set of indicators corresponding to all five stages of maturity. In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation, and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions, stakeholders should be able to provide or indicate evidence regarding the implementation of indicators so that subjective responses are minimised. If evidence cannot be provided for all of the indicators at one stage, then that nation has not yet reached that stage of maturity.

The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[29] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that, rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[30] It is this interaction and tension that offers advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[31]

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis is a systematic research methodology used to analyse qualitative data and is applied to the data generated by focus groups.[32] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[33]

There are three approaches to content analysis. The first is the inductive approach, which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[34] The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[35] Dey explains that this process categorises data as "belonging together".[36]

The second approach is "deductive content analysis", which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.

In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or by prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly, these novel categories that offer a refined perspective may be neglected. This is the reason why the GCSCC research team opts for a blended approach in the analysis of our data, which is a mixture of deductive and inductive approaches.

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each factor of the CMM. The GCSCC adopts a blended approach to analyse focus group data and uses the indicators of the CMM as our criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor our recommendations.

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official Government or ministry websites, annual reports of international organisations, university websites, etc.

For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is at a formative stage of maturity, then by looking at the CMM, the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders.

Using the GCSCC CMM methodology, this report presents results of the cybersecurity capacity review of Brazil conducted in March 2018 and March 2019. Data collected in 2019 and 2020 is marked in blue. Each section of the report concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country. Recommendations were revised and lightly edited, taking into account the outcomes of the 2019 validation workshop.

Cybersecurity

Capacity Review

Federative Republic of Brazil

Cybersecurity Context in Brazil

The percentage of individuals using the Internet in Brazil has grown rapidly over the past decade. Specifically, in 2017, 67 percent of the population were using the Internet.[37]

Such increases in adoption has led Brazil to be ranked sixty-sixth on the International Telecommunications Union (ITU) Global ICT Development Index ranking.[38] Moreover, according to the World Economic Forum[39] report (2017-2018), Brazil improved highly in the development of ICT infrastructure. Following two years of falling GDP growth and worsening macroeconomic conditions, Brazil has improved slightly this year, bringing inflation and Government deficits back under control. Brazil's greatest progress comes in the innovation pillar, with upturns in many of the indicators, indicating an enhanced capacity for innovation, more industry-university-business collaboration, a higher quality of research, and better-trained scientists and engineers.

Brazil has one of the largest economies in Latin America, representing 40 percent of Latin America's GDP.[40] According to the "Digital Market Overview: Brazil" report from HM Government,[41] cybersecurity is becoming one of the largest markets in the ICT domain because of escalating cyber-threats in the country.

Broadband investments are important, with a goal to provide broadband coverage in 95 percent of the municipalities by 2018. There also are 4.5G and 5G opportunities with telecommunications companies.

During the last decade, Brazil has witnessed a major increase in Internet access and mobile phone subscriptions with more than half of its population of 200 million people online by 2018. A number of factors relating to Brazil's improvements in social and economic development are driving these trends. Not surprisingly, digital empowerment is also accompanied by additional challenges ranging from mass protest to organised crime. The complex, multi-faceted nature of the "cyber-threat" – and the way it is interpreted in Brazil – has played a significant role in shaping the country's cyber-governance and cyber-security architecture.[42]

Review Report

Overview

In this section, we provide an overall representation of the cybersecurity capacity in Brazil. Figure 2, below, presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; “start-up” is closest to the centre of the graphic and “dynamic” at the perimeter.

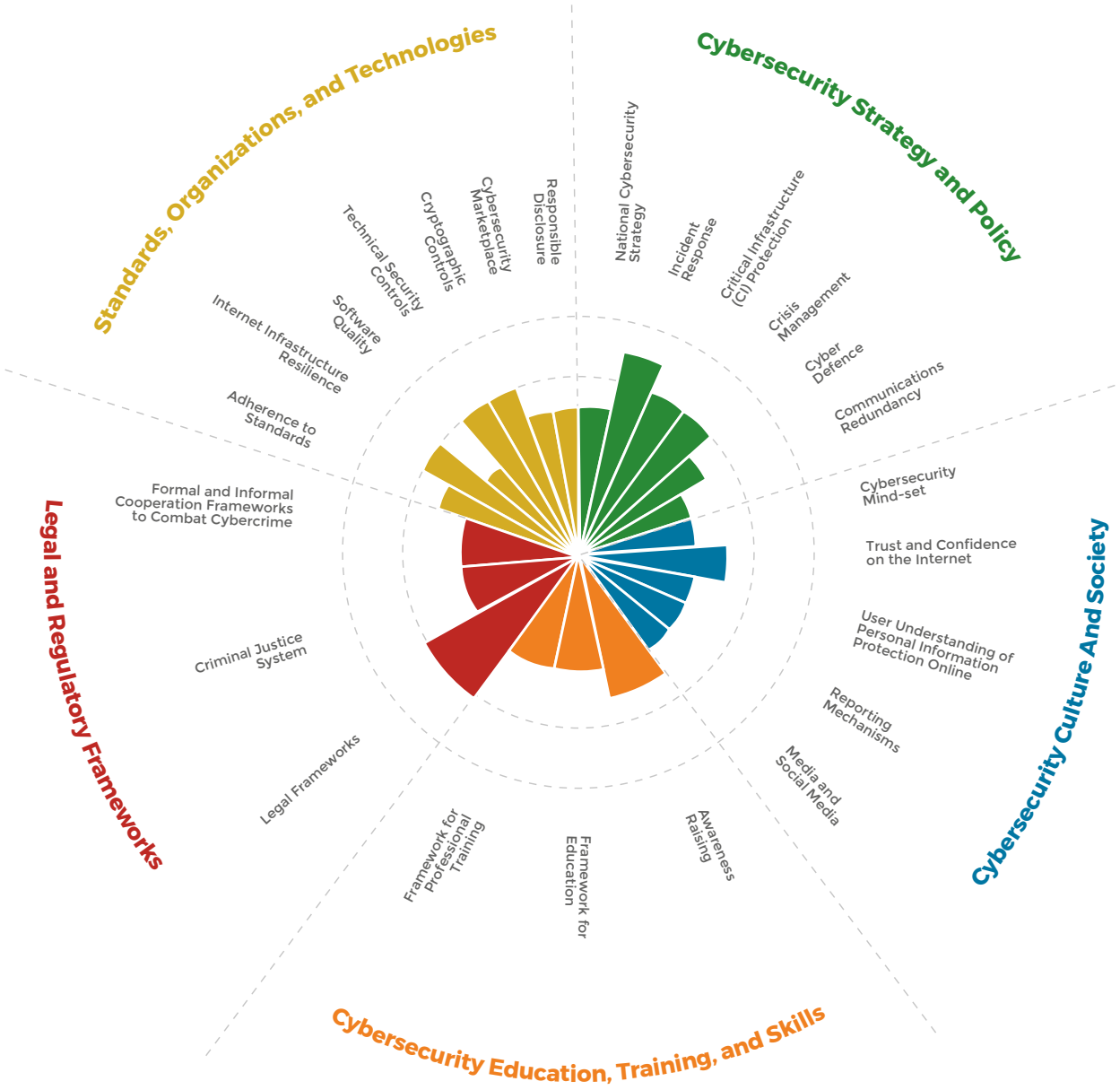


Figure 2: *Overall representation of the cybersecurity capacity in Brazil*

Dimension 1

Cybersecurity Policy and Strategy

The factors in Dimension 1 gauge Brazil's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The dimension also includes considerations for early warning, deterrence, defence and recovery. It considers effective policy in advancing national cyber-defence and resilience capacity while facilitating the effective access to cyberspace that is increasingly vital for government, international business and society in general.

D 1.1 - National Cybersecurity Strategy

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key government and non-governmental cybersecurity actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities

Stage: Formative – Established

Processes to support the development of a cybersecurity strategy were initiated in Brazil in 2010 with the "Plano Brazil 2022",[43] a document detailing the strategic plan for Brazil until 2022. Digitalisation of the economy, freedom of speech on the Internet and the protection of the right of public access to the Internet were key objectives of the plan, the success of which depended on developing a cybersecurity strategy. The first attempt for such a strategy was the Green Paper on Cyber Security in Brazil,[44] a document approved by the Government that provided guidance on cybersecurity-related issues for the state. The need for a cybersecurity strategy was also highlighted in the Ministry of Defence's National Strategy of Defence,[45] where cyberspace is recognised as a fundamental element of the Brazilian military function. Despite the importance of cyberspace, the defence strategy did not elaborate on how cybersecurity can be integrated into a national strategy. The culmination of these two initiatives was the *Estrategia*,[46] a broader framework of strategic planning for the Government of Brazil. Despite all these efforts, at the time of the review in March 2018, there was no official national cybersecurity document, approved by the National Congress that detailed how to establish co-ordination between key cybersecurity governmental and non-governmental actors.

The lack of collaboration between governmental institutions and the private sector, and the "fragmentation of responses", were potentially addressed with the *Estrategia* (2015–2018). The aim of the *Estrategia* was to provide the strategic guidelines for information and communications security and to co-ordinate these efforts between the various actors involved in order to mitigate risks to which organisations and society are exposed.[47] It provided the main principles to be followed, clear strategic objectives (inter alia, education of personnel and awareness-raising of cybersecurity issues, institutionalisation of cybersecurity policies, research and innovation in cybersecurity technologies, and strong security controls for CI stakeholders), actions to achieve these objectives and the institutions responsible for implementing these actions within predetermined timeframes. The strategy focused on the FPA of Brazil, which covers 29 Ministries, 6,000 public bodies, more than

1,000,000 employees, 320 digital networks and 12,000,000 websites.[48] Critics of the strategy highlighted the absence of a central authority to implement such a systematic and multi-stakeholder approach.[49]

At the time of the review in March 2018, participants explained that the cybernetic community, under the Ministry of Defence and Information Security, was the entity in charge of cybersecurity in the FPA. Therefore, an internal inter-ministerial group of more than 15 ministries of the FPA, with the assistance of a technical committee comprised of members from the Cabinet of Institutional Security, was tasked to draft the Estrategia document. The document was forwarded to 98 organisations including members of academia, national confederations, entities from the financial sector, CI stakeholders, software-engineering companies and private ISPs. As participants noted, more than 200 meetings and events have taken place thus far to further refine the document before it was forwarded to Parliament for approval. It is worth noting that in our review, we could not corroborate the participation of private organisations with people who work in the private sector.

Critics, however, emphasised the absence of civil society organisations, Internet stakeholders and the general public from this multi-stakeholder group.45,During our review, participants further emphasised the absence of private sector organisations that should be considered part of the CI but are, at the moment, neglected by the FPA. Rapid developments in e-governance, smart cities and innovative ICT solutions in Brazil have created the groundwork for fruitful discussions and collaboration between a wide range of stakeholders including civil rights organisations, the private sector and the Government. Currently, the debate for cybersecurity-related issues involves governmental officials, the armed forces, law enforcement, a handful of private institutions, public CIs and a small number of academic institutions. Participants suggested that extending the range of stakeholders which participate in shaping the national cybersecurity strategy, by including civil society and private organisations, will reassure the community that the strategy offers a balanced approach to cybersecurity and will help alleviate fears of failing to mention and protect human and civil rights.

Regarding the organisation of the cybersecurity programme, participants expressed their preference for a decentralised model, where commercial sectors will be overseen by existing regulatory agencies, with a newly established national agency to co-ordinate efforts. Participants suggested that the proposed model is inspired by the EU's approach, where the European Union Agency for Cybersecurity (ENISA) holds the central role in unifying and co-ordinating efforts across countries. The participants' opinion was informed by the current structure of Brazil, where multiple autonomous states exist, but the FPA has responsibility over critical processes in all states. Participants indicated that the size of the country hinders co-ordination between the states and that the key to a successful strategy is to enhance collaboration across all relevant public, federal, and private stakeholders without centralising responsibilities and initiatives.

Finally, the national cybersecurity strategy describes a generic framework of critical actions to implement the main objectives. However, as participants explained, this framework provides the mandate to authorities to design actions and details the deadlines for the main objectives. This is due to the fact that the strategy itself must be concise, be voted on by Congress, and will not be updated regularly. A more elaborate strategy with specific actions would require more political liaison.

Results from the validation process conducted in March 2019:

During the March 2019 validation focus-group interviews, the participants informed the researchers of the National Information Security Policy (Política Nacional de Segurança da Informação) published in a form of the presidential decree (No. 9.637) in December 2018.[50] The policy served as a foundation for the National Cybersecurity Strategy which was published in 2020.[51] The outline of the National Cybersecurity Strategy was elaborated on in the National Information Security Policy.[52] This policy promised an inclusive drafting process involving the participation of the multitude of stakeholders;[53] private sector has reportedly already been consulted.

Government feedback provided in 2020:

Following the validation focus-group interviews conducted in March 2019, the National Cybersecurity Strategy (Federal Decree No. 10.222) was finally adopted in February 2020.[54] The Decree "creates centralised governance model at the national level to promote co-ordination among different actors related to cybersecurity, establish a national cybersecurity council, and encourage internal cybersecurity compliance checks on public and private entities."[55] Furthermore, it "requires the notification of cybersecurity incidents against critical infrastructure to the Brazilian Government Response Team for Computer Security Incidents."[56] According to government sources it focuses on ten strategic actions that should guide the FPA to devise its own actions towards cybersecurity. The new developments (since 2018) with regards to Brazil's cybersecurity strategy indicate a "Formative to Established" stage of maturity.

Similarly, it was clarified that according to Article 10 of the Law No. 13.844 (June 2019) the co-ordination and supervision of information security activity within the scope of the FPA is the responsibility of the Institutional Security Office of the Presidency of the Republic.[57] While cyber-defence actions fall under the authority of the Ministry of Defence.

D 1.2 - Incident Response

This factor addresses the capacity of the Government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the Government's capacity to organise, co-ordinate, and operationalise incident response.

Stage: Established – Strategic

There are a multitude of Computer Security Incident Response Teams (CSIRTs), which range from government entities to private sector and academic institutions. Figure 3: Number of CERTs in Brazil illustrates geographically where CERTs are based in Brazil. Depending on the role of a CERT, these entities may be involved exclusively in managing the security of systems, enforcing cybersecurity guidelines or be responsible for co-ordinating efforts between national authorities and local levels. Internet-service initiatives are co-ordinated by the CGI.br and its executive branch, NIC.br. These two authorities oversee the operations of the national CERT.br, which is certified by FIRST and is responsible for handling incident reports for the private sector. Another institution, CTIR Gov, also acts as a CSIRT at the national level by providing incident response for the FPA while there are CERTs dedicated to specific sectors and CI stakeholders. Finally, there is a military

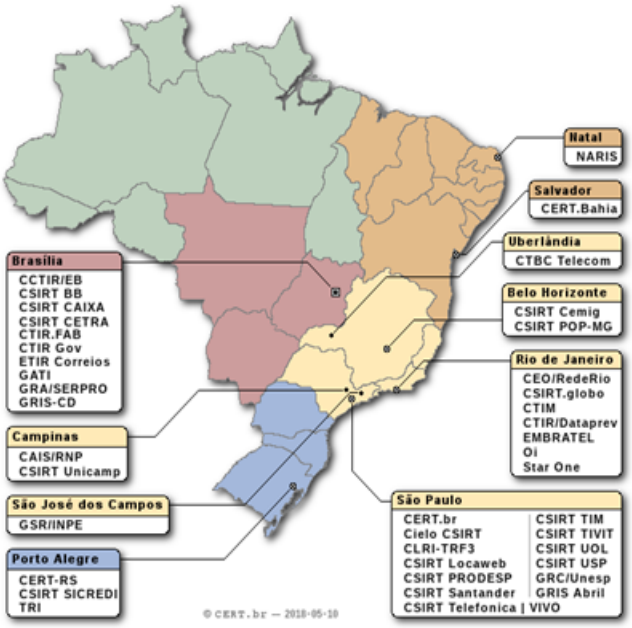


Figure 3: *Number of CERTs in Brazil*[58]

All these institutions have clear guidelines and roles regarding incident response and their maturity in this factor is at the established level, with certain indicators from the strategic level being present. The CERT.br holds the register for national incidents and publishes statistical data of threats and incidents on an annual basis. Similarly, CTIR Gov conducts the same activities for the FPA and also provides alerts and recommendations on its website (https://www.ctir.gov.br/). The classification schemes used for incident-handling are constantly updated to capture novel attacks and to share knowledge gained from these attacks more efficiently. Furthermore, all incidents are automatically incorporated into a database which supports business intelligence (BI) software. As suggested by the participants, this software uses visualisations to allow high-ranking officials to have access to relevant

information “with a single click”. Participants mentioned that when a national incident occurs, both the public and private sectors are involved in response procedures. There is also support from ABIN, which is the intelligence agency, as well as the Federal Police.

All CERTs provide reports to the CERT.br through official channels. Automated systems following international standards, such as STIX and Traffic Light Protocols (TLP), ensure that threat intelligence is shared to CERTs that collaborate with the national CERT. These systems also facilitate communications with international CERTs. Participants mentioned, however, that for bureaucratic reasons, the use of email is preferred for unofficial exchanges of threat intelligence with international partners. The CERT.br is a member of the FIRST community and frequently participates in events hosted by FIRST and the OAS.

Despite the automated systems in place, participants suggested that the response time from receiving intelligence, understanding the information and acting on it could be improved if CERT employees attended events and collaborated more closely to foster trust. Current legislative efforts focus on streamlining the sharing of threat intelligence between all CERTs, since not every private CI stakeholder is entitled to receive threat intelligence. Because the range of CI stakeholders is broadening and the sharing of trustworthy information is more complex, there is a need for major participation by research institutions. There are initiatives aimed at providing CERTs with better situation awareness, and with artificial intelligence utilised by various tools to provide insights based on correlation of events.

Regarding public CERTs, each of these is required to create a technical team to handle incidents and has clear instructions and policies on how to respond to different situations. Established points of conduct and specific procedures for preserving and storing evidence also exist. There are innovative systems in place to identify hacking activities, search for conversations on the dark web, prevent attacks of webpages and capture, in real-time on social media, content relevant to evolving attacks. Finally, two major projects funded by the national CERT aim to increase the capability of incident detection, event correlation and trend analysis (a “distributed honeypots” project), and to obtain details of spamming activity (“SpamPots”). For the needs of these projects, the CERT.br has established honeypots in more than 10 countries and frequently produces reports and academic publications with analyses of the data.

SERPRO, one of the largest government-owned corporations of IT services in Brazil, operates a CERT that has institutionalised incident-response procedures. These comprise a team responsible for network-level co-ordination, a team tasked to conduct penetration testing and another one performing network hardening. There are state-of-the-art laboratories for malware analysis and systems in place to sanitise networks, to act proactively by anticipating events and to predict vulnerabilities. Furthermore, there are internal processes for risk analysis, and maturity models to indicate how effectively an incident is being handled. SERPRO also maintains a direct telephone line that links several government bodies. In addition, there is an email group for public administration authorities and a discussion group where incidents are analysed. Finally, intelligence on hacking activities is gathered by SERPRO experts who have infiltrated hacker forums around the world.

Regarding education, there is a wide range of courses offered by CERTs as well as a number of awareness campaigns aimed at informing citizens. The CERT.br offers professional training programmes certified by CMU CERT, and methodologies proposed by FIRST. There is also a portal to promote best practices for system administrators[59] and a guidebook on

how Internet users can protect themselves online.[60] SERPRO also offers best-practice seminars, technical courses for CERT analysts, and holds weekly events to educate users about contemporary threats and fake news.

Results from the validation process conducted in March 2019:

Brazil has opted for a decentralised structure of incident response capacity. The co-ordination role among the 42 CERTs[61] in Brazil is entrusted to the CERT.br.[62] The latter is also responsible for co-ordinating international incident response activities.[63]

In addition to this, CERT.br is responsible for fostering the co-operation among the members of the national network of CERTs. Accordingly, CERT.br assists newly-established CERTs to develop their incident-handling capacity through various meetings, training, and presentations at conferences. It also organises the annual CSIRTs Forum (Fórum Brasileiro de CSIRTs) and specialised courses (e.g. "Overview of Creating and Managing CSIRTs", "Fundamentals of Incident Handling", "Advanced Incident Handling for Technical Staff" etc.) in Brazil[64] as overseas.[66] CERT.br's international engagement also includes its partnership with the Carnegie Mellon University's Software Engineering Institute (CMI CERT), and the Anti-Phishing Working Group as well as its role as co-ordinator for the SpamPots project, gathering and analysing data on the abuse of the Internet infrastructure by spammers from low-interaction honeypot sensors in 11 countries.[66]

Government feedback provided in 2020:

Following the validation focus-group interviews conducted in March 2019, it was clarified that Brazil has more than one CSIRT for its national operations: CTIR Gov and CERT.br. CTIR Gov co-ordinates activities related to the prevention, handling and response to cyber incidents related to the CSIRTs of the FPA. Also, each FPA entity must have its own CSIRT and IT body responsible for such interference. CTIR Gov, being a CSIRT of national responsibility, also handles requests for international co-operation on cyber incidents. CERT.br, on the other hand, is a body certified by FIRST and is responsible for the private sector. It should be noted that due to the collaborative nature of the work, in practice, the boundaries of competence between the CSIRTs is not strict in order to avoid jeopardising the prevention, handling and response to cyber incidents.

D 1.3 - Critical Infrastructure (CI) Protection

This factor studies the Government's capacity to identify CI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

Stage: Established

The maturity of Brazil's capacity to protect critical infrastructure differs between public and private CI stakeholders. Participants suggested that for publicly-operated segments of the CI, the Institutional Security Cabinet of the Presidency (GSI), in collaboration with the Ministry of Defence, has a detailed list of CI assets and performs audits on a regular basis. Risk assessments consider the impact of attacks on CI assets for national defence. All federal institutions are required to conduct internal cyber-risk assessments, which are updated annually based on lessons learnt from large incidents.[67] It was noted that the website of the Information Security Department (DSI) of GSI (http://dsic.planalto.gov.br) also gathers all national legislation regarding information security. Public CI stakeholders include telecommunication companies, transport, energy and financial institutions, all of which co-operate and co-ordinate through formal channels of communication with the Ministry of Defence. There are clearly defined policies and procedures in place for all public institutions to follow based on information provided by the national CERT's situational-awareness tool. Access to such information is provided to the Federal Police and to intelligence services to increase co-operation and incident handling among CI stakeholders. All protocols, procedures and risk assessments are annually assessed by a cyber-defence working group. This group has members from the management level chief information officers (CIOs), as well as technical members, and has identified processes on how to incorporate lessons learnt to enhance the protocols and systems currently in place. Participants commented on the oxymoron that lessons learnt are based on major incidents that helped to refine significantly the current protocols: the lack of a major incident over the last couple of years has hindered the constant refinement of these protocols.

Participants reported that at the moment, the private sector is not considered part of the country's CI. Since Brazil has endorsed privatisation in critical sectors such as finance, it is imperative that the list of CI stakeholders is revised to consider private institutions. Private institutions are under no obligation to inform the Government of a major incident, are restricted from obtaining access to threat intelligence and are oblivious to risk assessments and processes that the Government has in place for public CIs. They therefore need to develop their own internal risk assessments and security policies, the effectiveness of which will depend upon the degree of their maturity. Well-

established organisations have the resources to develop their internal cybersecurity policies, but participants expressed concerns for the capacity of SMEs and of the majority of organisations in the private sector in general.

A characteristic example of an important stakeholder being overlooked is SERPRO which is currently not considered part of the CI. As participants noted, all risk assessments are conducted from a business perspective and do not consider the impact on national defence. There are internal indicators and measures for SERPRO's incident-handling which are either corporate or related to its Government customers. Incident reports with confidential content are provided to customers. There are performance indicators to denote the effectiveness of processes such as the number of incidents handled, the number of incidents categorised and those handled outside of the accepted timeframe. When SERPRO decides that present threats may impact the company, and if there is a possibility of that incident affecting services or assets of the Government, then there are clear policies and directions on how to escalate these events to governmental authorities and to the Federal Police. In 2010, SERPRO drafted a book detailing strategies and policies on CI protection, but these are not followed in practice. Despite the fact that SERPRO has clear processes on how to report incidents and protocols to deal with situations and provides assistance to private organisations that should be considered as part of CI (such as financial institutions), participants emphasised that information security is like hygiene and cannot be implemented in isolation. Public CIs, albeit advanced in maturity, will be influenced by attacks that target weaker private institutions. Therefore, despite the clear differences in competence and cyber-capabilities between the public and private sectors, it is important that institutions enhance their co-ordination so as to increase maturity in the private sector.

The majority of the participants urged the Government to create a mechanism to identify the level of maturity in IT governance in both the public and the private sectors, a protocol of communication to distribute alerts across public and private sectors and an initiative to evaluate norms and standards which private and public organisations possess. It was acknowledged, however, that in the draft version of the national strategy these issues are potentially addressed. Specific actions are in place to identify CI assets in the private sector and to create formal channels of communication between all CI stakeholders.

Finally, participants would welcome the opportunity to collaborate closely with other countries and to impose responsibility on foreign governments for the damages that their hackers cause to Brazil. This is the reason why Brazilian CERTs strive to identify vulnerabilities globally. It was emphasised in our review discussions that closer co-operation with the OAS through the establishment of a threat-intelligence platform amongst the OAS countries should be the next step. The biggest obstacle for wider threat intelligence amongst countries is the lack of trust between them. Revealing vulnerabilities of national networks to other countries becomes intelligence that could potentially be acted upon. Therefore, a protocol of information exchange that will not create discomfort to countries needs to be agreed, in order to foster trust in the OAS community.

Results from the validation process conducted in March 2019:

In November 2018, Brazil published its National Critical Infrastructure Security Policy (Política Nacional de Segurança de Infraestruturas Críticas), which lays the groundwork for the Critical National Infrastructure Strategy and Critical National Infrastructure Plan.[68]

Participants in the 2019 CMM review-validation focus-group interviews noted that the presidency of the federation has done some prioritisation within the critical national infrastructure based on their vulnerability and impact although this does not seem to be reflected in official documentation. Nevertheless, it is understood that these documents, outlining a nationwide strategic direction to critical infrastructure protection, will provide for a more inclusive approach and thus address the issues surrounding the exclusion of private critical infrastructure operators observed during the CMM review in 2018.

As a matter of fact, some developments towards the inclusive approach to the CI protection have already been observed. Cyber Guardian, exercises which are mentioned in the following section of this report, involved not only Government and the military but also several private CI operators. Participants in the CMM review-validation interviews emphasised the "immense value" of such networking opportunities between the Government and private CI operators.

D 1.4 - Crisis Management

This factor addresses crisis management planning, addresses the conducting of specialised needs assessments, training exercises and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation as well as inform budgetary allocations.

Stage: Established

Over the last decade, Brazil has hosted a series of important events, inter alia the Pan American Games in 2007, the visit of the Pope in 2013, the FIFA World Cup in 2014 and the Olympic Games in 2016. Cybersecurity was a critical element for crisis management throughout these events and more than 40 organisations (including Rio CERT, SERPRO, the national CERT and CTIR Gov) were responsible for handling and mitigating incidents. The Cyber Defence Centre (CDCiber), a unit responsible for co-ordinating strategic and operational aspects of Brazil's cyber-defence architecture, oversaw the crisis-management procedures during these major events and co-ordinated with the Ministry of Defence and GSI.

As expected, Brazil experienced several cybersecurity issues during these major events. Two of the most significant incidents were multiple DDOS attacks that ranged from 300GB per second to 1TB per second, and a sabotage incident that destroyed the cable providing Internet access to the FIFA World Cup network. All events were handled efficiently and a return to normal activity was achieved within the approved service-level agreement. Participants explained that the incident-handling processes during these events demonstrated that organisations critical for cyber-defence are capable of collaborating and effectively mitigating the impact of such attacks. Organisations that participated in crisis management had clear roles, there were transparent protocols on how to disseminate information and escalate incidents, and specific guidance on how to protect systems. However, crisis-management processes were tailored to these specific events.

Participants expressed the opinion that major events obliged organisations to co-operate and helped to foster trust within Brazil's cybersecurity community. As an example of how trust is an important element in threat-intelligence sharing, participants mentioned the "wannacry" attack, which had minimum impact on the majority of organisations in Brazil. This was due to the fact that organisations shared information to their trusted peers fast, by issuing alerts and providing details on how to respond that were deemed trustworthy and actionable by all.

It was suggested during the review that the experience and lessons learnt from these events should underpin current efforts in crisis management. Crisis-management protocols should be designed and a network of public and private organisations should be created to handle major events. Training and exercises on simulated crisis events were suggested as the optimal way to validate communication protocols, to increase cybersecurity awareness and to test incident-handling processes. Towards this end, participants mentioned the Cyber Guardian exercise, which uses high-level planning to devise scenarios and simulation platforms for cyber operations that can emulate critical systems from the finance, nuclear and public sectors. Crisis situation exercises take place frequently and mainly involve military and Government systems. These exercises are also combined with physical simulations. Participants mentioned that an exercise that will include the financial sector and nuclear systems will be conducted soon. They further pointed out that more organisations need to take part in these exercises, including civil society.

Results from the validation process conducted in March 2019:

In 2019, the validation workshop largely confirmed the outcomes of the 2018 CMM report.

D 1.5 - Cyber Defence

This factor explores whether the Government has the capacity to design and implement a cyber defence strategy and lead its implementation, including through a designated cyber defence organisation. It also reviews the level of co-ordination between various public- and private-sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Stage: Formative – Established

Regarding cybersecurity governance, the Brazilian Government has assigned the political and strategic level to the GSI and the strategic, operational procedures and cyber defence to the Ministry of Defence. In recent years, the military has been restructured to fit the needs of an evolving democratic system, with focus on emerging cross-border threats and internal security events. According to secondary sources, the armed forces are regarded as the most trusted national institutions and have been tasked with crisis management for major civilian events.[69] They have therefore acquired government funding to lead the development of the nation's cyber-defence capabilities.

An official cyber-defence document was published in 2012 giving guidelines on cybersecurity policies. The military operates a CERT and provides training for risk management and incident response. There is a dedicated unit that specialises in planning and conducting cyber operations.[70] The same unit is responsible for co-ordinating with the Ministry of Interior, as well as with the intelligence services, the Federal Police and SERPRO, through formal and well-established channels of communication.

Participants suggested that the military possesses both offensive and defensive capabilities and focuses on the enhancement of defensive measures. They indicated that the military deploys systems that provide situational awareness and proactively defend against DDOS attacks and web defacement. There are laboratories to analyse malicious software, with a significant number of personnel being trained to execute these tasks. There are tools in place, such as BI, to facilitate cyber risks assessments and analyse the results. Finally, there are cyber exercises that take place frequently and for the next iteration, the military will invite private organisations to participate.

Results from the validation process conducted in March 2019:

In 2019, Brazil still had no dedicated cyber defence strategy; when adopted, one of the main elements of the National Information Security Strategy will be cyber defence.[71] Strategic directions for cyber defence are already being drafted by the Ministry of Defence and future consultations will reportedly include the private sector. Relevant strategic directions are currently outlined, briefly, in the National Defence Strategy (Estratégia Nacional De Defesa).[72]

D 1.6 - Communications Redundancy

This factor reviews the Government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Formative

It was not possible to obtain a comprehensive view regarding communications redundancy in the course of the CMM review. Participants suggested that the public sector has emergency-response assets hardwired into the national strategy's emergency communication network. There are appropriate resources available to evaluate the current protocols in place for redundancy, to test redundant systems, to conduct exercises and to perform communication drills. Multiple crisis centres are designated in dispersed geographical locations to ensure the participation of all stakeholders in the event of an emergency. In stark contrast, the private sector is neglected and is excluded from these plans, with the exception of a small number of private CERTs.

As participants explained, there are secure telephone systems between the national CERT and CSIRTs, and international standards are followed for the use of email and other methods as redundancy procedures for communication. However, the absence of the private sector from the emergency communication network remains problematic. It is important to obtain an holistic picture of the maturity of private CI stakeholders which support critical processes in national communication networks. There is a need to legislate requirements for ISPs to have redundant emergency response assets and to run stress tests for network availability frequently.

Results from the validation process conducted in March 2019:

Since 2018, the situation in Brazil has not changed drastically. According to a participant from the 2019 CMM review-validation workshop, "Brazil still needs to do more to establish proper communications redundancy measures."

Recommendations

Following the information presented during the review of the maturity of *cybersecurity policy and strategy,* the GCSCC has developed the following set of recommendations for consideration by the Government of Brazil. These recommendations provide advice and steps aimed at increasing existing cybersecurity capacity as per the considerations of the Centre's CMM. The recommendations are provided specifically for each factor.

National Cybersecurity Strategy

R 1.1
Design a complementary to the strategy document which will be aligned with national goals and risk priorities, to provide actionable directives with corresponding metrics to monitor progress of the implementation of the strategy;

R 1.2
Ensure that the stakeholders involved in the design of the national cybersecurity strategy include private-sector organisations that should be part of the CI (especially finance, energy, telecommunications, transport, SERPRO, Empresa de Tecnologia e Informações da Previdência Social (Dataprev), SMEs), civil society, academia and international partners;

R 1.3
Enhance collaboration with OAS and develop a common taxonomy for cybersecurity; and

R 1.4
Ensure that the information security standards developed by FPA are the minimum standards to be adopted for the public state authorities, and that its implementation is included into the national cybersecurity strategy programmes.

Incident Response

R 1.5
Establish a central national incident intelligence database which will include incident information from all the sectors. Assign CERTs for every critical sector (i.e., finance, telecommunications, Government, military, oil and gas etc.) with the responsibility to disseminate information tailored to the needs of the corresponding sector;

R 1.6
identify organisations in the private sector that are key to national cybersecurity and provide them with access to the information shared by national CERT;

R 1.7
obtain a consensus among stakeholders (especially from the private sector) on architecture, interfaces and standards for information exchange. Common standards promoted, for example, by the EU and the US, are STIX and TAXII. Stakeholders should include private and public sectors, as well as the cybersecurity community at national, regional and international levels;

R 1.8
establish metrics to monitor and evaluate the effectiveness of all CERTs. In addition, enhance collaboration between OAS, regional CERTs and other international bodies;

R 1.9
establish regular training for the employees of all CERTs and design metrics to assess the results of this training. Courses offered by the national CERT, the military CERT and SERPRO can underpin training for the other CERTs; and

R 1.10
identify and document key incident response processes highlighting when and how different ministries, the state government and private organisations should be involved.

Critical Infrastructure (CI) Protection

R 1.11
Develop and conduct a national risk assessment aiming to identify CI stakeholders and national threats with specific focus on private-sector organisations;

R 1.12
develop and disseminate a list of CI assets with identified risk-based priorities that will include assets from the private sector;

R 1.13
establish a mechanism for regular vulnerability disclosure and information-sharing between private and public CI asset owners and the Government. Establish regular dialogue between tactical, executive and strategic levels regarding cyber risk practices and encourage communication among CI operators;

R 1.14
identify internal and external CI communication strategies with clear points of contact that will include the private sector;

R 1.15
establish information protection and risk management procedures and processes within CI, supported by adequate technical security solutions, which inform the development of an incident response plan for cyber incidents;

R 1.16
establish common procedures to measure and assess the capability of CI asset owners to detect, identify, respond to, and recover from cyber threats;

R 1.17
mandate the design and implementation of appropriate regular cyber risk assessments for all CI stakeholders and identify the required information to be shared. Design cyber risk assessments for all CI stakeholders based on the national risk assessment approach; and

R 1.18
task regulators for every sector to mandate disclosure of incidents. Set thresholds for incident disclosure after consultations with private and public organisations from the respective sectors.

Crisis Management

R 1.19
A realistic high-level crisis scenario should inform a plan to test information flows, decision-making and resource investment at the national level;

R 1.20
develop Specific, Measurable, Attainable, Relevant, and Time-Bound (SMART) objectives and performance key indicators (PKI) to guide the decisions in crisis management;

R 1.21
ensure that the evaluation results of the previous two Cyber Guardian exercises inform future investment in national cybersecurity capacity and that the findings are evaluated against international crisis management good practice; and

R 1.22
tailored, sector-specific reports of crisis management exercises should be prepared for each stakeholder.

Cyber Defence

R 1.23
Ensure the development of a cyber-defence component in the national security strategy. This component should consider the threats to national security that might emerge from cyberspace;

R 1.24
assess and determine cyber defence capability requirements, and involve public and private sector stakeholders. Conduct continuous reviews of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives; and

R 1.25
design national cyber exercises that will involve a range of organisations from the private sector.

Communications Redundancy

R 1.26
Test the inter-operability and function of emergency response assets under compromised communications scenarios to inform strategic investment in future emergency response assets. Ensure that the private sector is considered as a key stakeholder in the emergency response plan;

R 1.27
establish a process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response asset communications and authority responsibilities;

R 1.28
connect all emergency response assets into a national emergency communications network with isolated but accessible in emergency situations backup systems;

R 1.29
establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities for redundant communications protocols tailored to the roles and responsibilities of each organisation in the emergency response plan; and

R 1.30
include cyber elements within existing emergency and crisis exercises and identify metrics to evaluate the success of the exercise. Evaluate the exercises and feed the findings back into the decision-making process.

Dimension 2

Cybersecurity Culture and Society

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including Internet users. The days when cybersecurity was left to experts formally charged with implementing cybersecurity have passed with the rise of the Internet. All those involved with the Internet and related technologies, such as social media, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of users in achieving cybersecurity but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, an important aspect of cybersecurity culture and society is an awareness among cybersecurity experts that they need to build systems and programmes for users – systems that can be used easily and can be incorporated into everyday practices online.

This dimension reviews important elements of a responsible cybersecurity culture and society, such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. This dimension also entails the existence of mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this dimension reviews the role of the media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D 2.1 - Cybersecurity Mind-Set

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society at large. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Formative

The Government has recognised the need to prioritise cybersecurity across its institutions. Also, aspects of governmental processes and institutional structures have been designed in response to risks to cybersecurity, but they are primarily lodged in particular leading agencies. Overall, participants noted that the security culture in Brazil varies across different parts of the country and different sectors of government, business and industry. All ministries have CISSP-certified employees and also, different agencies cover ICT management needs and establish requirements regarding software.

The President of the Republic Office has its own IT office which provides everything from software to personal computers, so the administrative support is centralised. As participants mentioned, within the federal government, resources are allocated to the training of employees managing security issues, towards efforts for compliance with ISACA and frameworks such as ISO 270001, and towards compliance with best practices related to information security that have been identified by the Government. Moreover, an auditing system is being applied within the federal government. All agencies have a department which is responsible for auditing. In 2017, a programme of auditing visits was carried out, to assess the level of maturity in 40 different agencies.

Participants were concerned by the complexity of the Government structure in Brazil. As the maturity of the public sector currently assessed, it is recognised that there will be varying stages of maturity within and across different departments. However, the federal government has limited control or influence on the state governments and municipalities.

Another concern raised by participants is the lack of a co-ordinating mechanism to identify and address inadequacies of maturity in government. As suggested, a protocol for the distribution of alerts, similar to those used by a CERT, is lacking and an integrated communication channel to evaluate the norms and the standards being followed is also needed.

DSI is the Information Security Department and can administer information security for the public sector in general. However, there are independent government departments and independent sets of guidelines. As examples, participants mentioned, among others, Serviço Federal de Processamento de Dados (Federal

Data Processing Service) and SERPRO,[73] which is a public administration unit responsible for providing IT services to the Ministry of Finance. Regulations and standards are obligatory for SERPRO because it belongs to the Government. However, state-owned agencies are not obliged to follow these rules, creating a need for the federal government to persuade state and local agencies to adopt cybersecurity initiatives.

Leading firms within the private sector have begun to place higher priority on a cybersecurity mind-set by identifying high-risk practices. Participants noted that among the barriers to developing a digital sphere are the high cost of implementation and a lack of clarity in return of investment, as well as the lack of well-understood norms and regulations, the lack of technical standards, and the need for education and training in this area.

The finance and IT sectors are relatively more advanced in cybersecurity, due to the fact that they are frequent targets of attacks. They therefore invest more in cybersecurity and could show other agencies how to adopt safer practices. Participants informed us that since central banks began to take proactive security measures, cyber-criminals have focused more on regional banks and SMEs.

A limited but growing proportion of Internet users have begun to place a higher priority on cybersecurity, such as becoming more aware of risks and threats. Society as a whole still lacks a cybersecurity mind-set. Internet users might be increasingly aware of cybersecurity risks, but they seldom act accordingly in their everyday practices. It was mentioned that it is common even for IT experts, who are arguably most aware of risks, to still click on phishing emails, or share sensitive information on social media sites such as Facebook. Also, in low-income districts, citizens tend to be dependent on the use of mobile phones in order to connect to Internet, in spite of the fact that the Government provides satellites for these communities for Internet connection. Raising awareness of the risks for these communities is an important need.

Overall, participants stressed the need for more awareness and education at all levels within all sectors.

Results from the validation process conducted in March 2019:

In 2019, interviewees noted that there has been some progress in cybersecurity mind-set maturity over the past year. In spite of this, some argued that issues with phishing and other similar cyber incidents persist, indicating that cybersecurity good practices are not widely employed by Government officials.

Representatives of the private sector reported that the main issue among their employees is the lack of cybersecurity awareness, especially related to the protection of personal data. “People share everything online,” the researchers heard during one of the group interviews in March 2019. Nevertheless, a cybersecurity mind-set in the private sector continues to grow and an increasing number of businesses a cybersecurity mind-set a priority. Similar observations can be made about the cybersecurity mind-set among the the Internet users. Although the cybersecurity mind-set in Brazilian society is still limited and people regularly disregard good practices, especially when it comes to sharing personal content online, secondary sources indicate that a limited proportion of internet users do place priority on cybersecurity in their daily lives. For example, nearly half of Brazil’s Internet users avoid clicking on unsolicited links in messages and more than a third of them makes use of the privacy settings offered by various online platforms. Additionally, almost half of Brazilian Internet users use antivirus software although only a quarter of them change their passwords regularly.[74]

D 2.2 - Trust and Confidence on the Internet

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Stage: Formative – Established

Overall, participating stakeholders believe that a small proportion of Internet users critically assess what they see or receive online. Similarly, few believe that they have the skills to use the Internet and to protect themselves online. Moreover, a limited proportion of users trust the security of the Internet and are not aware of ways to determine the legitimacy of a website.

E-government services have been developed, and a growing proportion of users trust in the security of these services. However, possible breaches in e-government services are being identified, acknowledged, and disclosed in an ad-hoc manner.

Currently, the Brazilian Government offers several government services to the citizens. Among the main ones are[75]:

- Federal Revenue – services for the collection of income tax, the taxpayer's tax situation, Cadastro de Pessoas Físicas (CPF) and Cadastro Nacional da Pessoa Jurídica (CNPJ) registration, and statements, among others;

- Federal Police – services such as passport applications, statements of criminal records, support for international adoptions, among others;

- Integrated System of Financial Administration of the Federal Government (SIAFI) – interests linked to the National Treasury national treasure, such as provision of public expenditure;

- Poupa Tempo (State of São Paulo) – access to information about public services, such as document requests and starting and closing businesses;

- OntoJuris Project – provision of information about legislation in the area of intellectual property rights, consumer rights and electronic law; and

- Public System of Digital Bookkeeping (SPED) – presents the promotion of tax information submission, rationalisation and standardisation of accessory obligations for taxpayers.

Services such as the sending of the Statement of Income Tax, information about social security and Government procurement have been available via the Internet since 1998 but these are largely information provision versus service delivery. In the year 2000, the Policy of EGovernment was defined and instituted and the Information Society Programme was launched, thus consolidating and disseminating egovernment strategies, the social importance of digital inclusion as well as actions related to information technology in the country, such as creating legal guidelines and structures in the country for e-government services (Scartezini, 2004).

A growing proportion of users trust in the secure use of e-commerce services. The Ministry of Justice is a secretariat that focuses on consumer rights and e-commerce. The Brazilian legislation includes provisions on e-commerce (Consumer Protection Code – Law No. 8.078/1990, the Decree No. 8,771/2016, which regulates the Brazilian Civil Rights Framework and the Brazilian Civil Rights Framework for the Internet or Internet Act (Law No 12,965/2012 – Marco Civil da Internet Law No. 12,965/2012), see D 4.1). Therefore, within this area, the highest tax rates on e-commerce are not for national trade but for cross-border trade.

Overall, there is general encouragement for companies to provide online services. E-commerce service provision is growing and has increased since 2017, when Brazil (the Brazilian Federal Police) and Europol signed a strategic agreement to expand co-operation to combat cross-border criminal activities, which could be considered as a formal co-operation. Companies increasingly tend to invest in e-commerce services which are fully established. Security solutions are updated and reliable payment systems have been made available. However, participants indicated that there are remaining challenges to cybersecurity and the protection of the data of users, such as from leakage of credit card data from cyber-attacks.

The banking sector organises awareness campaigns and provides online information for users, regarding their safety. For example, Banco do Brazil[76] and Banco Itaú[77] provide security tips for their customers. Although investments are being made in e-commerce services and participants believe that there will be an increase in the use of e-commerce services, hackers are perceived to be ahead of the curve.

Results from the validation process conducted in March 2019:

In May 2018, the Government published the revised version of the Digital Governance Strategy: *Digital Transformation – Citizenship and Government,*[78] which, inter alia, covers matters of cybersecurity in the context of e-government services. The strategy includes several applicable digital governance principles – cybersecurity being one of them – which are promoted by various governmental entities and even has a dedicated webpage.[79] The promotion of the principles likely contributed to the fact that, according to the 2018 research of the OECD, 94 percent of public-sector organisations are aware of the Digital Governance Strategy.[80]

Users as well as the Government are aware of the importance of secure e-government services.[81] Breach identification, announcement and analysis fall within the mandate of CTIR Gov and examples of public alerts related to the insecurity of Government e-services are available online.[82] According to the most recent official study, published in 2018, 64 percent (and rising) of all Brazilians over 16 years of age use Government e-services. Half of those who do not cited concerns over privacy and security as the main reason for their abstinence.[83]

In 2019, most of the e-commerce websites offered easily accessible terms and conditions of use.[84] Most of them also used encrypted connection between the user and their servers, and provided a wide array of secure payment options.[85] Security and trust was promoted by the e-commerce providers through the prominent display of security protocols available to the users. The Government was also active in fostering trust by publishing security advice to online shoppers.[86]

A growing proportion of Brazilians use e-commerce services. In 2018, 33 percent of the respondents in the Centre for International Governance Innovation study indicated that they shop online at least twice a month, up from 23 percent in 2017. A quarter of those who do not shop online, argued that it was because they do not trust online shopping (although this is not only due to the lack of trust in security of online shopping platforms).[87]

D 2.3 - User Understanding of Personal Information Protection Online

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Stage: Formative

Users and stakeholders within the public and private sectors have general knowledge about how personal information is handled online and employ good (proactive) cybersecurity practices to protect their personal information online.

The General Data Protection Bill was approved by Brazil in July 2018.[88] Moreover, many law firms in Brazil began to set up divisions that specialise in Data Protection, and events about Data Protection are being organised by private companies and non-profit organisations.

Moreover, there are provisions within other legislative frameworks that address this issue (see D 4.1). For instance, stakeholders mentioned that in Brazil, it is common for people to be asked to provide their personal information both offline and online. According to participants, Brazilians are used to giving away their privacy, even though there is awareness of large databases that have suffered important leakage events and misuse of data events.

In addition to a receipt, a consumer in Brazil will receive an invoice with a number and a barcode which they have to scan via their mobile phone. This practice has caused some incidents in the past such: for example, when malware called "boware" targeted e-commerce users, it changed the bar code on the invoice in ways that enabled fraud.

Regarding SMEs, stakeholders mentioned that there is a need to prepare them for such fraudulent activities. In this respect, the Government has taken steps to raise awareness regarding data privacy and personal information protection online (see D 3.1).

Last year, internal phishing exercises were conducted and an internal analysis of the level of awareness was developed in order to understand how to raise the level of awareness at the national level. There are continuing efforts to raise awareness, by disseminating leaflets on password protection and the need for back-ups, for example, and by establishing October as a security month, conducting lectures and other events, and generating a range of informative videos, audios and written material. These initiatives are being developed based on the thinking that the user should be able to follow the instructions given.

Results from the validation process conducted in March 2019:

Although it is hard to say that the maturity of the factor has changed since the CMM review in 2018, it is worth noting that in August 2018, Brazil enacted the Brazilian General Data Protection Law (Federal Law No. 13,709/2018). The participants in the 2019 focus-group interviews voiced dissatisfaction with the fact that this law would not come into force until August 2020.

D 2.4 - Reporting Mechanisms

This factor explores the existence of reporting mechanisms functioning as channels for users to report internet-related crime such as fraud, cyber-bullying, child abuse, identity theft, privacy and security breaches, and other incidents.

Stage: Formative

Reporting mechanisms have been established for users to report Internet-related crime and are regularly used. SaferNet Brasil[89] provides information on Internet safety and space for complaints on its website. The SaferNet Brasil is a non-profit organisation which was created in 2005. The organisation is a unique civil society body in Brazil, with formal agreements with the Ministry of Justice, the Federal Police and Human Rights Secretariat at the President of Republic Office which allow it to receive and process reports from the public. Its online-only hotline service can be used to report content anonymously.

Also, the Federal Police[90] has a dedicated page on its website for denouncements, which can also be made via its email address (denuncia.ddh@dpf.gov.br). Child and adolescent pornography[91] can be reported via the helpline created by the Government.

In Brazil in general there are different channels to report incidents. For incidents such as child pornography, an email has to be sent to police while for fraud incidents, reports have to go through the respectiv bank. All incidents are reported to the police, while those that are not clearly classified are sent to the CTIR Gov Brazil for categorisation before being forwarded to the relevant institutions. For example, if cybercrime is committed against a citizen, the incident will be dealt with by the civil police in that citizen's state. If the crime reaches federal public companies such as Caixa[92] or Banco Central do Brasil,[93] the competent agency is the federal police.

Overall, participants indicated that citizens in Brazil do not have a culture of reporting. Moreover, it was not possible to identify whether there are programmes to promote the use of existing mechanisms established by public and private sectors.

The most common incidents that users face are financial crimes such as fraud online. For such incidents, the Federation of Banks will have to take action. The CTIR Gov Brazil is involved in the monthly meetings and exchange of information in the financial area as well. The Government is also looking for ways to make reporting of incidents mandatory for the private sector.

Results from the validation process conducted in March 2019:

In 2019, the validation workshop largely confirmed the outcomes of the 2018 CMM report.

D 2.5 - Media and Social Media

This factor explores whether cybersecurity is a common subject across the mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of the media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Formative – Established

There is ad-hoc media coverage of cybersecurity in Brazil, with limited information and reporting provided on specific issues that individuals face online, such as online child protection. An example of social media coverage of cybersecurity is that from Facebook:[94] Facebook created a "Centre" to prevent cyberbullying in Brazil in 2016, in partnership with UNICEF and Safernet. Participants mentioned that there is also limited discussion on social media about cybersecurity. There are non-profit groups which discuss this topic on social media in Brazil. However, someone would have to be interested in this topic to receive this information. Usually, in the event of a cyber-incident, this is communicated through the print, television, audio and digital media, and guidance is also provided.

However, stakeholders indicated that no major incident has impacted the critical national infrastructure in Brazil that might lead to a broader coverage of the media and social media.

Results from the validation process conducted in March 2019:

In 2019, the validation workshop largely confirmed the outcomes of the 2018 CMM report.

Recommendations

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of cyber culture and society. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity as per the considerations of the Centre's CMM.

Cybersecurity Mind-Set

R 2.1
Enhance efforts at all levels of Government, especially officials, and the private sector to employ good (proactive) cybersecurity practices. Design systems that enable users across society to embed secure practices more easily into their everyday use of the Internet and online services;

R 2.2
develop co-ordinated training programmes for employees in the public sector;

R 2.3
make cross-sectorial co-operation and information sharing about cybersecurity risks and best practice routine among private and public-sector organisations; and

R 2.4
identify vulnerable groups and high-risk behaviour across society to inform targeted, co-ordinated awareness campaigns.

Trust and Confidence on the Internet

R 2.5
Establish ISP programmes to promote trust in their services based on measures of effectiveness of those programmes;

R 2.6
implement feedback mechanisms to ensure that e-services are continuously improved and that trust is strengthened among users; and

R 2.7
employ processes for gathering user feedback within government agencies, in order to ensure efficient management of online content.

User Understanding of Personal Information Protection Online

R 2.8
Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online;

R 2.9
encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making;

R 2.10
promote compliance with web standards that protect the anonymity of users; and

R 2.11
develop user-consent policies designed to notify practices on the collection, use or disclosure of sensitive personal information.

Reporting Mechanisms

R 2.12
Develop programmes to promote the use by public and private sectors of the existing reporting mechanisms for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents;

R 2.13
encourage different stakeholders (public and private sectors, police, CERT) to co-ordinate the reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms; and

R 2.14
employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.

Media and Social Media

R 2.15
Encourage the media and social media providers to further extend their coverage beyond threat reporting, and to focus on informing the public about proactive and actionable cybersecurity measures, as well economic and social impacts;

R 2.16
encourage a frequent discussion about cybersecurity on social media; and

R2.17
ensure that the debate in social and the mainstream media, and the attitudes expressed, inform policymaking.

Dimension 3

Cybersecurity Education, Training and Skills

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, in the private sector and the population as a whole.

D 3.1 - Awareness Raising

This factor focuses on the prevalence and design of programmes that raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and foher executive management.

Stage: Formative – Established

A national programme for raising awareness of cybersecurity, led by a designated organisation (from any sector) and which addresses a wide range of demographics, is established.

Due to the limited participation of the civil society, it was not possible to obtain a clear picture of the initiatives about raising cybersecurity awareness.

During the review, the most important awareness-raising body recognised by the participants was SaferNet Brazil, an NGO created in 2005.[95] It has unique partnerships

with the Ministry of Justice, the Federal Police and the Human Rights Secretariat at the President of the Republic Office which enable it to "protect human rights and serve as a Hotline, Helpline and Awareness node in Brazil."[96] It operates a Hotline service that receives anonymous complaints about crimes and violations against human rights on the Internet.[97] In addition, SaferNet is involved in the organisation of awareness-raising campaigns via educational institutions throughout Brazil.[98] In 2008, SaferNet expanded co-operation to involve technology companies such as Google, by signing a co-operation agreement that allows the monitoring and screening of child pornography crime.[99]

The Internet Steering Committee in Brazil (www.cgi.br) – a multi-stakeholder council created by Inter-ministerial Ordinance 147 of 31 May 1995 – is the main institution in charge of promoting ICT security standards and Internet best practices[100] and executes its activities via the Brazilian Network Information Centre (NIC.br) (http://nic.br/quem-somos/).[101] Based on desk research, NIC.br implements several initiatives such as the Antispam.br[102] (http://www.antispam.br/) and InternetSegura.br[103] (https://www.Internetsegura.br/); both are portals aimed at raising the awareness of parents and children about spam, and they disseminate materials about Internet safety. Furthermore, CERT.br, in collaboration with CGI.br and NIC.br, has been promoting and disseminating awareness materials (e-books, slides) to the public (https://cartilha.cert.br/) but especially designed for teachers and children and covering topics such as social networks, passwords, mobile devices and e-commerce.[104] (For more about NIC.br projects related to professional training, see D 3.3) One participant mentioned that there are some internal awareness-raising activities for administrative staff within federal institutions but it is not available to the public.

Some participants noted that awareness-raising activities focused on safe Internet use and aimed at public and private schools, were held between 2009 and 2013. It was added that in 2015, the Federal Prosecution Service launched a project called the Federal Prosecution Service for Digital Education in Schools (Ministério Público pela Educação Digital nas Escolas), to deliver workshops at universities (for 200 teachers and students), and hand out leaflets and materials.[105] After the workshop, teachers were encouraged to take the materials provided by the Federal Prosecution Service and were asked to provide feedback via the SaferNet website. In 2018, the same workshops were provided at universities but were aimed at professionals and psychologists.

Regarding raising cybersecurity awareness for executives, participants acknowledged that the senior management is often not aware and needs to be educated about how cybersecurity risks affect their organisations. For instance, within the Federation of Industry of the State of Sao Paulo (FIESP), there is a security department that leads the discussion on cybersecurity.[106] Also, Brasscom (the Brazilian Association of Information and Communication Technology Companies) organises cyber events to promote the ICT sector to public authorities, and public and private clients.[107] This does not involve the participation of major international organisations, financial institutions and telecommunication companies where the strategic implications of cybersecurity is a priority. There are some initiatives on awareness that are available for boards of directors, but there are no specific programmes. Also, executives are not obliged to attend cybersecurity training although it is considered to be best practice. According to the model for public or state-owned companies, the Government nominates the directors and it is a mandatory requirement that two of the appointed executives are from the House. A participant highlighted that usually, in the case

of technology companies the selected leaders have no prior knowledge of how such a company operates. This often leads to mismanagement since the executive is appointed based on political affiliations. However, one of the public technology companies is now planning to set up internal rules to rectify this procedure and the appointed board members are selected based on their knowledge and experience of cybersecurity. It was added that the state-owned company's security policy is directly linked to the President of the Republic Office in order to provide support and guidelines for the key leaders.

In addition, participants highlighted the importance to differentiating between IT companies and information security companies in Brazil since, in their opinion, the companies do not speak the same language. An IT company is more committed to client satisfaction and precision but the opposite is true for an information security company, therefore, different measures are taken in order to bridge the gap between business goals and IT security. Often when the new management arrives, the IT staff has to accommodate to the 'state of the art' of the company. This means that internal awareness raising training courses are provided to the new executive management (e.g.: explaining the importance of cyber security and information security norms). A participant revealed that at their company they have 24 security norms and four procedures to guide these processes.

One of the developments after the assessment in March 2018 was the introduction of the National Information Security Policy (Presidential decree (No 9.637)) in December 2018; it states that it is the responsibility of the Institutional Security Office of the Presidency of the Republic to "develop and implement programs on information security aimed at raising awareness and training of federal public servants and society."[108] It is therefore not clear to what extent the awareness-raising activities led by the Institutional Security Office of the Presidency of the Republic overlap with the awareness-raising activities of the NIC.br.[109]

Results from the validation process conducted in March 2019:

In 2019, the validation workshop largely confirmed the outcomes of the 2018 CMM report.

D 3.2 - Framework for Education

This factor addresses the importance of high-quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need to enhance cybersecurity education at national and institutional level, and the collaboration between Governmen, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Formative

Due to the lack of participation by academia, it was not possible to obtain a clear picture about cybersecurity education in Brazil. Therefore, the information provided below is based on desk research.

The need for enhancing cybersecurity education in schools and universities has been identified by leading government and industry stakeholders.

The Ministry of Education (MEC) sets the national curriculum on cybersecurity-related courses and requirements and standards but the level of development is left to the universities to decide. It is not regulated by a central agency. The Ministry of Education has a National Catalogue of High Education Programmes in Technology, which defines the requirements for creating programmes related to cybersecurity such as cyber defence and information security.[110] It presents the minimum workload and infrastructure recommended for each course.[111] The review did not reveal whether there is any distinct national budget given to cybersecurity education. Similarly, it was not clear from the focus-group discussions to what extent co-operation exists between the private sector and the universities.

Qualifications for and the supply of cybersecurity educators are readily available. In Brazil, specialised postgraduate courses in cybersecurity are offered at university level. One participant noted that most of the universities offering courses in computer science have laboratories. The University of Sao Paolo offers a Bachelor Degree in Computer Science,Computer Physics and Computer Engineering as well as Master's and Doctoral degrees in Computer Science.[112] Also, the Federal University of ABC offers both Master's and PhD programmes in Computer Science under the Computer Science Graduate Programme.[113] The research areas cover Applied and Scientific Computing, Computing Foundations and Computing Systems.[114]

In addition to private universities, postgraduate-level cybersecurity courses are also offered by the Brazilian National Research and Educational Network (Rede Nacional de Ensino e Pesquisa – RNP).[115] Also, every year RNP organises the International Computer Security Day (DISI), which is free, open to the public and broadcast live.[116] The National Service for Commercial Education (SENAC), a private non-profit institution, offers graduate-level courses on cyber defence in order to support that particular sector.[117]

In addition, according to Trend Micro's report on Brazil's cyber-criminal underground, there is a troubling trend of hackers "actually offering tutorials and courses to aspiring cyber criminals for a price (for e.g.: training videos, Skype tutorials)."[118]

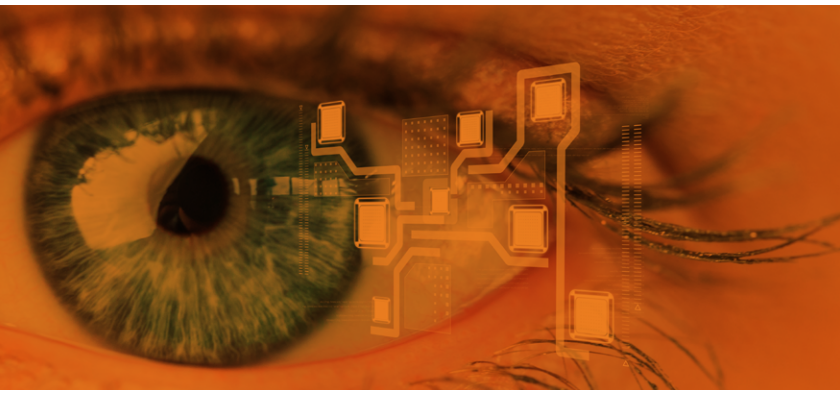
Currently, there is a national discussion about which aspects of cybersecurity should be taught to primary- and secondary-school pupils. The current curriculum features a small reference to IT systems, but mostly in the context of how to use digital media and information technologies to spread the acquired knowledge.[119]

There was no information about the exact involvement of stakeholders regarding the development of priorities for cybersecurity education programme. Since this topic is still very incipient, there is no discussion about priorities, but there is one about the implementation procedures.

Results from the validation process conducted in March 2019:

In 2019, representatives of academia participated in the validation workshop and largely confirmed the outcomes of the 2018 CMM report.

D 3.3 - Framework for Professional Training



This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Stage: Formative

The need to train professionals in cybersecurity has been recognised by the Government.

Based on desk research, the CGI.br (see D 3.1) co-ordinates training efforts via CERT.br, the Best Practices Portal (BCP.nic.br) and CGSIC. For instance, CERT.br, being a CME CERT Partner, has the license to offer professional training programmes such as the "Fundamentals of Incident Handling", "Advanced Incident Handling for Technical Staff" and "Overview of Creating and Managing Computer Security Incident Response Teams".[120] Also, the BCP.nic.br brings together a set of good operational practices for system administrators.[121] The national portal is maintained by professionals from several areas of NIC.br, such as CERT.br, Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (CEPTRO.br) and Registro.br, in collaboration with specialists outside NIC.br.[122] Furthermore, CGSIC offers a course in "Management of Information Security and Communications".[123]

Participants stated that most of the professionals within the public sector attend IT professional qualifications overseas and

receive ICT certificates such as the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM). Regarding technical accreditations, a participant mentioned that the computational forensics course offered by CERT.br is expensive but worthwhile.[124]

Based on desk research, the Cyber Defence Command (ComDCiber), within the Brazilian Army and in co-operation with the National School of Cyber Defence, provides training for civilian and military human resource executives required to counter cyber attacks effectively.[125] In addition, financial institutions such as Fundação Bradesco (a national bank) offers courses in information security.[126]

COBIT has been accepted as "a de facto standard for good practices throughout Brazil, in private, public and government organizations."[127] The Brazilian Federal Court of Accounts – the Tribunal de Contas da União (TCU) – conducted surveys, reports and audit initiatives about the use and acceptance of the framework and there has been a growing number of courses and IT-related certifications available for both professionals and public servants.[128] To complement COBIT, ISO 27000 is also used as a reference. Courses related to information management are offered within the federal government: four courses over a period of two years. CISSP is the most renowned and acknowledged certification available, together with the incident-response training offered by SANS Institute.

Participants suggested that there is a high demand for more cybersecurity professionals in Brazil. Most of the participants confirmed that there is a high uptake of cybersecurity courses and private enterprises usually train their own staff internally.

Results from the validation process conducted in March 2019:

In 2019, participants in the group interviews informed us of additional professional education providers (e.g., Febraban, a federation of Brazilian banks)[129] but a change in maturity of cybersecurity capacity of Brazil has not been recorded.

Recommendations

Following the information presented on the review of the maturity of cybersecurity education, training and skills, the following set of recommendations is provided to Brazil. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the Centre's CMM.

Awareness Raising

R 3.1
Appoint a dedicated organisation (e.g.: RNP) with a mandate to develop and implement a planned national cybersecurity awareness-raising programme. Co-ordinate and co-operate with key stakeholders from all sectors;

R 3.2
develop a dedicated awareness-raising programme for executive managers within the public and private sectors, as this group is usually the final arbiter of investments into security. The programme could focus on emphasising the responsibility and accountability of executive leaders and board members for cybersecurity;

R 3.3
promote awareness-raising efforts of cybersecurity crisis management at executive level;

R 3.4
promote awareness of risks and threats at all levels of the Government;

R 3.5
enact evaluation measurements to study effectiveness of the awareness programmes at a level where they inform future campaigns, taking into account gaps or failures; and

R 3.6
promote discussions that emphasise the core and inherent role of information and cyber security in all IT companies and operations, considering future risks.

Framework for Education

R 3.7
create cybersecurity education programmes for instructors of cybersecurity to ensure that skilled staff are available to teach newly-formed cybersecurity courses;

R 3.8
create accredited cybersecurity-specific degree courses at undergraduate and post-graduate level, in addition to the other existing cybersecurity-related courses in the various universities in Brazil;

R 3.9
promote efforts by universities and other bodies to hold seminars and lectures on cybersecurity issues, aimed at non-specialists;

R 3. 10
integrate specialised cybersecurity courses in all computer science degrees at universities and offer specialised cybersecurity courses in universities and other higher education bodies;

R 3.11
collect and evaluate feedback from existing students for further development and enhancement of cybersecurity course offerings;

R 3.12
create initiatives to advance cybersecurity education in the primary and secondary school curricula;

R 3.13
develop partnerships for the development of interfaces for research, innovation and interaction between universities and the private sector;

R 3.14 ensure the sustainability of research programmes;

R 3.15 develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment; and

R 3.16
gather statistics on the supply and demand of cybersecurity graduates.

FRAMEWORK FOR PROFESSIONAL TRAINING

R 3.17
Establish more affordable and structured cybersecurity training programmes to develop skills towards building a cadre of cybersecurity-specific professionals;

R 3.18
establish continuous training for IT employees and employees in general regarding cybersecurity issues within all sectors;

R 3.19
develop metrics to evaluate the take up and success of cybersecurity training courses;

R 3.20
create a knowledge exchange programme targeted at enhanced co-operation between training providers and academia;

R 3.21
ensure that affordable security professional certification is offered across sectors within the country;

R 3.22
develop a central platform for sharing training information for experts and create a national-level register of cybersecurity experts;

R 3.23
establish requirements for joint cybersecurity training for the public and private sectors, and develop collaborative training platforms;

R 3.24
create initiatives to develop a fast-track approach to cyber-capacity building;

R 3.25
establish initiatives to promote the attractiveness of the cybersecurity profession in order to encourage employers to train staff to become cybersecurity professionals; and

R 3.26
develop a skills framework in cybersecurity or use an existing skills framework in the country in order to define clear career paths for cybersecurity experts.

Cybersecurity

Capacity Review

Federative Republic of Brazil

Dimension 4

Legal and Regulatory Frameworks

This dimension examines the Government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data-protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law-enforcement, prosecution and court capacities. Moreover, this dimension observes issues such as formal and informal co-operation frameworks to combat cybercrime.

D 4.1 - Legal Frameworks

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Stage: Established

Brazil does not have an all-encompassing regulation that deals explicitly with cybersecurity. Despite efforts to introduce a binding legislative framework, cybersecurity legislation in Brazil is still under development. Instead, several official guidelines or "soft laws" have been adopted that refer to cybersecurity issues.

The most relevant legislative frameworks and guidelines related to Brazil's Internet landscape are:

- the Cyber Crimes Act (Law No. 12,737/2012)[130] (2012), also known as the "Carolina Dieckmann Law"
- the Brazilian Civil Rights Framework for the Internet (Law No. 12.965)[131] (2014) the Internet act also known as the "Marco Civil da Internet"
- the Green Book (Livro Verde) on Brazil's Cybersecurity[132] (2010)
- the Cyber Defence Policy[133] (2012) Administrative Normative Rule No. 3.389
- the White Paper on National Defence[134] (2012)
- National Defence Strategy (Estratégia Nacional De Defesa)[135] (2008)
- Critical Information and Communication Infrastructure Protection[136] (2010)
- Anatel – Public Consultation No. 21[137]

Criminal Legislation

Other legislations on cybercrime are covered by the following instruments:

- Law 8,137/1990, Art. 2
- Law 9,296/1996, Art. 10
- Law 11,829/2008
- Law 8,069/1990, Art. 241
- Law 9,504/1997
- Law 12,735/2012, Art.4
- Law 9,100/1995, Art. 67
- Law 9,983/2000

Regulation And Compliance

Other regulations related to cybersecurity are covered by the following instruments:

- Administrative Rule no. 35/2009
- Decree 3,505/2000
- Resolution No. 614/2013, Art. 53
- Administrative Rule No. 45/2009
- Administrative Rule No. 34/2009
- Decree 7,845/2012
- Resolution No. 617/2013, Art. 47

(Adapted from ITU, Cyberwellness Profile, Brazil)[138]

The introduction of "emergency" criminal laws is not new in the history of the Brazilian legal system, especially when legislators hastily approve these laws in order to satisfy the public demand for justice.[139] Similarly, in 2012, the Cyber Crimes Act86 (Law No. 12,737/2012) that is also known unofficially as the "Carolina Dieckmann[140] Law", was approved in a hurry by Congress and added to the Penal Code[141] in order to address computer misuse. The two articles 154-A and 154-B that were introduced refer to cybercrime such as computer intrusion, misuse of user data or taking down websites.

Invasion of computer device

Article 154-A.

Invade another computer device, connected or not to the computer network through improper breach of security mechanism, and for the purpose of obtaining, tampering or destroying data or information without the express or tacit authorization of the device owner or installing vulnerabilities to gain an illicit advantage:

Penalty – detention, from 3 (three) months to 1 (one) year, and fine.

Criminal action

Article 154-B.

In the crimes defined in Art. 154-A, shall only proceed by means of representation, unless the crime is committed against the direct or indirect public administration of any of the Powers of the Union, States, Federal District or Municipalities or against utilities.

Article 154-A criminalises computer intrusion and provides increased penalties if it results in economic loss and data breach.[142] During the review, some participants raised their concern that the penalties are too light (three months to one year in prison, in addition to a fine). This is considered to create a low-risk activity for the criminal and encourages malicious behaviour online.

Article 154-B lets the victim decide whether to proceed with the criminal charges, unless the attack was against the Government or a public body.[143]

The Brazilian Civil Rights Framework for the Internet[144] (Law No. 12.965) (Marco Civil da Internet) was developed via a multi-stakeholder consultation process with the involvement of the civil society over several years and was finally adopted in 2014. The law intends to regulate the use of the Internet in Brazil through principles, guarantees, rights and duties for the users. The legislation addresses several issues including: net neutrality; Internet-related data privacy; data retention in relation to the Internet; Internet-related civil rights with obligations on Internet users and Internet service providers (ISPs); freedom of expression, of speech and of communication.[145] Furthermore, this law is considered to be a pioneer in the protection of Internet users' rights that also strictly limits access to data required for investigations.[146]

In July 2018, Brazil adopted the General Data Protection Legislation (Lei Geral de Proteção de Dados, or LGPD) that came into force in February 2020.[147] Also, Brazil relies on various provisions stated in the Federal Constitution,[148] the Brazilian Penal Code,[149] Consumer Protection Code[150] and the Brazilian Civil Rights Framework for the Internet:

Brazilian Civil Rights Framework for the Internet

Section II
Protection of Logs, Personal Data and Private Communications

Article 10.

The storage and the availability of connection and access logs to Internet applications mentioned in this law, as well as personal data and the content of private communications, must take into account the preservation of intimacy, privacy, honour and image of the parties directly or indirectly involved.

Article 11.

In any operation of gathering, storage, custody and treatment of records, personal data or communications by connection and Internet application providers in which at least one of these acts occurs in national territory, the Brazilian law and the rights to privacy, protection of personal data and the confidentiality of private communications and records must be mandatorily respected.[151]

During the review (March 2018), many expressed the need for the approval of a statute for the regulation of data protection that was finally adopted in July 2018.[152] The Brazilian Civil Rights Framework for the Internet only applies to Internet-related issues.[153] This framework "protects personal data (without defining what would be considered personal data), private communication content and access logs, regarding both Internet connection and applications."[154] In addition, according to the Brazilian Civil Code,[155] directors of an organisation might be held liable in the case of negligence of the organisation's protection of networks and data.[156] Despite the fact that the Brazilian Copyright Law[157] has a specific provision on data protection, it only refers to the protection of the titleholder.

The recently approved Data Protection Bill of Law (the "Bill") – inspired by the EU's GDPR – requires the creation of a national data protection authority and the notification of data breaches to the data protection authority.[158] Since there was no national data protection authority, victims of data breaches often filed a complaint against a data controller who might be penalised based on the Brazilian Civil Rights Framework for the Internet and the Carolina Dieckmann Law, as well as incurring civil liability.[159]

Brazil can be considered to be at the forefront of digital rights, with the adoption of the Brazilian Civil Rights Framework for the Internet (also known as the Brazilian Internet Bill of Rights) in 2014, which intends to protect privacy and free expression rights online.[160] Furthermore, in 2015, Brazil "co-led an initiative at the United Nation Human Rights Council to create a new UN special rapporteur on the right to privacy."[161] Despite implementing this landmark piece of legislation, comprehensively protecting human rights online, according to Human Rights Watch there have been some violations that threatened the right to privacy in Brazil. For instance, in 2015, mobile phone companies received a court order to temporarily block WhatsApp (the Facebook-owned messaging service) for two days.[162] Then in 2016, a Facebook executive was arrested by the federal police because the company denied the authorities access to user data.[163]

Comprehensive legislation on the protection of children online has been adopted and enforced:

- under Articles 240* and 241A-E* of the Law 11.829/2008 that amended the Statute of the Child and Adolescent (Estatuto da Criança e do Adolescente – ECA) (Law No. 8.069/90) in 2008.[164] [165]

- under Articles 218, 218A, 218B* of the Penal Code, amended and included by the Law No. 12015/2009 in 2009.[166]

Also, "Articles 17, 18, 143 and 247 of the Statute of the Child and Adolescent contain provisions to protect the image and reputation of children and adolescents by punishing anyone who exposes them in a negative or injurious manner."[167] Article 241-D of the ECA defines online grooming and imposes a penalty of one to three years' imprisonment.[168] Some participants criticised this penalty as being too lenient and raised concern about the lack of legislation to criminalise cyber-bullying, sexting and accessing or downloading child-pornography images. Also, in Brazil's legislation, there is no mandatory reporting of suspected child pornography for ISPs unless they receive an official notification to deny access to child-abuse images.[169] In addition, the Convention on the Rights of the Child was signed and ratified by Brazil, with no declarations or reservations to Articles 16, 17(e) and 34(c).[170] Similarly, the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography was signed and ratified, with no declarations or reservations to Articles 2 and 3.[171]

Brazil currently lacks legislation that deals explicitly with cyber threats to IP. However, the Law on Copyright (Law No. 9.610/1998)[172] guarantees the protection of any type of intellectual product, irrespective of being registered or published.[173] Also, the protection of the IP of a computer programme is regulated under the Law on Protection of Intellectual Property of Software (Law No. 9,609/1998).[174]

Businesses on the Internet are regulated by the Internet Act[175] (Law No. 12,965/2014), its Regulating Decree[176] (Decree No. 8,771/2016) and the Consumer Protection Code[177] (Law No. 8,078/1990), which applies to all consumers and suppliers of services or goods.[178] Consumer Protection Offices are responsible for consumers' rights. In addition, the Consumer Protection Code guarantees an individual's right to "access all data stored about themselves and to request changes, corrections and even its removal from a database."[179] Failure to provide a consumer access to information about him- or herself is subject to a penalty of imprisonment or a fine.[180] The National Telecommunications Agency (Anatel) regulates Internet access and has the power to suppress abuses and establish guidelines; for instance, the obligation to notify customers of price charges in a timely fashion.[181]

The Cyber Crimes Act (Law No. 12.737/2012)86 and the Brazilian Civil Rights Framework for the Internet (Law No. 12.965)[182] (2014) are considered to be the most relevant substantive legislations currently in place to formally handle cybercrime offences and provide procedural powers when handling electronic evidence (Figure 4).

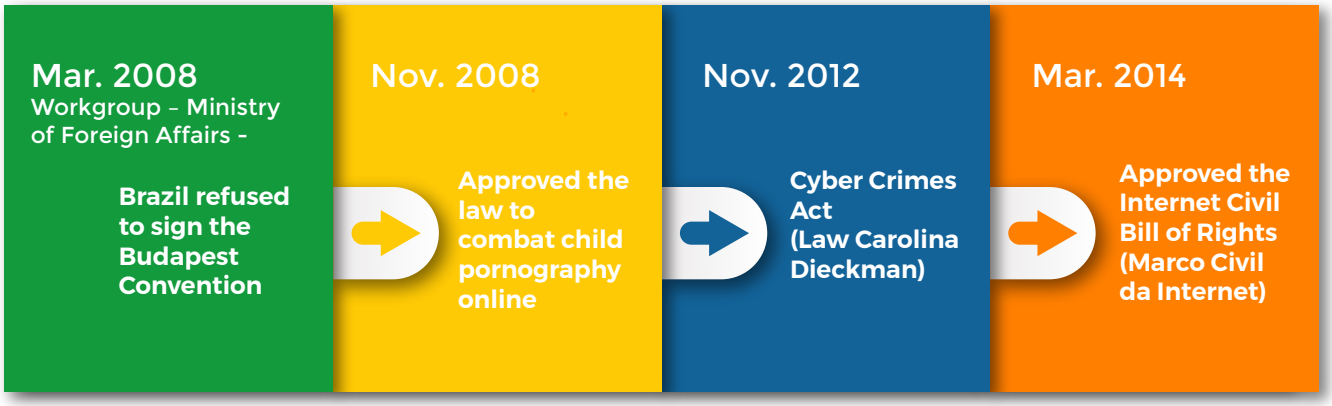


Figure 4: *Timeline of cybercrime legislation in Brazil*

Some participants noted that the problem is not the legislation per se, but enforcement and responsiveness. Despite the ongoing political discussions about these issues, there are still legislative gaps in the implementation process that Brazil should overcome. One participant noted that:

"For instance, Carolina Dieckmann Law was introduced because of the media questioning what happened. We do not have the same level of commitment. The legislation progress should continuously evolve however, it is still lagging behind cybercriminals. The media sometimes disclose cyber events but what should be the norm and line of thought in legislating? We are not in the desired level yet."

Therefore, the lack of enforcement of cybercrime legislation and lenient punishments tend to encourage cybercriminals.

"Phishing" was another concern raised by one participant, because it is not penalised in Brazil and not considered as a criminal activity. The participant argued that many view "phishing" as just a preparation – brandishing a firearm at someone without using it. The technical discussion in the legal sphere is hampered by lack of knowledge of IT technologies. Generally, lawyers do not understand the severity of cases (e.g., leakage of information or online fraud) and therefore they do not think that this is a problem.

Brazil has not signed the Council of Europe's (CoE) Convention on Cybercrime yet. However, some participants stressed the need for Brazil to accede to the Convention.

Results from the validation process conducted in March 2019:

The legislative landscape has not changed significantly since the 2018 CMM review. Once again, the participants in the 2019 focus-group interviews noted the need for Brazil to sign the Convention on Cybercrime; some internal discussions between various entities of the Government have been undertaken. In December, following the focus-group interviews in March 2019, Brazil started its accession process to the Budapest Convention, as an observer.

One notable addition to the Brazilian legislative landscape is the Data Protection Law, enacted in August 2018. In December 2018, the Provision Measure No. 869/2018 was published, thus amending the Data Protection Law and creating the National Data Protection Authority. In accordance with the aforementioned amendment, the Data Protection Law is expected to take effect in August 2020.

Similarly, the Sexual Harassment Law (No. 13,718) that came into force in September 2018 to amend the Penal Code (Decree-Law No. 2,848, of December 7, 1940), criminalises the performance of libidinous behaviour (non-consensual) and the disclosure of the rape scene, which was previously only a criminal misdemeanour.[183] The new law provides for punishment such as imprisonment from one to five years.[184] This repeals the provisions in the Law of Criminal Misdemeanours (Decree-Law No. 3,688, of October 3, 1941). The Sexual Harassment Law represents a significant advance in combating revenge pornography that "covers the leaking of sex, nudity or pornographic scenes, either in video or photo form, without the victim's consent".[185]

Sexual Harassment Law (No. 13.718)

Disclosure of rape scene or rape scene of vulnerable, sex scene or pornography

Article. 218–C.

Offer, exchange, make available, transmit, sell or exhibit for sale, distribute, publish or disclose, by any means – including through mass communication or a computer or telematics system – photography, video or other audio-visual record containing a scene of rape or rape of vulnerable or who condone or induce their practice, or, without the consent of the victim, sex scene, nudity or pornography:

Penalty - imprisonment, from 1 (one) to 5 (five) years, if the fact does not constitute a more serious crime.

Last but not least, the participants in the 2019 focus-group interviews noted several initiatives intended to modernise the existing legislation (including the Cyber Crimes Act) and to make sure it adequately addresses cybersecurity, although no new cybersecurity-related legislation is envisioned in 2019.

D 4.2 - Criminal Justice System

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Formative

Across the criminal justice system, capacities are between the start-up and formative stages of maturity in Brazil.

The main regulatory authority that implements cybersecurity rules in Brazil is the Ministry of Justice via the Federal Prosecutors' Office and the Federal Police department.[186]

The Federal Police's URCC, based in Brasilia, is the main law-enforcement actor in charge of fighting cybercrime and therefore plays a critical operational role in pursuing cybercriminals both within and beyond Brazil's borders.[187] Among its competencies, the unit is involved in the investigation of electronic fraud (e-banking and credit card scams), of criminal networks supporting online child abuse, of the unauthorised access of IT systems and networks, and also in addressing crimes against federal public institutions.[188] It was acknowledged during the review that the Federal Police has a good track record in tackling online banking fraud and online child pornography.

Participants expressed several concerns that the law-enforcement community faces with regard to the enforcement of cybercrime laws:

• lack of an adequate level of training and certifications in many of the institutions which

are needed to carry out prosecutions, since police officers have poor knowledge of IT, therefore the provision of basic knowledge of IT is essential for the investigation to be successful (e.g.: training on ISPs, analysis of malicious code, attribution of cybercrimes);

- lack of technical and financial resources for poorly-trained personnel;
- police officers invited to attend cybercrime training in Brasilia are often relocated elsewhere, hence a difficulty in retaining officers in specific areas of cybercrime;
- different levels of capacity between the cybercrime units of the Federal Police and those of the Civil Police (small budget, lack of advanced forensic tools, lack of specific training);
- lack of trust between law enforcement agencies and private companies for carrying out cybercrime investigations;
- lack of standardisation in digital-evidence gathering and forensic procedures;
- limited competency in cyber-intelligence collection; and
- the need to clarify the roles and responsibilities of institutional players in order to manage cybercrime in a complex federal structure.

The URCC has mostly informal arrangements with the law enforcement agencies of the 26 Brazilian states, when carrying out cybercrime investigations at the sub-national level. It was highlighted during the review that since police officers have only a basic knowledge if IT, cybercrime specialists from overseas are often called in to help with the investigations. Also, the National Police Academy provides online cybersecurity courses and training for Federal Police officers.

Brazil has a digital forensics laboratory located at the National Institute of Criminalistics (Instituto Nacional de Criminalística – INC) within the Federal Police in Brasilia.[189] Also, each state in Brazil has set up its own IT laboratory with specific roles, such as to crack a phone's encrypted data. In the event that the IT laboratory at the state level lacks some capacity, then contact is made with the URCC or a private organisation. Participants described the working-level co-operation and information-sharing between the Federal Police and State Civil Police as very efficient. One participant acknowledged that within the Federal Police, there is no restriction that would prevent information-sharing. There is no formal structure of information-sharing between the Federal Police and State Civil Police and co-operation is based on trust. With regards to security information-sharing among law-enforcement agencies, Brazil follows a top-down approach.

According to Brazilian law, ISPs are required to co-operate with government authorities upon receipt of official requests (e.g., court order, search warrant, subpoenas) and to divulge customer data.[190] Once a request is received from a competent authority, a judge might issue a warrant or order to conduct an investigation due to the violation of the law.[191] The Brazilian Civil Rights Framework for the Internet guarantees that legal constraints should not limit law enforcers' capacity to carry out their duties and to access personal data, when they have the legal authority to do so.[192] In addition, according to the Brazilian Telecommunications Regulation, under Law 9.296/96, "interception of telephone communications and information technology systems may take place upon court order – if there is a suspicion that the perpetrator committed a crime and there is no other way to produce evidence."[193]

During the 2018 review, it was not possible to obtain a clear picture of the capacity of prosecutors and judges to handle cybercrime

cases and cases involving digital evidence. Based on follow-up interviews, the capacity of prosecutors and judges to handle cybercrime cases and cases involving digital evidence was considered by the participants to be ad-hoc and un-institutionalised. Brazil currently has 1,000 federal prosecutors and 2,400 prosecutors. There are no special courts for handling cybercrime cases, nor specialised cybercrime judges. Judges receive training only via the training held for federal prosecutors.

In 2011, a special working group on cybercrime was created, consisting of eight federal prosecutors.[194] New federal prosecutors and federal judges (since 2015) are eligible to participate in this working group but it is available only once a year. This has a negative impact on the effectiveness of law enforcement to handle cybercrime cases. If these are brought to court, it potentially leads to ineffective investigations and prosecutions, and, subsequently, a failure to convict. Also, it was highlighted during the review that, at the state level, the biggest problem is that the state prosecutor often lacks the knowledge and capacity to carry out the cybercrime investigation. Also, there are difficulties when prosecutors request digital data from ISPs, partially due to the fact that Brazil is unable to move to Internet Protocol version 6 (IPv6). Currently, ISPs are operating with IPv4, which is insufficient because there are not enough IP addresses in the IPv4 address pool. As a result, ISPs share the same IP address among many people, making it very difficult to identify the actual criminal. One suggestion was to try to establish standards on the number of people that can have the same IP. At the moment, in Brazil, ISPs provide the same IP address to as many as 32 people.

Brazil regularly participates in cybercrime training overseas, sponsored by regional bodies such as the CoE and the (OAS). For instance, the Cybercrime Programme Office of the Council of Europe (C-PROC) provided Brazil with support in legislation, judicial and law-enforcement training and in institution-building.[195] In July 2018, federal prosecutors were invited to attend the Octopus Conference on Cybercrime in Strasbourg.[196] One participant added that federal and state prosecutors are invited to participate in cybercrime meetings with the OAS – the Working Group on Cybercrime of the Meetings of Ministers of Justice or other Ministers or Attorneys General of the Americas (REMJA) – in Washington D.C. every two years.[197]

In 2018, Microsoft Brazil signed a co-operation agreement with São Paulo's Public Prosecutor's Office (MPSP) to deliver a digital-crime training programme to public prosecutors and other initiatives related to fighting online crime.[198]

Results from the validation process conducted in March 2019:

In addition to reaffirming the CMM review outcomes, participants in the 2019 focus-group interviews pointed out recent training for the judiciary. They also informed the researchers of the existence of specialised prosecution teams in certain federative states. In spite of this, the participants were of the opinion that Brazil still does not have enough prosecutors and judges trained to successfully bring a growing number of cybercriminals to justice.

Government feedback provided in 2020:

Based on the desktop research following the March 2019 focus-groups interviews, the regulatory authority for cybercrime is the Ministry of Justice and Public Security.[199] According to Article 10, Item V of the Law No. 13,844, the Institutional Security Office of the Presidency of the Republic is responsible for other cybersecurity matters.[200] This is not a significant departure from the 2018 CMM review results and thus does not change the cybersecurity capacity maturity of Brazil.

D 4.3 - Formal and Informal Co-operation Frameworks to Combat Cybercrime

This factor addresses the existence and functioning of formal and informal mechanisms that enable co-operation between domestic actors and across borders to deter and combat cybercrime.

Stage: Formative

The authorities in Brazil have recognised the need to improve both formal and informal co-operation mechanisms, domestically and across borders, but these mechanisms remain ad-hoc. Participants mentioned in particular that co-operation in the fight against cybercrime is an area with great difficulties, especially at international level.

Formal co-operation exists at both the inter-state and inter-agency levels. A partnership with the CICTE is a good example of inter-state co-operation, in facilitating an exchange of information on cybersecurity beyond the borders of Brazil.[201] Also, the SegInfo blog serves as the national programme for disseminating cybersecurity-related information (e.g., vulnerability warnings, latest events and projects) within the public sector.[202] Brazil, is a member of the ITU-IMPACT initiative and has also participated in the Latin American and Caribbean Regional CSIRTs Meeting organised by Latin American and Caribbean Internet Addresses Registry (LACNIC).[203] Moreover, CERT.br has been a member of FIRST since 2002.[204]

Informal co-operation exists with multi-national ISPs on a voluntary basis since they have no legal responsibility and are not obliged to answer requests from law enforcement unless they receive an official request (e.g., a court order or a search warrant). Currently, Brazil is in the process of developing a bilateral agreement between ISPs and law enforcement that allows ISPs to share data directly with the law-enforcement authorities. For instance, in May 2018, the INTERPOL National Central Bureau (NCB) in Brasilia and Banco do Brasil S/A signed an agreement to co-operate and to share information in order to tackle cybercrime. "This public-private partnership will foster a systematic exchange of data related to cyber threats."[205]

Among the various international co-operation channels available, the engagements with INTERPOL, Ameripol and Europol were described as the most important channels for facilitating cross-border co-operation and information sharing. Based on desk research, the URCC is in charge of co-ordinating "all international law-enforcement networks to facilitate the exchange of information and manage operational protocols."[206] At the operational level, exchanging information with foreign law-enforcement agencies and courts was described as effective but problems arise when requesting information from ISPs overseas and from private Internet companies (such as Facebook and Google) in the US, since they rarely respond and avoid co-operating with law enforcement in Brazil. In other words, if companies are based in Brazil,

requesting information is easier because they have to comply with Brazilian law. Another concern raised during the review was an issue regarding Mutual Legal Assistance Treaties (MLATs) because they are very slow and this slows down investigations. It often takes as long as two years to get an answer to an official request from the US because they have only a few prosecutors dealing with MLATs from around the world.

INTERPOL Brasilia has access to INTERPOL's secure communication linkage, I-24/7, which is a restricted-access Internet portal that provides police across the country with instant and automated access to INTERPOL's criminal databases.[207] The I-24/7 network is considered to be an informal co-operation because it is used only to share information for intelligence purposes and not for gathering evidence. In 2017, Brazil (the Brazilian Federal Police) and Europol signed a strategic agreement to expand co-operation to combat cross-border criminal activities, which could be considered as a formal co-operation.[208]

A participant added that cybercrime training and international cyber-related events serve as another platform on which to create trust and connections between different stakeholders, in order to enable informal requests for support in preserving data or obtaining information to determine the best way forward. The Government is in the process of taking steps to put Brazil into a legislative position to ultimately ratify the Budapest Convention on Cybercrime.

Results from the validation process conducted in March 2019:

Once again, the participants in the 2019 validation focus-group interviews noted that the collaboration between ISPs and law-enforcement authorities is ongoing but there are still examples of ISPs refusing to do so. An issue is exacerbated by, inter alia, the sheer number of ISPs in the country, many of which do not have dedicated IT personnel and rely on external consultants to deal with cybersecurity issues.

The co-operation between the CERT.br and CTIR Gov, on the other hand, has arguably improved. The same has been claimed by the interviewees in 2019 about the co-operation between the various levels of law enforcement in the country; roles and responsibilities between state and federal law enforcement agencies are clear and relationships are arguably functional. All these entities have a designated round-the-clock contact point, which contributes to what was assessed by the 2019 review-validation interviewees as "good communication".

Recommendations

Following the information presented on the review of the maturity of cybersecurity legal and regulatory frameworks, the following set of recommendations is provided to Brazil. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the Centre's CMM.

Legal Frameworks

R 4.1
Consider setting up a periodic process of reviewing and enhancing Brazil's laws relating to cyberspace to address the dynamics of cybersecurity threats (e.g.: cyber-bullying, sexting and accessing and downloading child pornography images);

R 4.2
develop new legislative provisions through multi-stakeholder consultation processes on IP online and human rights online;

R 4.3
enact commencement orders for existing legislation and assign bodies to monitor the enforcement of cybersecurity and cybercrime;

R 4.4
dedicate resources to ensure full enforcement of existing and new cybersecurity laws and monitor implementation;

R 4.5
ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted in order to successfully investigate cybercrime;

R 4.6
consider developing a strategy that covers cybersecurity and cybercrime and that would also clarify the roles and responsibilities of the actors (CIRTs, law enforcement, ministries) involved in handling computer-security incident response and cybercrime investigations;

R 4.7
adapt and implement legal provisions on e-commerce, regarding cybercrime incidents such as online fraud, spam, and phishing sites;

R 4.8
consider developing a platform for sharing electronic evidence between regional cybercrime forces;

R 4.9
enhance the existing co-operation between ISPs and law-enforcement agencies for removal of copyright-infringing content from websites;

R 4.10
revise and enforce legislative provisions that obliges ISPs to provide technical assistance for law enforcement when they conduct lawful electronic surveillance; and

R 4.11
consider signing the Council of Europe's Budapest Convention on Cybercrime.

Criminal Justice System

R 4.12
Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators;

R 4.13
allocate resources dedicated to fully operational cybercrime units based on strategic decision-making in order to support investigations, especially at the state level;

R 4.14
establish institutional capacity-building programmes for judges, prosecutors and police personnel (for instance through Ameripol, Interpol, Europol or other organisations) in order to acquire new ICT skills needed for cybercrime investigations (e.g.: digital evidence gathering) and effective ways of enforcing cyber-laws;

R 4.15
strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody;

R 4.16
build a cadre of specialist prosecutors and judges to handle cybercrime cases and cases involving electronic evidence;

R 4.17
consider establishing standards for the training of law enforcement officers on cybercrime;

R 4.18
dedicate sufficient human and technological resources in order to ensure effective legal proceedings regarding cybercrime cases;

R 4.19
consider requesting reliable and accurate cybercrime statistics from the Federal Police's URCC and the CERT.br in order to better inform decision-makers about the current cybercrime threat landscape in Brazil when developing policies and legislations to address this matter;

R 4.20
consider creating a National Cybercrime Laboratory under the auspices of the Federal Police's URCC in order to facilitate digital forensics;

R 4.21
establish a formal mechanism to enable the exchange of information and good practices between prosecutors and judges in order to ensure efficient and effective prosecution of cybercrime cases; and

R 4.22
collect and analyse statistics and trends regularly on cybercrime investigations, on cybercrime prosecutions and on cybercrime convictions.

Formal and Informal Co-operation Frameworks

R 4.23
strengthen international co-operation to combat cybercrime based on existing legal assistance frameworks and enter further bilateral or international agreements;

R 4.24
consider setting up a Threat Intelligence Platform for real-time information sharing between the Federal Police's URCC and the CERT (CERT.br);

R 4.25
allocate resources to support the exchange of information between domestic public and private sectors and to enhance the legislative framework and communication mechanisms;

R 4.26
enhance co-operation between the public sector and banks and other financial institutions regarding the sharing of incidents, in order to increase the level of cybersecurity awareness in Brazil;

R 4.27
facilitate informal co-operation mechanisms within the police and criminal justice systems, and between the police and third parties, both domestically and across borders, in particular ISPs; and

R 4.28
strengthen informal co-operation mechanisms within the police and criminal-justice systems, and between police and third parties, both domestically and across borders. Consider know-hows from other areas, such as anti-corruption co-operation.

Cybersecurity

Capacity Review

Federative Republic of Brazil

Dimension 5

Standards, Organisations and Technologies

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

D 5.1 - Adherence to Standards

This factor reviews the Government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Formative – Established

Brazil has established a number of institutions that organisations, both private and public, can refer to for certification against ICT standards, best practices and guidelines. More specifically, Associação Brasileira de Normas Técnicas (ABNT) provides the Brazilian versions of ISO IEC standards such as ABNT NBR ISO/IEC 270001; CEPESC is the Research and Development Centre for the Security of Communication which is responsible for the development of projects related to the security of communications, including

technology-transfer; CAIS RNP, despite being the incident-response team for the Brazilian academic networks, is responsible for creating and promoting security practices for networks in general. According to government sources, there are normative instruction and complementary norms elaborated in the Information Security Department of GSI, which deal with the normalisation of information security and cybersecurity in the realm of the FPA.

Participants suggested that the design, adoption and audit of cybersecurity standards vary significantly across the public and private sectors. Regarding the public sector, there are strict rules that have been converted into standards since 2001, and which apply to the FPA.[209] There is a system in place for auditing and all federal agencies are required to designate a unit within their organisation to perform audits. Furthermore, there is a general controls office that is tasked to design standards, and to assess the progress of implementation of these standards by all departments. In addition, there is a self-evaluation tool at the disposal of departments to help them prepare for future audits. Finally, participants mentioned that the FPA has designed a maturity model and visited more than 40 agencies to establish a comprehensive picture of its overall level of maturity. In stark contrast, there are significant differences in maturity in public state-level organisations. The main reason is the absence of a mechanism to enforce a uniform application of policies, as well as a lack of expertise and funding. Furthermore, a lack of accountability when employees do not comply with policies and the absence of metrics to measure compliance all contribute to poor cybersecurity practice in the states.

Interesting cases are SERPRO and DATAPREV, two companies that are not part of the FPA but which provide critical services to the Brazilian Government. Both adhere to the highest of international standards, with DATAPREV having obtained Tier 4 certification for two of their data centres, while the third has a Tier 3 certification.

Focusing on the private sector, participants postulated that the rate of adoption differs between sectors, with finance and electronic communication companies being pioneers in this area. Certain sectors, such as electronic communications and finance, have some mandatory security requirements; however, in the majority of cases, the driving force for adherence to standards is market demand and business need. ISO 27001 is the most frequently adopted framework, with the NIST cybersecurity framework being considered as well.

Participants agreed that the Central Bank can impose security requirements, but there is no specific standard promoted by the regulator. There are a combination of international standards, such as Payment Card Industry Data Security Standard (PCI DSS)[210] for data security imposed by MasterCard[211] and Visa,[212] which companies set out to follow strictly. It is worth noting that during the review, we did not have the opportunity to speak with private financial institutions, to corroborate these findings.

Focusing on standards in software development and procurement, there are specific guidelines in place for the public sector but the extent to which these guidelines are related to cybersecurity is not clear. Participants suggested that there are requirements in the FPA regarding purchase of cybersecurity equipment and the development of software. These requirements are generic and organisations develop internal processes. Overall, participants claimed that the guidelines are effective and provide transparency. We were not able to obtain a clear picture for the private sector.

Participants acknowledged the need for a security-related authority to set standards

across all sectors (not only in the FPA) and to promote adherence to these standards. The importance of streamlining the process of software and hardware procurement was highlighted as well. It was further suggested that discussions with all relevant stakeholders and regulators must commence before the adoption of the national cybersecurity strategy.

Results from the validation process conducted in March 2019:

In March 2018, there were no nationwide ICT standards prescribed in the banking sector, which was reflected in our report. Since then, the situation has changed. According to the Brazilian National Monetary Council's Resolution, CMN 4,658, of April 26, 2018,[213] all financial institutions under the regulatory umbrella of the Central Bank of Brazil had to put in place a cybersecurity policy by 6 May 2019, and have to take measures in accordance with the cybersecurity standards prescribed by this resolution by the end of 2021. Aside from this, no new cybersecurity standards have been reported by the 2019 interviewees.

D 5.2 - Internet Infrastructure Resilience

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the Government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Established

Review participants suggested that the Internet infrastructure in Brazil is very resilient. There has been a constant increase in the number of Internet users over the last five years. Currently, the Internet penetration rate in Brazil is above 67 percent.[214]

There is also a significant mobile-Internet market with more than 81 million people using mobile Internet.[215] E-commerce sales are rising and currently exceed $20 billion, since more than 61 million people are digital buyers, with mobile-commerce reaching a penetration rate of 32 percent.

These statistics provide the foundations for understanding the maturity of Internet infrastructure resilience and of security standards in e-services offered by public and private organisations. Participants suggested that a wide range of e-government services are offered, such as e-voting. Similar observations can be drawn for the private sector, where there is an abundance of e-services, with participants believing that their uptake is increasing.

There is a wide range of public and private ISPs in Brazil, with varying degrees of quality, services and pricing. There are regulations

imposed by Abranet,[216] but we were unable to interview people from the telecommunications sector during our review. Based on our desktop research, there are more than 25 Internet eXchange Points (IXPs), which are maintained by an overarching project named IX.br. The number of IXs ensures an appealing environment for innovation and Internet connectivity, while it increases the resilience of the Internet infrastructure.[217] It is worth noting that the IX.br project achieves a maximum throughput of 5,060GB per second with an average of 3,260GB per second for Brazil, broadly equivalent to the services offered by German provider DE-CIX, which are the highest in the world.[218]

Results from the validation process conducted in March 2019:

In addition to the information gathered during the review, participants in the 2019 review-validation group interviews informed us of NIC.br's activities to advance Internet infrastructure resilience. In particular, we learned about the promotion of Mutually Agreed Norms for Routing Security (MANRS), which aim to encourage network operators and internet exchange points to nurture resilience in Brazil's Internet infrastructure.

D 5.3 - Software Quality

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Stage: Formative

Software quality varies significantly in the public sector depending on whether organisations are part of the FPA or not. There is an inventory of secure software for the FPA and networks are monitored for malware. Patching of outdated software is achieved automatically and there are KPIs in place to evaluate the effectiveness of the patching mechanisms. Furthermore, all ministries have agencies that cover ICT management and establish requirements regarding software. There is a dedicated IT office that provides both software and hardware solutions, so the administration support is centralised.

Participants suggested that organisations in state government do not have a catalogue of secure software and that patching is not consistently implemented. Regarding the private sector, software quality depends largely on the size of the organisation, with corporations in the financial and telecommunication sectors being more mature.

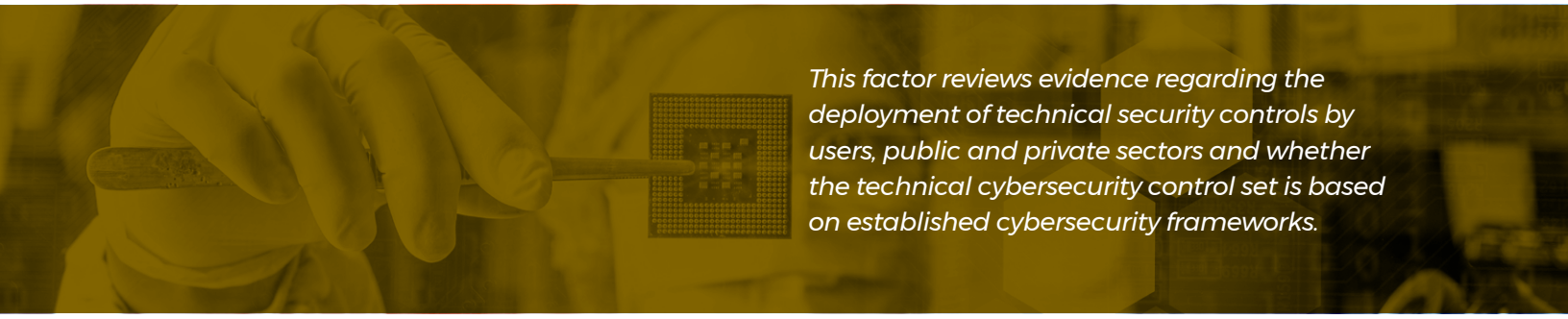
Software development is common practice in both the public and private sectors,. Participants mentioned that in-house software tools are developed to monitor networks, classify incidents and provide situational awareness.

Artificial intelligence and machine-learning techniques are utilised by organisations to deter, detect and mitigate cyber-attacks.
As participants explained, technology-transfer is problematic in Brazil due to the lack of legislation to establish and protect IP. Many international organisations in the technology sector are therefore hesitant to provide software solutions to Brazil. This has led to an increase in the design of domestic cybersecurity products. We were not able to obtain a clear picture on whether in-house software is tested to validate security properties.

Results from the validation process conducted in March 2019:

During the 2019 validation workshop, participants added that neither the aviation industry nor the financial sector[219] has a catalogue of secure software platforms and applications, although both industries are reportedly security-conscious when it comes to software in use. Nevertheless, due to budgetary constraints, software used by the financial institutions is not regularly updated.

D 5.4 - Technical Security Controls



This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

Stage: Established

The adoption of technical security controls in Brazil varies across sectors and organisations. Participants suggested that the adoption and implementation of controls in government bodies is very advanced in the FPA, but rather elementary and inconsistently promoted in the state governments due to financial restrictions, limitations in human resources and a lack of appropriate organisational structure. Brazil has an extensive constitution that currently does not cater for cybersecurity. There is a strategy for the implementation of controls in the FPA which includes a detailed model for assessing the maturity of organisations, but it has no control over the states and municipalities. As a result, any technical control that is mandatory for the FPA cannot be enforced in the states, nor can auditing agencies monitor them for compliance.

Participants mentioned that there are 22 complementary rules which describe the technical controls for the FPA. There are decentralised networks protected by a CERT, filters and firewalls, intrusion detection systems (IDS) that utilise artificial intelligence to determine trends, back-up systems, incident-response and recovery processes, as well as platforms for sharing threat intelligence with other stakeholders. Participants mentioned the "wannacry" incident as an example where, thanks to platforms for sharing threat intelligence, they were able to automatically exchange information about the malware, readjust the hardening of networks and exchange patches and software updates. Finally, there are metrics for all the controls and risk assessments that are conducted frequently.

In the private sector, there is an understanding that well-established organisations adopt adequate technical controls tailored to their networks. Network-segmentation controls and monitoring tools are evident in this sector, as well as the use of IDSs and other Security Information and Event Management (SIEM) tools. Specific organisations have established a CERT to monitor their networks. Of particular concern, however, is the fact that organisations in the private sector are not required to share information about incidents with the national CERT and may not receive threat intelligence.

Generally, the level of understanding and deployment of security controls in the private and public sectors is thought by the participants to be adequate. However, no mechanisms are in place to assess the effectiveness of these controls in specific organisations, nor processes to recommend further improvements. Participants concurred that a single authority should be responsible for strategic decisions on technical controls and should promote the adoption of a unified framework as a minimal set of security controls.

Results from the validation process conducted in March 2019:

The research conducted in 2019 largely confirms the evidence obtained during the 2018 CMM review, which was further substantiated by the outcomes of desktop research. Data from NIC.br[220] indicates that 93 percent of public-sector organisations in Brazil perform data backups regularly and 85 percent of them set up physical controls to prevent unauthorised personnel from accessing computing facilities.

D 5.5 - Cryptographic Controls

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up to date.

Stage: Established

The Brazilian Public Key Infrastructure (ICP-Brazil) is the entity responsible for ensuring authenticity, integrity and legal validity of documents in electronic form; supporting applications and accredited applications using digital certificates; and ensuring secure electronic transactions.[221] ICP-Brazil comprises a number of certification authorities which provide different services, such as a Root Certification Authority (Root CA), certification authorities (CAs) and registration authorities (RAs). ICP Brazil has established technical standards for the accreditation of CAs and RAs, provides audits, and supervises the Root CA and its service providers. Participants noted that there are very strict requirements both for

Root CAs (Level 5) and CAs which provide the Public Key Infrastructure (PKI).

In the federal government, ABIN is the accreditation centre for encryption and provides specific rules on how classified information should be transmitted, defines the communication protocol for sensitive information (PGP is used) and instructs how data should be stored. Focusing on DATAPREV, they use SSH for their services, and encrypt data in transit but do not encrypt the data in the repositories. The use of cryptographic emails is prevalent in DATAPREV, but this has created problems with auditing. Therefore, for non-sensitive information the use of encrypted emails is discouraged. Participants mentioned that there is a master key to decrypt information for auditing purposes. Regarding the private sector, similar observations can be made. Encryption is considered mainly for critical systems for both data in transit and data at rest. We were not able to obtain a clear picture of whether web service providers offer SSH connections between servers and web browsers.

Results from the validation process conducted in March 2019:

The importance of cryptography has been recognised by the federal authorities and use of it is encouraged by the National Information Security Policy adopted at the end of 2018.[222] Participants of the 2019 validation group interviews did note that this policy is only aimed at the federal public institutions and should be expanded across all sectors to have a tangible impact on the cybersecurity capacity maturity of Brazil. It is hoped this would spread the use of cryptography, which is reportedly not yet widely used in all the critical sectors.

D 5.6 - Cybersecurity Marketplace

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Formative – Established

The domestic market for cybersecurity technologies in Brazil is at an established level of maturity. There is a wide range of cybersecurity software products developed in-house by both public and private companies. Participants mentioned that some of these technologies are exported and used by other countries. Similarly, there is less dependence on foreign cybersecurity technologies. According to participants, the prevalence of hackers in Brazil has resulted in an ever-increasing demand for cybersecurity products. To meet this demand, local companies develop and offer solutions for national security software. An important factor for the established domestic market is the lack of legislation to protect IP, which renders foreign organisations reluctant to deploy their software solutions in Brazil for fear of IP theft.

The cyber-insurance market in Brazil is at a formative level of maturity. There are a range of policies on offer and the demand from organisations is increasing. Usually policies detail situations under which the insurance is valid and, on a positive note, specify security guidelines that organisations must adhere to in order to be insurable. A small number of participants noted that their organisations are covered for specific cyber-incidents.

Participants concurred that it is beneficial for all organisations to obtain cyber insurance since, as they suggested, the cost of even one incident justifies the expense. Additionally, they highlighted that the support offered during incidents and specifically the forensic analysis, which is invaluable.

Results from the validation process conducted in March 2019:

In 2019, the validation workshop largely confirmed the outcomes of the 2018 CMM report.

D 5.5 - Cryptographic Controls

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up to date.

Stage: Formative – Established

Participants concluded that responsible disclosure varies between sectors, with the FPA achieving an established degree of maturity with some indicators from the strategic level being present. In stark contrast, the state governments and the private sector are in the formative stage of maturity.

More specifically, a vulnerability-disclosure framework is in place for the FPA. Organisations have established formal processes to disseminate information automatically and the national CERT receives this information and provides comprehensive reports on how to address incidents. There were cases, such as the "wannacry" event, where technical details and patches were shared in a timely manner to all relevant stakeholders, which were able to automatically parse the information and act to protect their networks.

Conversely, private organisations are excluded from the Government's threat-intelligence sharing. Moreover, they are not obliged to report incidents so they tend to conceal any issues that they detect. Considering the fact that Brazil has started to privatise critical parts of the national infrastructure, participants urged the Government to acknowledge the important role played by private organisations in the national cybersecurity strategy and to give them access to threat-intelligence systems.

Finally, there are various means for citizens to report incidents, either via the state police (the maturity of which is, however, not comparable to that of the Federal Police) or via websites. There are dedicated channels of communication in the banking sector for customers to report online fraud, and several public organisations, such as SERPRO, provide guidance on how to defend against threats, through social media, radio programmes and newspapers.

Recommendations

Following the information presented on the review of the maturity of cybersecurity standards, organisations and technologies, the following set of recommendations is provided to Brazil. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the Centre's CMM.

Adherence To Standards

R 5.1
Adopt a nationally agreed baseline of cybersecurity-related standards and good practices across the public and private sectors, including standards in procurement and software development;

R 5.2
establish or assign an institution responsible for the implementation, auditing and measurement of the success of standards across public and private sectors. Apply metrics to monitor compliance and establish periodic audits;

R 5.3
promote discussions on how standards and good practices can be used to address risk within CI supply chains by both government and private organisations. Identify and mandate standards to which CIs should adhere to;

R 5.4
identify a minimum set of controls for all governmental departments (including state government) based on annual assessments and threat intelligence from national CERT, and establish a controls review to assess the effectiveness of the current controls and practices;

R 5.5
establish mandatory requirements for the adherence to standards by appointing security officers who will be held responsible for their implementation;

R 5.6
enact legislation to allow the enforcement of disciplinary action for policy violations;

R 5.7
streamline clear guidance for the procurement of hardware and software by considering standards that cater for cybersecurity;

R 5.8
promote the awareness and implementation of standards among SMEs; and

R 5.9
establish a framework to assess the effectiveness of standards for procurement and software development.

Internet Infrastructure Resilience

R 5.10
Enhance co-ordination and collaboration regarding resilience of Internet infrastructure across public and private sectors;

R 5.11
conduct regular assessments of processes according to international standards and guidelines, together with assessment of national information infrastructure security and critical services that drive investment in new technologies;

R 5.12
identify and map potential points of critical failure within the Internet infrastructure; and

R 5.13
establish a system to formally manage the national infrastructure, with documented processes, roles and responsibilities, and adequate redundancy.

Software Quality

R 5.14
Develop a catalogue of secure software platforms and applications within the public and private sectors;

R 5.15
develop an inventory of software and applications used in public sector and CI;

R 5.16
develop policies and processes on software updates and maintenance and enforce these for CIs in the public and private sector;

R 5.17
gather and assess evidence of software quality deficiencies regarding their impact on usability and performance;

R 5.18
establish or assign an institution to elicit, in a strategic manner, common requirements for software quality and functionality across all public and private sectors; and

R 5.19
monitor and assess the quality of software used in public and private sectors.

Technical Security Controls

R 5.20
Establish frequent training for IT employees;

R 5.21
encourage ISPs and banks to offer anti-malware and anti-virus services;

R 5.22
establish metrics for measuring the effectiveness of technical controls across the public domain (including the state government) and advise the private sector to adopt these metrics;

R 5.23
develop processes for reasoning about the adoption of more technical controls based on risk-assessment methodologies across the public domain;

R 5.24
promote best practices in cybersecurity for users;

R 5.25
designate an authority to be responsible for strategic decisions on technical controls, that will supervise all networks, end-to-end, and promote the adoption of a unified framework for security controls;

R 5.26
deep technical security controls up to date within the public and private sectors, monitor their effectiveness and review on a regular basis; and

R 5.27
conduct penetration testing for the protection of both private and public sectors regularly.

Cryptographic Controls

R 5.28
Encourage the development and dissemination of cryptographic controls across all sectors and users for the protection of data at rest and in transit, according to international standards and guidelines;

R 5.29
raise public awareness of secure communication services, such as encrypted/signed emails;

R 5.30
consider encryption of data at rest in the data centres; and

R 5.31
establish or assign an institution to be responsible for designing a policy that will assess the deployment of cryptographic controls according to their objectives and priorities within the public and private sector.

Cybersecurity Marketplace

R 5.32
Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development;

R 5.33
Promote sharing of information and best practices among organisations, to explore potential insurance coverage.

Responsible Disclosure

R 5.34
Develop a responsible vulnerability-disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledgment report;

R 5.35
establish or assign an institution responsible for supervising the process of responsible disclosure and ensure that organisations do not conceal vulnerability information;

R 5.36
redesign the current system which facilitates threat-intelligence sharing among the critical infrastructure partners to include private sector and civil service. Promote sharing of threat intelligence and incentivise private companies to actively participate;

R 5.37
promote the existing incident-reporting mechanisms in the public sector;

R 5.38
define thresholds and notification requirements for all sectors. These requirements should not only consider availability of services but the integrity and confidentiality of data; and

R 5.39
agree on clear instructions on how to share information uniformly within other countries in the LAC region (and not only) in a formal and structured manner.

Additional Reflections

Although the level of stakeholder engagement in the review was more limited than we might have hoped, which limits the completeness of evidence in some areas, the representation and composition of stakeholder groups was, overall, balanced and broad.

The 2018 CMM review was the twenty-third country review that we have directly supported.

The 2019 review-validation workshop was the first attempt by the GCSCC researchers to seek confirmation of the initial review results and to investigate changes in cybersecurity capacity maturity of a nation. Although no major changes in maturity were detected, the validation activity is considered to have been useful.

Global Cyber Security Capacity Centre
Department of Computer Science, University of Oxford
Wolfson Building, Oxford OX1 3QD,
United Kingdom

Tel: +44 (0)1865 287434
Email: cybercapacity@cs.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk/cyber-security
Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity

Prepared and published by the Cybersecurity Program of the Inter-American Committee against Terrorism (cybersecurity@oas.org).

This Publication has been made possible thanks to the financial support of the UKFCO, as part of its Digital Access Programme.

References

1. "Cybersecurity Capacity Maturity Model for Nations" (CMM), Revised Edition, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (assessed 25 February 2018).

2. "Estrategia de segurance da informacao e comunicacoes e de segurance cibernetica da administracao publica federal 2015–2018", Presidência da República Gabinete de Segurança Institucional Secretaria-Executiva Departamento de Segurança da Informação e Comunicações, 2015, http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf (accessed 29 July 2018).

3. National Cybersecurity Strategy, 2020, Federal Decree No. 10.222, http://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419 (accessed 16 April 2020).

4. Some are called CSIRTs and other CERTs.
5. "About CERT.br", https://www.cert.br/about/ (accessed 1 June 2020).

6. http://www.inhope.org/gns/our-members/Brazil.aspx; http://new.safernet.org.br/ (accessed 7 May 2019).

7. http://www.pf.gov.br/ (accessed 7 May 2019).

8. www.disque100.gov.br (accessed 7 May 2019).

9. SaferNet Brazil, http://new.safernet.org.br/content/o-que-fazemos (accessed 14 July2018).

10. INHOPE Association–SaferNet Brazil, https://www.inhope.org/EN/become-a-partner (accessed 14 July 2018).

11. CGI.br, https://www.cgi.br/about/ (accessed 14 July2018)

12. Brazilian Network Information Centre (NIC.br), Available at https://www.nic.br/who-we-are/ (accessed 14 July 2018).

13. Antispam.br, http://www.antispam.br/ (accessed 14 July2018).

14. InternetSegura.br, https://www.internetsegura.br/ (accessed 14 July2018).

15. J. L. Marciano, "Applying COBIT in a Government Organization," ResearchGate, April 2015, https://www.researchgate.net/publication/275638852 (accessed 13 July 2018).

16. Cyber Crimes Act (Law No. 12,737/2012), also known as "Carolina Dieckmann Law", http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm (accessed 14 May 2018).

17. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishes the principles, guarantees, rights and duties for use of the Internet in Brazil – Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 Brazilian Civil Framework of the Internet in English (accessed 14 April 2018).

18. Constitution of the Federative Republic of Brazil, 1998, http://english.tse.jus.br/arquivos/federal-constitution (accessed 14 May 2018).

19. Penal Code 1940, Decree-Law No. 2.848, 7 December, 1940, http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm (accessed 11 May 2018).

20. Consumer Protection Code (Law 8,078/1990) (1990), https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf (accessed 14 May 2018).

21. Janice K. Song, "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying", World Bank, 2015; License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf (accessed 16 June 2018).

22. Law on Copyright and Neighbouring Rights, 1998, (Law No. 9.610), http://www.wipo.int/wipolex/en/text.jsp?file_id=125393 (accessed 14 June 2018).

23. Rafael Mendes Loureiro and Leonardo A F Palhares, "Cybersecurity – Brazil. Getting the Deal Through", Law Business Research Ltd., https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (accessed 14 June 2018).

24. Ministry of Foreign Affairs, Process of accession to the Budapest Convention – Joint Note by the Ministry of Foreign Affairs and the Ministry of Justice and Public Security, Note 309, 2019, http://www.itamaraty.gov.br/en/press-releases/21149-accession-process-to-the-budapest-convention-joint-note-by-the-ministry-of-foreign-affairs-and-the-ministry-of-justice-and-public-security (accessed 15 April 2020).

25. Ministry of Justice and Public Security, Ministry of Justice and Public Security co-ordinates integrated operation against sexual abuse and sexual exploitation committed through the internet, 2019, https://www.justica.gov.br/news/collective-nitf-content-1553775485.52 (accessed 15 April 2020).

26. Law No. 13,844, June 2019, establishing the basic organisation of the organs of the Presidency of the Republic and the Ministries, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm (accessed 15 April 2020).

27. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (accessed 14 April 2018).

28. See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (accessed 7 May 2019).

29. Relevant publications: M. Williams, Making sense of social research (London: Sage Publications Ltd. 2003), doi: 10.4135/9781849209434; J. Knodel, "The design and analysis of focus group studies: A practical approach", in D. L. Morgan, Successful focus groups: Advancing the state of the art (SAGE Focus Editions 1993) 35–50; Thousand Oaks, CA: SAGE Publications Ltd., doi: 10.4135/9781483349008; R. A. Krueger, and M. A. Casey, Focus groups: A practical guide for applied research (London: Sage Publications Ltd. 2009).

30. Relevant publications: J. Kitzinger, "The methodology of focus groups: the importance of interaction between research participants", Sociology of Health & Illness, 16(1) (1994), 103–121; J. Kitzinger, 'Qualitative research: introducing focus groups', British Medical Journal, 311(7000) (1995), 299– 302; E. F. Fern, 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality', Journal of Marketing Research, Vol. 19, No. 1 (1982), 1–13.

31. J. Kitzinger, 'Qualitative research: introducing focus groups', British Medical Journal, 311(7000) (1995), 299–302.

32. K. Krippendorff, Content analysis: An introduction to its methodology (Sage Publications Inc., 2004). H. F. Hsieh and S. E. Shannon, "Three approaches to qualitative content analysis", Qualitative Health Research, 15(9) (2005), 1277–1288; K. A. Neuendorf, The ContentAanalysis Guidebook (Sage Publications Inc., 2002).

33. E. F. Fern, "The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality", Journal of Marketing Research, Vol. 19, No. 1 (1982), 1–13, 1982.

34. S. Elo and H. Kyngas, "The qualitative content analysis process", Journal of Advanced Nursing, 62(1) (2008), 107–115; H. F. Hsieh and S. E. Shannon, "Three approaches to qualitative content analysis," Qualitative Health Research, 15(9) (2005), 1277–1288.

35. P. D. Barbara Downe-Wamboldt RN, "Content analysis: Method, applications, and issues", Health Care for Women International, 13(3) (1992, 313–321.

36. I. Dey, Qualitative data analysis: A user-friendly guide for social scientists (London: Routledge, 1993).

37. https://cetic.br/noticia/acesso-a-internet-por-banda-larga-volta-a-crescer-nos-domicilios-brasileiros/ (accessed 7 May 2019).

38. https://www.itu.int/net4/ITU-D/idi/2017/index.html (accessed 7 May 2019).

39.http://reports.weforum.org/global-competitiveness-index-2017-2018/countryeconomy-profiles/#economy=BRA (accessed 7 May 2019).

40.https://ww2.frost.com/files/5515/2878/9339/Digital_Market_Overview_FCO_Brazil_25May18.pdf (accessed 7 May 2019).

41. Ibid..

42. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (accessed 7 May 2019).

43. Brazil 2022, Presidencia da Republica Secretaria De Assuntos Estrategicos, 2010.

44. Livro Verde: Segurança Cibernética no Brasil, Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações, Brasília, 2010, http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf/view (accessed 29 July 2018).

45. National Strategy of Defence, Ministry of Defence, 2012, http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm (accessed 29 July 2018).

46. Estrategia de segurance da informacao e comunicacoes e de segurance cibernetica da administracao publica federal 2015–2018, Presidência da República Gabinete de Segurança Institucional Secretaria-Executiva Departamento de Segurança da Informação e Comunicações, 2015, http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf (accessed 29 July 2018).

47. The Estrategia document is not translated into English and we used the translations services of Google.

48. http://www2.planalto.gov.br/conheca-a-presidencia/ministros (accessed 7 May 2019).

49. Article 19, "Brazil: Cyber-security strategy", 2016; G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil", 2014, Strategic Paper.

50. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 (accessed 7 May 2019).

51. Ibid., Art. 5.

52. Ibid., Art. 6.

53. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 art 6 (accessed 7 May 2019).

54. National Cybersecurity Strategy 2020, Federal Decree No. 10.222, http://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419 (accessed 16 April 2020).

55. OneTrust Data Guidance, "Brazil: President approves national cybersecurity strategy", 2020, https://platform.dataguidance.com/news/brazil-president-approves-national-cybersecurity-strategy (accessed 16 April 2020).

56. Ibid.

57. Law No. 13,844, June 2019, establishing the basic organisation of the organs of the Presidency of the Republic and the Ministries, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm (accessed 15 April 2020).

58. Image from https://www.cert.br/csirts/brazil/ (accessed 7 May 2019).

59. Núcleo de Informação e Coordenação do Ponto BR, https://bcp.nic.br/ (accessed 7 May 2019).

60. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, https://cartilha.cert.br/ (accessed 7 May 2019).

61. Brazilian Computer Security and Incident Response Teams, https://www.cert.br/csirts/brazil/ (accessed 7 May 2019).

62. Cristine Hoepers, "Incident Handling in Brazil," 2010, https://www.cert.br/docs/palestras/certbr-certpt2010.pdf 12 (accessed 7 May 2019).

63. Lucimara Desiderá, "Incident Handling in High Profile International Events: Lessons Learned and the Road Ahead", 2016, https://www.cert.br/docs/palestras/certbr-tcfirst-praga2016.pdf (accessed 7 May 2019).

64. Cristine Hoepers, "Evolution of the Scenario of Incidents in Brazil", 2018, https://www.cert.br/docs/palestras/certbr-oas2018.pdf 21 (accessed 7 May 2019).

65. Ibid.

66. Brazilian Computer Security and Incident Response Teams, Spampots Project, https://honeytarg.cert.br/spampots/ (accessed 7 May 2019)

67. Department of Information Security, http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view
(accessed 7 May 2019)

68. http://www.planejamento.gov.br/assuntos/orcamento-1/orcamentos-anuais/2018/legislacao/alteracoes/lei-no-13-749-de-22-de-novembro-de-2018.pdf (accessed 7 May 2019).

69. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil", Strategic Paper, 2014.

70. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8491.htm#art2 (accessed 7 May 2019).

71. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 art 6 (accessed 7 May 2019).

72. https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf 93-95 (accessed 7 May 2019).

73. http://www.serpro.gov.br/ (accessed 7 May 2019).

74. CICG-IPSOS "Global Survey on Internet Security and Trust" (2018 Poll, "Part 1: Privacy, Security, Access and Trust").

75. https://gvpesquisa.fgv.br/sites/gvpesquisa.fgv.br/files/arquivos/meirelles_-_information_technology_and_egovernment_in_brazil_.pdf (accessed 7 May 2019).

76. https://www.bb.com.br/pbb/pagina-inicial/bb-seguranca/dicas-de-seguranca#/ (accessed 7 May 2019).

77. https://www.itau.com.br/seguranca/ (accessed 7 May 2019).

78. http://www.planejamento.gov.br/EGD/arquivos/revisao-da-estrategia-de-governanca-digital-2015-2019.pdf (accessed 7 May 2019).

79. https://principios.cgi.br/ (accessed 7 May 2019).

80. "Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector", OECD, 2018.

81. See e.g. http://www.ejeg.com/issue/download.html?idArticle=417 147; https://www.cetic.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf 219 (accessed 7 May 2019).

82. https://www.ctir.gov.br/arquivos/alertas/2018/ALERTA_CTIRGOV_2018_03_SQL_Injection.pdf (accessed 7 May 2019).

83. https://www.cetic.br/media/docs/publicacoes/2/tic_dom_2017_livro_eletronico.pdf 253 & 333 (accessed 7 May 2019).

84. See e.g. https://www.kabum.com.br/cgi-local/site/institucional/politicas.cgi (accessed 7 May 2019).

85. See e.g. https://www.magazineluiza.com.br/estaticas/seguranca-maxima/ (accessed 7 May 2019).

86. https://nic.br/media/docs/publicacoes/13/fasciculo-comercio-eletronico.pdf (accessed 7 May 2019).

87. CIGI-IPSOS "Global Survey on Internet Security and Trust" (2018 Poll, "Part 2: E-commerce") https://www.cigionline.org/internet-survey-2018 (accessed 7 May 2019).

88. https://www1.folha.uol.com.br/mercado/2018/07/senado-aprova-projeto-sobre-protecao-de-dados-pessoais.shtml; g1.globo.com/jornal-nacional/noticia/2018/07/comissao-do-senado-aprova-projeto-de-lei-de-protecao-de-dados-pessoais.html (accessed 7 May 2019); https://www.cartacapital.com.br/sociedade/entenda-o-que-muda-com-a-nova-lei-de-protecao-de-dados (accessed 7 May 2019).

89. http://www.inhope.org/gns/our-members/Brazil.aspx , http://new.safernet.org.br/ (accessed 7 May 2019).

90. http://www.pf.gov.br/ (accessed 7 May 2019).

91. www.disque100.gov.br (accessed 7 May 2019).

92. http://www.caixa.gov.br/site/english/About-Caixa/Paginas/default.aspx (accessed 7 May 2019).

93. http://www.bcb.gov.br/en#!/home (accessed 7 May 2019).

94. http://g1.globo.com/tecnologia/noticia/2016/02/facebook-cria-central-de-prevencao-ao-bullying-no-brasil.html (accessed 7 May 2019).

95. SaferNet Brazil, http://new.safernet.org.br/content/o-que-fazemos (accessed 14 July 2018).

96. INHOPE Association, SaferNet Brazil, http://www.inhope.org/gns/our-members/Brazil.aspx (accessed 14 July 2018).

97. Hotline, http://new.safernet.org.br/denuncie (accessed 14 July 2018).

98. SaferNet Brazil, http://new.safernet.org.br/content/o-que-fazemos (accessed 14 July 2018).

99. SaferNet Brazil partnership with Google Brazil, http://www.safernet.org.br/site/institucional/parcerias/google (accessed 14 July 2018).

100. CGI.br, https://www.cgi.br/about/ (accessed 14 July 2018).

101. Brazilian Network Information Centre (NIC.br), https://www.nic.br/who-we-are/ (accessed 14 July 2018

102. Antispam.br, http://www.antispam.br/ (accessed 14 July 2018).

103. InternetSegura.br, https://www.internetsegura.br/ (accessed 14 July 2018).

104. CERT.br "Team Update: New Awareness Materials", 2017, https://www.cert.br/docs/palestras/certbr-natcsirts2017-2.pdf (accessed 12 July 2018).

105. Ministerio Publico Federal, Em parceria com Safernet, MPF debate segurança e bom uso da internet com educadores pessoenses, 2015, http://pfdc.pgr.mpf.mp.br/informativos/edicoes-2015/dezembro/em-parceria-com-safernet-mpf-debate-seguranca-e-bom-uso-da-internet-com-educadores-pessoenses (accessed 10 September 2018).

106.Federation of Industry of the State of Sao Paulo (FIESP) http://www.fiesp.com.br/?temas=seguranca (accessed 10 September 2018).

107. Brasscom, https://brasscom.org.br/events/forum-nacional-seguranca-cibernetica-nas-instituicoes-financeiras-impactos-da-resolucao-no-4-658/ (accessed 10 September 2018).

108. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 (accessed 7 May 2019).

109. See Footnote 94.

110. Ministry of Education, Catálogo Nacional dos Cursos Superiores de Tecnologia, http://portal.mec.gov.br/catalogo-nacional-dos-cursos-superiores-de-tecnologia- (accessed 10 September 2018).

111. Ibid.

112. University of Sao Paolo courses, http://www5.usp.br/english/education/undergraduate/courses-offered/?lang=en (accessed 25 July 2018).

113. Federal University of ABC, Computer Science, http://ufabc.edu.br/en/graduate-program/?id=6 (accessed 25 July 2018).

114. Ibid.

115. RNP, Cybersecurity Training, https://esr.rnp.br/seg12 (accessed 25 July 2018).

116. RNP, International Computer Security Day, https://disi.rnp.br/en (accessed 10 September 2018).

117. Senac College, post-graduate course in cyber-defence, https://www.df.senac.br/faculdade/wp-content/uploads/2018/01/desefa-ciberntica.pdf (accessed 25 July 2018).

118. Trend Micro, "The rise of the Brazilian underground", 2016, https://blog.trendmicro.com/the-rise-of-the-brazilian-underground/ (accessed 11 July 2018).

119. Base Nacional Comum, http://basenacionalcomum.mec.gov.br/wp-content/uploads/2018/04/BNCC_EnsinoMedio_embaixa_site.pdf https:/www.youtube.com/watch/?v=NT9Whez23gE (accessed 25 July 2018).

120. Division courses taught by CERT.br, https://www.cert.br/cursos/ (accessed 14 July 2018).

121. Best Practices Portal (BCP.nic.br) https://bcp.nic.br/sobre/ (accessed 14 July 2018).

122. Ibid.

123. ITU, Cyberwellness Profile, Brazil, 2012, https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf (accessed 11 May 2018).

124. CERT.br courses, https://www.cert.br/cursos/ (accessed 10 September 2018).

125. Cyber Defense Command. https://ava-enadciber.eb.mil.br/ (accessed 25 July 2018).

126. Fundação Bradesco, Information Security course, https://www.ev.org.br/curso/informatica/infraestrutura-de-ti/seguranca-da-informacao?return=/cursos/informatica (accessed 25 July 2018).

127. J. L. Marciano, "Applying COBIT in a Government Organization", 2015, http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Focus-Applying-COBIT-in-a-Government-Organization_nlt_Eng_0415.pdf (accessed 13 July 2018).

128. Ibid.

129. Federação Brasileira de Bancos, https://portal.febraban.org.br/ (accessed 8 May 2019).

130. Cyber Crimes Act (Law No. 12,737/2012) also known as "Carolina Dieckmann Law", http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm (accessed 14 May 2018).

131. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishing the principles, guarantees, rights and duties for use of the Internet in Brazil – Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 The Brazilian Civil Framework of the Internet in English (accessed 14 April 2018).

132. Diego R. Canabarro and Thiago Borne, "Reflections on the Fog of (Cyber) War", NCDG Policy Working Paper No. 13-002 (2013), https://www.umass.edu/digitalcenter/sites/default/files/Brazil%20and%20The%20Fog%20of%20%28Cyber%29War.pdf (accessed 11 May 2018).

133.Ministry of Defence, Cyber Defence Policy, Administrative Normative Rule No. 3,389, 2012, http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2012&jornal=1&pagina=11&totalArquivos=304 (accessed 11 May 2018).

134. White Paper on National Defence 2012, https://www.defesa.gov.br/arquivos/estado_e_defesa/livro_branco/lbdn_2013_ing_net.pdf (accessed 11 May 2018).

135. National Defence Strategy Decree 6703, 2008, http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm (accessed 11 May 2018).

136. Presidency of the Republic, Critical Information and Communication Infrastructure Protection, 2010, http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view (accessed 11 May 2018).

137. Anatel – Public Consultation No. 21, "Regulation on the risk management of telecommunications networks and use of telecommunications services in emergency and disaster situations", https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C1674&Tipo=1&Opcao=finalizadas (accessed 11 May 2018).

138. ITU, Cyberwellness Profile, Brazil, 2012, https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf (accessed 11 May 2018).

139. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review (Fourth Edition, Law Business Research Ltd., 2017).

140. Carolina Dieckmann is a famous Brazilian actress whose email account was hacked and her intimate photos were published on the Internet.

141. Penal Code (1940) Decree-Law No. 2.848, 7 December 1940, http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm (accessed 11 May 2018).

142. S. S. M. Ribeiro, Democracy after the internet: Brazil between facts, norms, and code (Vol. 27, Springer 2016).

143. Ibid.

144. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishing the principles, guarantees, rights and duties for use of the Internet in Brazil. Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 Brazilian Civil Framework of the Internet in English (accessed 14 April 2018).

145. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd. 2017).

146. Federal Prosecution Service, technical note about the ETS 185 Convention of the Council of Europe – convention on cybercrime – Budapest convention, Technical note 2nd CCR/SCI No. 1/2018, 2018, http://www.transparencia.mpf.mp.br/conteudo/servico-de-informacao-ao-cidadao/validacao-de-documentos (accessed 14 June 2018).

147. "How to be compliant with Brazil's Data Protection Act", IAPP, 2018, https://iapp.org/news/a/how-tobecompliantwithbrazilsdataprotectionact/?mkt_

148. Constitution of the Federative Republic of Brazil, 1998, http://english.tse.jus.br/arquivos/federal-constitution (accessed 14 May 2018).

149. Penal Code (Decree-Law No. 2.848, 7 December 1940) (1940) http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm (accessed 11 May 2018).

150. Consumer Protection Code (Law 8,078/1990) (1990) https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf (accessed 14 May 2018).

151. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishing the principles, guarantees, rights and duties for use of the Internet in Brazil. Brasília: Chamber of Deputies, Edições Câmara, 2016, (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 Brazilian Civil Framework of the Internet in English (accessed 14 April 2018).

152. "Brazil president approves data protection bill – but vetoes key accountability measures", Accessnow, 2018, https://www.accessnow.org/brazil-president-approves-data-protection-bill-but-vetoes-key-accountability-measures/ (accessed 10 September 2018).

153. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd., 2017).

154. C. Barbosa, P. Vilhena, K. L. Advogados, "Data protection in Brazil: overview", Practical Law, Global Guide 2016-17, 2016, https://uk.practicallaw.thomsonreuters.com/4-520 1732?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk (accessed 14 June 2018).

155. Brazilian Civil Code, 2002, http://www.wipo.int/wipolex/en/text.jsp?file_id=226198 (accessed 14 June 2018).

156.Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity - Brazil. Getting the Deal Through (Law Business Research Ltd.) https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (accessed 14 June 2018).

157. Law on Copyright and Neighbouring Rights, Law No. 9.610, 1998, http://www.wipo.int/wipolex/en/text.jsp?file_id=125393 (accessed 14 June 2018).

158. Hunton Andrews Kurth, "Brazil's Senate Passes General Data Protection Law", 2018, https://www.huntonprivacyblog.com/2018/07/11/brazils-senate-passes-general-data-protection-law/ (accessed 10 September 2018).

159. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity - Brazil. Getting the Deal Through (Law Business Research Ltd.) https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (accessed 14 June 2018).

160. Human Rights Watch, World Report 2017, https://www.hrw.org/world-report/2017/country-chapters/brazil ((accessed 14 June 2018).

161. Ibid.

162. "Brazil court orders WhatsApp messaging to be suspended", BBC News, 2015, https://www.bbc.co.uk/news/world-latin-america-35119235 (accessed 14 June 2018).

163. W. Connors, "Facebook Executive Arrested in Brazil", Wall Street Journal, 2016, https://www.wsj.com/articles/facebook-executive-arrested-in-brazil-1456851506 (accessed 16 June 2018).

164. Law to combat child pornography online, "Statute of Children and Adolescents, to improve combat the production, sale and distribution of child pornography and criminalize the acquisition and possession of such material and other related behaviors to pedophilia on the internet", 2008, https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm (accessed 16 June 2018).

165. ITU, Cyberwellness Profile, Brazil, 2012, https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf (accessed 11 May 2018).

166. Ibid.

167. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd. 2017).

168. Janice K. Song, "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying", World Bank, License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 2015,_ https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf (accessed 16 June 2018).

169. Ibid.

170. ITU, Cyberwellness Profile, Brazil, 2012,
https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf (accessed 11 May 2018).

171. Ibid.

172. Law on Copyright and Neighbouring Rights, Law No. 9.610 (1998),
http://www.wipo.int/wipolex/en/text.jsp?file_id=125393 (accessed 14 June 2018).

173. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity – Brazil Getting the Deal Through (Law Business Research Ltd.)
https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (accessed 14 June 2018).

174. Law on Protection of Intellectual Property of Software, its Commercialisation in the Country, and Other Provisions, Law No. 9.609 (1998),
http://www.wipo.int/wipolex/en/details.jsp?id=513 (accessed 14 June 2018).

175. Internet Act Decree No. 8,771/2016 (2016),
http://www.internetlab.org.br/wp-content/uploads/2016/05/Decree-MarcoCivil-English.pdf (accessed 14 June 2018).

176. Ibid.

177. Consumer Protection Code (Law 8,078/1990) (1990)
https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf (accessed 14 May 2018).

178. C. Barbosa, P. Vilhena, and K. L. Advogados, "Data protection in Brazil: overview", Practical Law, Global Guide 2016-17, 2016,
https://uk.practicallaw.thomsonreuters.com/4-520 1732?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk
(accessed 14 June 2018).

179. Data protection and Privacy – Brazil, 2017, Ricardo Barretto Ferreira da Silva and Paulo Branch, ",Getting the Deal Through", Law Business Research Ltd., https://gettingthedealthrough.com/area/52/jurisdiction/6/data-protection-privacy-brazil/ (accessed 14 June 2018).

180. Ibid.

181. E-commerce – Brazil, 2017, Raphael de Cunto, Pedro Paulo Barradas Barata and Beatriz Landi Laterza Figueiredo, "Getting the Deal Through", https://gettingthedealthrough.com/area/11/jurisdiction/6/e-commerce-brazil/ (accessed 14 June 2018).

182. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishing the principles, guarantees, rights and duties for use of the Internet in Brazil. Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204),
bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 Brazilian Civil Framework of the Internet in English (accessed 14 April 2018).

183. Sexual Harassment Law (No. 13,718) http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm (accessed 16 April 2020).

184. Economic Commission for Latin America, Comprehensive National-Level Review Report on the Implementation of the Beijing Declaration and Platform for Action – Brazil, 2019, https://www.cepal.org/sites/default/files/informe_beijing25_brasil.pdf (accessed 16 April 2020).

185. "Brazilian government approves law that guarantees more protection to women", Government of Brazil, 2018,
http://www.brazil.gov.br/about-brazil/news/2018/09/brazilian-government-approves-law-that-guarantees-more-protection-to-women-1
(accessed 16 April 2020).

186. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (accessed 14 April 2018).

187. Ibid.

188. Ibid.

189. "Skills of the Federal Police gain international recognition", Federal Police, 2014,
http://www.pf.gov.br/agencia/noticias/2014/10/pericias-da-policia-federal-ganham-reconhecimento-internacional
(accessed 10 September 2018).

190. Janice K. Song, "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying", World Bank, 2015, license: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO),
https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf (accessed 16 June 2018).

191. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity – Brazil. Getting the Deal Through (Law Business Research Ltd.)
https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (accessed 14 June 2018).

192. Brazilian Civil Rights Framework for the Internet, Act 12.965, 23 April 2014, establishes the principles, guarantees, rights and duties for use of the Internet in Brazil. Brasília: Chamber of Deputies, Edições Câmara, 2016 (Série legislação; No. 204),
bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 The Brazilian Civil Framework of the Internet in English (accessed 14 April 2018).

193. Electronic Frontier Communication, "State Surveillance of Communications in Brazil",
https://necessaryandproportionate.org/files/2016/07/08/brazil_faq_en.pdf (accessed 14 June 2018).

194. Federal Public Ministry, 2014, http://www.mpf.mp.br/atuacaotematica/ccr2/coordenacao/comissoesegruposdetrabalho/combatecrimescirberneticos/relatorios/Oficio%20PRSP%20GABPRR28MGBAS%2066526%20-%2014.11.12.pdf (accessed 10 September 2018).

195. Cybercrime@coe Update, Council of Europe, 2018, https://rm.coe.int/cybercrime-coe-update-2018-q1/16807baf95 (accessed 14 June 2018).

196. Octopus 2018: Co-operation against Cybercrime, 11–13 July 2018, Council of Europe, Strasbourg, France, https://www.coe.int/en/web/cybercrime/octopus-interface-2018 (accessed 14 July 2018).

197. OAS, Cybercrime, https://www.oas.org/juridico/english/cyber.htm (accessed 10 September 2018).

198. A. Mari, "Microsoft Brazil to deliver digital crime training program to Public Prosecutor's Office", ZDnet, 2018, https://www.zdnet.com/article/microsoft-brazil-to-deliver-digital-crime-training-program-to-public-prosecutors-office/ (accessed 14 June 2018)

199. Ministry of Justice and Public Security, "Ministry of Justice and Public Security co-ordinates integrated operation against sexual abuse and sexual exploitation committed through the internet", 2019, https://www.justica.gov.br/news/collective-nitf-content-1553775485.52 (accessed 15 April 2020)

200. Law No. 13,844, June 2019, establishing the basic organisation of the organs of the Presidency of the Republic and the Ministries, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm (accessed 15 April 2020).

201. ITU, Cyberwellness Profile, Brazil, 2012, https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf (accessed 11 May 2018)

202. Ibid.

203. Ibid.

204. FIRST, Cert.br, https://www.first.org/members/teams/cert-br (accessed 11 May 2018)

205. "INTERPOL and Banco do Brasil S/A sign co-operation agreement against cybercrime", INTERPOL, 2018, https://www.interpol.int/News-and-media/News/2018/N2018-046 (accessed 14 July 2018)

206. G. Diniz, R. Muggah, and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (accessed 14 April 2018).

207. INTERPOL, Brazil, https://www.interpol.int/Member-countries/Americas/Brazil (accessed 14 July 2018).

208. "Today, Brazil and Europol signed an agreement to expand co-operation to combat cross-border criminal activities", Europol, 2017, https://www.europol.europa.eu/newsroom/news/today-brazil-and-europol-signed-agreement-to-expand-co-operation-to-combat-cross-border-criminal-activities (accessed 14 July 2018).

209. http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view (accessed 11 May 2019).

210. https://www.pcisecuritystandards.org (accessed 11 May 2019).

211. http://www.mastercard.com/sea/consumer/standard-mastercard.html (accessed 11 May 2019).

212. https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf (accessed 11 May 2019).

213. https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf (accessed 10 May 2019).

214. https://cetic.br/noticia/acesso-a-internet-por-banda-larga-volta-a-crescer-nos-domicilios-brasileiros/ (accessed 11 May 2019).

215. http://www.allisps.com/en/offers/BRAZIL (accessed 11 May 2019).

216. http://www.abranet.org.br/?UserActiveTemplate=site (accessed 11 May 2019).

217. S. H. Bucke Brito, M. A. Silva Santos, R. dos Reis Fontes, D. A. Lachos Perez, H. Lourenço da Silva, and C. R. Esteve Rothenberg, "An Analysis of the Largest National Ecosystem of Public Internet eXchange Points: The Case of Brazil", Journal of Communication and Information Systems, 31(1), 2016.

218. http://ix.br (accessed 11 May 2019).

219. See e.g., Central Bank of Brazil, Resolution CMN 4,658, 26 April, 2018, https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf (accessed 13 May 2019).

220. CGI.br-NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro – TIC Governo Eletrônico, 2017, https://www.cetic.br/tics/governo/2017/orgaos/B6/ (accessed 17 May 2019).

221. http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm (accessed 13 May 2019).

222. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 (accessed 7 May 2019).

Cybersecurity

Capacity Review

Federative Republic of Brazil

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

GSI-PR

GREAT for PARTNERSHIP

OAS More rights for more people

Cybersecurity Capacity Review

Federative Republic of Brazil