CYBERWELLNESS PROFILE BRAZIL

BACKGROUND

Total Population: 198 361 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 51.60%
(data source: ITU Statistics, December 2012)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Law 8,137/1990, Art. 2
- Law 8,069/1990, Art. 241
- Law 9,100/1995, Art. 67
- Law 9,296/1996, Art. 10
- Law 9,504/1997
- Law 9,983/2000
- Law 11,829/2008
- Law 12,735/2012, Art.4
- Law 12,737/2012

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

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

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Brazil has officially recognized a national CERT, a government CSIRT and a sector specific SCIRT.

1.2.2 STANDARDS

Brazil has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through three instruments:
-Normative Instruction GSI no 1/2008 which organizes the Management of Information and Communications Security in the Federal Public Administration, direct and indirect, among other provisions.

-Normative Instruction GSI no 2/2008 which provides for accreditation on security for the treatment of classified information at any level of confidentiality in the under the Federal Executive Branch.

-Normative Instruction GSI no 3/2008 that defines minimum parameters and standards for cryptographic algorithms for encryption of classified information under the Federal Executive Branch.

1.2.3 CERTIFICATION

The Complementary Standards offer a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.
Complementary Standard no. nº 17 establishes guidelines for the certification and accreditation for information and communication security professionals of the direct and indirect Federal Public Administration.
Complementary Standard no. nº 18 establishes guidelines for training of the information and communication security professionals of the direct and indirect Federal Public Administration.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Brazil has an officially recognized national cybersecurity policy through the following instruments:

- Decree 6703/2008 - National Defense Strategy
- Information Technology Strategy, 2013-2015
- Anatel - Public Consultation no. 21, on a regulation for critical telecommunication infrastructure protection. This regulation establishes measures to be undertaken by telecom operators to promote risk management processes related to security and performance of network and telecommunication services. It also promotes coordination among telecom operators for disaster relief.
- Administrative Normative Rule no. 3,389 of the Ministry of Defense, which establishes the Cyber Defence Policy
- Critical Information and Communication Infrastructure protection

1.3.2 ROADMAP FOR GOVERNANCE

Brazil does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

Brazil does not have an officially recognised national or sector-specific agency responsible for implementing a national cybersecurity strategy, policy and roadmap since responsibilities are shared among the following several entities:

- National Defense Council in charge of planning and conducting the policy and strategy for national defence
- Cabinet of Institutional Security of the Presidency of the Republic which proposes guidelines and strategies for the cybersecurity in the scope of the Federal Public Administration, by means of the Communication and Information Safety Department
- Cyber defense Centre of the Brazilian Army
- Brazilian Intelligency Agency
- Ministry of Justice – Department of Federal Police

1.3.4 NATIONAL BENCHMARKING

Brazil has officially recognized the following national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

- TIC Kids Online 2012 - Survey on Internet Use by Children in Brazil
- ICT Households and Enterprises - Survey on the Use of Information and Communication Technologies in Brazil
- Survey on the Use of Information and Communication Technologies in Brazil
- The Bureau of Information Technology Audit (Sefti/TCU) conducts benchmark exercises periodically to measure cybersecurity development in government sector.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Brazil has officially recognized the following national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

- ABNT which defines the Brazilian versions of ISO IEC standards (e.g. ABNT NBR ISO/IEC 27000 series)
- CEPESC - Research and Development Center for the Security of Communication – that develops scientific and technological research applied to projects related to the security of communications including technology transfer.
- CAIS RNP – Security Incident Response Team – which acts in the detection, solution and prevention of security incidents in the Brazilian academic network, besides creating, promoting and spreading security practices in networks.

1.4.2 MANPOWER DEVELOPMENT

The Brazilian Internet Steering Committee (CGI.br) is responsible for recommending technical standards and best practices related to the Internet, and promoting security best practices. In order to perform its activities the CGI.br created the Brazilian Network Information Center (NIC.br) which implements these efforts through:

- Brazilian national (CERT.br) which offers professional training programs.
- Best practices Portal BCP.nic.br - a portal to promote Current Best Practices (BCPs) for system administrators.
- Antispam.br - a portal for awareness about spam, with contents to both end users and system administrators.
- InternetSegura.br - a portal with links to all currently known awareness materials developed by Brazilian organizations.
- SaferNet Brazil works with prevention, providing information to the users and organizing awareness campaigns, but it also functions as an internet complaint center for crimes against human rights.
- CEGSIC which offers specialization course in Management of Information Security and Communications.

1.4.3 PROFESSIONAL CERTIFICATION

Brazil has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity. However it did not conduct a survey to gather the exact statistic.

1.4.4 AGENCY CERTIFICATION

Brazil has numerous certified government and public sector agencies under internationally recognized standards in cybersecurity. However it did not conduct a survey to gather the exact statistic.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets access borders and with other nation states, Brazil has officially recognized a partnership with the Inter-American Committee Against Terrorism (CICTE) by enhancing the exchange of information via the competent national authorities.

1.5.2 INTRA-AGENCY COOPERATION

The SegInfo blog is the officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector since it offers to its readers the main news related to information security, and frequent articles by renowned professionals in the information security area. The site aims to collect, catalog and spray events, news, vulnerability warnings and most relevant projects in the information security area, among countless other aspects.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Brazilian national CERT (CERT.br) participates in several initiatives for sharing cybersecurity assets within the public and private sector.

- SpamPots Project which gathers data related to the abuse of Internet infrastructure by spammers in order to identify malware botnets etc

- Distributed Honeypots Project which objective is to increase the capacity of incident detection and trend analysis in the Brazilian Internet Space.

- Tentacles Project : a Cooperation Agreement between the Brazilian Federal Police Department and FEBRABAN (Brazil´s Bank Federation) in which the Brazilian Federal Police Department receives on line information on almost the entire electronic frauds committed inside Brazil borders, allowing the continuous feeding of the National Electronic Frauds Database and the quick generation of statistics, crime analysis and strategic planning, among other means known to be effective in combating this type of illicit act.

1.5.4 INTERNATIONAL COOPERATION

Brazil is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Brazil participated in the following cybersecurity activities.

- Latin American and Caribbean Regional CSIRTs Meeting organized by LACNIC.
- Brazilian Federal Police participates in the I-24/7 global police communications system developed by Interpol to connect law enforcement officers, including cybercrimes:

CERT.br is a member of FIRST.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-Articles 218, 218A, 218B* of the Criminal Code, amended and included by the Law n. 12015/2009.

-Articles 240* and 241A-E* of the Law n. 8069/1990, amended by the law n. 11829/2008.

2.2 UN CONVENTION AND PROTOCOL

Brazil has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Brazil has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The Brazilian national CERT (CERT-BR*) provides for information* on internet security in its website. Also there is a Website* gathering Brazilian initiatives on internet security, built by the Brazilian Internet Steering Committee*.

2.4 REPORTING MECHANISM

Online illegal content can be reported in the helpline on child and adolescent pornography in internet created by the government: www.disque100.gov.br* Available as a telephone number in: 100.

SaferNet Brasil provides information on internet safety and space for complaints in its website.

The Federal Police* has a dedicated space to receive denouncements at its website, which can also be made by its email address denuncia.ddh@dpf.gov.br.

More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

Last updated on 25th November 2014