



The 5th Annual  
**INTERNET OF THINGS**  
Global Summit

October 10 - 11, 2017  
The National Press Club, Washington D.C.

Forum GLOBAL

Platinum Sponsors: AT&T, BlackBerry, ESOA, LYA, Microsoft

Gold Sponsors: ARM, CAMGIAN

Event Partners: ctia, IoT DC, SIA

# Session 3: Cyber-criminality, security and risk in an IoT world

---

Belisario Contreras  
October 2017

**The opinions expressed in this presentation do not necessarily reflect the views of the General Secretariat of the Organization of American States or the governments of its member states.**

---

Cybersecurity Program  
**Organization of American States**


cybersecurity@oas.org

 @belisarioc


# How will IoT change the future of cybercrime and how is it being addressed?

- Absence of security protocols related to IoTs makes them easy targets for data mining
- IoT are now hyper connected and expands the sources of data that law enforcement will need access to
- Ease of use for users = Ease of access for attackers (e.g. webcams default settings)
- Privacy vs Public Safety concerns

# Threats

- 
- IoT mostly consists of systems or services traditionally called “M2M” (Machine to Machine) e.g. smart meters connected to national grids
  - Application platforms built operating systems that have exploitable vulnerabilities
  - Criminal activities could involve disruption of services such as traffic control systems or public transportation systems

# Advances in legislation




Most countries have no laws that specifically mention IoT devices, so general privacy laws would apply

European Commission draft ePrivacy Regulation of IoT:

*“In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications.”*

# Advances in legislation



In Canada, a federal law called the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) sets rules on how companies who collect personal data should protect it. The law requires companies to do things like create a privacy management program, limit collection, use and retention of data, give users access to information that the company has about them and provide a way for users to file complaints with the company.

In the USA, according to the [National Conference of State Legislatures](#) website, 31 states have data disposal laws and 47 states have security breach notification laws, but the laws are not uniform.

# Conversion of IT, Operations Technology and IoT

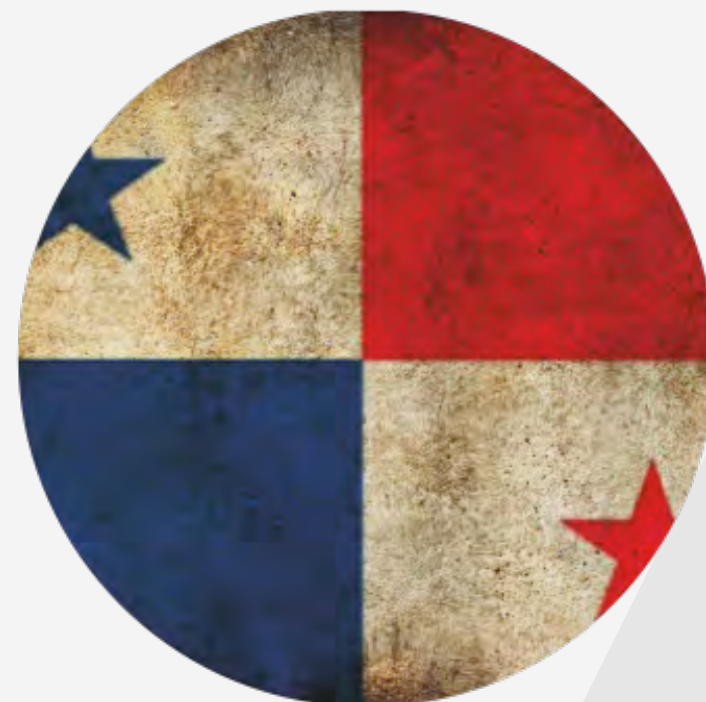
A recent example is the Target case, where a cybercriminal was able to install malware into numerous company point-of-sales terminals by first gaining entry through a vulnerability in the company's IoT HVAC system.



# National Strategies Adopted



**Colombia**  
(2011 & 2016)



**Panama**  
2013



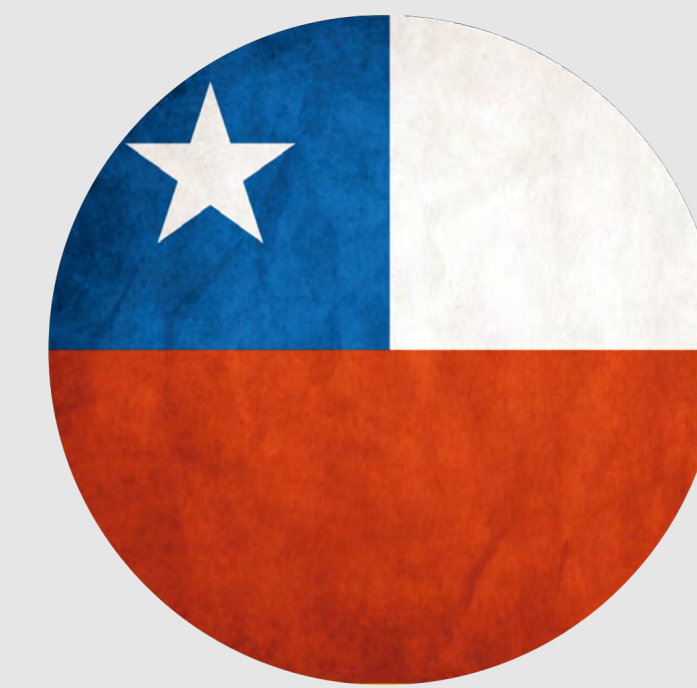
**Trinidad  
and Tobago**  
2013



**Jamaica**  
2013



**Paraguay**  
2017



**Chile**  
2017



# National Strategies under development



**Costa Rica**



**Argentina**



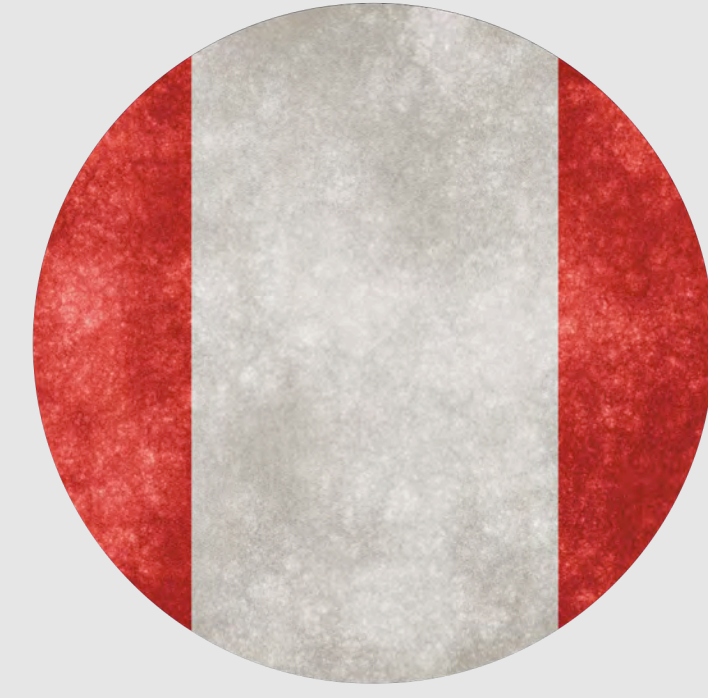
**Dominican  
Republic**



**Guatemala**



**Mexico**



**Peru**

# New Requests of Assistance



**Honduras**



**Belize**



**Barbados**

# Cybersecurity: Are we ready in Latin America and the Caribbean?



OBSERVATORY  
**CYBERSECURITY**  
IN LATIN AMERICA AND THE CARIBBEAN

## Cybersecurity

### Are We Ready in Latin America and the Caribbean?

2016 Cybersecurity Report

www.cybersecurityobservatory.com

**Download Report**

### Incident Response Capacity Building in the Americas

FIRST | Forum of Incident Response and Security Teams  
Maarten Van Hovenbeek, Cristine Hospes and Peter Allart

**Maria Maciel**  
Researcher and coordinator of the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. She serves as a consultant at the Generic Names Supporting Organization of the Internet Corporation for Assigned Names and Numbers (ICANN), representing the Non-commercial Stakeholder Group. She is a member of the Advisory Board on Internet Security, created under the Brazilian Internet Steering Committee. Maria is a PhD candidate in International Relations at the Pontifical Catholic University (PUC - Rio de Janeiro).

**Natália Feduch**  
Researcher at the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. She has worked for international organizations, the Brazilian Federal Government, as well as law firms and think tanks on communications law and policy matters. Feduch is a licensed attorney and holds a Master's degree in Law and another in Public Policy, both from the American University.

**Lara Belli**  
Researcher at the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. He holds a PhD in Public Law from the Universidade Federal do Rio de Janeiro (UFRJ) and is a founder and coordinator of the Dynamic Coalition on Network Neutrality, as well as of the Dynamic Coalition on Platform Responsibility, multi-stakeholder components of the United Nations' Internet Governance Forum.

**Nicolás Castañeda**  
Visiting researcher at the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. He specializes in cybersecurity governance, focusing on critical infrastructures and humanitarian uses for Big Data. He holds a Master's degree in Crisis and Security Management from Leiden University's Faculty of Governance and Global Affairs.

**FGV FUNDEJO DIREITO RIO**  
FUNDACÃO DE GESTÃO DE PESQUISA E DESENVOLVIMENTO DE SERVIÇOS JURÍDICOS

**FGV FUNDEJO DIREITO RIO**  
www.fundajo.org.br

### CYBERSECURITY

IN LATIN AMERICA AND THE CARIBBEAN

- Costa Rica**
  - Attorney General of the Republic
  - Costa Rican Institute of Electricity
  - Judicial Investigations Department
  - Ministry of the Presidency
  - Ministry of Science, Technology and Telecommunications
  - Superintendence of Telecommunications
  - University of Costa Rica
- El Salvador**
  - Ministry of Justice and Public Security
- Grenada**
  - Naval Grenada Police Force
- Guatemala**
  - CERT-GT
  - Ministry of the Interior
  - Ministry of National Security
  - Superintendence of Telecommunications
  - Technical Secretariat of the National Security Council
- Goyana**
  - CERT-gy - Ministry of Home Affairs
  - Guyana Energy Agency
  - Guyana Defense Force
  - Guyana Police Force
  - University of Guyana
- Haiti**
  - National Telecommunications Council
- Honduras**
  - CONOS
  - National Telecommunications Commission
  - Ministry of Foreign Relations and International Cooperation
  - National Police of Honduras
  - National Property Management System
- Jamaica**
  - Jamaica Bank Association
  - Jamaica Constabulary Force
  - Ministry of National Security
  - Ministry of Science, Technology, Energy and Mining
  - Public Ministry
  - University of the West Indies
- Mexico**
  - Attorney General's Office
  - Mexican Internet Association, A.C.
  - Mexican Notarariat
  - Secretariat of the Interior
  - Specialized Committee on Information Security
- Nicaragua**
  - National Engineering University
- Panama**
  - National Authority for Governmental Innovation
  - Panama Canal Authority
- Paraguay**
  - Attorney General's Office
  - Ministry of Foreign Affairs
  - National Secretariat of Information and Communications Technology
- Peru**
  - Joint Command of the Armed Forces
  - Ministry of Defense
  - Ministry of Foreign Relations
  - Ministry of the Interior
  - National Office of Government and Information
  - National Police of Peru
  - Public Ministry - Prosecutor's Office
- Saint Kitts and Nevis**
  - Financial Services Regulatory Commission
  - LIME
  - Ministry of Energy, Finance, Trade and Industries
  - Ministry of Health, Employment, Sports, Information Communications and Technology
  - Telecommunications and Post
  - Royal Saint Kitts and Nevis Police
  - Saint Kitts Electricity Company, Ltd.

### Argentina

**Policy and Strategy**

Lead by the National Program for Critical Information Infrastructure and Cybersecurity (CNCI) in coordination with various agencies, academic institutions and the private sector, the Government of Argentina has developed a draft National Cybersecurity Strategy that is currently awaiting adoption. Argentina is notable for forming one of the first national CERTs in 1994 (SocSI), which functioned under the CCI. ICC-CERT maintains a central register of cybersecurity events and threats. The Armed Forces run annual Cyber Incident Response Exercises to share best practices and review command and control functions; however, they currently have limited capacity for cyber resilience.

**Culture and Society**

As Argentina's a government and e-commerce services continue to expand, government agencies have led awareness-raising campaigns to educate the public about cybersecurity. Two notable examples are Internet Safe (Healthy) or -Secure (Inmortal) led by the ICC, which focuses on best practices for safe internet use, and With You on the Web under the Ministry of Justice and Human Rights, which teaches children, parents and teachers about the threat of online grooming (the predatory befriending of children on the web to lure them into sexual abuse or trafficking). In addition, a number of universities offer degree programs in cybersecurity and digital forensics.

**Legal Frameworks**

Previously, CNCI was managed more-or-less informally. However, in June 2015, the Presidency of the Republic of Argentina issued Decree No. 2807/2015, which restructured government control of CNCI, establishing a National Office within the Undersecretariat for the Protection of Critical Information and Cybersecurity Infrastructure, under the fiscal Office of the Cabinet of Ministers - Cabinet Secretariat. This new program will work to develop cybersecurity norms and standards, as well as collaborate with the private sector to improve CNCI resilience.

**Technologies**

Amid increases in cybercrime, the Government of Argentina conducted a comprehensive legal framework for ICT, including Penal Code Law 26,386, and Law 25,226 on data protection. It is also developing procedural law for handling digital evidence. While mechanisms are in place for disclosure, the private sector is not legally required to report breaches to cybersecurity authorities, awareness of cybersecurity risks among businesses has grown significantly. The Technology Crimes Division of the Argentine Federal Police Force is responsible for investigating cases of cybercrime.

**Internet penetration**

TOTAL POPULATION IN THE COUNTRY: 42,980,026  
Mobile phone subscriptions: 66,356,009  
People with internet access: 27,937,016  
Internet penetration: 65%

### Corporate Governance, Knowledge and Standards

**Private and State Owned Companies' Understanding**

Private and state-owned companies' understanding of cybersecurity is critical in their application of best practices within their governance structure. Executive boards should understand the risks that companies face, some of the primary methods of attack and how their company deals with cyber issues and evaluates them.

**EMERGING**  
Boards have minimal or no understanding of cybersecurity, and fiduciary duties considerations are not discussed.

**EMERGING**  
Executive boards have some awareness of cybersecurity issues, but not how they might affect the organization or what direct threats they may be faced with.

**ESTABLISHED**  
Executive boards understand how companies are at risk, in general, some of the primary methods of attack, and how their company deals with cyber issues (usually entrusted to the Chief Information Officer) and incident management is largely reactive.

**ESTABLISHED**  
Executive boards are aware of their strategic assets, have put specific measures in place to protect them, and know the mechanisms which protect them; the executive board can allocate specific funding and assign people to prevent other risk; corporate contingency plans are in place to address various cyber-based attacks and their aftermath; executive board members are provided with some cybersecurity education; and the board has a clear sense of cyber fiduciary duties.

**DYNAMIC**  
Executive boards are able to change cybersecurity strategy quickly and appropriately; new threats are considered at every board meeting; and funding and attention is reallocated to address those threats; the executive board is looked to as a source of knowledge in corporate cybersecurity governance; governance is based on cyber risk and improves governance, specifically in this area.

### CYBERSECURITY

IN LATIN AMERICA AND THE CARIBBEAN

**Policy and Strategy**

Official National Cybersecurity Strategy

Strategy development: **EMERGING**

Organization: **EMERGING**

Content: **EMERGING**

**Cyber Defense Coordination**

Strategy: **EMERGING**

Organization: **EMERGING**

Coordination: **EMERGING**

**Culture and Society**

Cybersecurity Mind Set

Government: **EMERGING**

Private Sector: **EMERGING**

Society: **EMERGING**

Cybersecurity Awareness

Awareness raising: **EMERGING**

Trust in e-commerce: **EMERGING**

**Confidence and Trust on the Internet**

Trust in e-commerce: **EMERGING**

Trust in government: **EMERGING**

Trust in companies: **EMERGING**

**Online Privacy**

Privacy standards: **EMERGING**

Employee privacy: **EMERGING**

**Education**

National Availability of Cyber Education and Training

Education: **EMERGING**

Training: **EMERGING**

**National Development of Cybersecurity Education**

National development of cybersecurity education: **EMERGING**

**Training and Educational Initiatives**

Transparency in cybersecurity: **EMERGING**

Corporate Governance, Knowledge and Standards

Private and state-owned companies' understanding: **EMERGING**

**Legal Frameworks**

Cybersecurity Legal Frameworks

Legislative frameworks for ICT security: **EMERGING**

Privacy, data protection and other human rights: **EMERGING**

Substantive cybercrime law: **EMERGING**

Procedural cybercrime law: **EMERGING**

**Legal Investigation**

Law enforcement: **EMERGING**

Prosecution services: **EMERGING**

Courts: **EMERGING**

**Responsible Reporting**

Responsible disclosure: **EMERGING**

**Adherence to Standards**

Adherence to standards: **EMERGING**

**Cyber Security Coordinating Organizations**

Coordinating and central bodies: **EMERGING**

Other coordinating bodies: **EMERGING**

**Incident Response**

Incident response: **EMERGING**

Coordination: **EMERGING**

**National Infrastructure Resilience**

Critical national infrastructure: **EMERGING**

National resilience: **EMERGING**

**Critical National Infrastructure Protection**

Identification: **EMERGING**

Organization: **EMERGING**

Response planning: **EMERGING**

Coordination: **EMERGING**

**Crisis Management**

Planning: **EMERGING**

Organization: **EMERGING**

**Digital Resilience**

Digital resilience: **EMERGING**

**Cybersecurity Marketplace**

Cybersecurity technologies: **EMERGING**

Operational resilience: **EMERGING**

### Legal Frameworks

**Cybersecurity Legal Frameworks**

Legislative frameworks for ICT security: **EMERGING**

Privacy, data protection and other human rights: **EMERGING**

Substantive cybercrime law: **EMERGING**

Procedural cybercrime law: **EMERGING**

**Legal Investigation**

Law enforcement: **EMERGING**

Prosecution services: **EMERGING**

Courts: **EMERGING**

**Responsible Reporting**

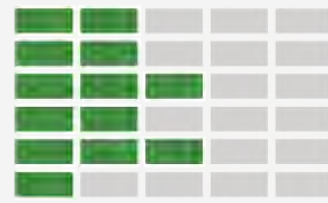
Responsible disclosure: **EMERGING**

# Advances in the region

Argentina



Policy and Strategy



Culture and Society



Education



Legal Frameworks



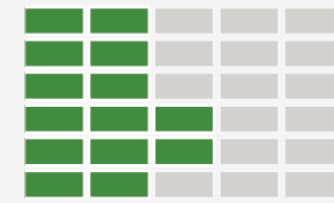
Technologies



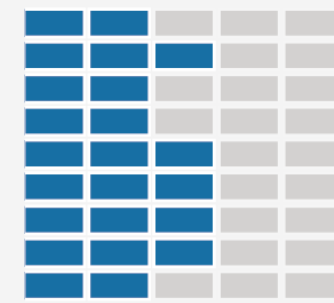
Brazil



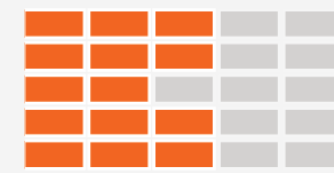
Policy and Strategy



Culture and Society



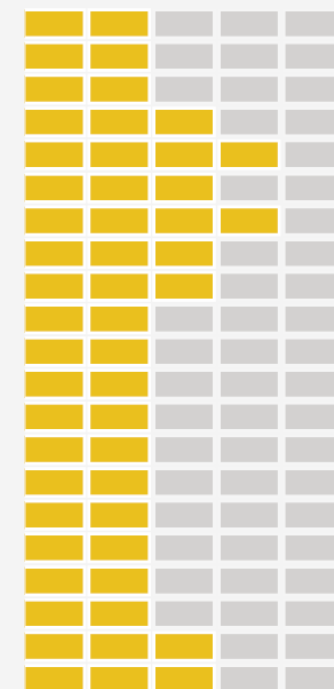
Education



Legal Frameworks



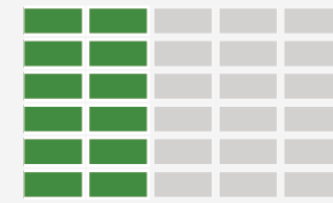
Technologies



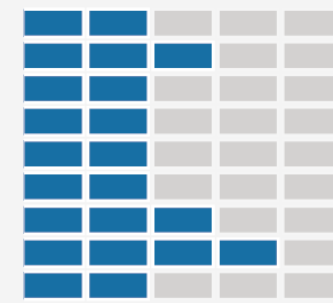
Chile



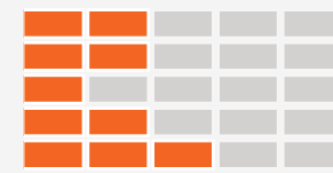
Policy and Strategy



Culture and Society



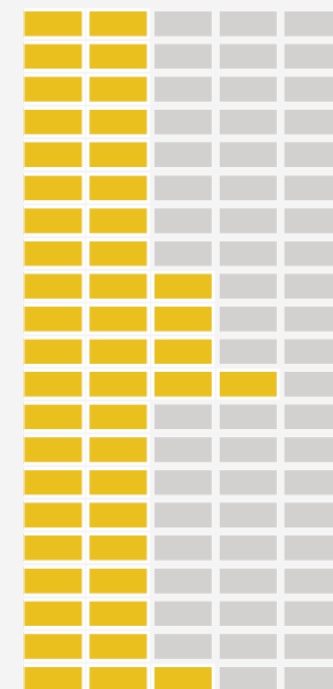
Education



Legal Frameworks



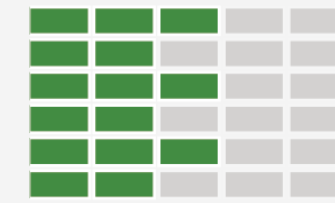
Technologies



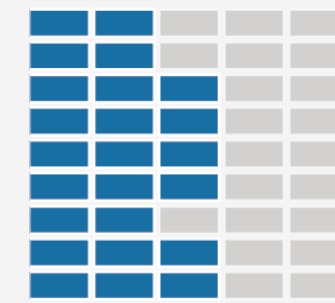
Colombia



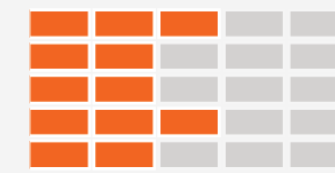
Policy and Strategy



Culture and Society



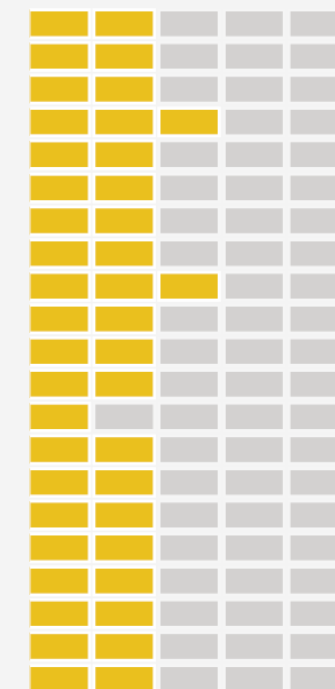
Education



Legal Frameworks



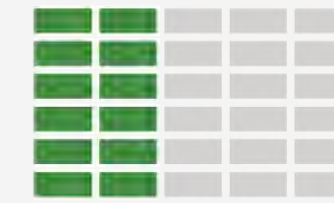
Technologies



Mexico



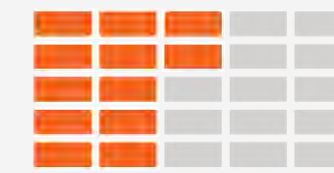
Policy and Strategy



Culture and Society



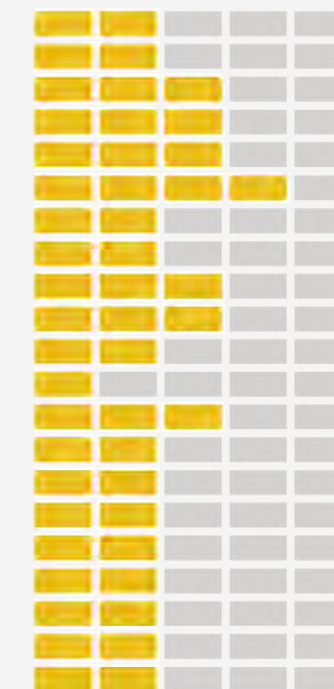
Education



Legal Frameworks



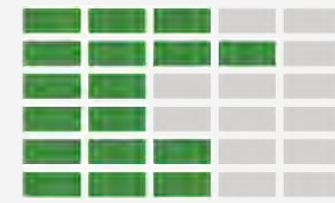
Technologies



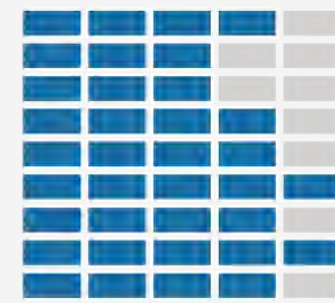
Uruguay



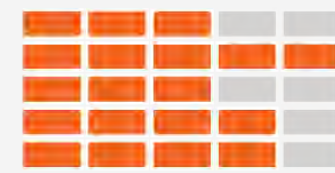
Policy and Strategy



Culture and Society



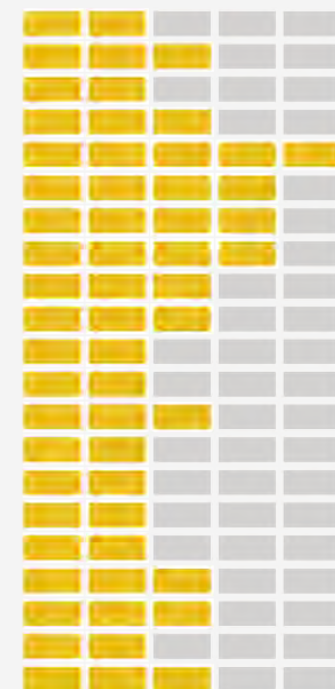
Education



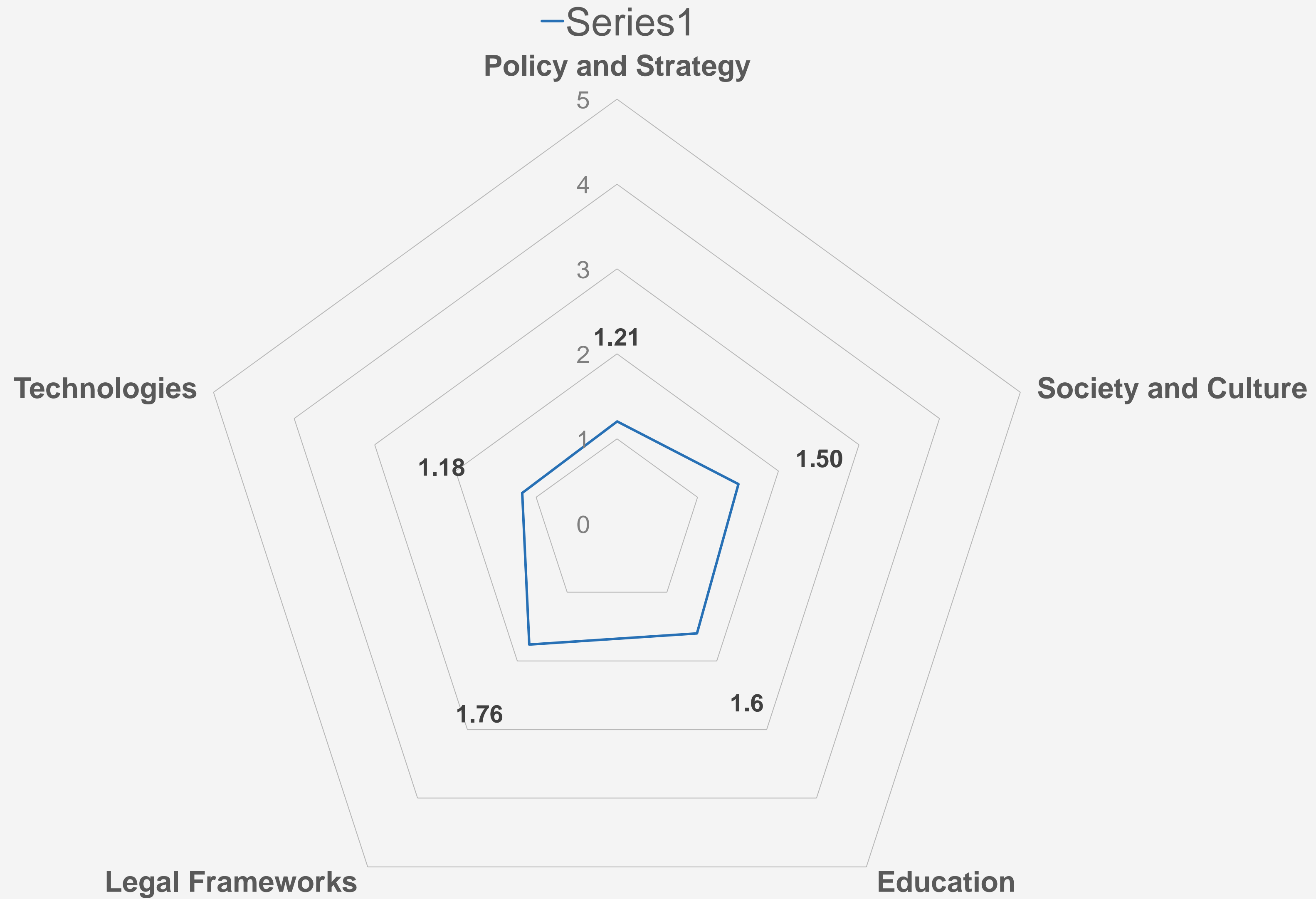
Legal Frameworks



Technologies



# The Caribbean



# Challenges in the region



**28 of 32 countries**  
do not have cyber  
security strategies

**18 countries** have NOT  
identified “key elements”  
of their National Critical  
Infrastructure



**24** do not count with  
mechanism for planning  
and coordination on Critical  
Infrastructure Issues



# Challenges in the region



In **20 countries** no command and control center exist, and in another 7 this function is performed without formality

**26 countries** in the region do not have a structured cybersecurity education program



In **30 of the 32 countries**, there is no national cyber security awareness programs





# **Current Overview of CSIRTs in the Region**



## OVERVIEW OF CSIRTs

# National CSIRTs

(2017) estado actual

- ICIC CERT
- CCIRC
- US-CERT
- CTIRGov
- CERT-MX
- CSIRT GOB CL
- CL-CERT
- ADSIB
- CSIRTGt
- PE-CERT
- SurCSIRT
- EcuCERT
- ColCert
- CSIRT-GY
- TT-CSIRT
- JM-CSIRT
- VenCERT
- CERT-PY
- CERTUy
- CSIRT Costa Rica
- CSIRT Panama





**CSIRT Americas.org**

**Hemispheric Network**



**CSIRT**americas.org



**Consolidating an  
Operational Community  
in the Americas**



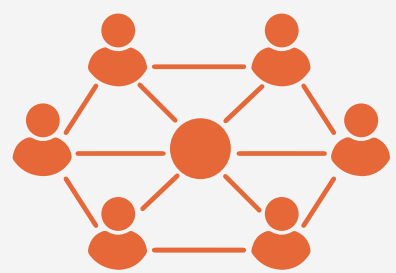
**Encourage the  
exchange of alerts  
and information**

**+ 65**

Procedures, scripts, manuals sharing between CSIRTs

**+ 3000**

Monthly alerts are notified to CSIRTs in the region



Large scale incident coordination operations  
(WannaCry / - Petya / nopetya)



Subregional trends every 6 hours  
North, Central, South, Caribbean



**CSIRTamericas.org**

**14** CSIRTs

**55** members



Bolivia



Mexico



Colombia



Venezuela



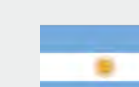
Paraguay



Panama



Ecuador



Argentina



Chile



Trinidad and Tobago



Guyana



Suriname



Jamaica



Costa Rica



Peru

**Thank you!**  
**Merci**  
**Gracias**  
**Obrigado**

## **Belisario Contreras**

---

Cybersecurity Program  
**Organization of American States**

cybersecurity@oas.org

 @OEA\_Cyber