OAS More rights for more people

Cybersecurity

Are We Ready in Latin America and the Caribbean?

2016 Cybersecurity Report

www.cybersecurityobservatory.com

Belisario Contreras

Cybersecurity Program Manager
Organization of American States
BContreras@oas.org

@belisarioc

What the OAS does on Cybersecurity issues?

- Development of National Cybersecurity Strategies
- Trainings, Workshops and Technical Missions
- Cybersecurity Exercises
- Development of national CSIRTs and a regional CSIRT Hemispheric Network
- Awareness Raising, Research and Expertise

Why this report?

- Inter-American Development Bank (IDB) support to cybersecurity issues
- Need for more tangible and reliable data
- Need for baseline data to better monitor regional developments in cybersecurity
- OAS experience with previous reports
  - 2013: Latin American and Caribbean Trends and Government Responses
  - 2014: Latin American + Caribbean Cybersecurity Trends
  - 2015: Cybersecurity and Critical Infrastructure in the Americas
- Increasing interest from member states

Global Attacks

2013

Multi Locker
Famously known as "Trojan police" because it simulates that the user computer has been intervened and blocked

Rodpicom Botnet
Malware sends a message to the victim with a link to a malicious site that leads to downloadable content (skype)

2014

Sony attack
Hollywood studio to cancel the release of satirical comedy The Interview

Target attack
Leak of tens of millions of credit- and debit-card accounts.

Heartbleed vulnerability
Vulnerability in the popular OpenSSL cryptographic software library

2015

Disclosure of Information

Whatsapp phishing
Fake invitation messages to the new Whatsapp Call functionality

US Federal attack
Personal information of four million federal employees

Overview-2016 Cybersecurity Report

Expert Contributions

- Cyber Confidence Building and Diplomacy in Latin America and the Caribbean
- Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean
- Incident Response Capacity Building in the Americas
- The State of Cybercrime Legislation in Latin America and the Caribbean
- Digital Economy and Cybersecurity in Latin America and the Caribbean
- Sustainable and Secure Development: A Framework for Resilient Connected Societies

Country Profiles

- 32 countries from Latin America and the Caribbean region

“Backstage”

- OAS – IDB Agreement.
- Regional Activity in October 2014 for launching this initiative.
- Initial support from Microsoft to identify key areas of study.
- Partnership with the University of Oxford to develop an “Application Tool” based on the Cybersecurity Capability Maturity Model (CMM).
- 3-4 intense weeks of work, making substantial adaptations to CMM for the LAC region.

“Backstage”

- In-country application of the CMM and distribution of digital survey.
- Desktop Research and consolidation of other sources of available data.
- Validation process of approximately 60 days of the application tool.
- Lots of trial & error, amendments and back and forth!

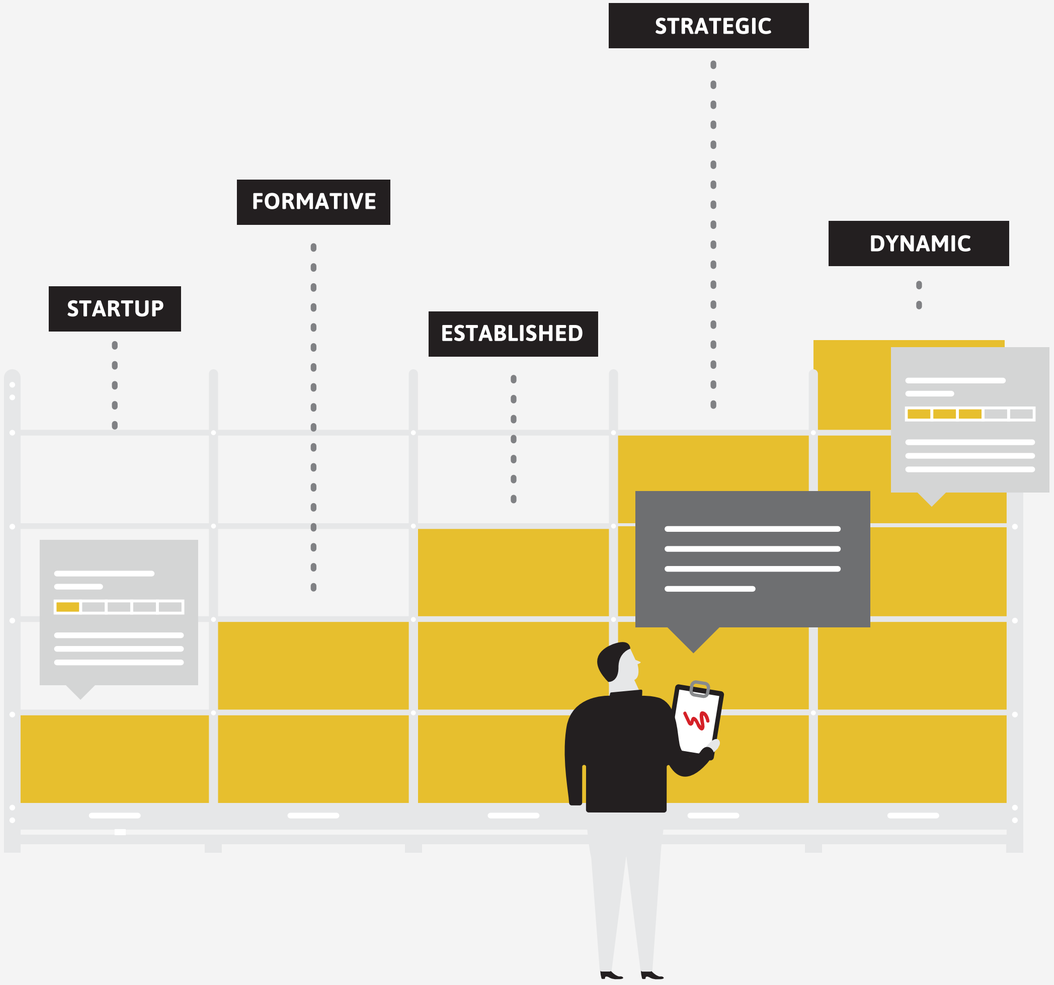
Timeline

May 2014	September 2014	October 2014	October-November 2014	December 2014	February 2015	March-April 2015	July 2015	August 2015	September 2015	March 2016
OAS-IDB Preliminary discussions	Formal OAS-IDB Agreement	Regional Activity	Preparation Application Tool	Validation Process Starts	Validation Process Finish	Request for Experts Contributions	Collection of Data Ends	Receive Final Expert Contributions	Validation Process Ends	Release Date
				Desk Research	Graphics Concepts Starts		Validation Process Starts		Graphic Design	
					Collection of Data Starts				Editorial Process	

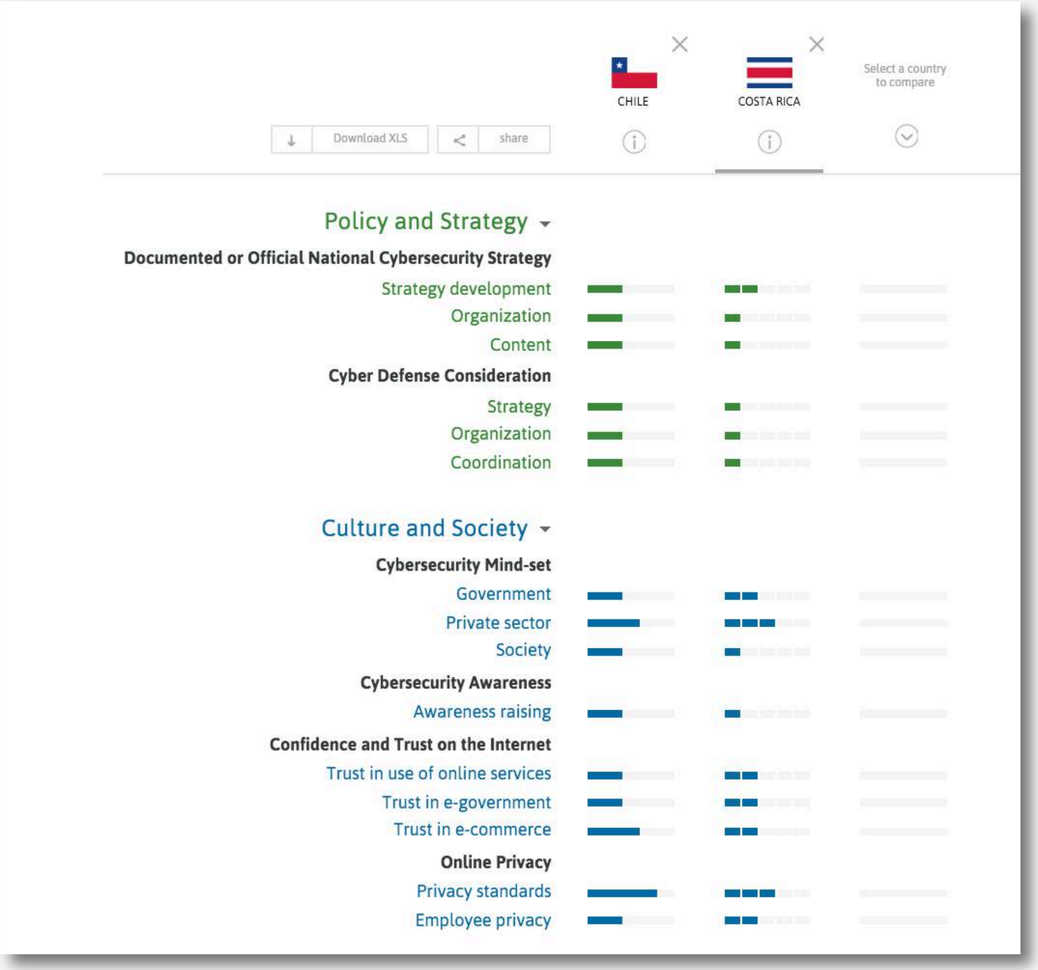
CMM - 5 Dimensions

- Policy and Strategy
- Legal Frameworks
- Culture and Society
- Technologies
- Education

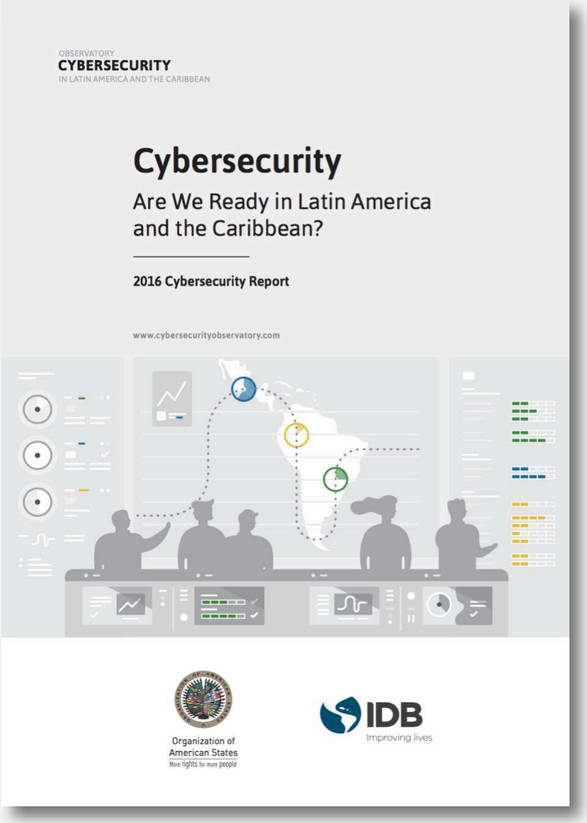
CMM - 5 Levels of Maturity

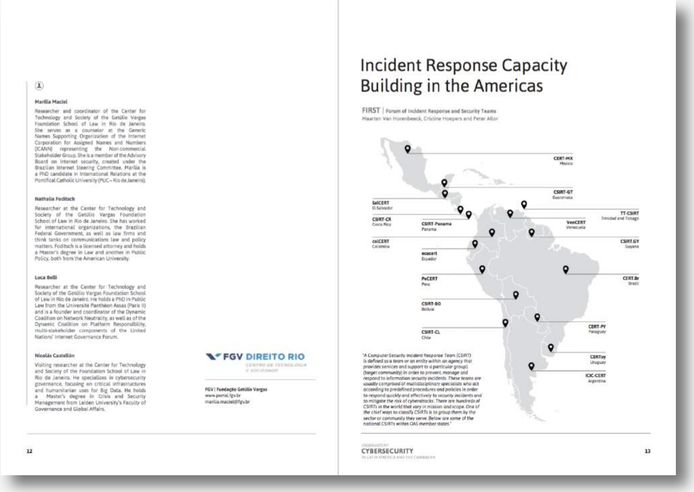


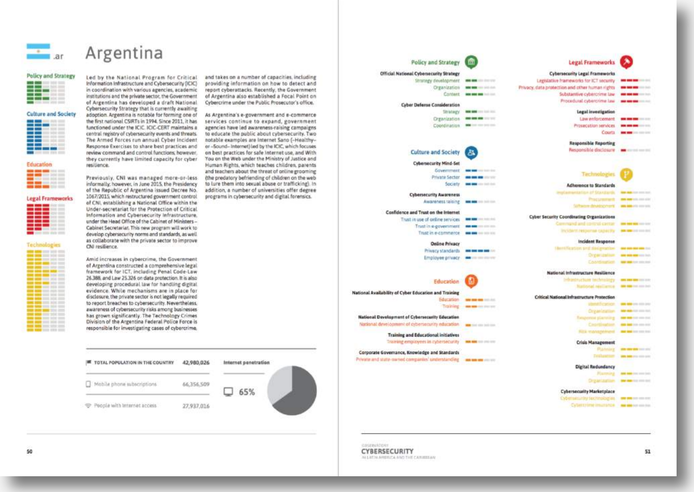
Observatory

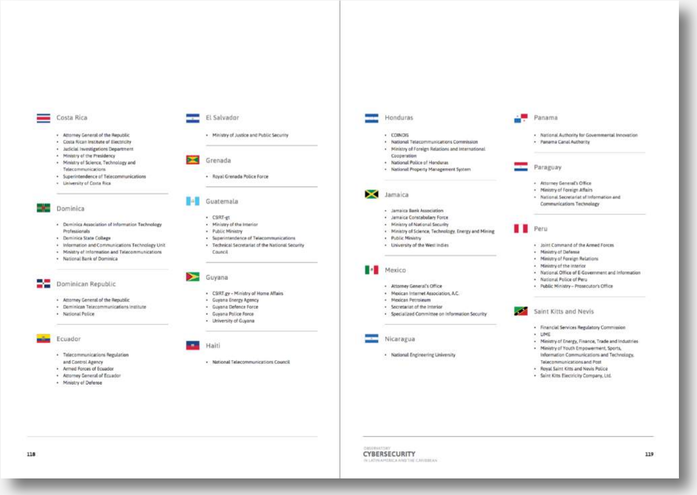


How the report looks?



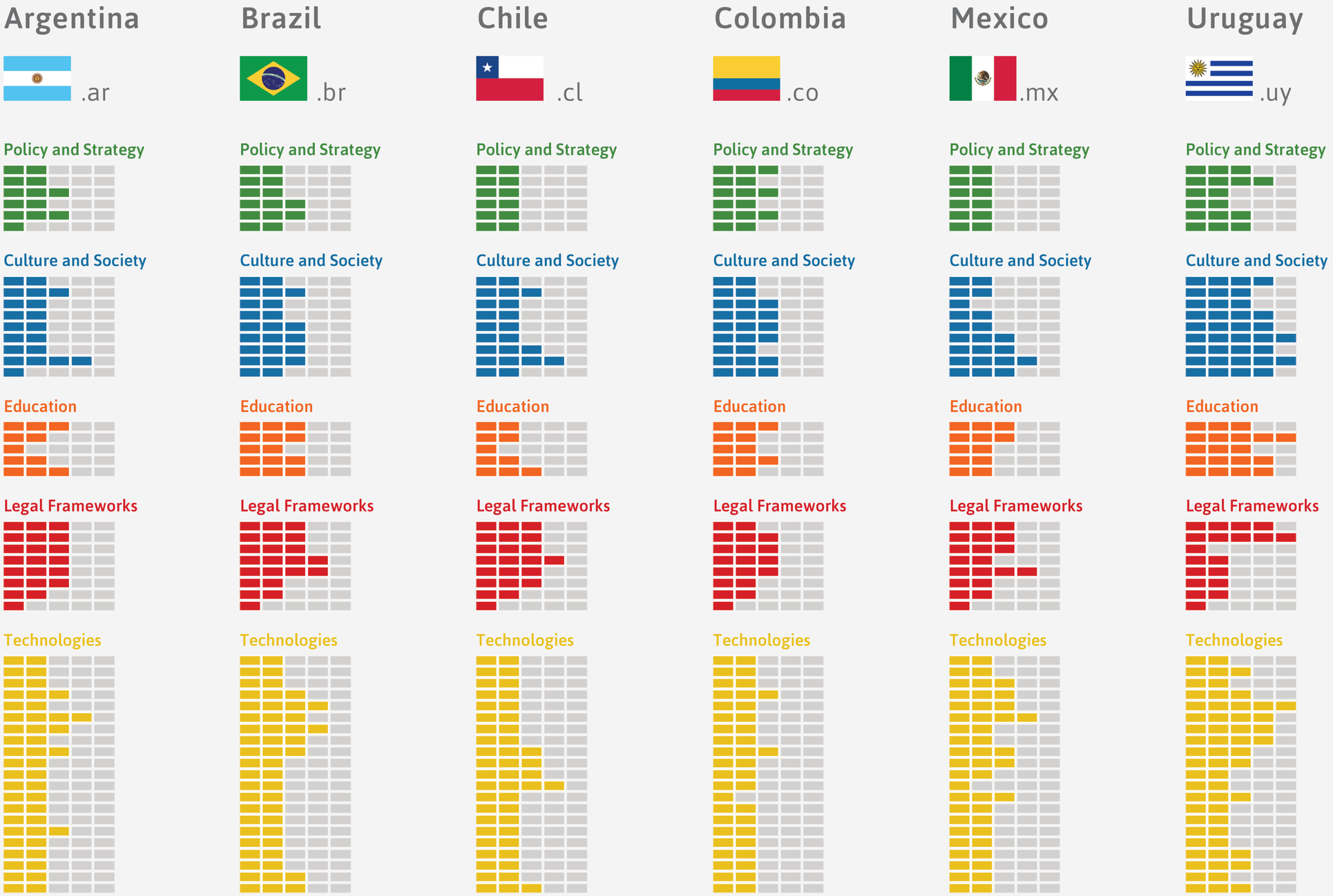






Download Report

Advances in the region



Incident Response Capacity Building in the Americas

FIRST | **Forum of Incident Response and Security Teams**
Maarten Van Horenbeeck, Cristine Hoepers and Peter Allor

"A Computer Security Incident Response Team (CSIRT) is defined as a team or an entity within an agency that provides services and support to a particular group1 (target community) in order to prevent, manage and respond to information security incidents. These teams are usually comprised of multidisciplinary specialists who act according to predefined procedures and policies in order to respond quickly and effectively to security incidents and to mitigate the risk of cyberattacks. There are hundreds of CSIRTs in the world that vary in mission and scope. One of the chief ways to classify CSIRTs is to group them by the sector or community they serve. Below are some of the national CSIRTs within OAS member states."

Challenges in the region

27 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

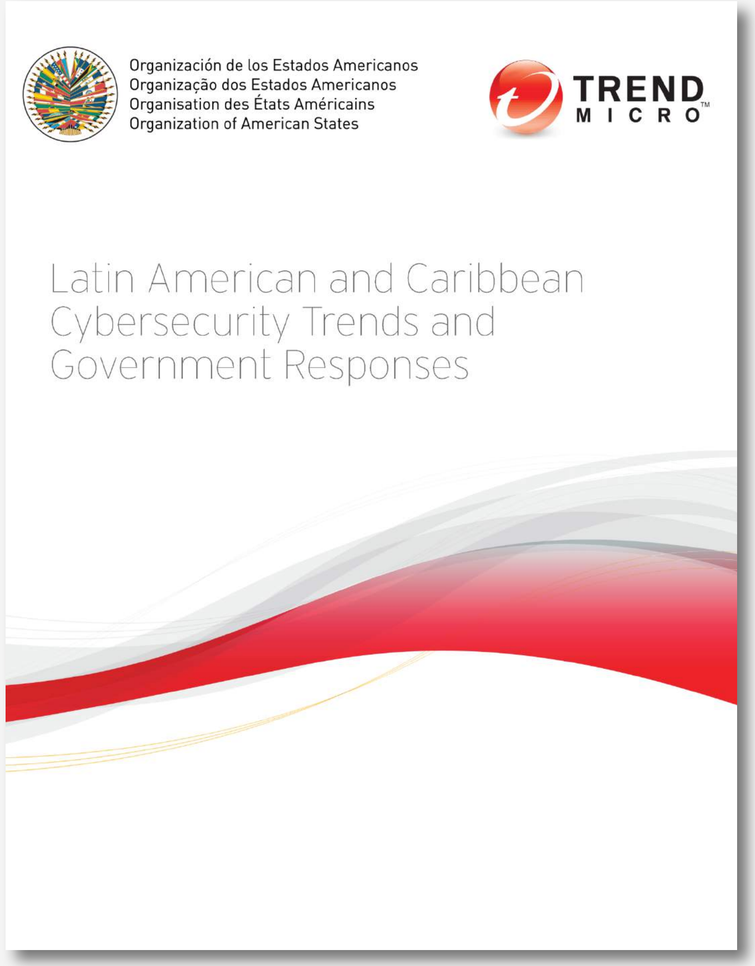
In **20 countries** no command and control center exist, and in another 7 this function is performed without formality

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

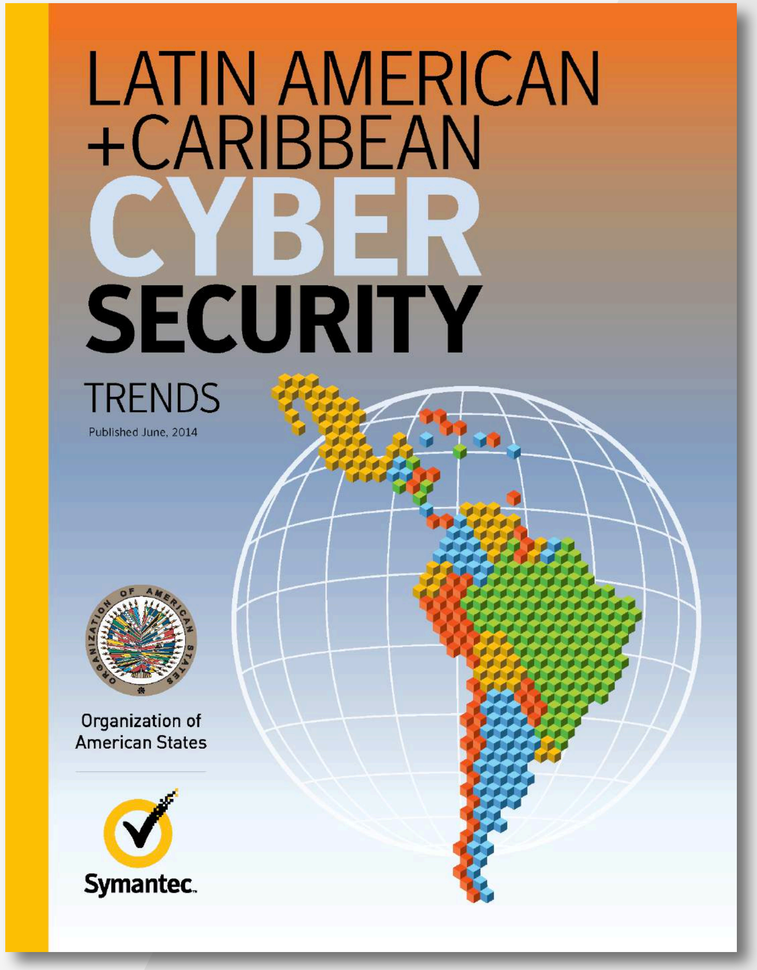
In **28 of the 32 countries**, there is no national cyber security awareness programs

Challenges in the Financial Sector

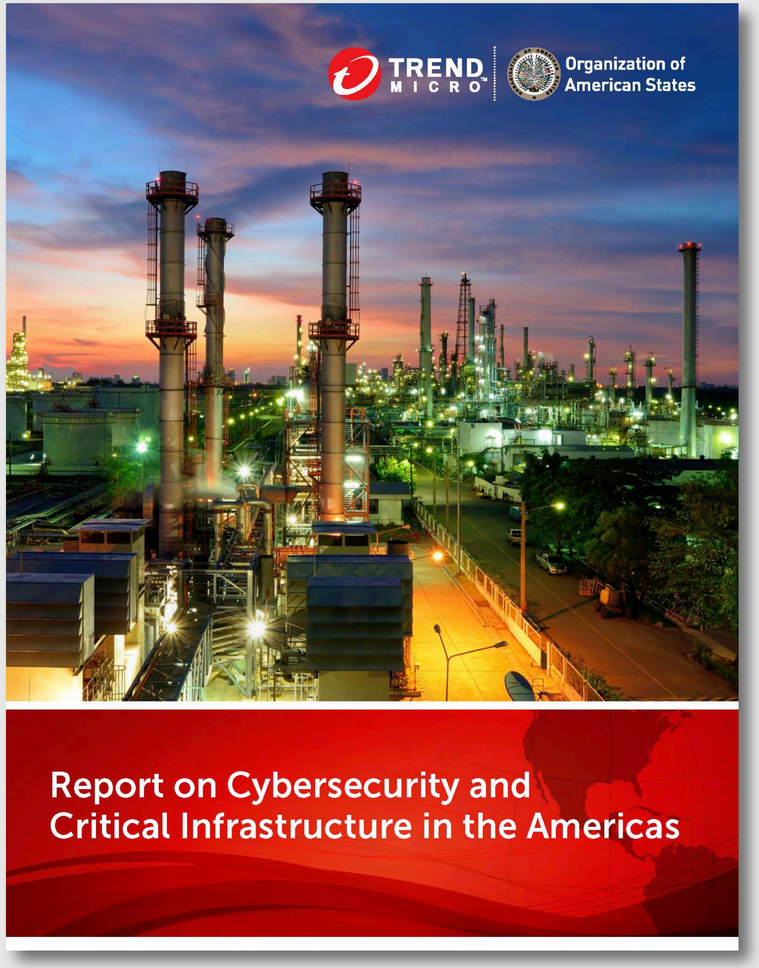
- There is limited formal/informal channels of communication between the Financial Sector and national incident response institutions.
- Attacks are getting more sophisticated everyday and the response time is getting shorter.
- Terrorist and criminal organizations have identified the internet as one of their primary sources for revenue.
- Lack of proper regulation and legislation. Financial Sector institutions don’t need to be afraid to these words, instead they must need to take part of the dialogue.
- Unregulated electronic currencies is a revenue stream for criminals and they make it difficult for law enforcement to trace.



2013



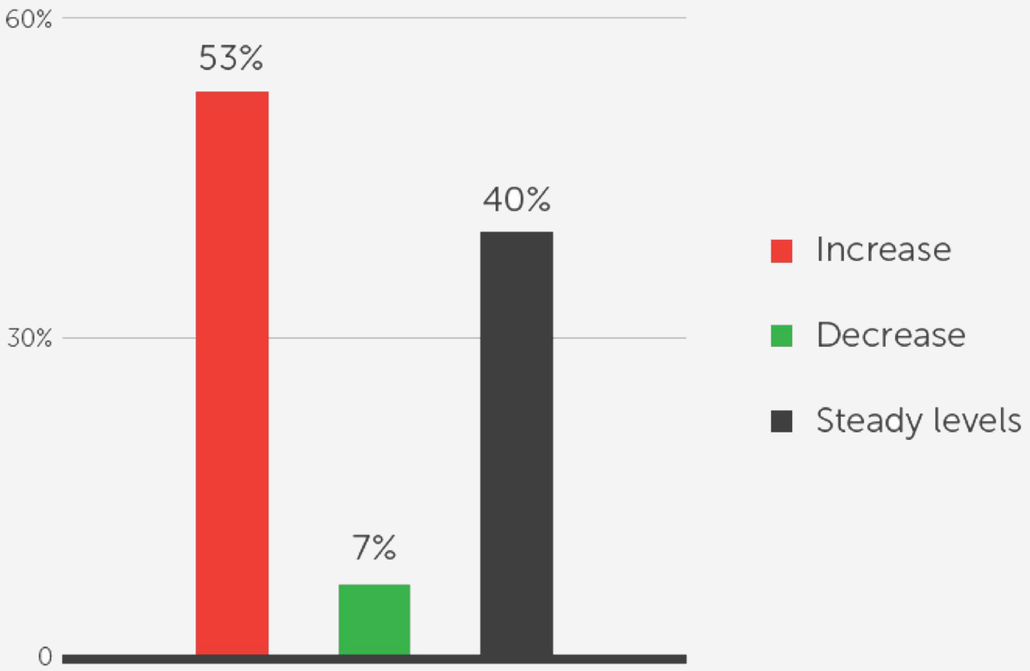
2014



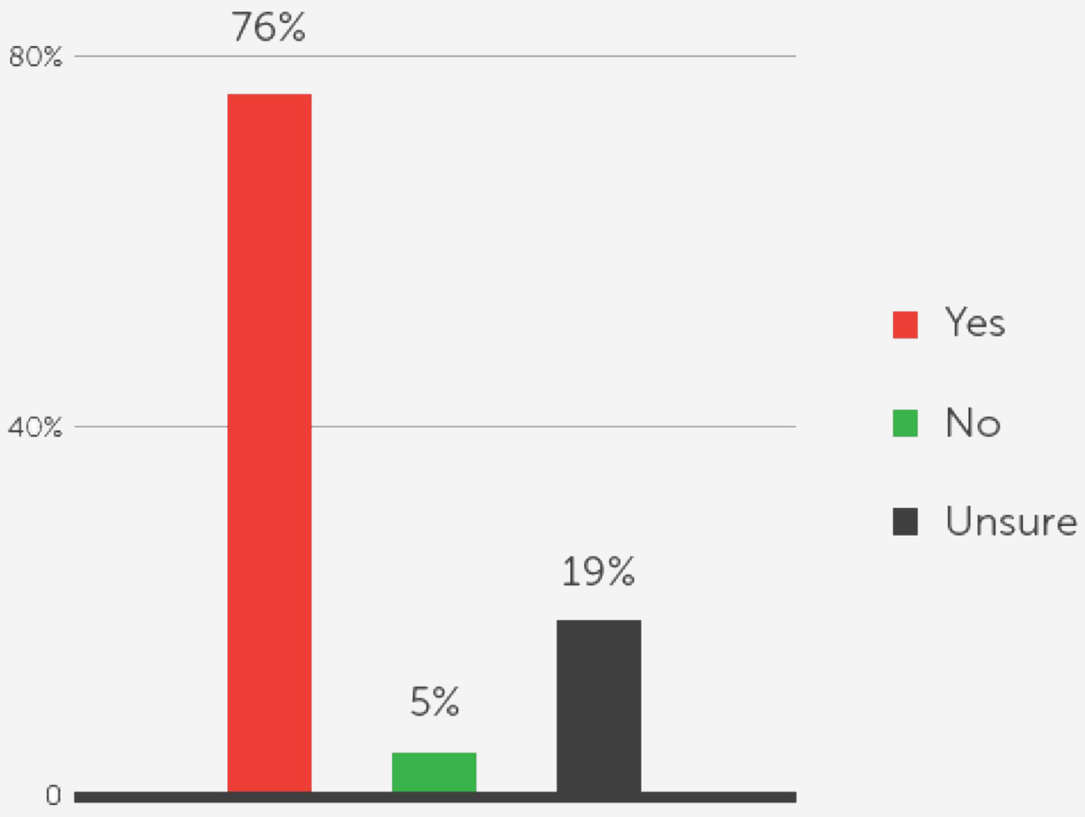
2015

Level of Incidents to the Computer System in the Last Year

Have you noticed an increase, decrease, or steady level of incidents to your computer systems in the last year?

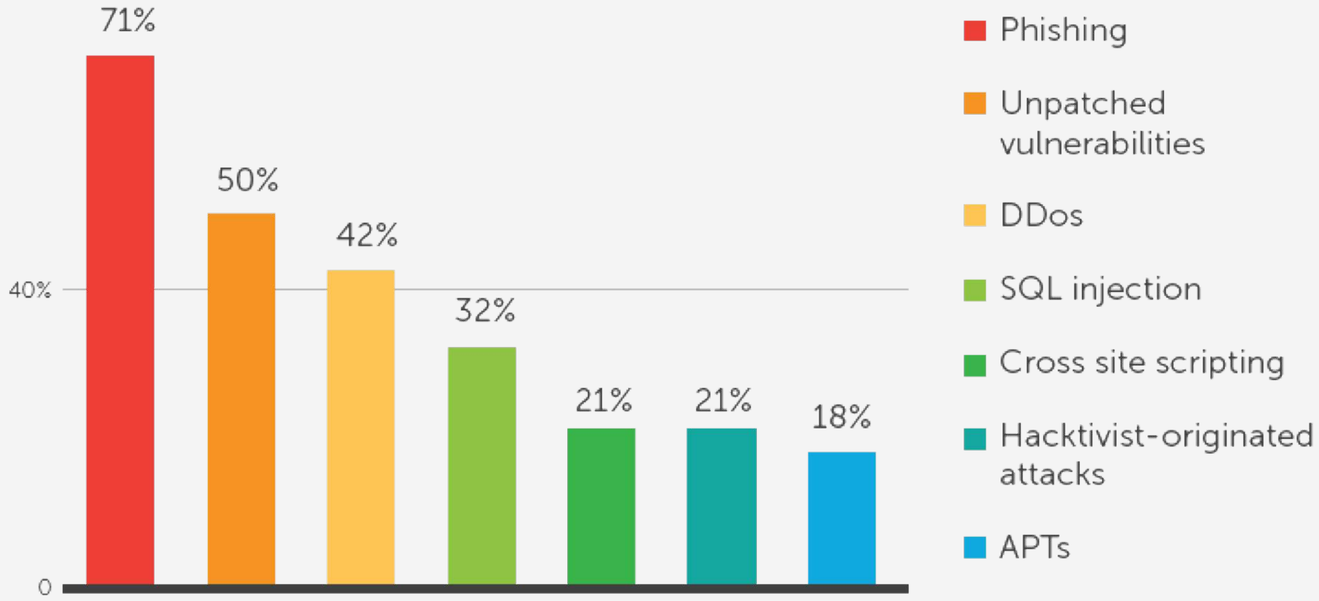


Are incidents against infrastructures getting more sophisticated?



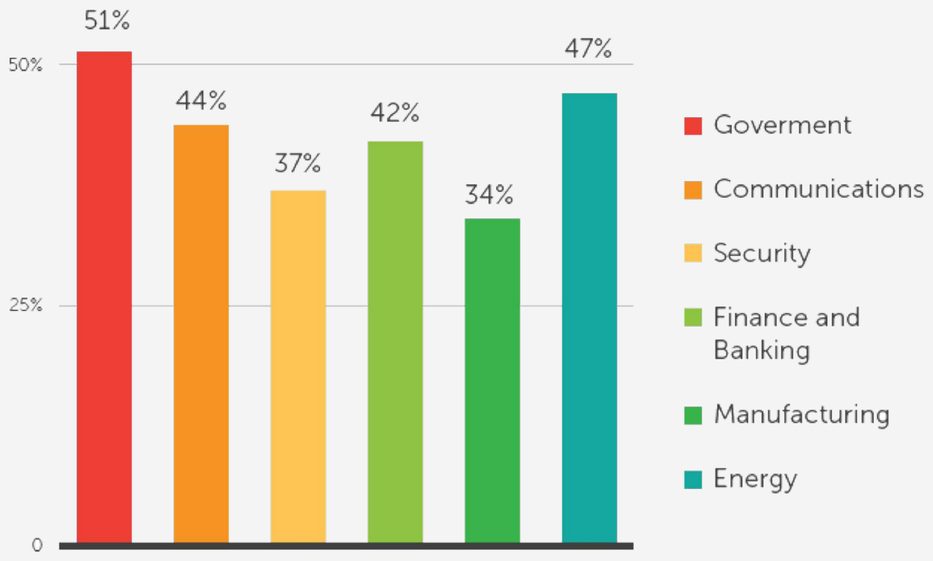
Types of Cyber Attack Methods

What types of cyber attack methods have been used against your organization?



Experience with Various Incidents

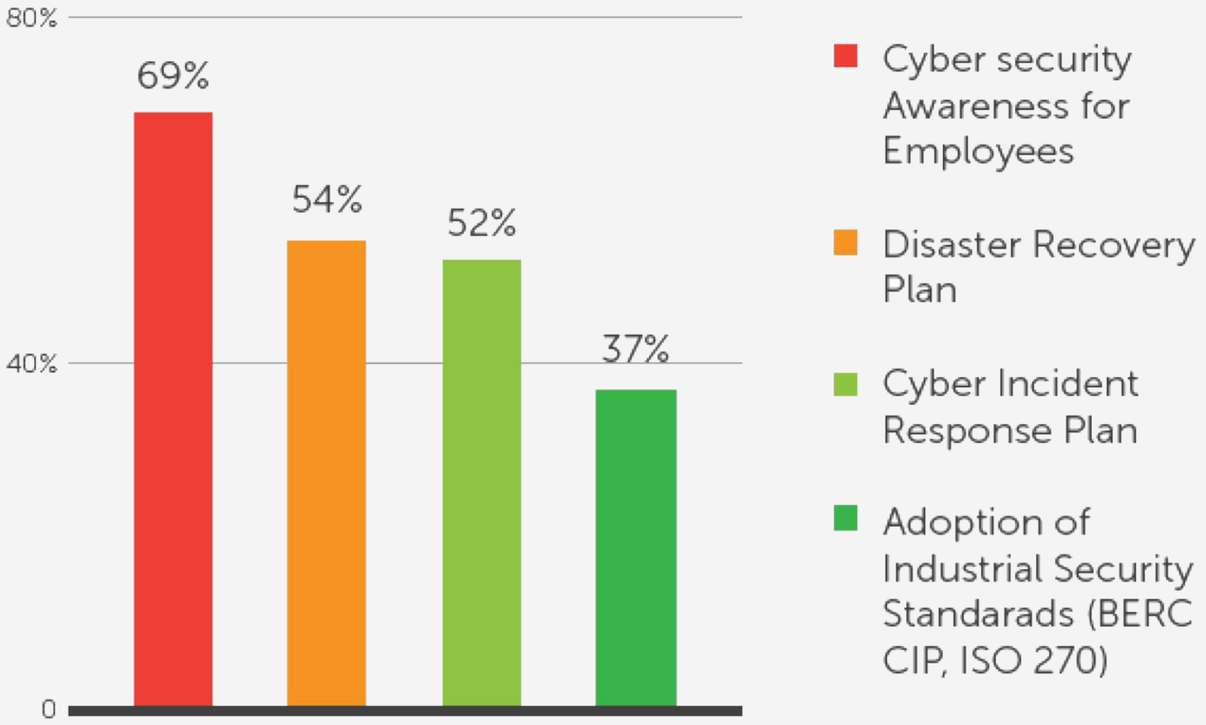
Percentage of organizations that experienced attempts to have information deleted or destroyed by organization type



According to the survey results, the government and energy sectors are the top two industries that experience destructive attacks by threat, followed by communications and finance and banking.

Cybersecurity Policies

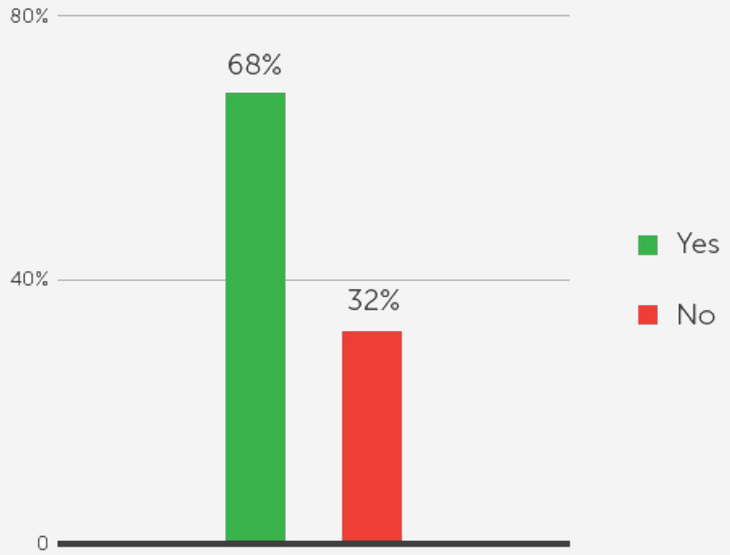
Does your organization have cybersecurity policies and/or plans?



If Respondents trust the Government to advance a Cybersecurity Agenda in Critical Infrastructure Industries

The good news is most respondents (68%) claim they trust their government to support advancements in dealing with the threat. This may indicate the barrier of implementing more dialogue is lower than it may seem and simply requires the public-private organizations to reach out to each other and start the process.

Do you trust the government to advance a cyber-security agenda in critical infrastructure industries? How willing are you to work with them?



What are we doing?

OAS Regional Approach

CICTE Secretariat

REMJA Cybercrime (Legislation)

CITEL (Telecommunications)

OAS Hemispheric Cyber Security Strategy (2004)

Declaration “Strengthening Cyber Security in the Americas” (2012)

Declaration “Protection of Critical Infrastructure from Emerging Threats” (2015)

Declaration “Strengthening Hemispheric Cooperation to Counter Terrorism and Promote Security, Cooperation and Development in Cyberspace” (2016)

National Cyber Security Strategies

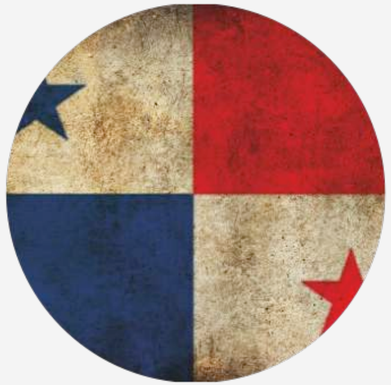
National Strategies Adopted

Colombia

(2011 & 2016)

Trinidad and Tobago

2013



Panama

2013

Jamaica

2015

National Strategies under development

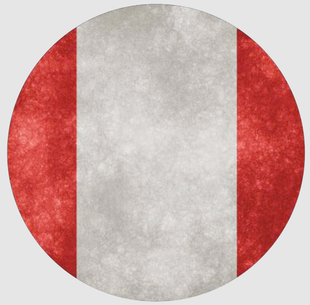
Costa Rica

Dominica

Dominican Republic

Guatemala

Paraguay



Peru

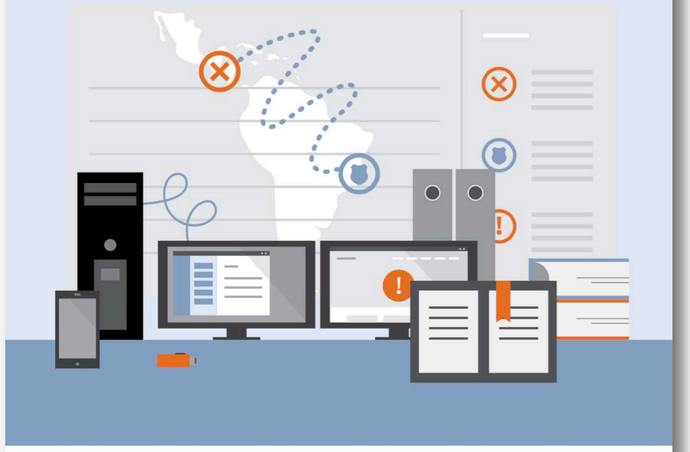
Suriname

Technical Training, Workshops and Technical Missions

Cybersecurity Exercises

Development of National CSIRTs

Best Practices
for Establishing a National CSIRT

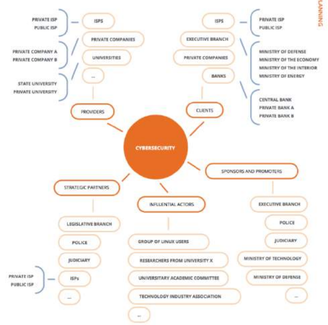


Organization of American States | More rights for more people

Once the groups are defined, brainstorming helps to categorize the nominated actors in each group.

The diagram above shows an example of a mind map midway through the organization process.

As seen in the diagram, a stakeholder may occupy several roles simultaneously. This situation will often present itself both within government and with the private sector, academia and civil society. The clearest example of this is within an ISP and the Government. These groups are strategic partners without whom it would be almost impossible to establish and operate a national CSIRT. At the same time, they are recipients of CSIRT services since they may become a victim of a cyberattack or cyber security incident. The groupings can be further broken down into subgroups, as seen below:



Finally, a list of the stakeholders and their roles will be generated in a formal document.

This list should contain each of the groups involved, the justification for their participation in the CSIRT project, and an officially designation point of contact.

These groups are strategic partners without whom it would be almost impossible to establish and operate a national CSIRT

Reactive Services

Reactive services are the most important services provided by a CSIRT. In essence, "reactive services" respond to cyber security incidents occurring within the CSIRT's community or within its own infrastructure. A response can be launched based either on a request for assistance or from monitoring and sensor networks maintained by the team. The principle types of reactive services are incident management, vulnerability response, and artifact response.

Incident management

Incident management service consists of several phases: notification and receipt of an incident, classification or triage, response, analysis and resolution. The CSIRT must first determine the type, potential impact, and severity of an incident, followed closely by designating a response team to devise a plan of action that will restore services or systems to normal operation or otherwise mitigate the impact of a cyber-security event. In certain cases, this will necessitate that CSIRT personnel visit the site of the security event.

Many actors are typically involved in cyber-incident response, including ISPs, other CSIRTs, technology providers, law enforcement agencies, international actors, legal teams, press departments, and different areas of an affected organization. The CSIRT coordinates response activities and communications of the various stakeholders to optimize efforts and reduce incident resolution times. To accomplish this, the CSIRT should know the requirements and procedures of each of the stakeholders in order to positively manage interaction between them.

Vulnerability response

This comprises a variety of vulnerability management processes, including patching, implementation of countermeasures, and other mitigation strategies. As new patches become available for detected vulnerabilities, the CSIRT must notify all stakeholders and distribute patches or describe techniques for implementing countermeasures while coordinating and confirming that adequate measures are taken.

Response to malicious artifacts

A malicious artifact is a file or object in a system that is involved in an attack on a network or system, or used to evade security controls or measures. Managing malicious artifacts requires removing them from an affected system or informing stakeholders of how to do the same.

Proactive Services

These services aim to improve the infrastructure and security processes of the target community to prevent security incidents or reduce their impact when they occur. The main types of proactive services are performing monitoring, distributing alerts, and offering research and development services.

Monitoring and alert services

1 First Level

One of the most basic services offered by a CSIRT, monitoring and alerting involve the implementation of systems that detect security events, perform event and incident correlation, produce automated reports, and scan for vulnerabilities within the target community. To perform these functions, the CSIRT can either develop its own in-house solutions or employ third party commercial or open source tools and sensors. Information produced by monitoring and alert initiatives will inform strategic decision making and improve incident response processes.

2 Second Level

A more developed CSIRT will offer more advanced monitoring and alert services. These track target community infrastructure and systems in much more depth, but generally provide similar types of alerts and incident correlation as first level monitoring and alerts. More closely monitoring client systems allows for earlier detection of security events, vulnerabilities, or malicious artifacts. To perform this kind of in-depth monitoring, system interconnection or installation of safety sensors in community infrastructure is generally needed.

As a coordinator and collaborator, the CSIRT generates knowledge of the systems, processes, and infrastructure of the target community. Accordingly, the response team can develop strategies, specific tools, and plug-ins from existing systems to analyze, monitor and protect the particular infrastructure of the community it serves.

Research and Development

1 First Level

These services allow the CSIRT and its community to stay abreast of developments in the field of information security and incident response. Specifically, it will allow them to stay up to date on alerts, evolving threats, emerging attack vectors, best practices and new norms in services and device maintenance and operation, defense strategies, and a host of other topics.

2 Second Level

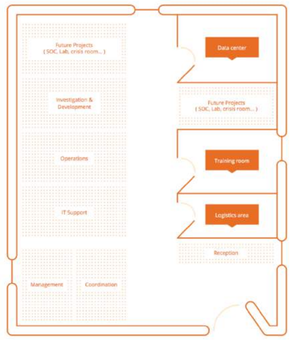
As a CSIRT matures, it will develop more robust R&D capabilities. With the information it gathers and generates, the CSIRT can carry out security audits and assessments on its own systems or those of the target community. This may include application or infrastructure analysis, review of security policies, vulnerability scanning, penetration testing, and compliance with market standards or norms.

As technology evolves, threats and vulnerabilities change. The CSIRT must be able to detect emerging threats or vulnerabilities inherent to new technologies and distribute information relevant to them that can improve security levels.

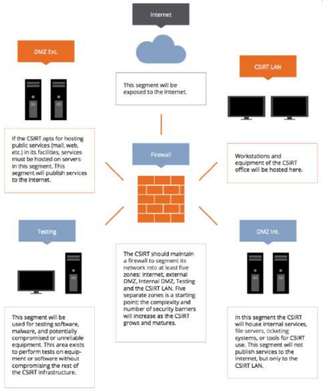
3 Third Level

The most advanced CSIRTs will continue to develop R&D capabilities, for example, malicious code analysis, so as to be able to determine the nature, behavior and purpose of a specific artifact.

Basic Floor Plan



CSIRT Network Basic Design



Formal Closure occurs when all the information generated in the CSIRT establishment process, including its completeness, is analyzed and verified. After the closure process is complete, the National CSIRT will be formally established.

Upon closing the establishment process, the CSIRT Project Manager will have:

- A list of stakeholders
- Statements of establishment of the CSIRT (Mission, Vision, services, etc.)
- Legal documents for the creation of CSIRT
- Physical facilities, leases, etc.
- Hired and trained human resources
- Operations Manual with policies and procedures
- Technological infrastructure and respective support contracts

In addition, other documents are drafted during the establishment phase, including definition of scope, timeline and budget. The project team should be convened for a debriefing session to discuss lessons learned and where the process might be improved upon.

Finally, with all the information generated, it is essential to make a closing report containing:

- The overall objective of the project
- Activities performed
- Performance of the project (scope, timeline, budget)
- Lessons learned
- Future Recommendations

This report will be attached to the project documentation and it will give formal closure to the project.

Formal Completion of Activities

During planning, the Project Team establishes clear steps to be completed during project implementation. Each of these has a clear indicator of completion, such as "Trained Human Resources." To record the activity as formally completed, the project team must verify that all necessary staff received the training and then collect appropriate documentation. Similarly, all contracts and service agreements must be verified and have legal approval and necessary documentation.

Finally, the closing report should be approved by the project sponsor in order to complete the implementation phase of the CSIRT.

CSIRTamericas.org

Comunicación en tiempo real |
Intercambio de información | Proyectos colaborativos

CSIRTamericas.org

Online platform designed to:

- Facilitate real-time communication and information sharing.
- Provide early warning feeds and alerts.
- Identify incident trends in the region.
- Facilitate online and real-time collaboration between national CSIRTs.
- Virtual sandboxes to develop tools.

CSIRTamericas.org

Technological platform / to offer

BASIC SERVICES

- Chat and multichat
- Forum
- CSIRTs news
- Digital Library
- Directory
- Events
- Polls

SPECIALIZED SERVICES

- Early warning systems
- (ftp) - performance improvement for second half of 2016

PARTNER SERVICES

- International Partners

CSIRT of the Americas / for

CSIRT Defense

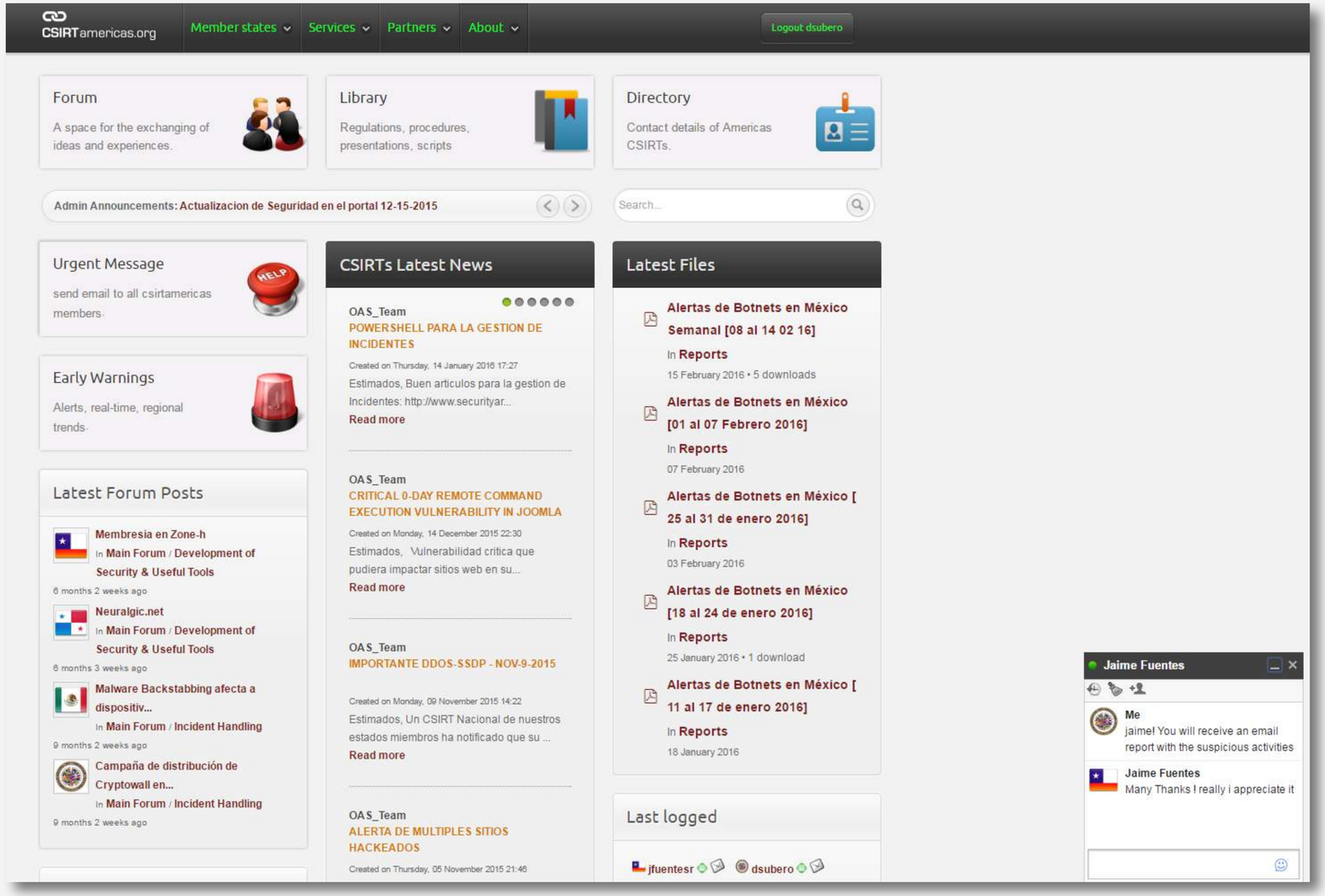
CSIRT Police

CSIRT Gob

CSIRT National

CSIRTamericas.org

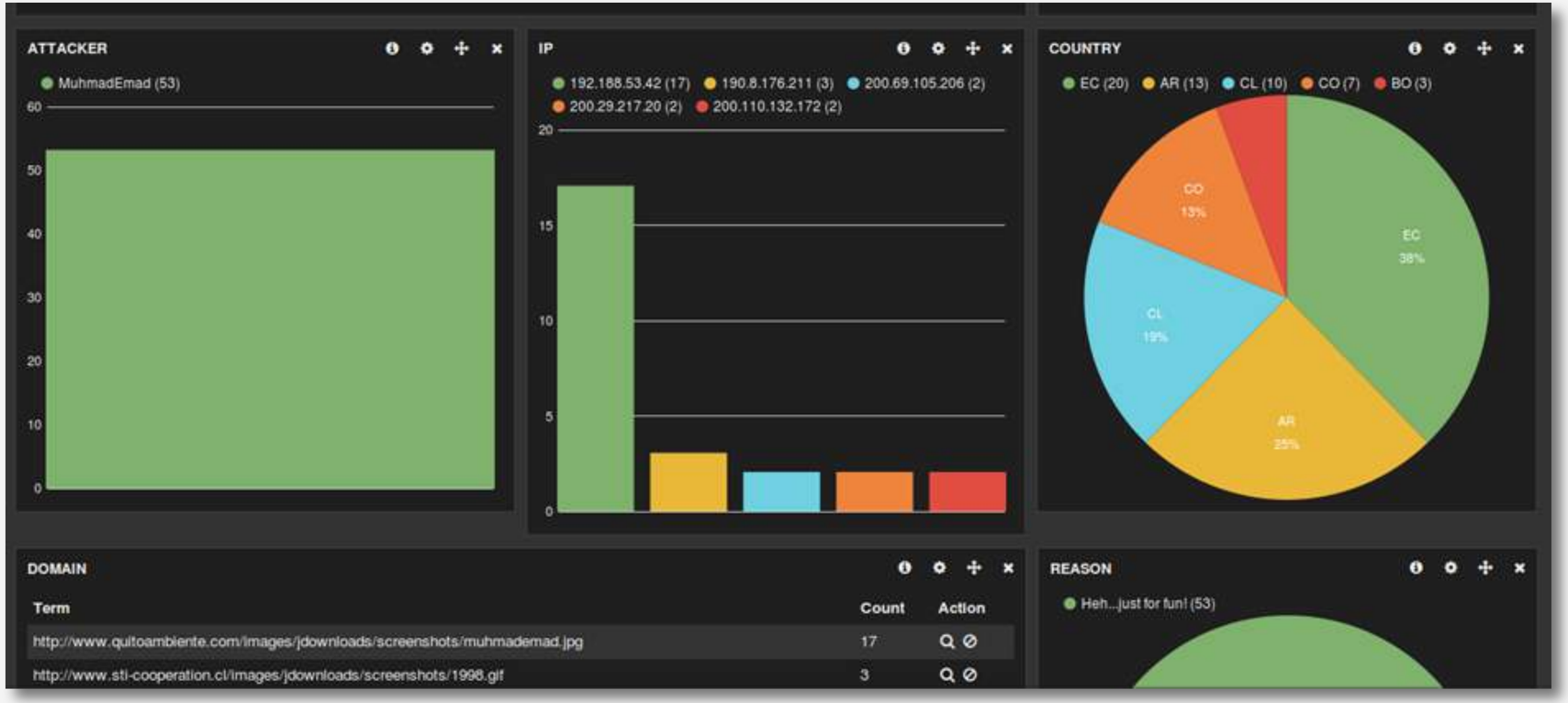
Unify the Community



CSIRTamericas.org

```
Alerts
Vulnerability: “jdownloads” | “ joomla core”
Same attacker : MuhmadEmad
period of time: 6 hours
At 53 websites
At 5 countries affected
Action:
```

Early Regional Warning



CSIRTamericas.org

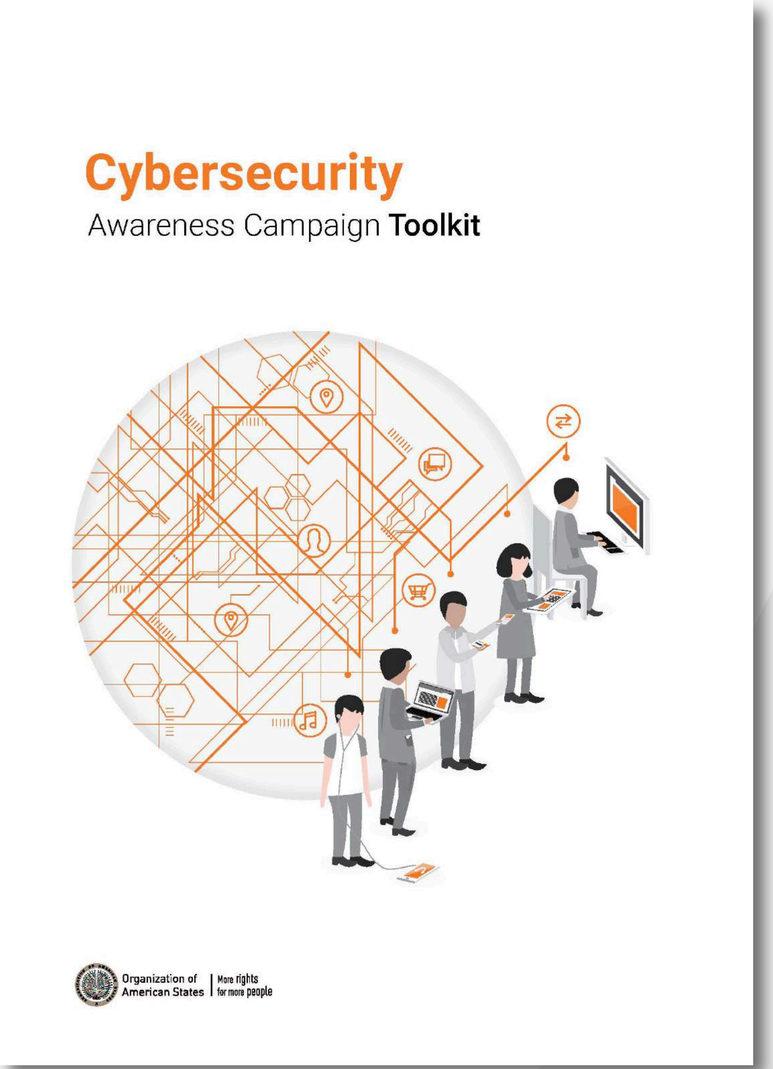
Early Regional Warning

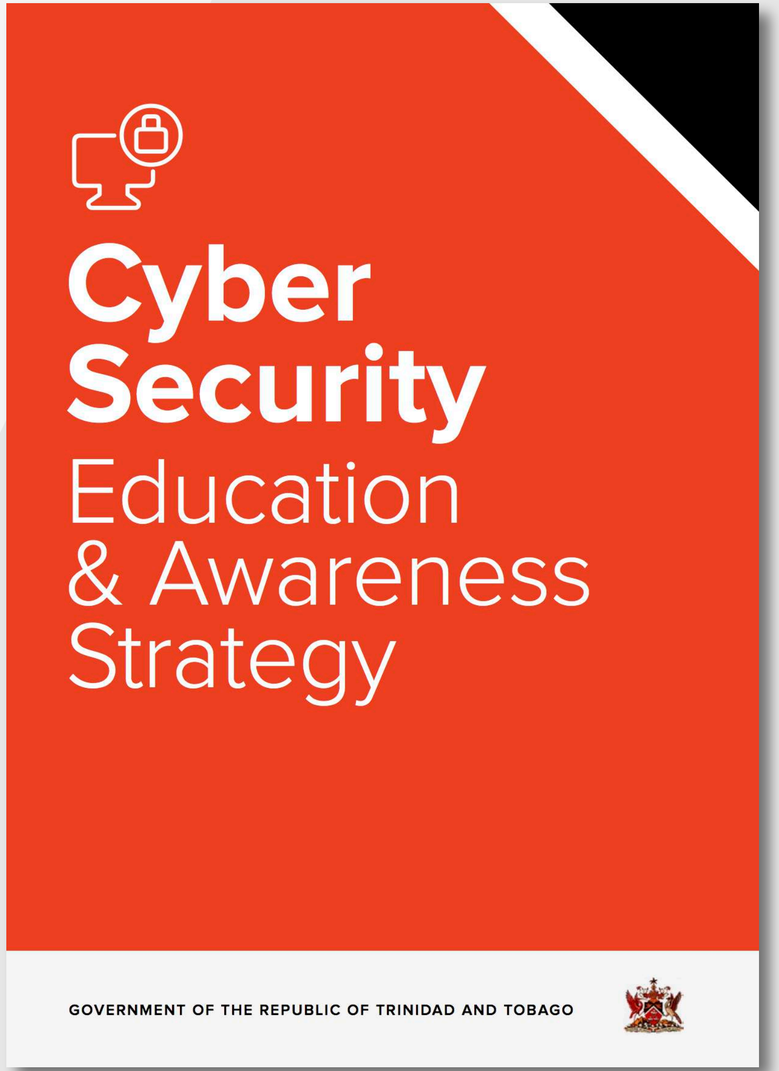
North

AlfabetoVirtual: continued attacks | AR,VE, CL, US, MX | Gov,gob sites

South

Awareness Raising, Research and Expertise


Cybersecurity
Awareness Campaign Toolkit
Organization of American States
More rights for more people


Cyber Security
Education & Awareness Strategy
GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

Our Recommendations

- Promote the establishment of cybersecurity working groups (financial sector) in each of your countries.
- There is still much to do for the exchange of experiences and information at the Regional Level with other key and trusted actors.
- Organize cybersecurity crisis management exercises at the national and regional level.
- Establish informal communication protocols with the sector and with Government as a start.
- Encourage the establishment of financial sector incident response teams.

Our Recommendations

- Implement cybersecurity awareness campaign for employees and customers.
- Reach out to government representatives and support the implementation of the National Digital Security Policy.

Our Proposal

- Participate in the study on the cost of digital security incidents in Colombia (Your commitment is essential!)
- Promote the organization of a regional workshop for the financial sector and incident response representatives from the LAC region.
- Participate in the upcoming International CyberEx2017.
- Participate in the upcoming 2017 Summer BootCamp.
- Examine the challenges faced by the Financial Sector that are unique and engage researchers and ThinkTanks to find solutions.

Creating a career path in digital security

"Through the driving force of the IDB and OAS, the region is the **first in the world** to undertake this deep and broad understanding of cybersecurity capacity across an entire region using the CMM."

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Thank you!
Merci
Gracias
Obrigado

Belisario Contreras

Cybersecurity Program Manager
Organization of American States

BContreras@oas.org

@belisarioc