



OAS

More rights  
for more people

# Cybersecurity

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

---

2016 Cybersecurity Report

[www.cybersecurityobservatory.com](http://www.cybersecurityobservatory.com)

The opinions expressed in this publication are of the authors and do not necessarily reflect the point of view of the Inter-American Development Bank, its Executive Directors, or the countries they represent, or the Organization of American States or the countries that comprise it.

## 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



# 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

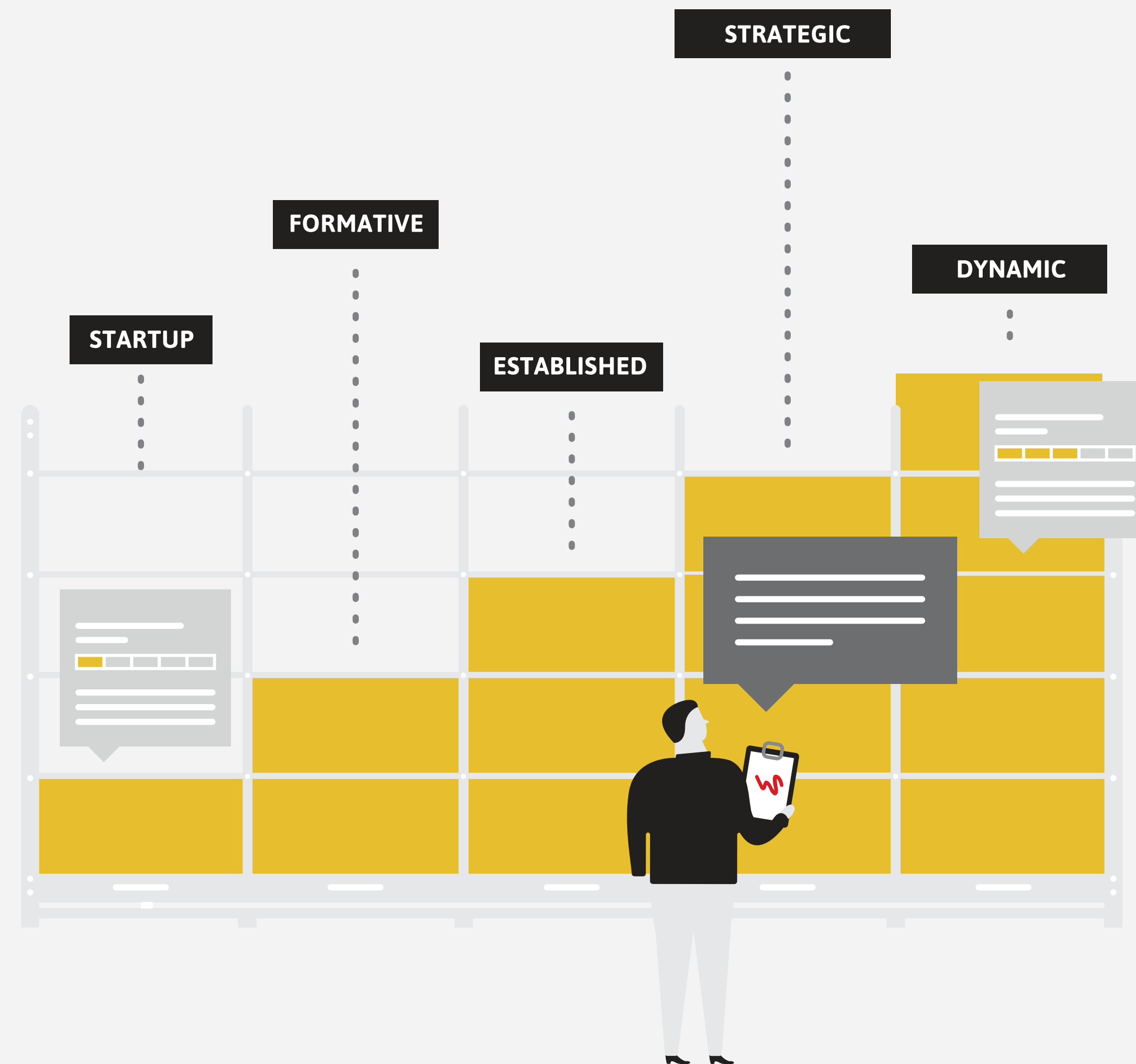


Technologies



Education

# CMM - 5 Levels of Maturity



# Observatory

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

ENGLISH ▾

  
Organization of  
American States  
More rights for more people

 IDB  
Inter-American  
Development Bank

This site shows the levels of maturity on Cybersecurity in Latin America and The Caribbean. Please select te countries you want to compare and **scroll down** to see the results.

Compare another country ▾

Deselect all	Ok
BAHAMAS	
BARBADOS	
BELIZE	
BOLIVIA	
✓ BRAZIL	

promote economic growth and social progress. In light of its increased adoption of ICT, Brazil has become a prime target of cyberattacks and

**Read more >>**

#### BRAZIL

##### Policy and Strategy



##### Culture and Society



##### Education



##### Legal Frameworks



##### Technologies





CHILE

COSTA RICA

Select a country to compare

Download XLS

share

### Policy and Strategy

**Documented or Official National Cybersecurity Strategy**

Strategy development	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Organization	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Content	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>

**Cyber Defense Consideration**

Strategy	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Organization	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Coordination	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>

### Culture and Society

**Cybersecurity Mind-set**

Government	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Private sector	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Society	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>

**Cybersecurity Awareness**

Awareness raising	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
-------------------	------------------------	------------------------	------------------------

**Confidence and Trust on the Internet**

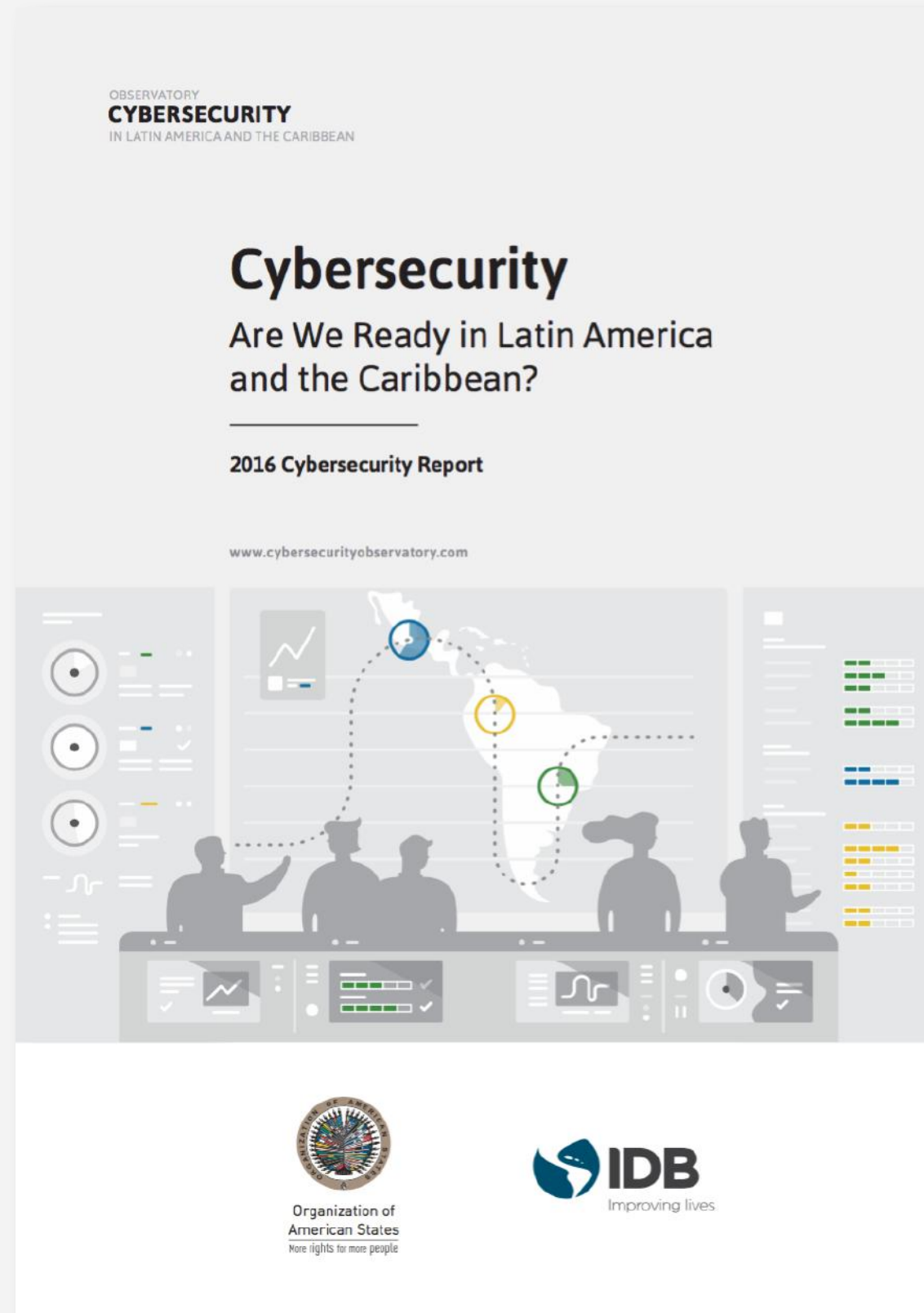
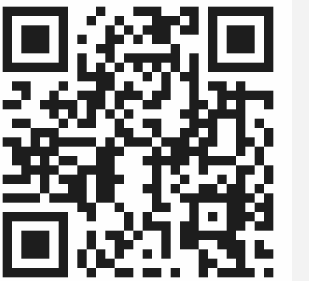
Trust in use of online services	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Trust in e-government	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Trust in e-commerce	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>

**Online Privacy**

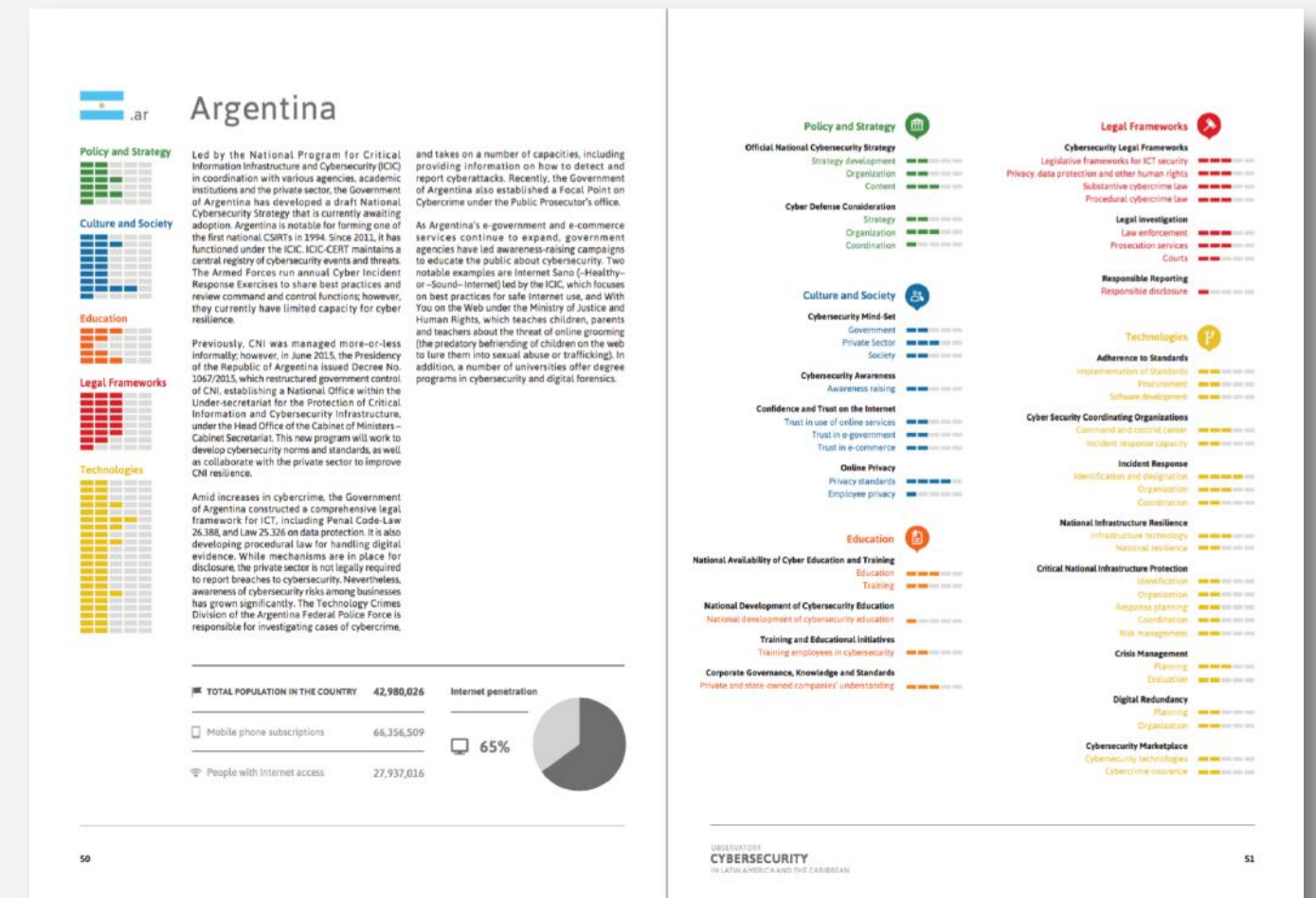
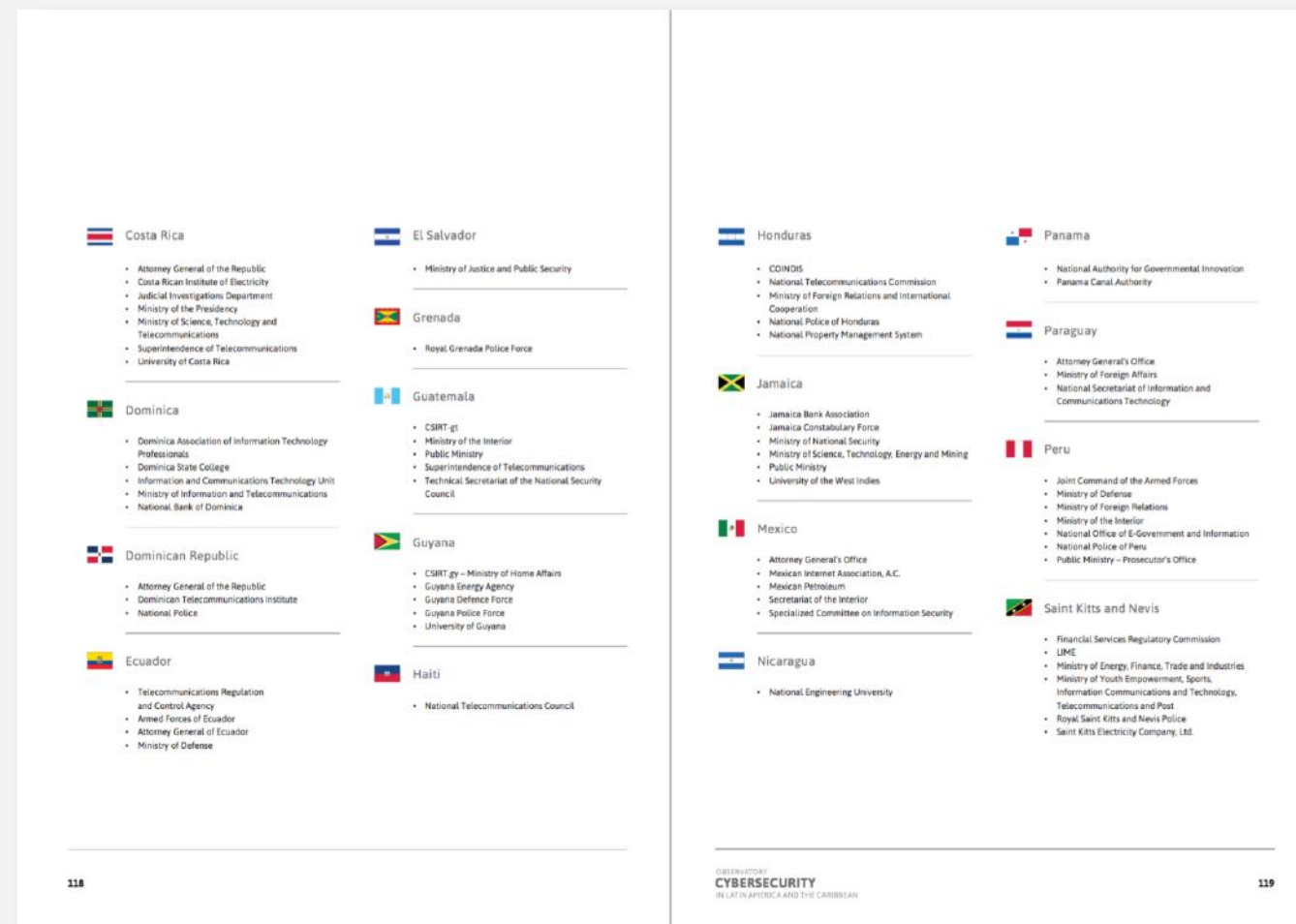
Privacy standards	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
Employee privacy	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>



# How the report looks?



Download Report





on Cybersecurity in Latin America and The Caribbean. Please select te countries you want to compare and **scroll down** to see the results.

Compare another country 

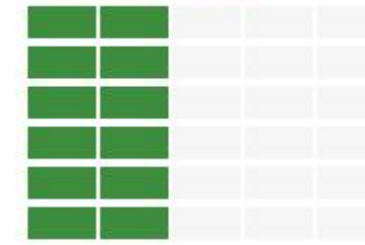


## MEXICO

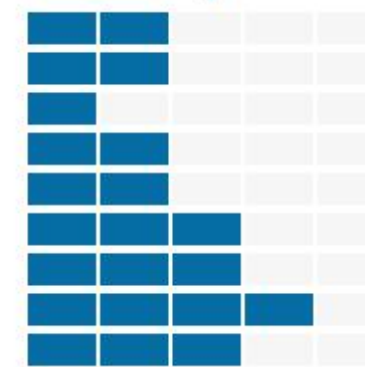
In 2012, the Government of Mexico created the Specialized Information Security Committee, which was tasked with the development of a National

**Read more >>**

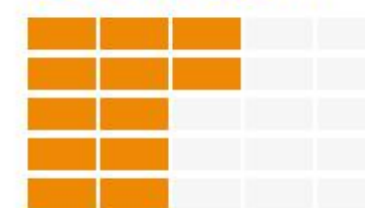
### Policy and Strategy



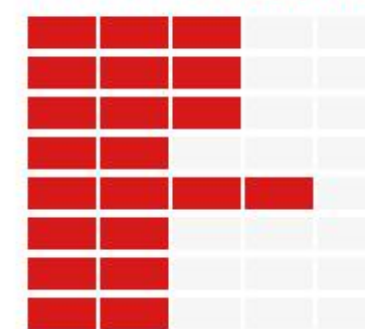
### Culture and Society



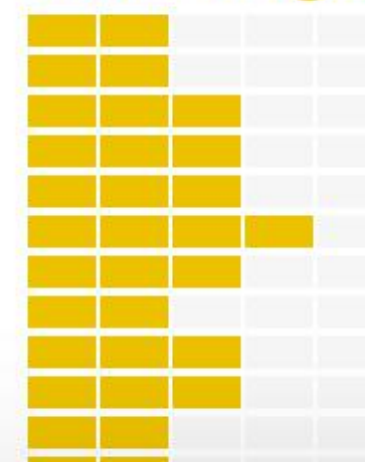
### Education



### Legal Frameworks



### Technologies

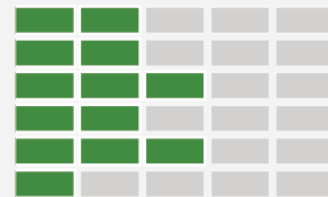


# Advances in the region

Argentina



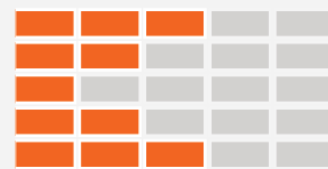
Policy and Strategy



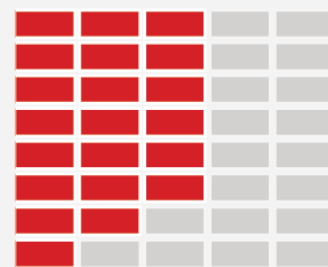
Culture and Society



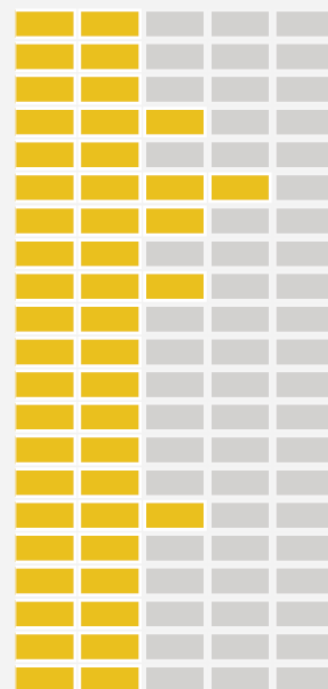
Education



Legal Frameworks



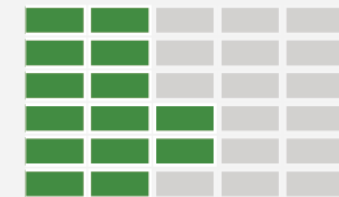
Technologies



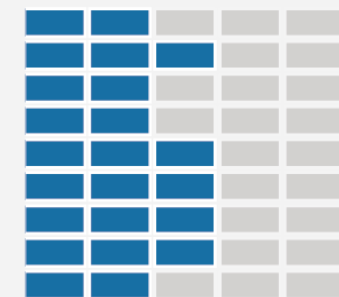
Brazil



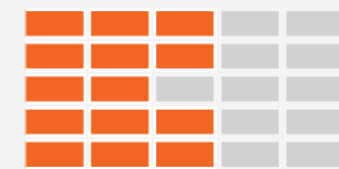
Policy and Strategy



Culture and Society



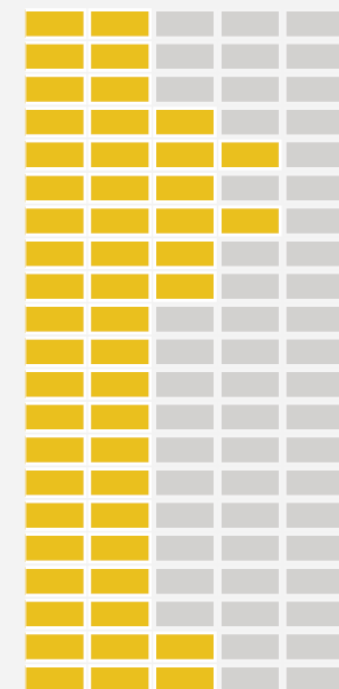
Education



Legal Frameworks



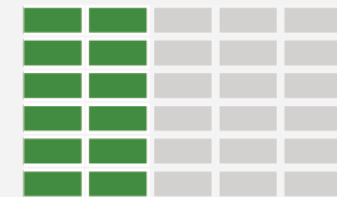
Technologies



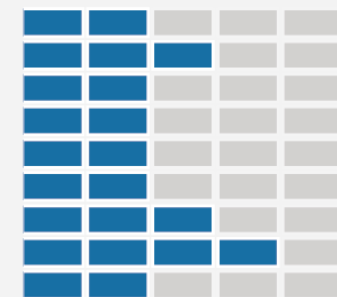
Chile



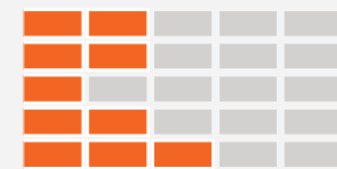
Policy and Strategy



Culture and Society



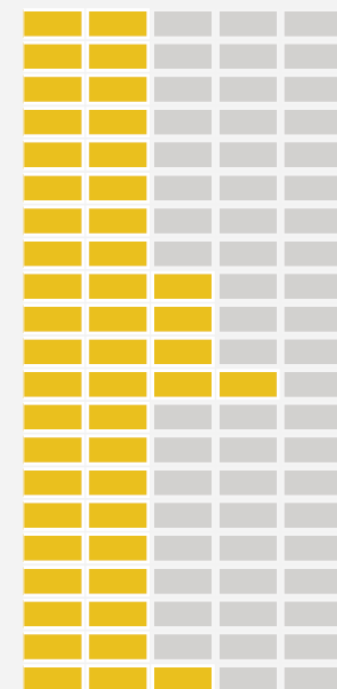
Education



Legal Frameworks



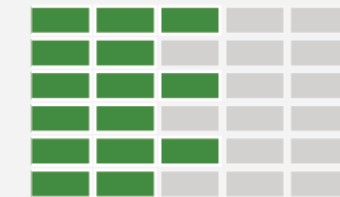
Technologies



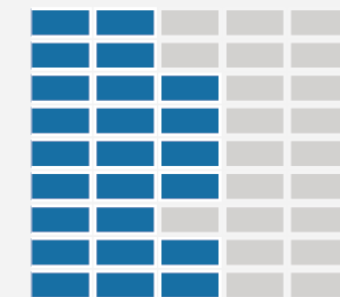
Colombia



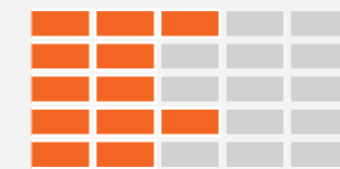
Policy and Strategy



Culture and Society



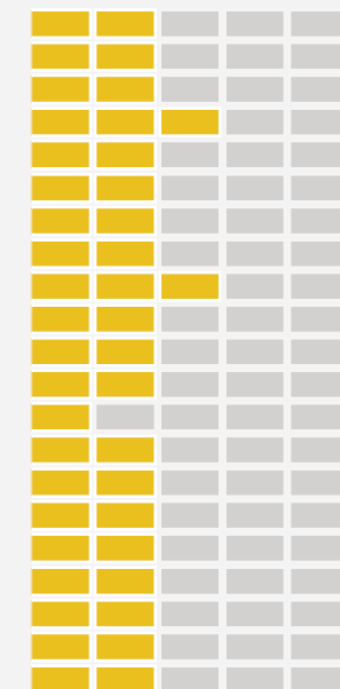
Education



Legal Frameworks



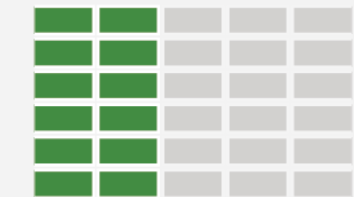
Technologies



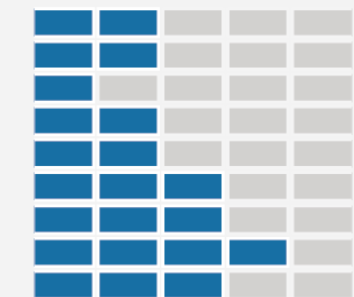
Mexico



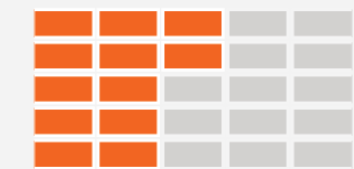
Policy and Strategy



Culture and Society



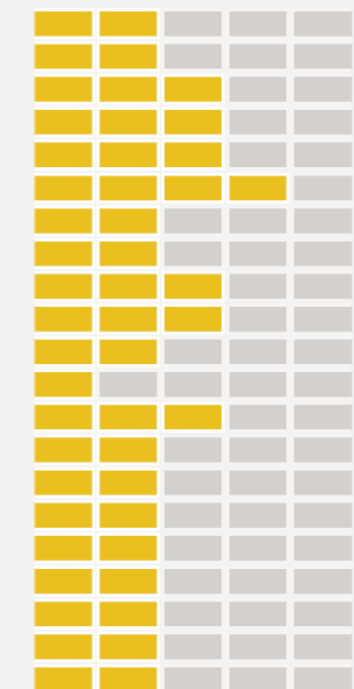
Education



Legal Frameworks



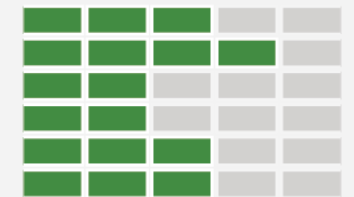
Technologies



Uruguay



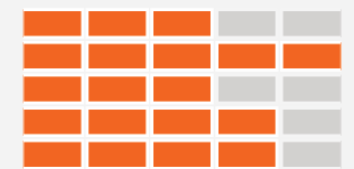
Policy and Strategy



Culture and Society



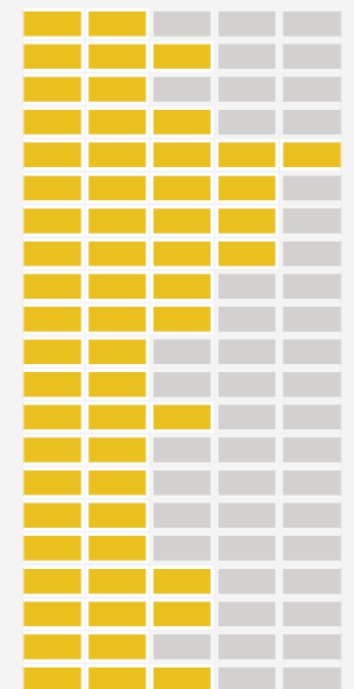
Education



Legal Frameworks



Technologies



# 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 group<sup>1</sup> (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.

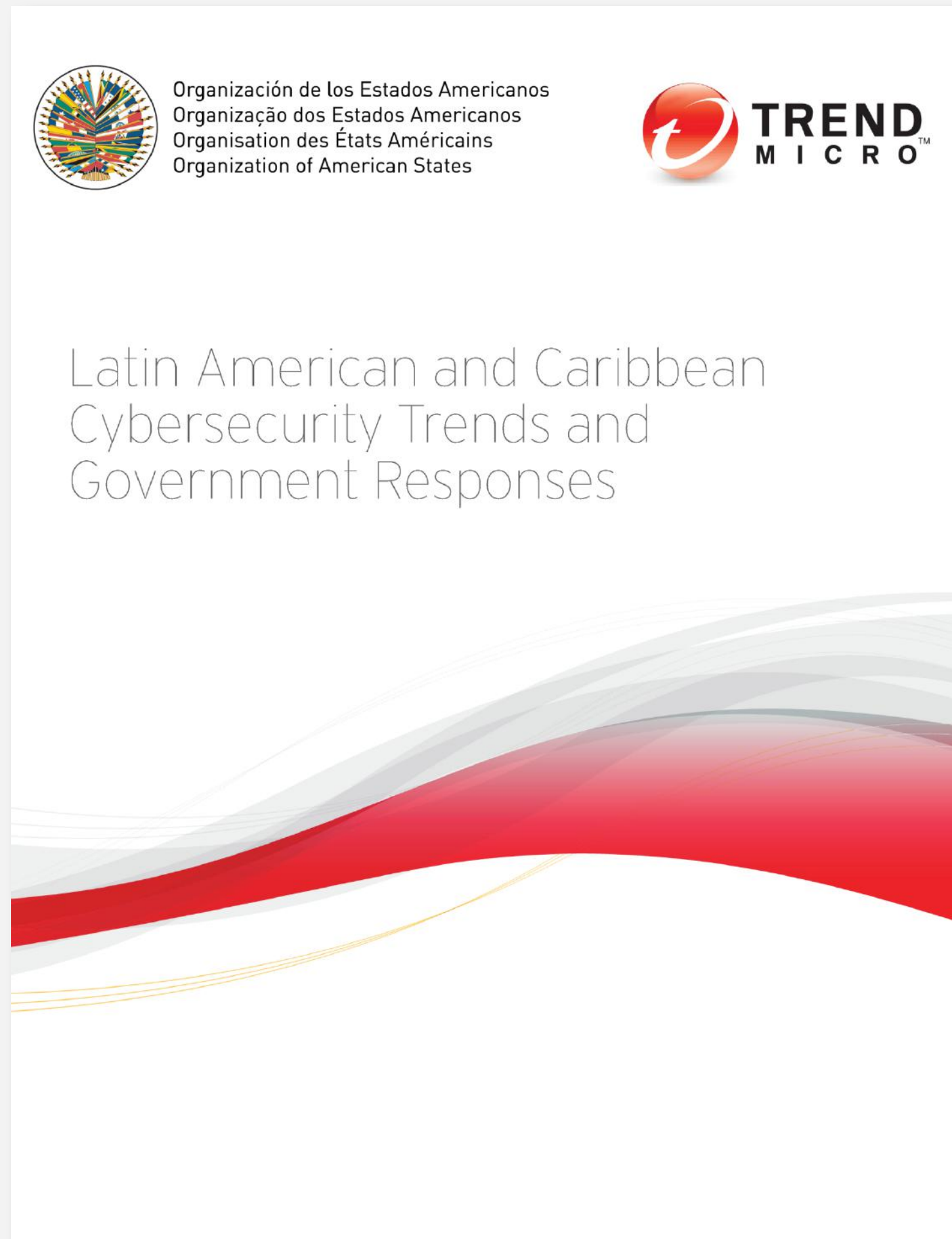
Attacks are getting more sophisticated everyday and the response time is getting shorter.

Terrorist and criminal organizations have identified the internet as one of their primary sources for revenue.

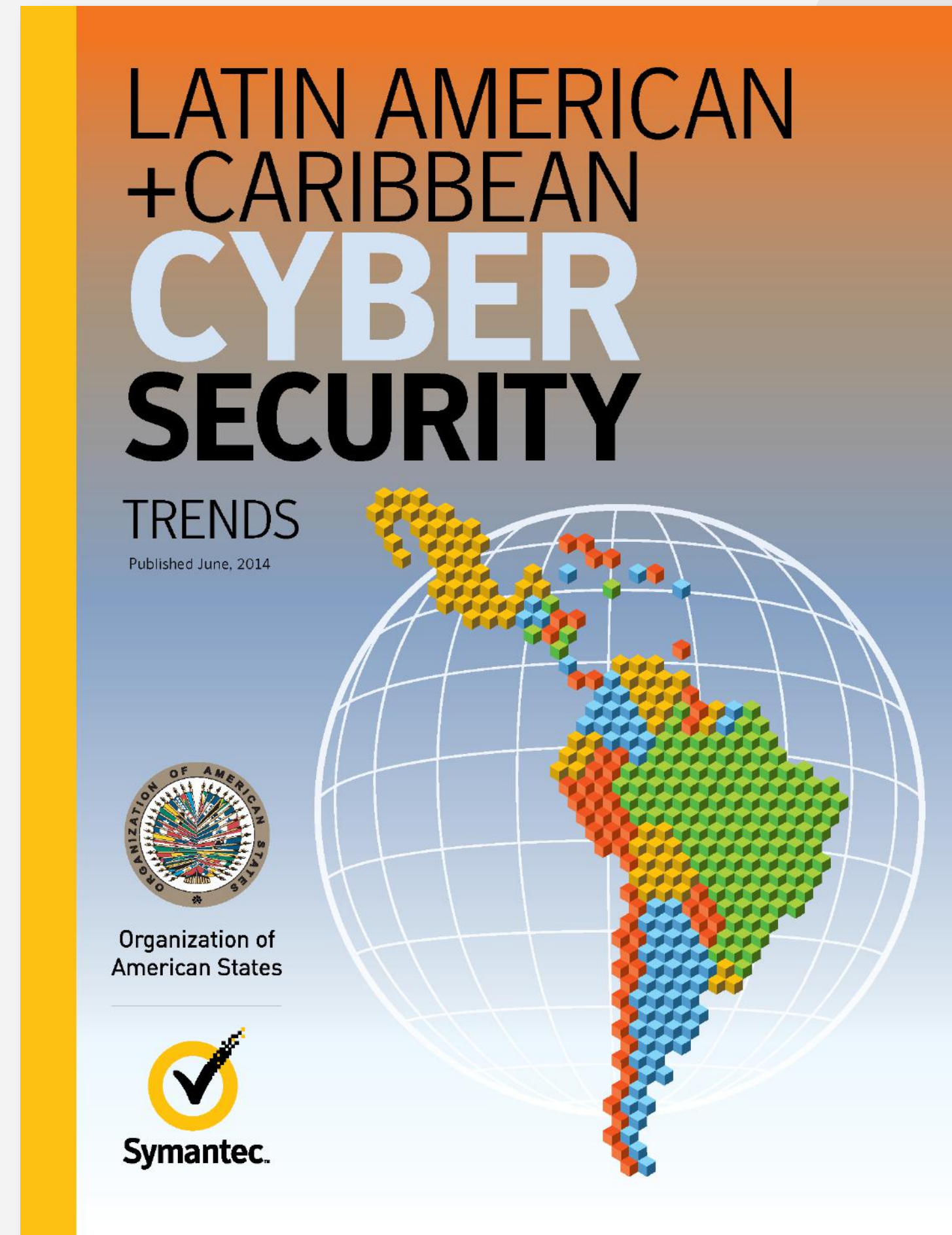
Lack of proper regulation and legislation. Financial Sector institutions don't need to be afraid to these words, instead they must need to take part of the dialogue.

Unregulated electronic currencies is a revenue stream for criminals and they make it difficult for law enforcement to trace.

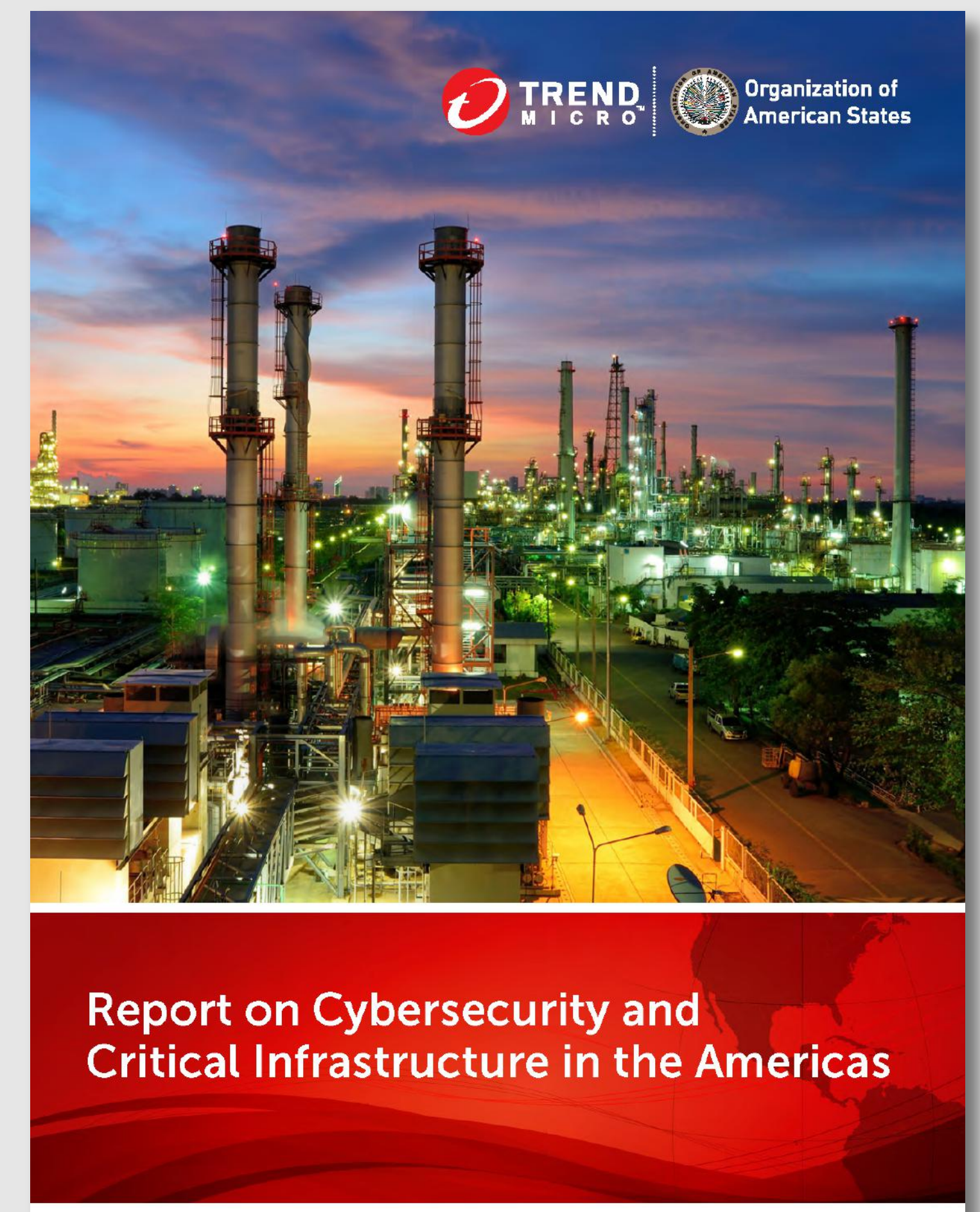




2013



2014

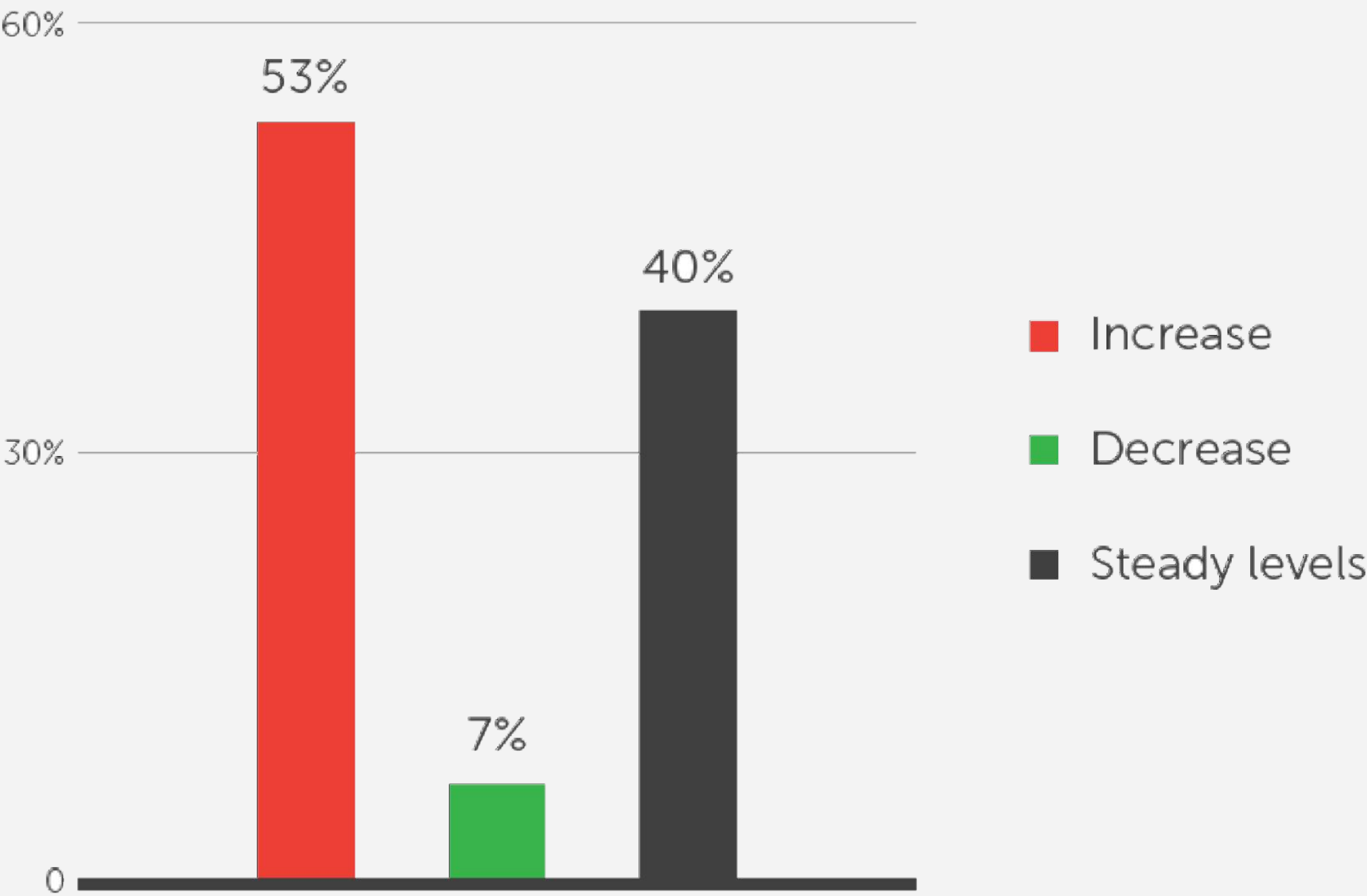


2015

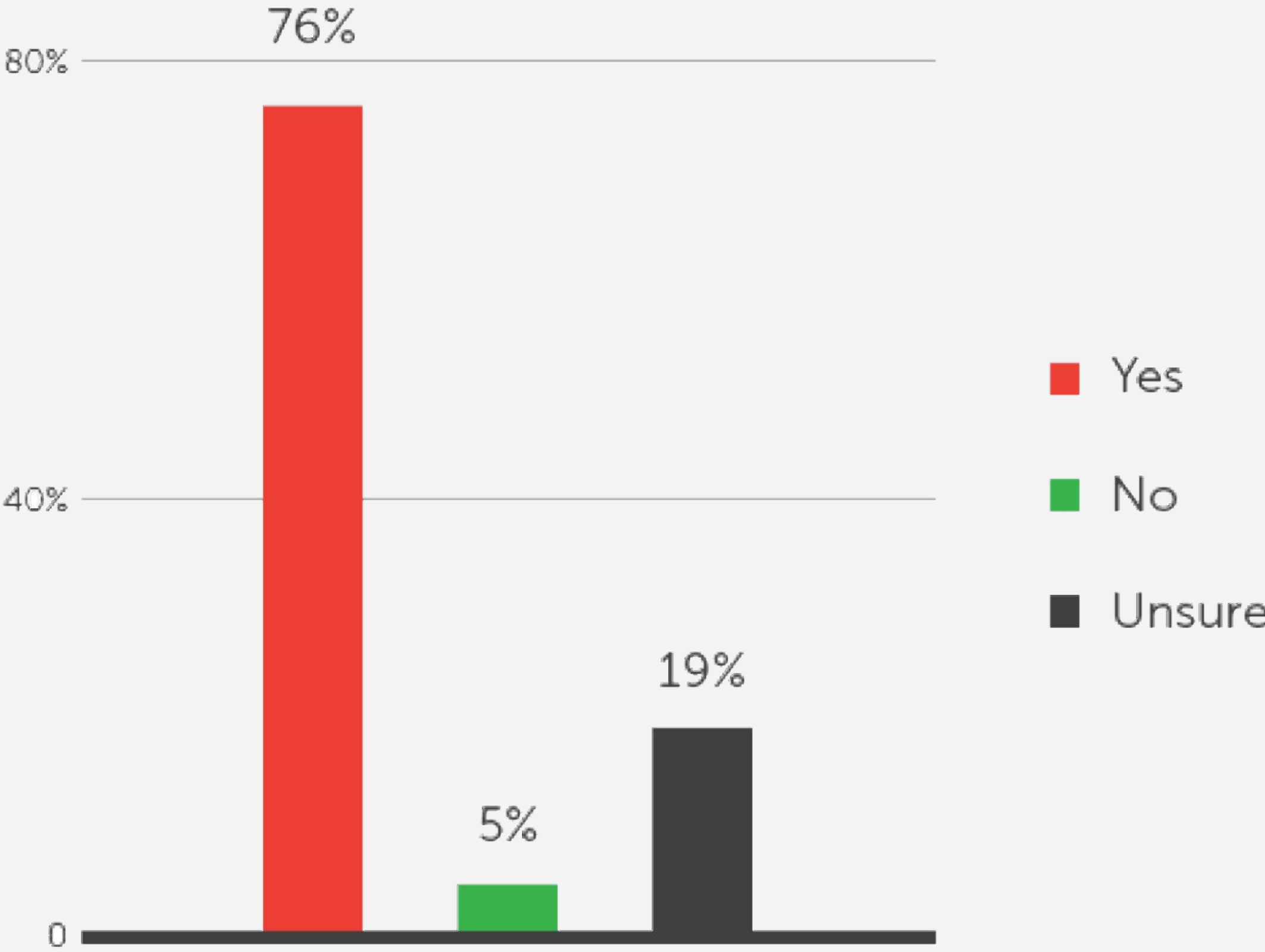


# Level of Incidents to the Computer System in the Last Year

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

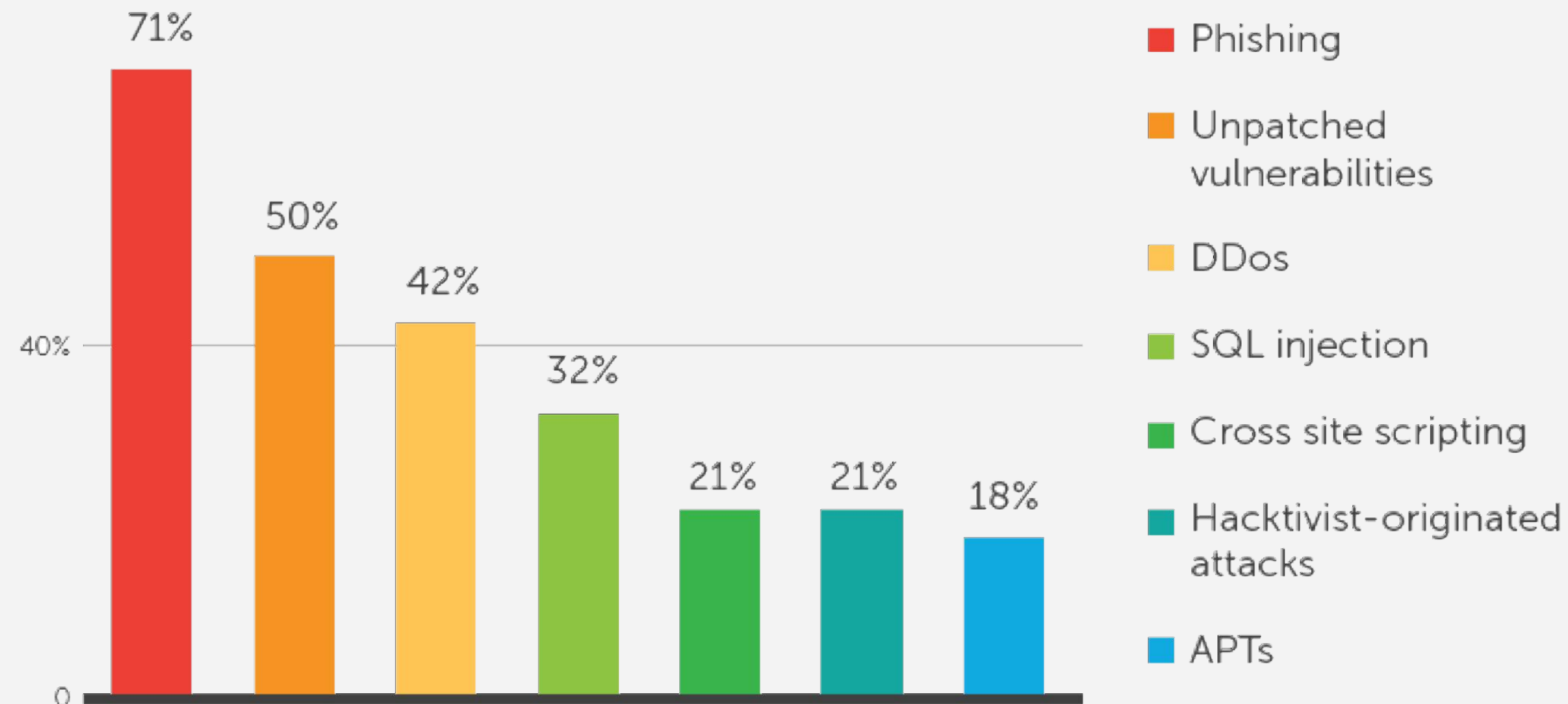


# Are incidents against infrastructures getting more sophisticated?



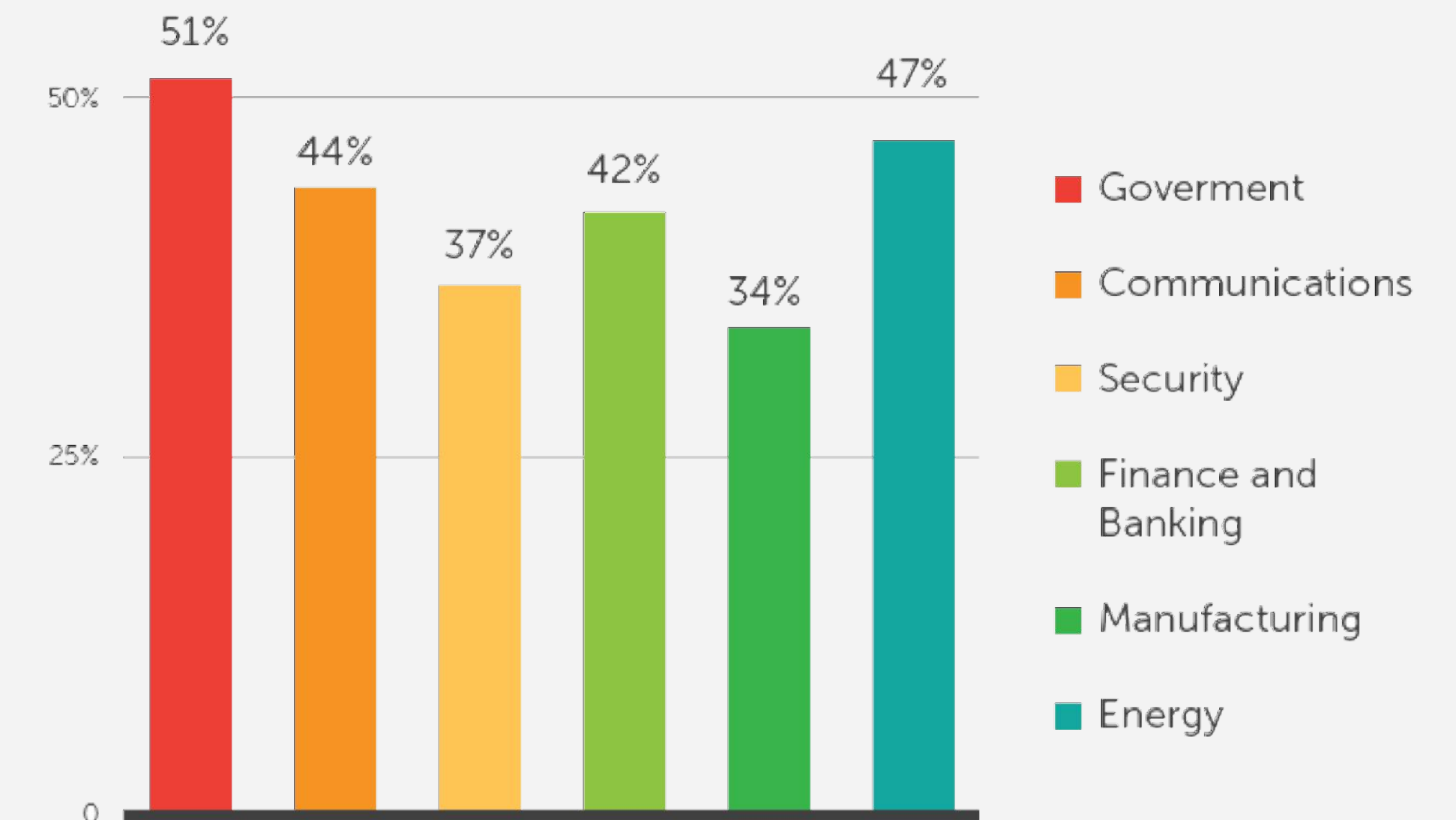
## Types of Cyber Attack Methods

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



## Experience with Various Incidents

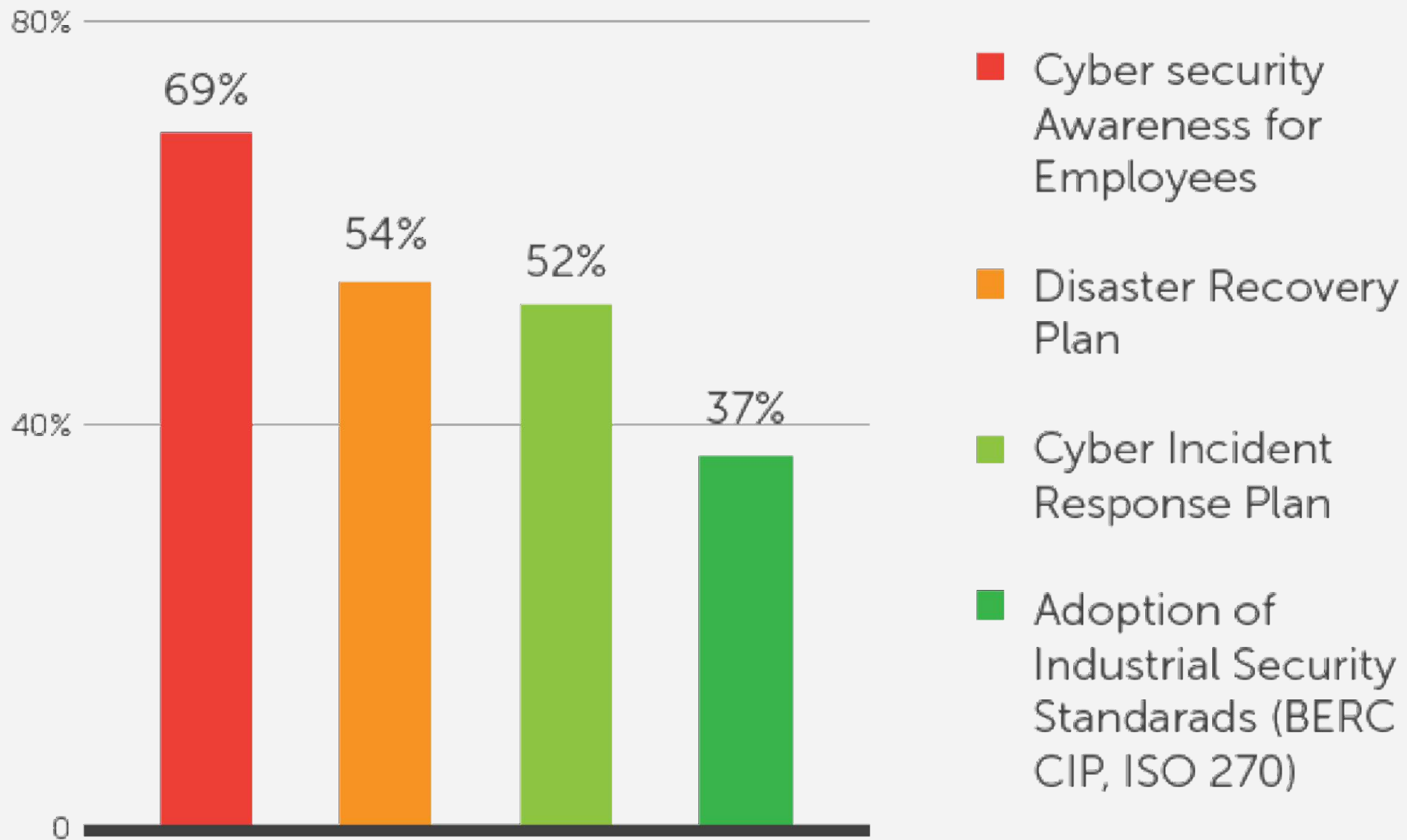
*Percentage of organizations that experienced attempts to have information deleted or destroyed by organization type*



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

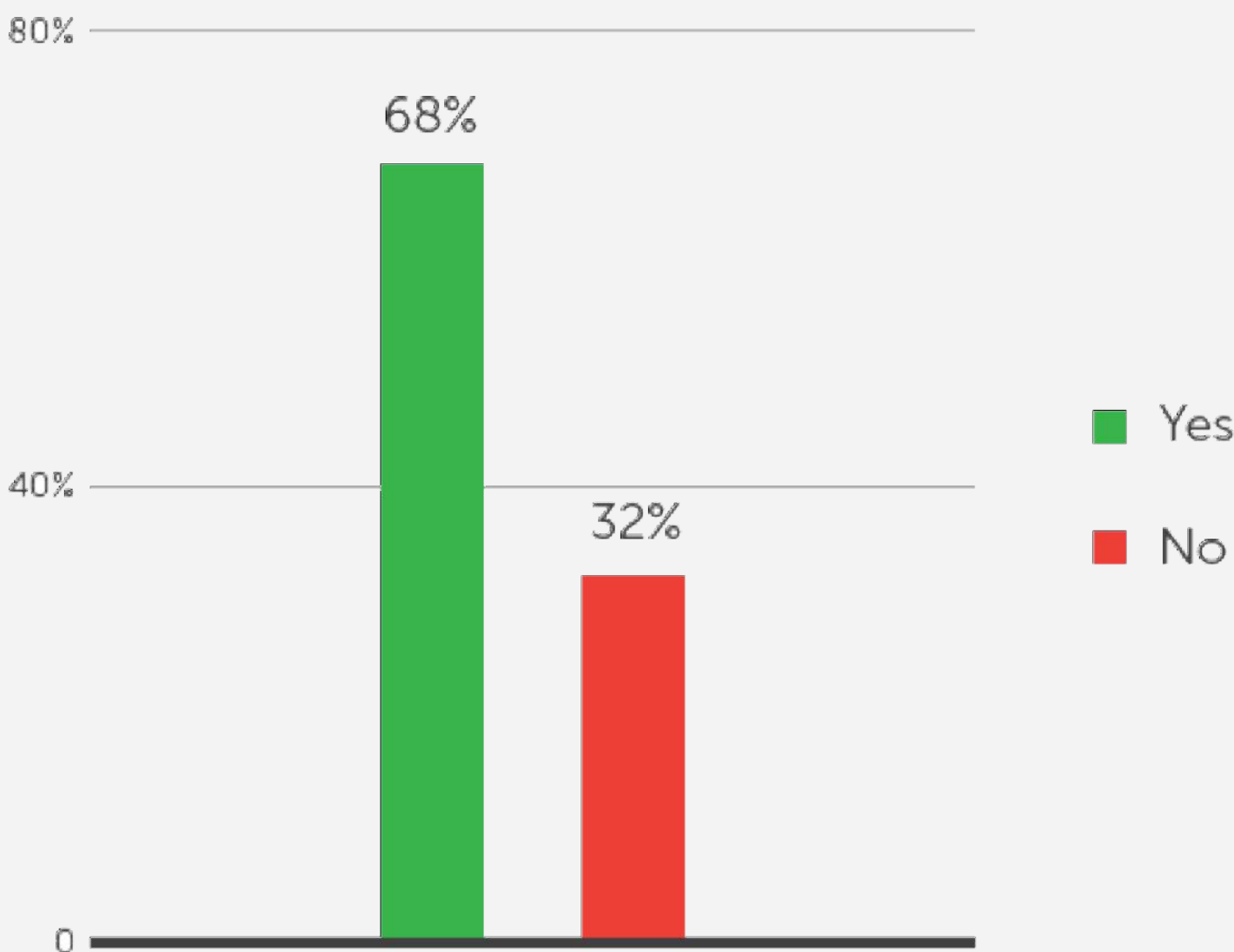
Does your organization have cybersecurity policies and/or plans?



## 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?





# TARGETED ATTACK

## KEY STAGES

Source: Symantec



**01 INCURSION** The attacker gains entry to the targeted organization. This is often preceded by reconnaissance activities where the attacker is looking for a suitable social engineering tactic.



**02 DISCOVERY** Once the attacker has gained entry, they will seek to maintain that access as well as discover what data and other valuable resources they may wish to access.



**03 CAPTURE** Once the valuable data has been discovered and identified, the attacker will find a way to collect and gather that data before trying to exfiltrate it.

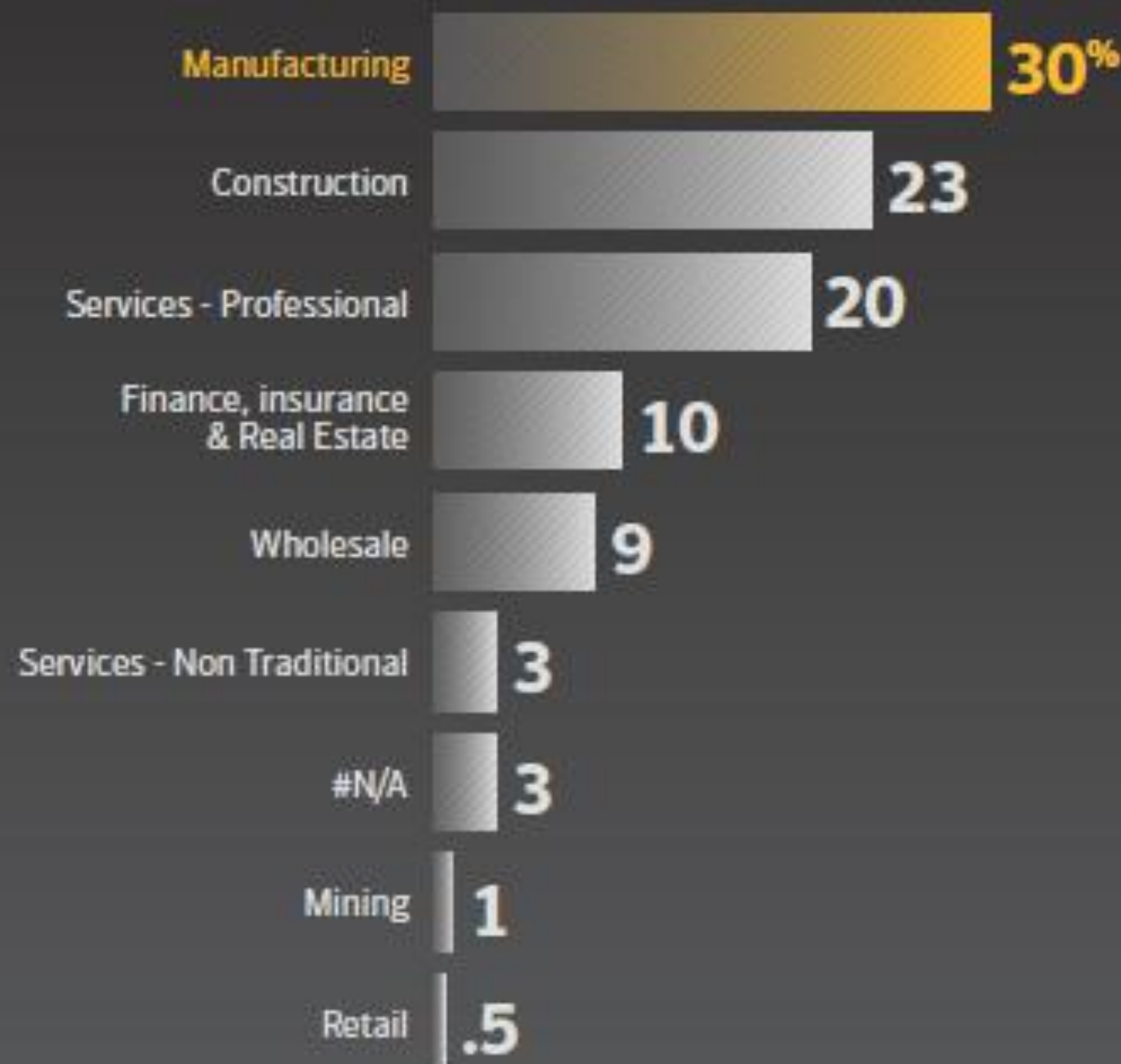


**04 EXFILTRATION** The attacker will find a mechanism to steal the data from the targeted organization. This may be by uploading it to a remote server or website the attackers have access to. More covert methods may involve encryption and steganography, to further obfuscate the exfiltration process, such as hiding data inside DNS request packets.



## Top-Ten Industries Targeted in Spear-Phishing Attacks, Latin America and the Caribbean, 2013

Source: Symantec





# 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

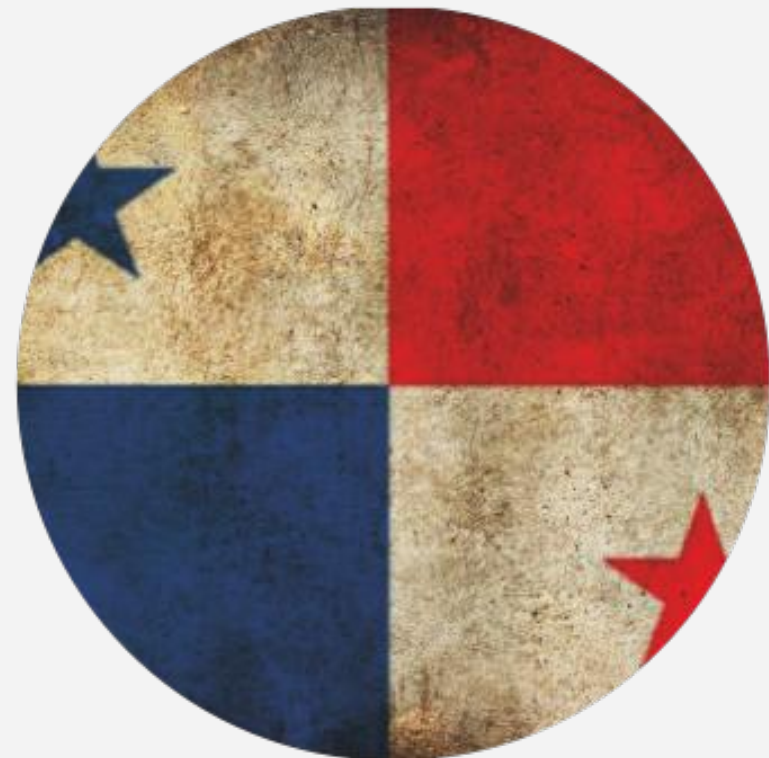
# National Strategies Adopted



**Colombia**  
(2011 & 2016)



**Trinidad and Tobago**  
2013



**Panama**  
2013



**Jamaica**  
2015



# National Strategies under development



**Costa Rica**



**Dominica**



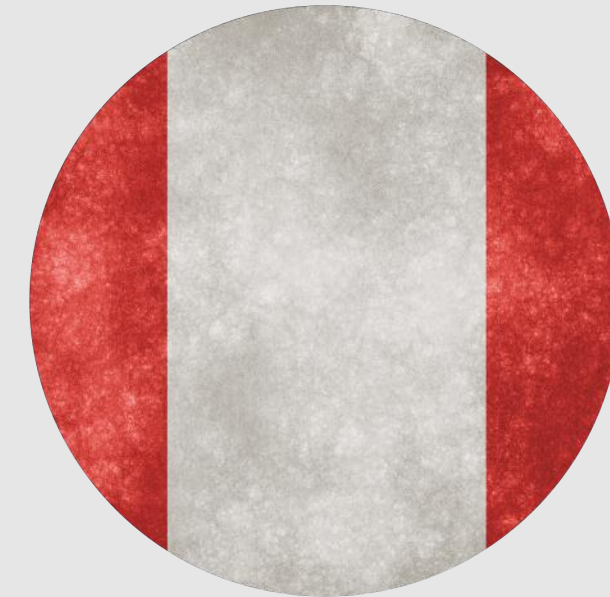
**Dominican  
Republic**



**Guatemala**



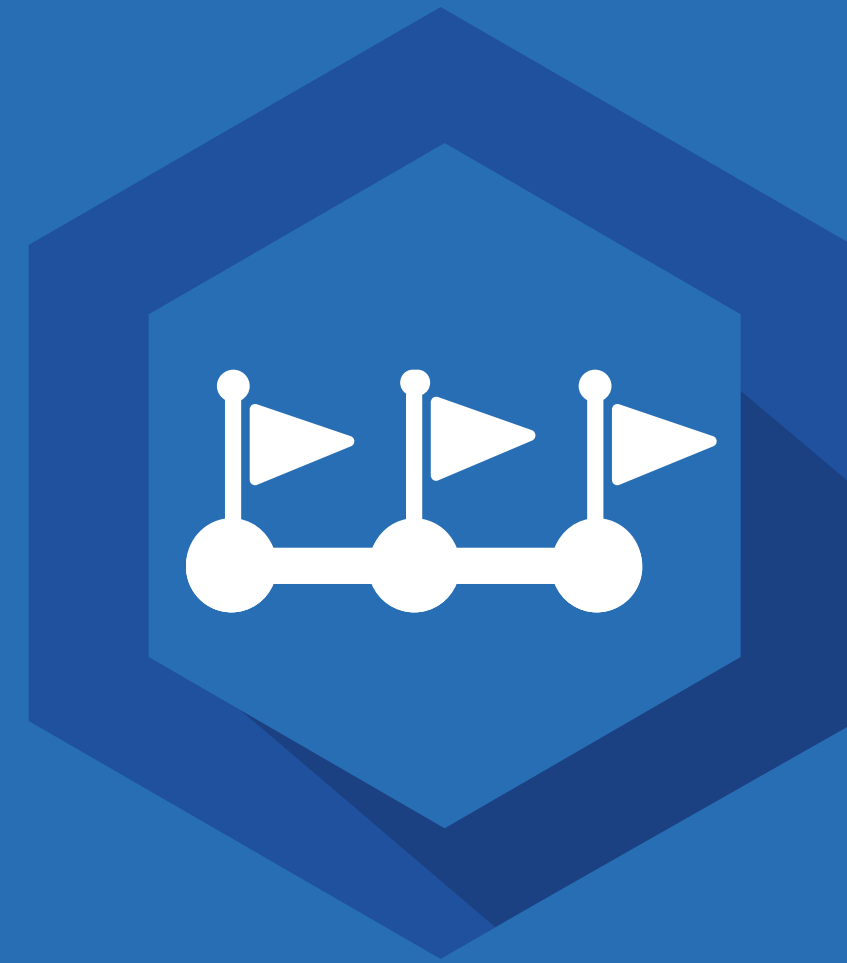
**Paraguay**



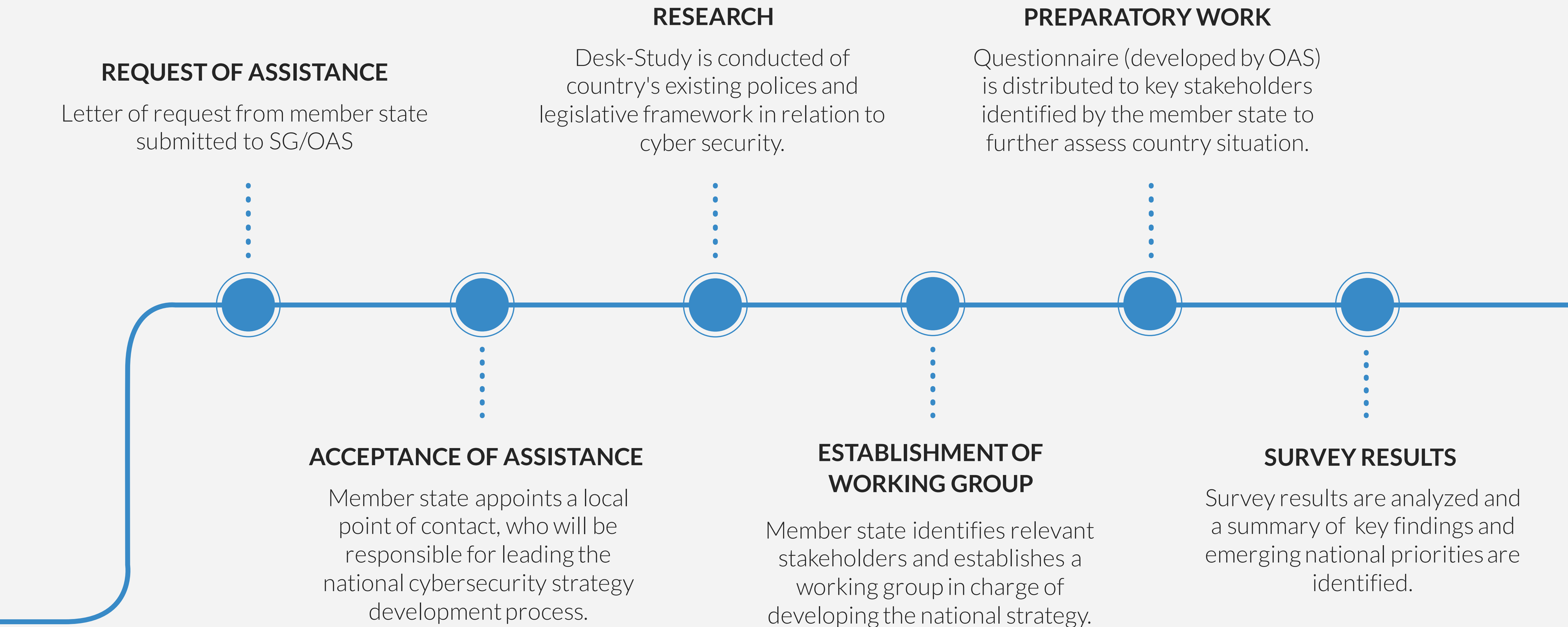
**Peru**



**Suriname**



# **National Cyber Security Strategy Development Process**



**DEVELOPMENT OF DRAFT STRATEGY**

Stakeholders are placed in working groups based on broad national priorities and consulted to identify activities, roles, responsibilities, and time frame for implementation and possible costs.

**REVIEW OF DRAFT STRATEGY**

Comments and amendments are incorporated.

**IN-COUNTRY VISIT**

In-situ visit is conducted with member state's officials and all relevant stakeholders for the national cybersecurity strategy development process.

**DRAFT STRATEGY**

The working group with the support of the OAS prepares a draft taking into account findings of the consultations and international best practice.

**ADOPTION OF STRATEGY**

Draft strategy is validated on another in-situ visit and finalized for adoption and official approval by Government.







# Technical Training, Workshops and Technical Missions



# Technical Training, Workshops and Technical Missions

- Regional and Sub regional technical training and workshops on various skillsets e.g. industrial control systems and critical infrastructure protection, cybersecurity incident handling and digital forensics.
- Variety of country-specific technical training based on needs.
- Workshops on exchange of best practices to encourage information sharing.
- Tailored in-situ missions with the participation of recognized experts to address specific country needs.

- **Webinars on cybersecurity topics**, including developing trends and new tools.
- Approximately **30** activities per year.
- Over **4,500 participants benefited** from our events since 2003. Not only government officials, but also civil society, academia, private sector, critical infrastructure operators.
- Model is based on south-south collaboration and global exchange of best practices.



**OAS**  
CYBER  
SECURITY  
LAB



**OAS**  
CYBER  
SECURITY  
LAB

# Cybersecurity Exercises





# Cybersecurity Exercises



With the support of the Department of Information and Technology Services (DOITS) of the OAS, we have built a robust virtual platform to carry both national and regional exercises.



**8** National Exercises to date and **3** Regional Exercises.



With the support of the government of Spain, the OAS organized the first International CyberEx in 2015 and 2016:

- **300+** regional and international participants
- **45** teams
- **21** participating countries
- **2** day Capture-the-Flag Exercise



There are a variety of themes and process that these exercises cover. It is important to identify the right fit for you!



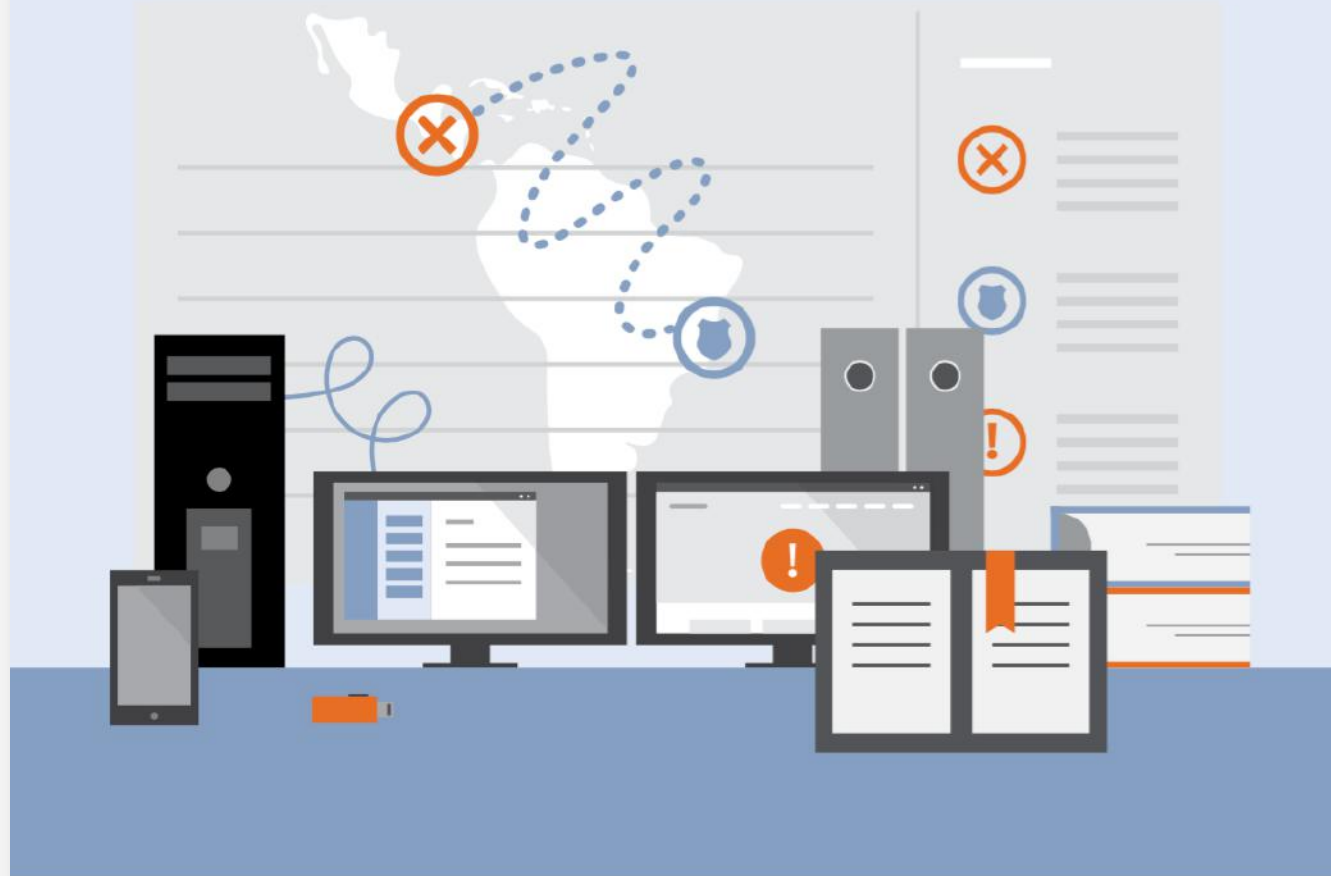
# Development of National CSIRTs

# Development of National CSIRTs

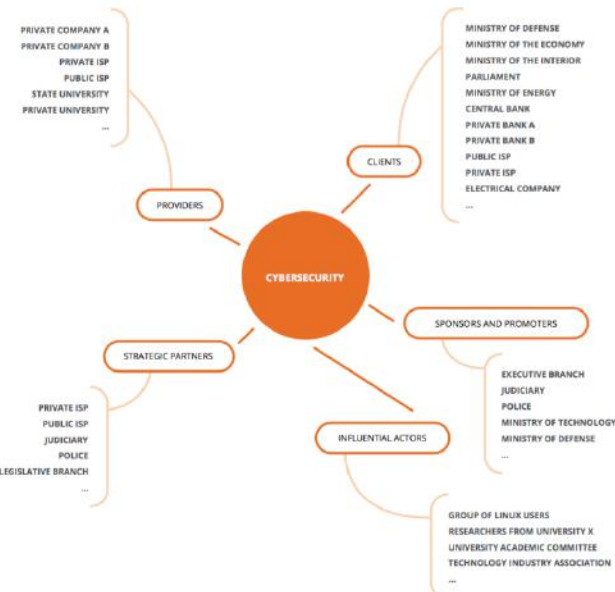
- 22 National CSIRTs in the Americas. **Only 5 in 2004.**
- Every CSIRT has a different level of maturity.
- OAS provides **technical support + equipment.**
- “**Best Practices for Establishing a National CSIRT**” - in-house designed methodology to establish and improve CSIRTs in the Americas .



# Best Practices for Establishing a National CSIRT



Organization of American States | More rights for more people

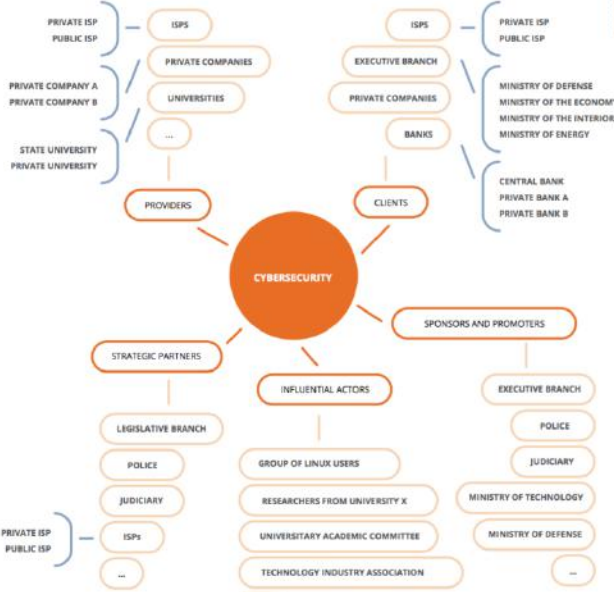


Once the groups are defined, brainstorming helps to categorize the nominated actors in each group. The diagram above shows an example of a mind map midway through the organization process.

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 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:

22 A B C D Definition



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 official designation point of contact.

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

23

## 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.

42 A B C D Scope

## 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 involves 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 system, 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.

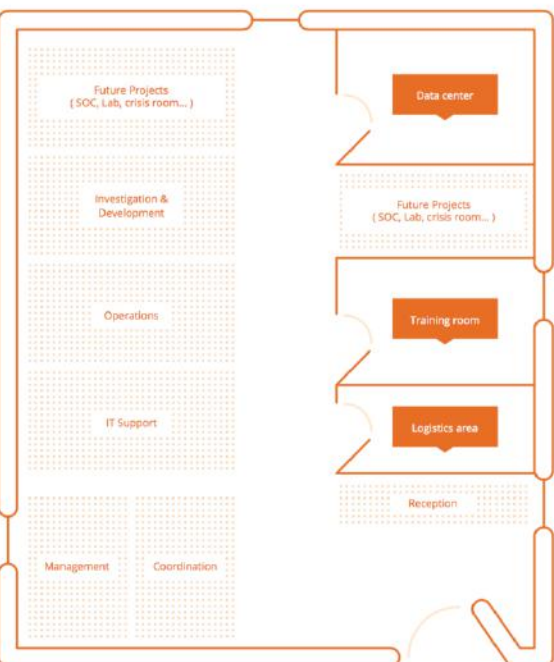
As technology evolves, threats and vulnerabilities change. The CSIRT must be able to detect emerging threats or vulnerabilities inherent to new technologies and distribute information relevant to them that can improve security levels.

#### 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.

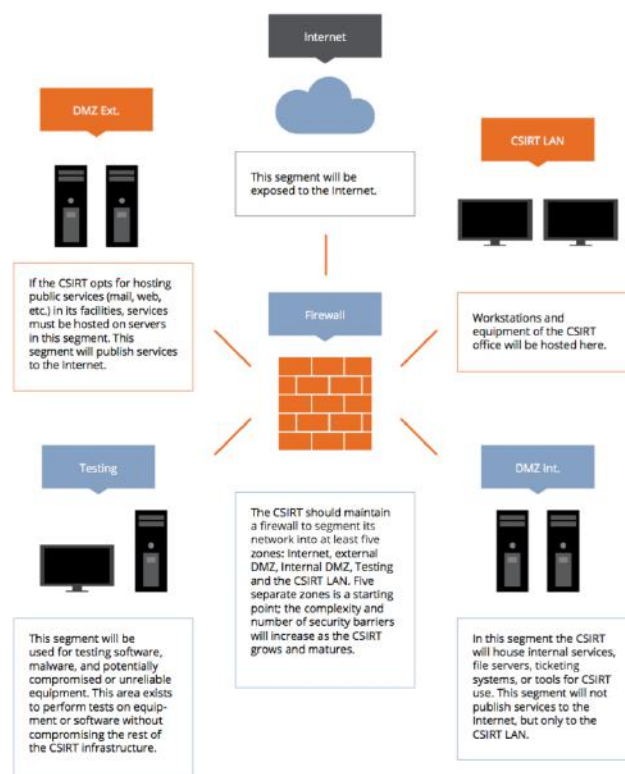
43

### Basic Floor Plan



76 A B C D IT Facilities and Infrastructure

### CSIRT Network Basic Design



77

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.

84

85



# 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.

## 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

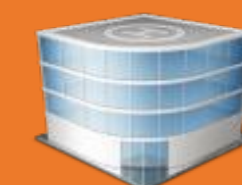
## CSIRT of the Americas / for



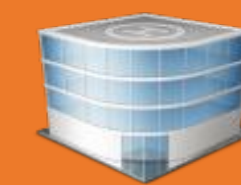
CSIRT Defense



CSIRT Police





CSIRT Gob





CSIRT National


# Unify the Community

CSIRTamericas.org

[Member states](#) 

[Services](#) 


[Partners](#) 

[About](#) 

[Logout dsuero](#)


Forum

A space for the exchanging of ideas and experiences.




Library

Regulations, procedures, presentations, scripts



Directory

Contact details of Americas CSIRTs.




Admin Announcements: Actualizacion de Seguridad en el portal 12-15-2015

Search...


Urgent Message

send email to all csirtamericas members.





Early Warnings


Alerts, real-time, regional trends.




Latest Forum Posts

**Membresia en Zone-h**  
In [Main Forum / Development of Security & Useful Tools](#)  
6 months 2 weeks ago

**Neuralgic.net**  
In [Main Forum / Development of Security & Useful Tools](#)  
6 months 3 weeks ago

**Malware Backstabbing afecta a dispositiv...**  
In [Main Forum / Incident Handling](#)  
9 months 2 weeks ago

**Campaña de distribución de Cryptowall en...**  
In [Main Forum / Incident Handling](#)  
9 months 2 weeks ago

CSIRTs Latest News

OAS\_Team

**POWERSHELL PARA LA GESTION DE INCIDENTES**  
Created on Thursday, 14 January 2016 17:27  
Estimados, Buen articulos para la gestion de Incidentes: <http://www.securityar...>  
[Read more](#)

OAS\_Team

**CRITICAL 0-DAY REMOTE COMMAND EXECUTION VULNERABILITY IN JOOMLA**  
Created on Monday, 14 December 2015 22:30  
Estimados, Vulnerabilidad critica que pudiera impactar sitios web en su...  
[Read more](#)


OAS\_Team


**IMPORTANTE DDOS-SSDP - NOV-9-2015**  
Created on Monday, 09 November 2015 14:22  
Estimados, Un CSIRT Nacional de nuestros estados miembros ha notificado que su ...  
[Read more](#)


OAS\_Team


**ALERTA DE MULTIPLES SITIOS HACKEADOS**  
Created on Thursday, 05 November 2015 21:46


Latest Files

**Alertas de Botnets en México Semanal [08 al 14 02 16]**  
In [Reports](#)  
15 February 2016 • 5 downloads





**Alertas de Botnets en México [01 al 07 Febrero 2016]**  
In [Reports](#)  
07 February 2016

**Alertas de Botnets en México [ 25 al 31 de enero 2016]**  
In [Reports](#)  
03 February 2016


**Alertas de Botnets en México [18 al 24 de enero 2016]**  
In [Reports](#)  
25 January 2016 • 1 download


**Alertas de Botnets en México [ 11 al 17 de enero 2016]**  
In [Reports](#)  
18 January 2016

Last logged

jfuentesr  dsuero 

Jaime Fuentes

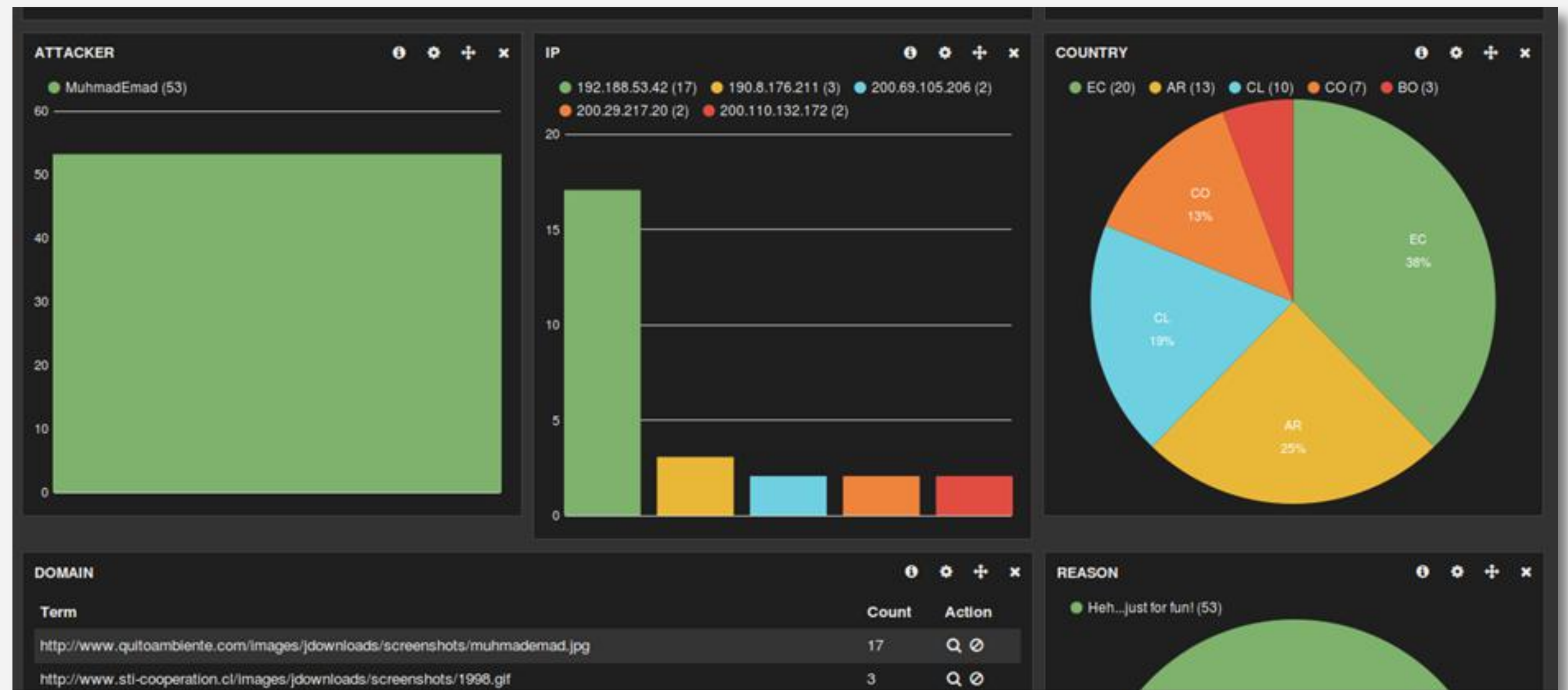
**Me**  
jaimel! You will receive an email report with the suspicious activities

**Jaime Fuentes**  
Many Thanks I really i appreciate it



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

# Early Regional Warning

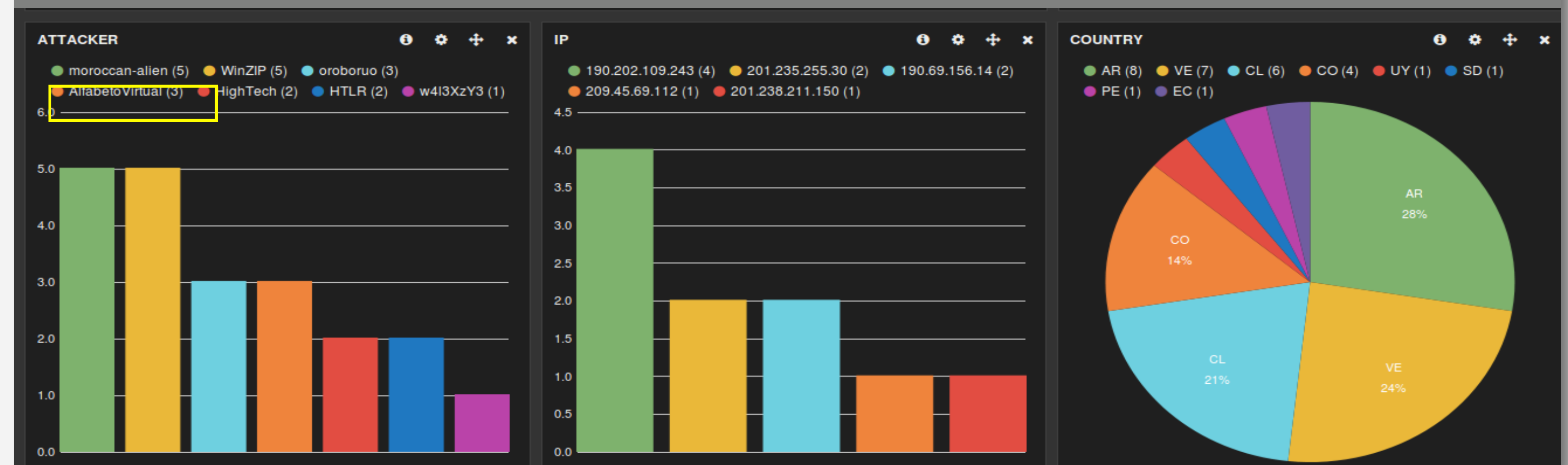


North



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

South



Early  
Regional  
Warning





**Awareness Raising,  
Research and Expertise**

# Awareness Raising, Research and Expertise



Raising cybersecurity awareness through multi-stakeholder outreach.



Producing research and data focused on cybersecurity in Latin America and the Caribbean region.



Developing expertise in the area of cybersecurity from the Latin America and the Caribbean region.

# Cybersecurity

Awareness Campaign **Toolkit**



# Cyber Security

## Education & Awareness Strategy





# Our Recommendations

- Promote the establishment of cybersecurity working groups (financial sector) in each of your countries
- Organize cybersecurity crisis management exercises at the national and regional level
- Encourage the establishment of financial sector incident response teams
- Implement cybersecurity awareness campaign for employees and customers
- Reach out to government representatives and support the development of National Cybersecurity Policies and Strategies
- SHARE! Information, threats, attacks, lessons learnt, etc.

# Our Proposal

- Conduct a study on cyber security and the financial sector in Latin America and the Caribbean. (Your commitment is essential!)
- Organize a 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

**The Financial Sector is a part of the Critical Infrastructure of the Americas and we are here to work with you!**

“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.”





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

## **Belisario Contreras**

---

Cybersecurity Program Manager  
**Organization of American States**

BContreras@oas.org

 @belisarioc