OAS More rights for more people

National Cybersecurity: A Latin American and Caribbean's View

Cybersecurity Program
Organization of American States

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.

Barbara Marchiori de Assis

Organization of American States

BMarchiori@oas.org
www.oas.org/cyber
@bamassis
@OEA_Cyber

Program Objective

Strengthen the capacity of Member States to detect cyber threats, as well as to prevent, respond to and recover from cyber incidents through the comprehensive program “Strengthening Cyber Security Capabilities in the Americas” that works in 3 core areas:

- Policy Development
- Capacity Building
- Research and Outreach

National Strategies Approved

Colombia
(2011 & 2016)

Panama
2013

Trinidad and Tobago
2013

Jamaica
2015

Costa Rica
2017

Paraguay
2017

Chile
2017

Mexico
2017

Guatemala
2018

Dominican Republic
2018

National Strategies – In Progress

Argentina

Peru

CRITICAL INFRASTRUCTURE PROTECTION IN LATIN AMERICA AND THE CARIBBEAN 2018

OAS More rights for more people

Microsoft

WHICH INDUSTRY DO YOU BELONG TO?

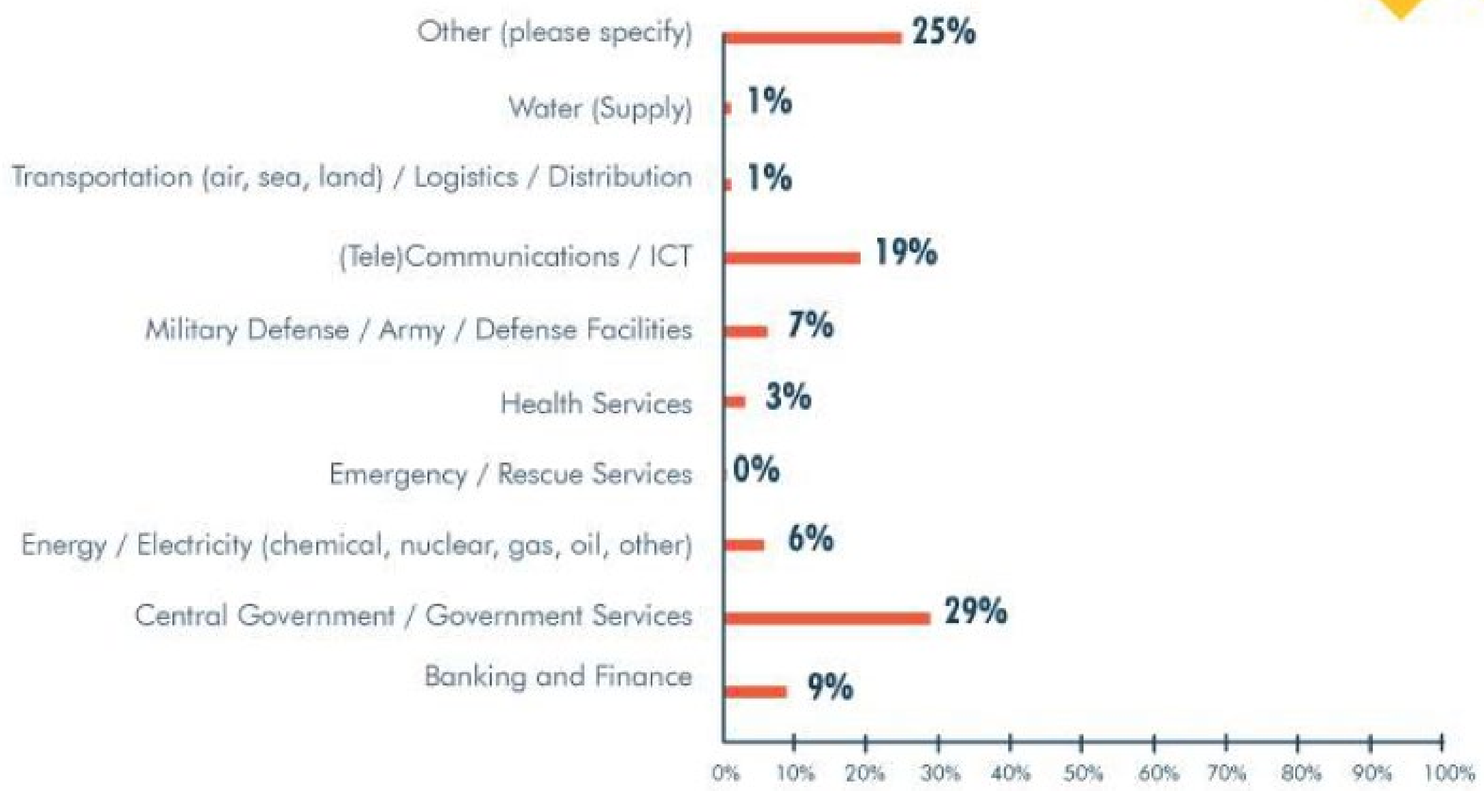


Figure 1 Total respondents, n= 497

HOW WOULD YOU DESCRIBE YOUR ORGANIZATION'S ABILITY TO DETECT A CYBER INCIDENT AND/OR CYBER ATTACK?

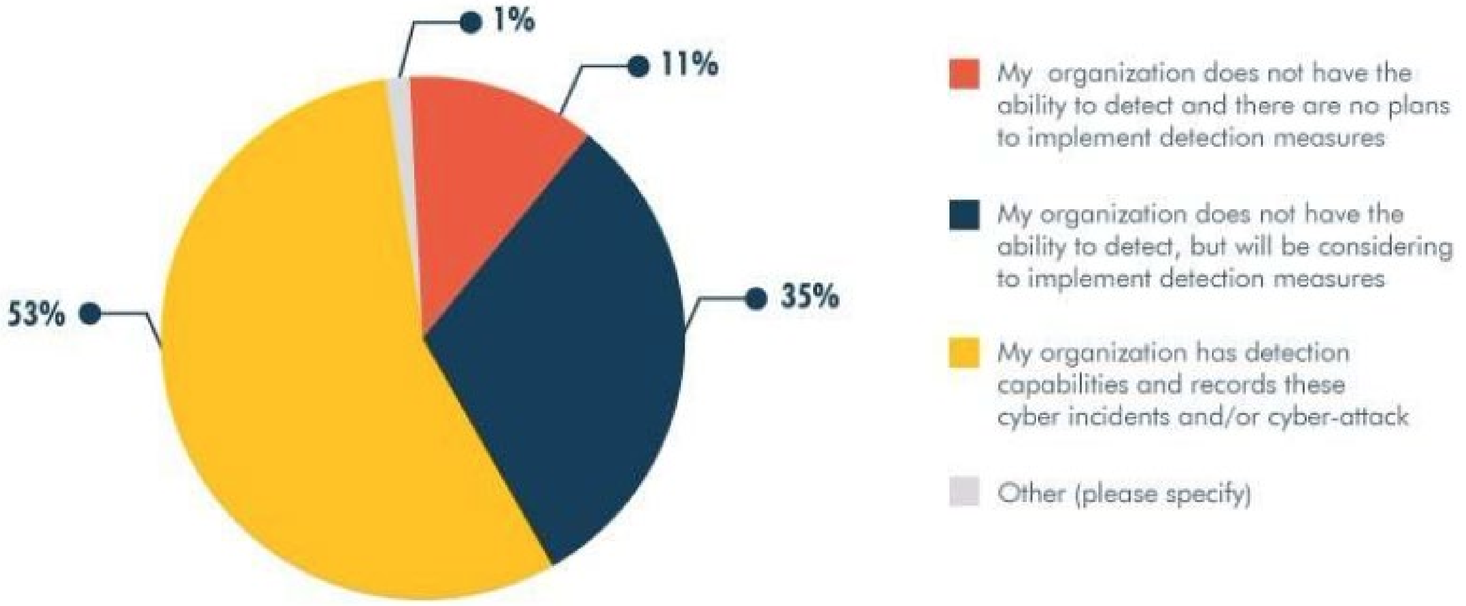


Figure 2 Total respondents, n= 455

HAS YOUR ORGANIZATION DETECTED ATTACKS AND/OR INCIDENTS ON OR AGAINST YOUR ORGANIZATION'S COMPUTER SYSTEMS AND/OR NETWORK EXPERIENCED IN THE LAST 12 MONTHS?

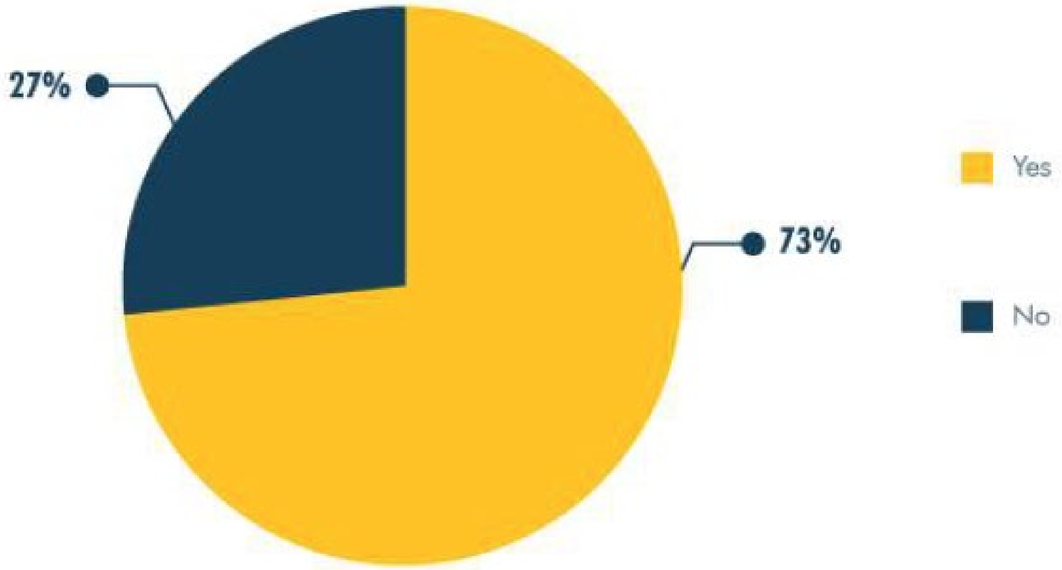


Figure 3 Total respondents, n= 453

HAVE YOU NOTICED AN INCREASE, DECREASE, OR NO CHANGE IN THE NUMBER OF ATTACKS TO YOUR ORGANIZATION'S COMPUTER SYSTEMS AND/OR NETWORK IN THE LAST 12 MONTHS?

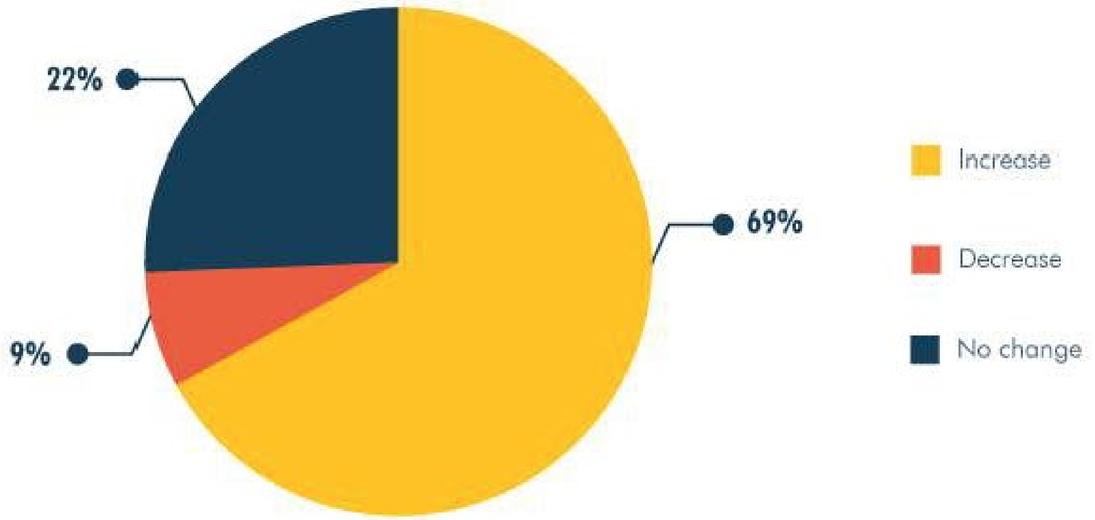


Figure 4 Total respondents, n= 330

ARE THE ATTACKS AGAINST YOU GETTING MORE SOPHISTICATED?

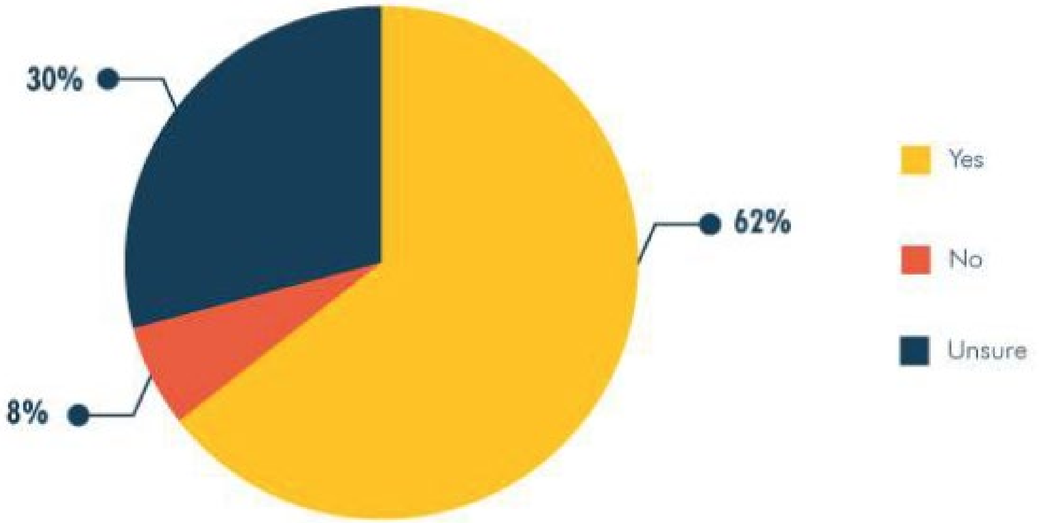
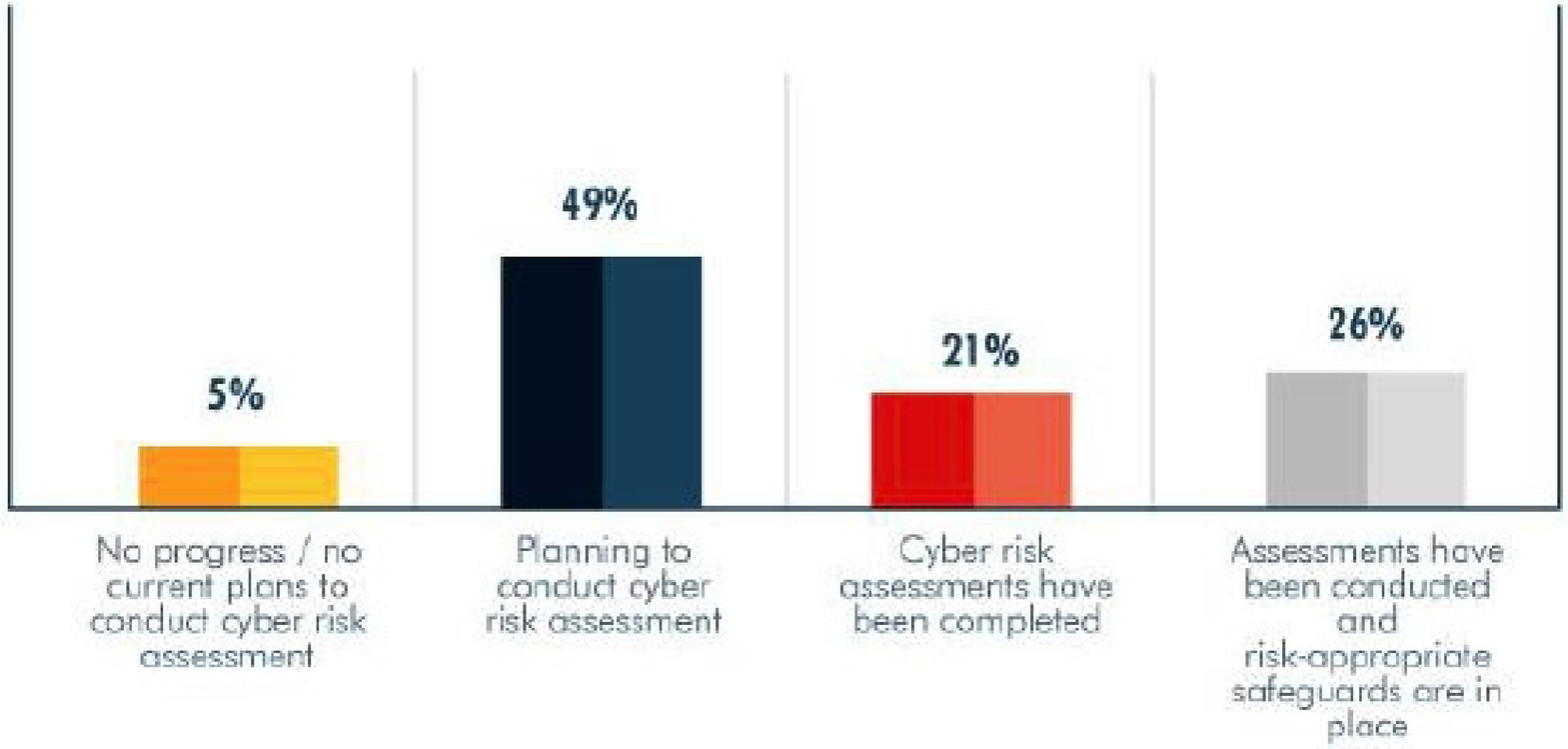
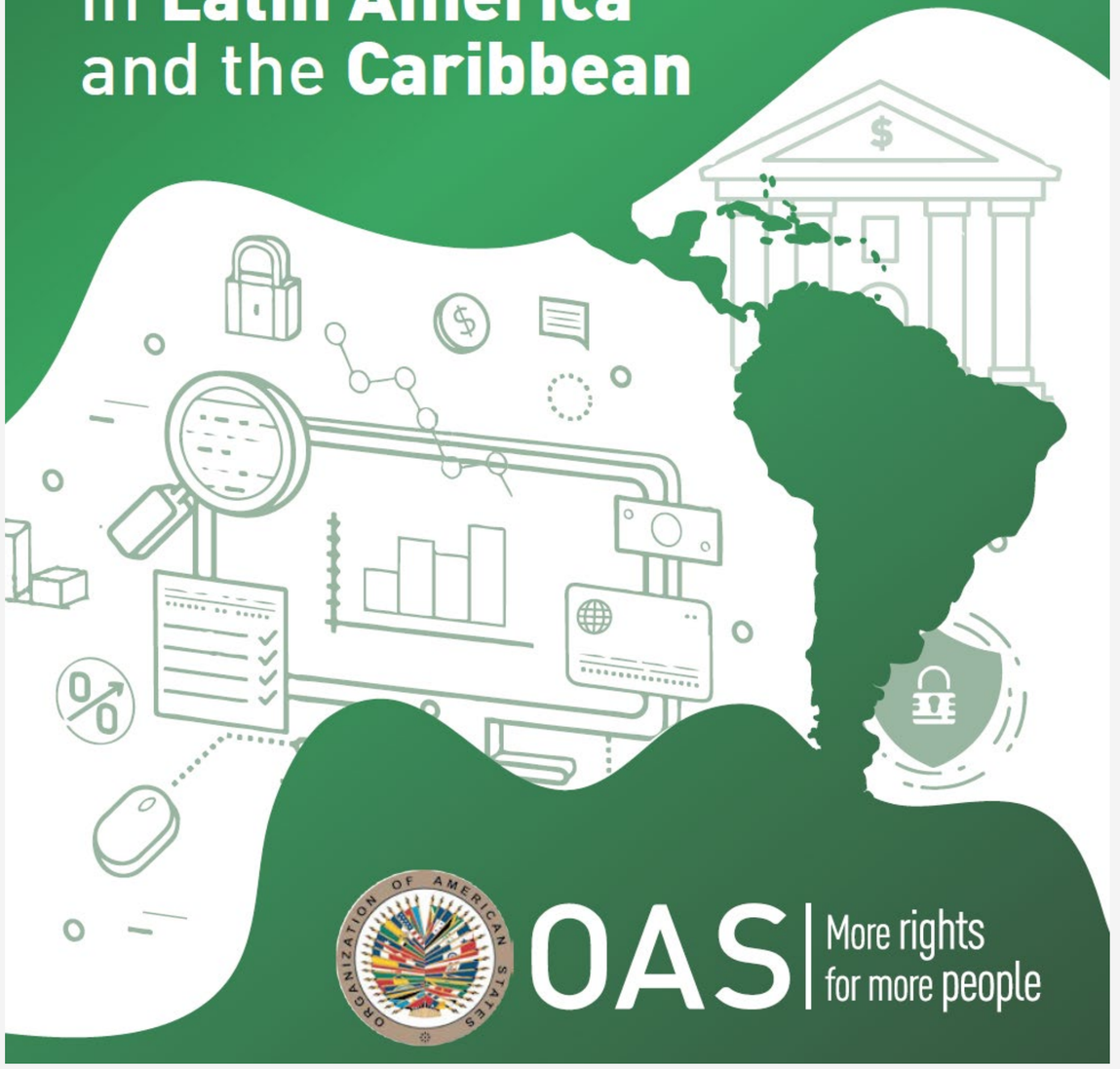


Figure 7 Total respondents, n= 320

IN RELATION TO CYBERSECURITY RISK MANAGEMENT, HOW WOULD YOU DESCRIBE YOUR COMPANY'S EFFORTS?

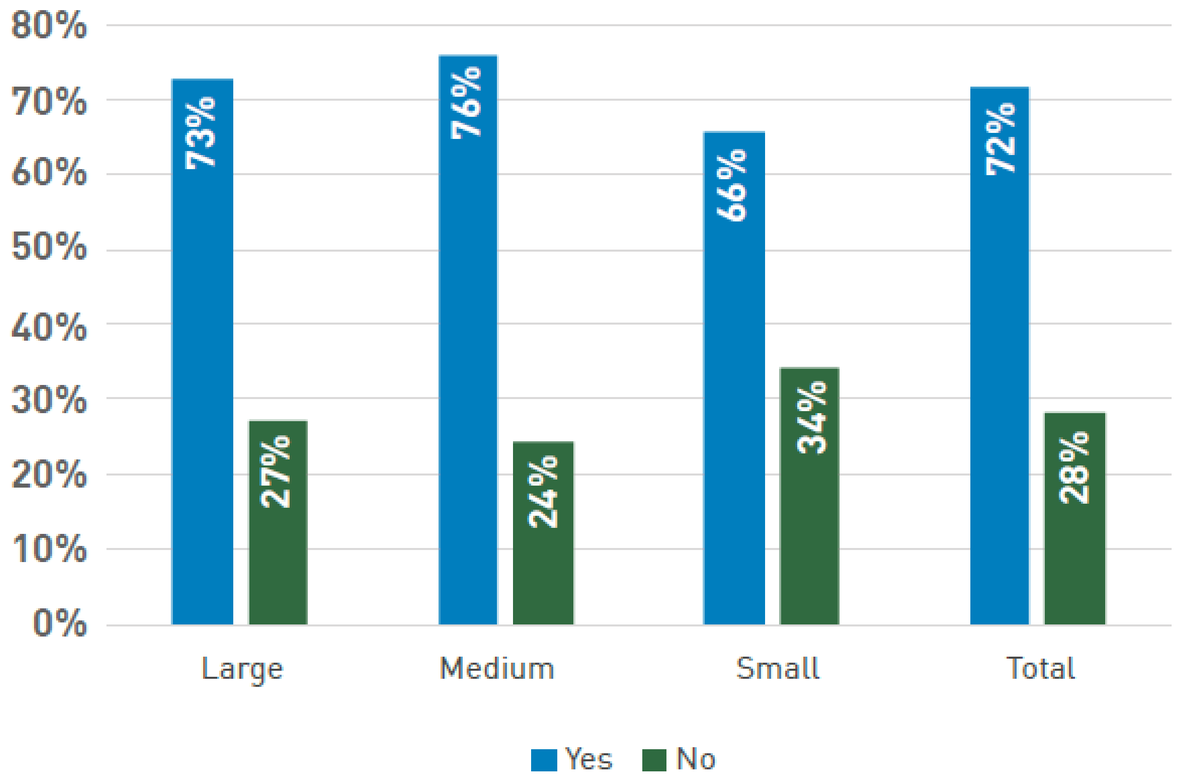


State of Cybersecurity in the Banking Sector in Latin America and the Caribbean

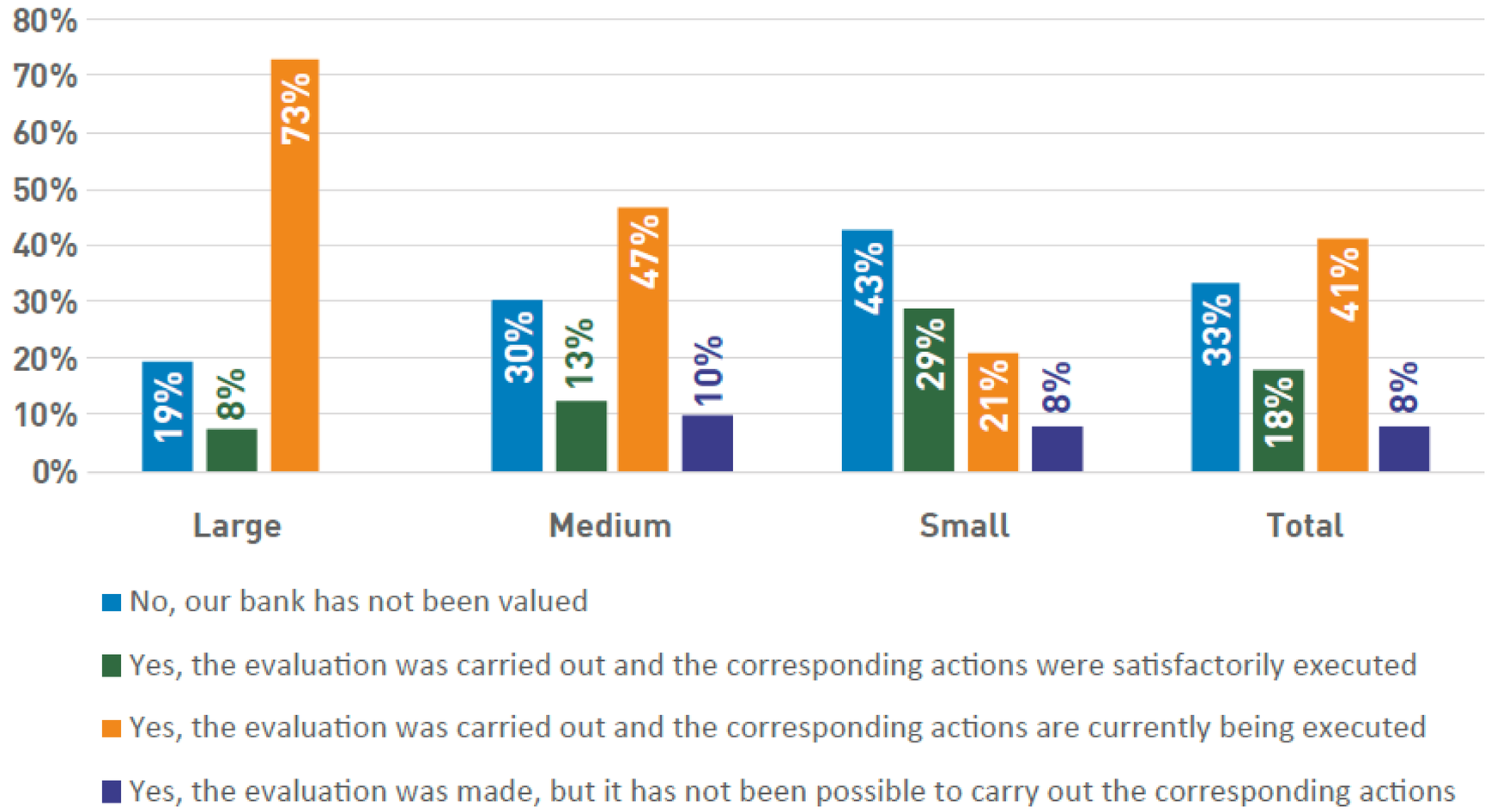


OAS | More rights for more people

Graph 9. Does the board of directors of the banking entity receive periodic reports on indicators and digital security risk management?

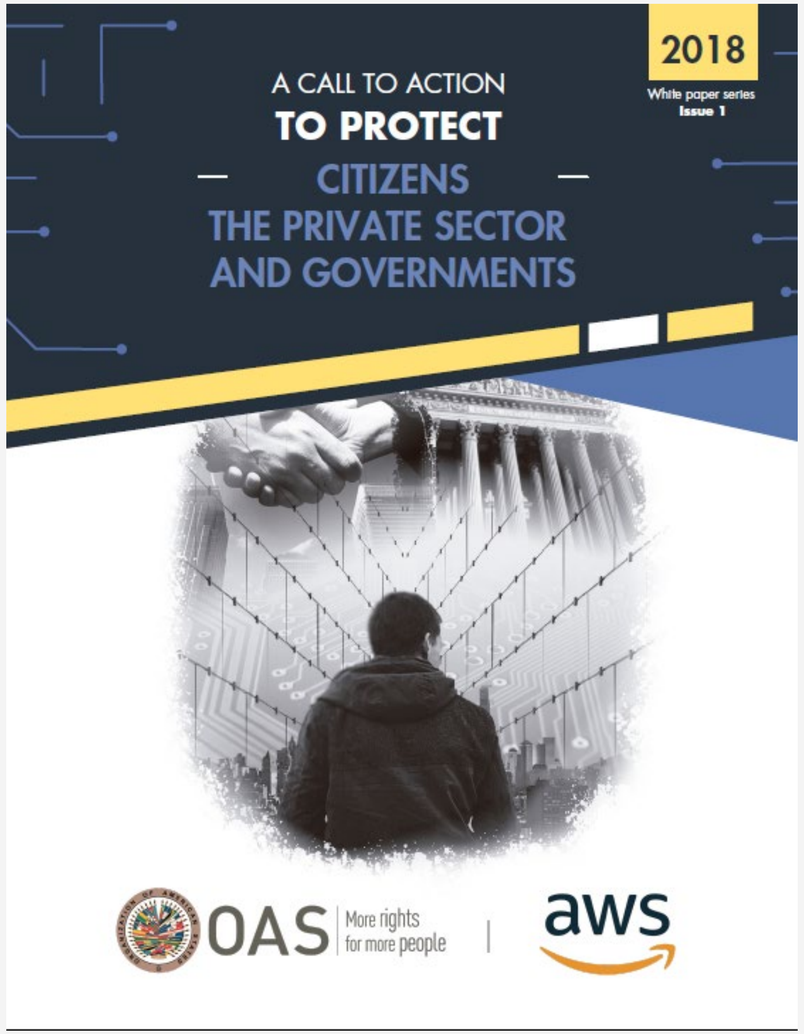


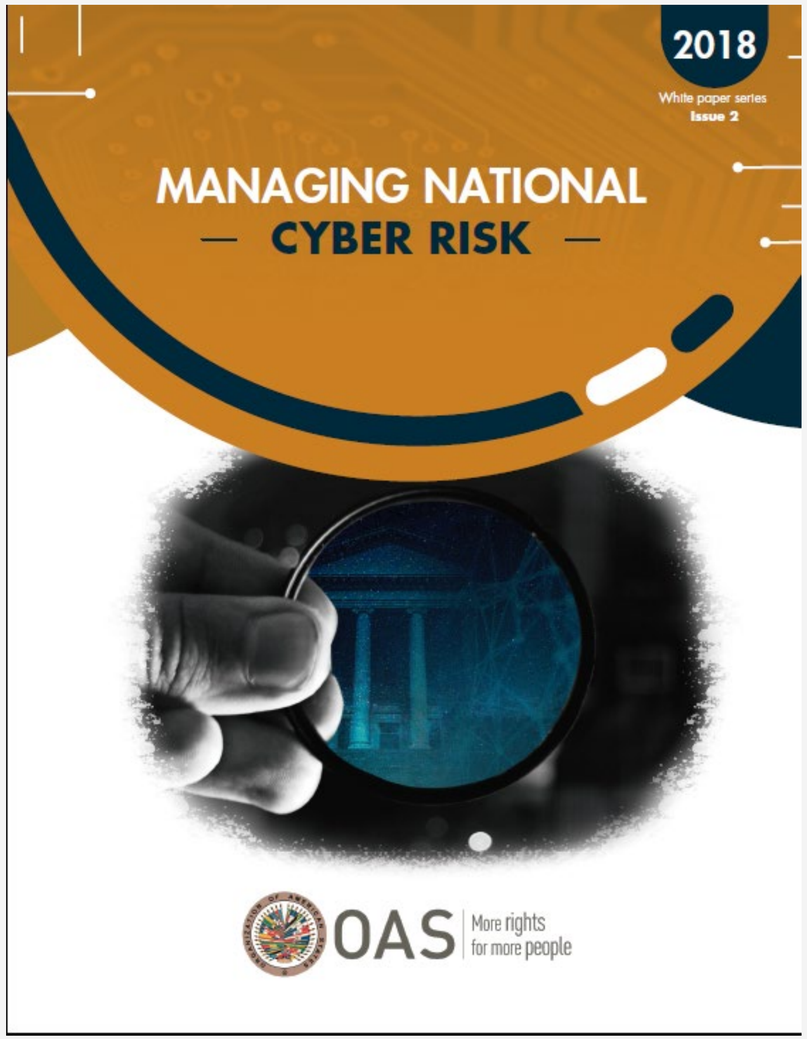
Graph 19. **Has the bank been externally rated in the last two (2) years under any digital security maturity assessment methodology and has it completed that evaluation?**



Note: 168 records

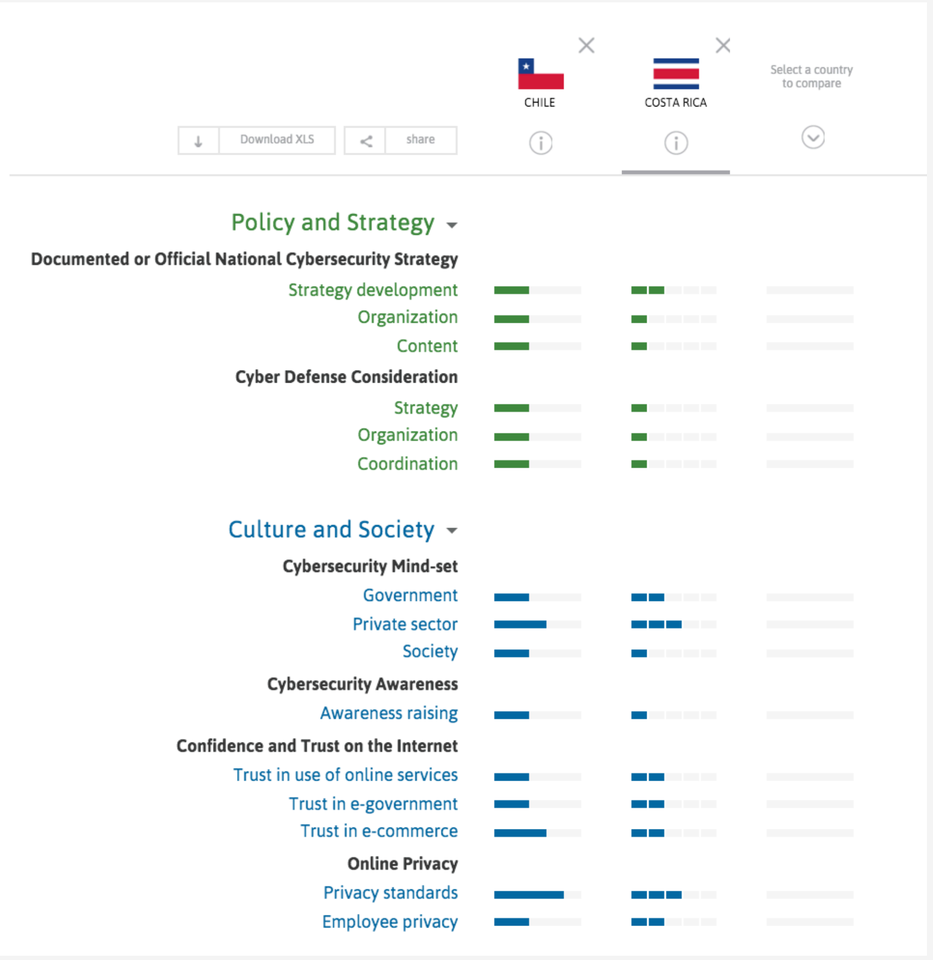
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean


2018
White paper series
Issue 1
A CALL TO ACTION
TO PROTECT
CITIZENS
THE PRIVATE SECTOR
AND GOVERNMENTS
OAS
More rights
for more people
aws

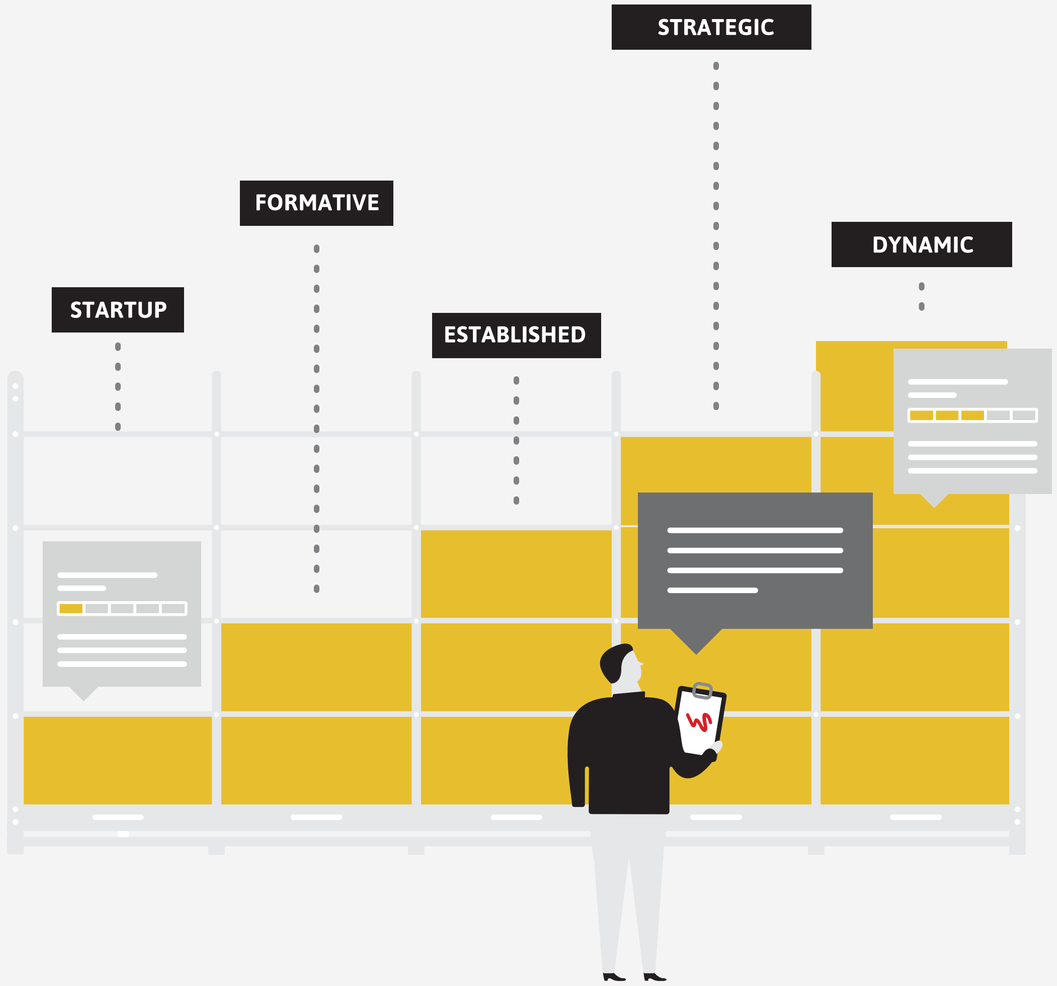

2018
White paper series
Issue 2
MANAGING NATIONAL
CYBER RISK
OAS
More rights
for more people

Observatory

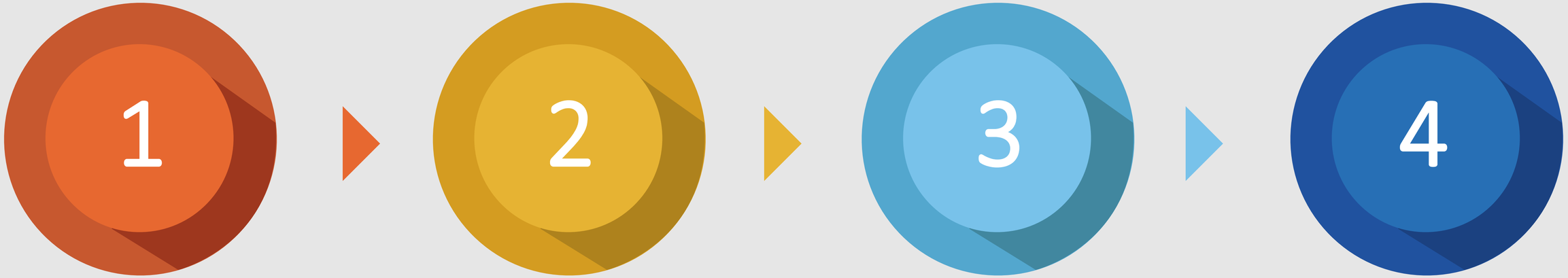
www.cybersecurityobservatory.com



CMM - 5 Levels of Maturity



Implementation



Every good plan must have **ownership** or else fingers will always be pointing when something goes wrong or nothing happens.

Identify a responsible entity for each activity and allocate a **budget**.

Develop a **monitoring mechanism**: This could be done by a public body or an interagency/inter-ministerial working group defined as the coordinator of the strategy. This will be the entity that has the overall responsibility for the strategy lifecycle and the strategy documentation itself.

Define the structure of the **coordinating entity**, its exact responsibilities and its **relationships with the other stakeholders** (ENISA, 2012).

Thank you!
Merci
Gracias
Obrigado

Barbara Marchiori de Assis

Organization of American States

BMarchiori@oas.org
www.oas.org/cyber
@bamassis
@OEA_Cyber