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
Figure 1: Which industry do you belong to?

- Central Government / Government Services: 29%
- Energy / Electricity (chemical, nuclear, gas, oil, other): 6%
- (Tele)Communications / ICT: 19%
- Military Defense / Army / Defense Facilities: 7%
- Health Services: 3%
- Emergency / Rescue Services: 0%
- Energy / Electricity (chemical, nuclear, gas, oil, other): 6%
- Central Government / Government Services: 29%
- Banking and Finance: 9%
- Transportation (air, sea, land) / Logistics / Distribution: 1%
- Water (Supply): 1%
- Other (please specify): 25%

Total respondents, n = 497
HOW WOULD YOU DESCRIBE YOUR ORGANIZATION’S ABILITY TO DETECT A CYBER INCIDENT AND/OR CYBER ATTACK?

- 53%: My organization has detection capabilities and records these cyber incidents and/or cyber-attack.
- 35%: My organization does not have the ability to detect, but will be considering to implement detection measures.
- 11%: My organization does not have the ability to detect and there are no plans to implement detection measures.
- 1%: Other (please specify)

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?

- Increase: 69%
- Decrease: 9%
- No change: 22%

Figure 4  Total respondents, n = 330
ARE THE ATTACKS AGAINST YOU GETTING MORE SOPHISTICATED?

- Yes: 62%
- No: 30%
- Unsure: 8%

Total respondents, n = 320

Figure 7
IN RELATION TO CYBERSECURITY RISK MANAGEMENT, HOW WOULD YOU DESCRIBE YOUR COMPANY’S EFFORTS?

- No progress / no current plans to conduct cyber risk assessment: 5%
- Planning to conduct cyber risk assessment: 49%
- Cyber risk assessments have been completed: 21%
- Assessments have been conducted and risk-appropriate safeguards are in place: 26%
Graph 9. Does the board of directors of the banking entity receive periodic reports on indicators and digital security risk management?

<table>
<thead>
<tr>
<th>Category</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large</td>
<td>73%</td>
<td>27%</td>
</tr>
<tr>
<td>Medium</td>
<td>76%</td>
<td>24%</td>
</tr>
<tr>
<td>Small</td>
<td>66%</td>
<td>34%</td>
</tr>
<tr>
<td>Total</td>
<td>72%</td>
<td>28%</td>
</tr>
</tbody>
</table>
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?

- No, our bank has not been valued
- Yes, the evaluation was carried out and the corresponding actions were satisfactorily executed
- Yes, the evaluation was carried out and the corresponding actions are currently being executed
- Yes, the evaluation was made, but it has not been possible to carry out the corresponding actions

Note: 168 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean
This site shows the levels of maturity on Cybersecurity in Latin America and The Caribbean. Please select the countries you want to compare and scroll down to see the results.

Promote economic growth and social progress. In light of its increased adoption of ICT, Brazil has become a prime target of cyberattacks and...
CMM - 5 Levels of Maturity
Define the structure of the coordinating entity, its exact responsibilities and its relationships with the other stakeholders (ENISA, 2012).

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