Management of a cyber resilience and wholesale payment security agenda

Ángel González Tejada
Director of Payment Systems Department

Regional Payments Week 2019
Willemstad, Curacao, 20 November 2019
Why cybersecurity?

**CYBERCRIME WILL BE MORE PROFITABLE THAN ILLEGAL DRUGS**
By 2021, it is estimated that cybercrime will take $6 quintillion from the global pocket. It is currently costing almost $4 trillion in damages, however, the number is steadily increasing as criminals become more wiser.

**54% OF COMPANY VIOLATIONS ARE DUE TO EMPLOYEES**
Employees without knowing it, allow hacking to occur by opening an phishing email or following an insecure link. The second aspect is when the employee performs the attack by himself.

THE ORGANIZATION NEEDS AN AVERAGE OF 191 DAYS TO DETECT AN ATTACK
AN ATTACK OCCURS EVERY 39 SECONDS IN THE USA
Dominican Republic in an International Context

National Cybersecurity Strategy in Latin America

Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) of the OAS

Panama  Chile  Guatemala  Mexico

Colombia  Costa Rica  Jamaica  Dominican Republic

http://www.oas.org/juridico/spanish/cybersp.htm
Convention on Cybercrime (Budapest Convention)

- Standardization of criminal regulations for cybercrime;
- Strengthening procedural powers in the prerogatives of persecution;
- Establishment an international cooperation regime.
National context

MONETARY AND FINANCIAL LAW (2002)
It focuses on cybersecurity as part of operational risk.

HIGH TECHNOLOGY CRIMES AND CRIMES LAW (2007)
It focuses on the criminal prosecution of cybercrime.

PERSONAL DATA PROTECTION LAW (2013)
Vision focused on users and the protection of their information.
National Policy Development

National Development Strategy 2030

- Digital Republic (2016-2020)
- National Cyber Security Policy
- Electronic Government Agenda

Pillars

- Education and creation of a cybersecurity culture
- Legal framework
- Critical Infrastructure Protection
- Public-private partnerships

- INDOTEL
- OAS

Enactment (2018)
- Common cybersecurity framework for institutions
- Protection of national critical infrastructures

Critical Financial Infrastructures
- National Payment System
- Need for risk management at EIF

Cooperative Framework
- It contemplates the creation of national CSIRT and sector CSIRT
Regulation of Cyber Security and Information for the Financial System

- Prepared by the Central Bank.
- Approved by the Monetary Board in November 2018.
- Main mechanism to promote capacity development in the financial system of cyber risk mitigation and its impact on the technological infrastructures of its entities.
- Entry into force in November 2019.
Purpose and scope of the Regulation

Purpose

• Establish the general principles and guidelines for regulators to ensure integrity, availability and confidentiality of the information and the optimal functioning of their Information Systems and the Technological Infrastructure.
Highlights

**CYBER SECURITY PROGRAM**
- Information security governance
- Risk assessment to internal suppliers

**SECTORAL COORDINATION**
- Creation of the Cyber Security Sector Council
- Creation of the Cyber Security Incident Response Team for the Financial Sector

**CONSEQUENCES REGIME**
- Penalty regime for EIFs
- Precautionary measures based on the interconnection with SIPARD
Cyber Security and Information Program

Technology Risk Management
- Self-assessment of technological risks taking into account risk appetite
- Evaluation of technological risks of interconnected entities

Development of a control framework
- Elaboration an internal cyber security and information policy
- Controls for the active management of information, networks, information systems and technological infrastructures

Program monitoring and evaluation
- Internal audits process
- Cyber security and information monitoring

International standards
- Applicable to the regulated that access products and services of international suppliers
- Applicable to outsourced providers of bank card production and identification token services

Compliance reports
- Financial Intermediation Entities (Superintendency of Banks)
- Administrators and Participants SIPARD, Support Entities and Related Services (Central Bank)
Sector Council for the Response to Cyber Security Incidents of the Financial Sector

From the Monetary and Financial Administration

- Governor of the Central Bank, who chairs the Council
- Superintendent of Banks
- Comptroller of the Central Bank
- Assistant Manager of Systems and Technological Innovation of the Central Bank

Private Financial Sector Guilds

- President of the Association of Commercial Banks of the Dominican Republic (ABA)
- President of the Security Committee of the League of Savings and Loans Associations Dominican (LIDAAPI)
- President of the Technology Committee of the Association of Savings and Credit Banks and Credit Corporations

Cyber Security Incident Response Team (CSIRT)

- Under the administrative dependency of the BCRD and functional of the Sectorial Council
- Defines immediate actions for prevention, detection, containment, eradication and recovery against Cyber Security Incidents that affect the regulated
Global Cybersecurity Index 2018
## Country engagement level

<table>
<thead>
<tr>
<th>Year</th>
<th>Score</th>
<th>Regional Rank</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>0.430</td>
<td>10</td>
<td>92</td>
</tr>
<tr>
<td>2017</td>
<td>0.162</td>
<td>22</td>
<td>121</td>
</tr>
</tbody>
</table>

### Member States are classified according to their level of commitment: high, medium, and low.

1. **High**
   - Countries that demonstrate high commitment in all five pillars of the index.

2. **Medium**
   - Countries that have developed complex commitments and engage in cybersecurity programmes and initiatives.

3. **Low**
   - Countries that have started to initiate commitments in cybersecurity.
## Regional Ranking of the Global Cybersecurity Index 2018

<table>
<thead>
<tr>
<th>Member State</th>
<th>Score</th>
<th>Regional Rank</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States of America*</td>
<td>0.926</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Canada*</td>
<td>0.892</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Uruguay</td>
<td>0.681</td>
<td>3</td>
<td>51</td>
</tr>
<tr>
<td>Mexico</td>
<td>0.629</td>
<td>4</td>
<td>63</td>
</tr>
<tr>
<td>Paraguay</td>
<td>0.603</td>
<td>5</td>
<td>66</td>
</tr>
<tr>
<td>Brazil</td>
<td>0.577</td>
<td>6</td>
<td>70</td>
</tr>
<tr>
<td>Colombia</td>
<td>0.565</td>
<td>7</td>
<td>73</td>
</tr>
<tr>
<td>Cuba</td>
<td>0.481</td>
<td>8</td>
<td>81</td>
</tr>
<tr>
<td>Chile</td>
<td>0.470</td>
<td>9</td>
<td>83</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>0.430</td>
<td>10</td>
<td>92</td>
</tr>
<tr>
<td>Jamaica</td>
<td>0.407</td>
<td>11</td>
<td>94</td>
</tr>
<tr>
<td>Argentina</td>
<td>0.407</td>
<td>11</td>
<td>94</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Member State</th>
<th>Score</th>
<th>Regional Rank</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paraguay</td>
<td>0.603</td>
<td>5</td>
<td>66</td>
</tr>
<tr>
<td>Brazil</td>
<td>0.577</td>
<td>6</td>
<td>70</td>
</tr>
<tr>
<td>Colombia</td>
<td>0.565</td>
<td>7</td>
<td>73</td>
</tr>
<tr>
<td>Cuba</td>
<td>0.481</td>
<td>8</td>
<td>81</td>
</tr>
<tr>
<td>Chile</td>
<td>0.470</td>
<td>9</td>
<td>83</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>0.430</td>
<td>10</td>
<td>92</td>
</tr>
<tr>
<td>Jamaica</td>
<td>0.407</td>
<td>11</td>
<td>94</td>
</tr>
<tr>
<td>Argentina</td>
<td>0.407</td>
<td>11</td>
<td>94</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Member State</th>
<th>Score</th>
<th>Regional Rank</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Punta</td>
<td>0.401</td>
<td>12</td>
<td>95</td>
</tr>
<tr>
<td>Panama</td>
<td>0.369</td>
<td>13</td>
<td>97</td>
</tr>
<tr>
<td>Ecuador</td>
<td>0.367</td>
<td>14</td>
<td>98</td>
</tr>
<tr>
<td>Venezuela</td>
<td>0.354</td>
<td>15</td>
<td>99</td>
</tr>
<tr>
<td>Guatemala</td>
<td>0.251</td>
<td>16</td>
<td>112</td>
</tr>
<tr>
<td>Antigua and Barbuda</td>
<td>0.247</td>
<td>17</td>
<td>113</td>
</tr>
<tr>
<td>Costa Rica*</td>
<td>0.231</td>
<td>18</td>
<td>115</td>
</tr>
<tr>
<td>Trinidad and Tobago</td>
<td>0.188</td>
<td>19</td>
<td>123</td>
</tr>
<tr>
<td>Barbados</td>
<td>0.173</td>
<td>20</td>
<td>127</td>
</tr>
<tr>
<td>Saint Vincent and the Grenadines</td>
<td>0.159</td>
<td>21</td>
<td>129</td>
</tr>
<tr>
<td>Bahamas</td>
<td>0.147</td>
<td>22</td>
<td>133</td>
</tr>
<tr>
<td>Grenada</td>
<td>0.143</td>
<td>23</td>
<td>134</td>
</tr>
</tbody>
</table>

### Year 2018

<table>
<thead>
<tr>
<th>Year</th>
<th>Score</th>
<th>Regional Rank</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>0.430</td>
<td>10</td>
<td>92</td>
</tr>
</tbody>
</table>

### Year 2017

<table>
<thead>
<tr>
<th>Year</th>
<th>Score</th>
<th>Regional Rank</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>0.162</td>
<td>22</td>
<td>121</td>
</tr>
</tbody>
</table>
Greater understanding of cyber risk

Regulated entities are expected to pay more attention to such threats.

Increasing efficiency in supervisory efforts

The regulation will allow greater monitoring and control of the regulated entities of the Financial System.

Commissioning of the CSIRT

It is planned that the Sector Information Security Incident Response Team operates with contributions from regulated financial intermediation entities.

Risk mitigation in regulated entities

This regulation will allow the establishment a framework for prevention and detection of threats of this nature.

Future Perspectives
THANK YOU