Cybersecurity for Critical Sectors
(including financial and therefore e-commerce)

Marco Obiso
Head ITU Applications and Cyber Security Division, ITU
Growing Cyber Security Threats

- ICTs have become an integral part of information society.
- ICT networks are regarded as basic national infrastructure.
- ICTs are also exposing our societies to the threat of cyber attacks.
- Vulnerability of national infrastructures increases as the use of ICTs take root.
- Cyber attacks on ICTs are borderless and can be launched from virtually anywhere.
- As global reliance on ICTs grows, so does vulnerability to attacks on critical infrastructures through cyberspace.
Our data are valuable

Source: experian
Snapshot of the situation on eCommerce

The Global Fraud Index analyses and reports on the changing state of fraud by examining transactions of more than 5000 eCommerce merchants across North America, Asia, Europe.

**$57.8 BILLION**
Amount lost by eight identified industry segments

**+171.9%**
COSMETICS AND PERFUMES
Increase in eCommerce fraud from Q2 2016 to Q2 2017

**+11.9%**
CONSUMER ELECTRONICS
Increase in eCommerce fraud from Q2 2016 to Q2 2017

**+36.7%**
JEWELRY AND PRECIOUS METALS
Increase in eCommerce fraud from Q2 2016 to Q2 2017

**FRAUD IN Q2 2017**
+5.5%
Percentage increase in total eCommerce fraud from Q2 2016 to Q2 2017

Friendly fraud
Account takeover
Stolen financials

Source: PYMNTS.com and Signifyd
Main considerations

- Malware as gate to company’s data
- Corporate secrets get revealed
- Accounts associated to the business more vulnerable
- Insider Trading Cyber Attacks

...and generally (at the national level)

- Weak regulations
- Lack of awareness and human capacity building
- Lack of vertical capabilities (related to the specific sector)

..finally (and overall)

- Need to address critical infrastructure protection holistically and as comprehensively
In general, we can identify 10 Critical National Infrastructure sectors.
## ITU Global Cybersecurity Index (GCI)

The GCI measures the level of commitment on cybersecurity (193 countries)

<table>
<thead>
<tr>
<th>Country</th>
<th>GCI Score</th>
<th>Legal</th>
<th>Technical</th>
<th>Organizational</th>
<th>Capacity Building</th>
<th>Cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singapore</td>
<td>0.92</td>
<td>0.95</td>
<td>0.96</td>
<td>0.88</td>
<td>0.97</td>
<td>0.87</td>
</tr>
<tr>
<td>United States</td>
<td>0.91</td>
<td>1</td>
<td>0.96</td>
<td>0.92</td>
<td>1</td>
<td>0.73</td>
</tr>
<tr>
<td>Malaysia</td>
<td>0.89</td>
<td>0.87</td>
<td>0.96</td>
<td>0.77</td>
<td>1</td>
<td>0.87</td>
</tr>
<tr>
<td>Oman</td>
<td>0.87</td>
<td>0.98</td>
<td>0.82</td>
<td>0.85</td>
<td>0.95</td>
<td>0.75</td>
</tr>
<tr>
<td>Estonia</td>
<td>0.84</td>
<td>0.99</td>
<td>0.82</td>
<td>0.85</td>
<td>0.94</td>
<td>0.64</td>
</tr>
<tr>
<td>Mauritius</td>
<td>0.82</td>
<td>0.85</td>
<td>0.96</td>
<td>0.74</td>
<td>0.91</td>
<td>0.70</td>
</tr>
<tr>
<td>Australia</td>
<td>0.82</td>
<td>0.94</td>
<td>0.96</td>
<td>0.86</td>
<td>0.94</td>
<td>0.44</td>
</tr>
<tr>
<td>Georgia</td>
<td>0.81</td>
<td>0.91</td>
<td>0.77</td>
<td>0.82</td>
<td>0.90</td>
<td>0.70</td>
</tr>
<tr>
<td>France</td>
<td>0.81</td>
<td>0.94</td>
<td>0.96</td>
<td>0.60</td>
<td>1</td>
<td>0.61</td>
</tr>
<tr>
<td>Canada</td>
<td>0.81</td>
<td>0.94</td>
<td>0.93</td>
<td>0.71</td>
<td>0.82</td>
<td>0.70</td>
</tr>
</tbody>
</table>

Source: ITU GCI
Heat Map (CGI)

Source: ITU GCI
Key Findings of GCI 2017 on CIP

Does the legislation or regulation impose the implementation of cybersecurity measures on the critical infrastructure operators?

- Yes: 28%
- No: 72%

Does the legislation or regulation impose cybersecurity audits on the critical infrastructure operators?

- Yes: 21%
- No: 79%

Source: ITU GCI
Does national cybersecurity strategy include a national resilience plan?

In the national strategy for cybersecurity, Is there a section on the protection of critical information infrastructure?

Source: ITU GCI
Key Findings of GCI 2017 on CIP

- Governments are responsible for the country’s overall security, public safety, the effective functioning of the economy, and the continuity of government services in case of an emergency or crisis.
- Government has responsibility to lead.
- Most of the critical infrastructures are administered by the private sector operators.
- The CIP is the shared responsibility of both public and private organizations who develop, own, provide, manage and/or use this critical infrastructure.

Do you have an responsible agency responsible for critical information infrastructure protection?

Source: ITU GCI
Currently around 72 countries have published National Cybersecurity Strategies

Source: ITU GCI
Computer Incident Response Teams

Currently around 103 countries have published National Cybersecurity Strategies

Source: ITU GCI
What to do

From simple steps (which any company engaged in eCommerce should adopt)

- Use of a secure eCommerce platform
- Using a secure connection for online checkout
- Use of complex passwords

...to more a nation wide approach

- National Cybersecurity Strategy
- Regulations (cyber ready)
- Incident response capabilities
- Information sharing (e.g. FS-ISAC)
Thank you
cybersecurity@itu.int