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

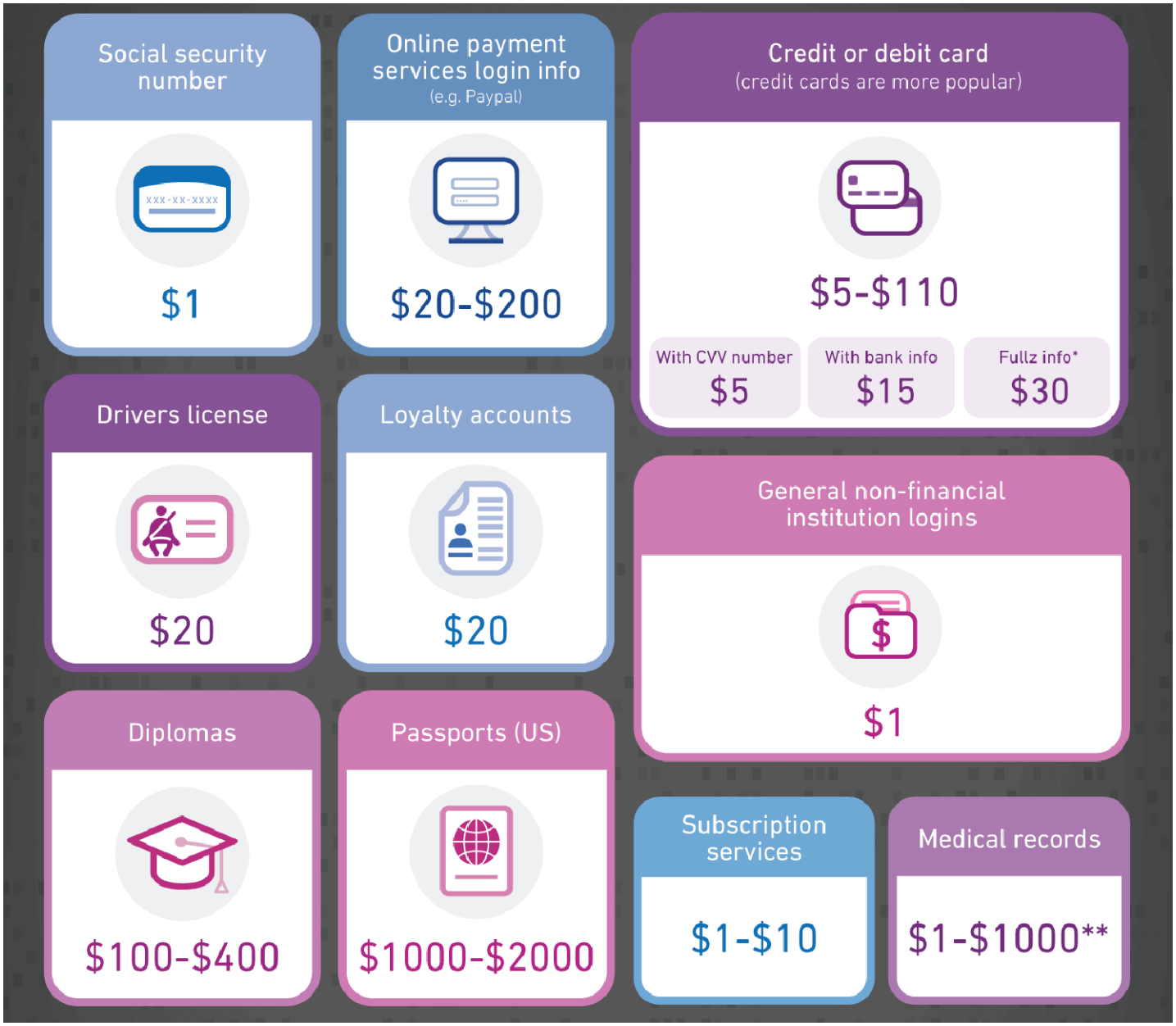
Marco Obiso
Head ITU Applications and Cyber Security Division, ITU

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 the examining transactions of more than 5000 eCommerce merchants across North America, Asia, Europe

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

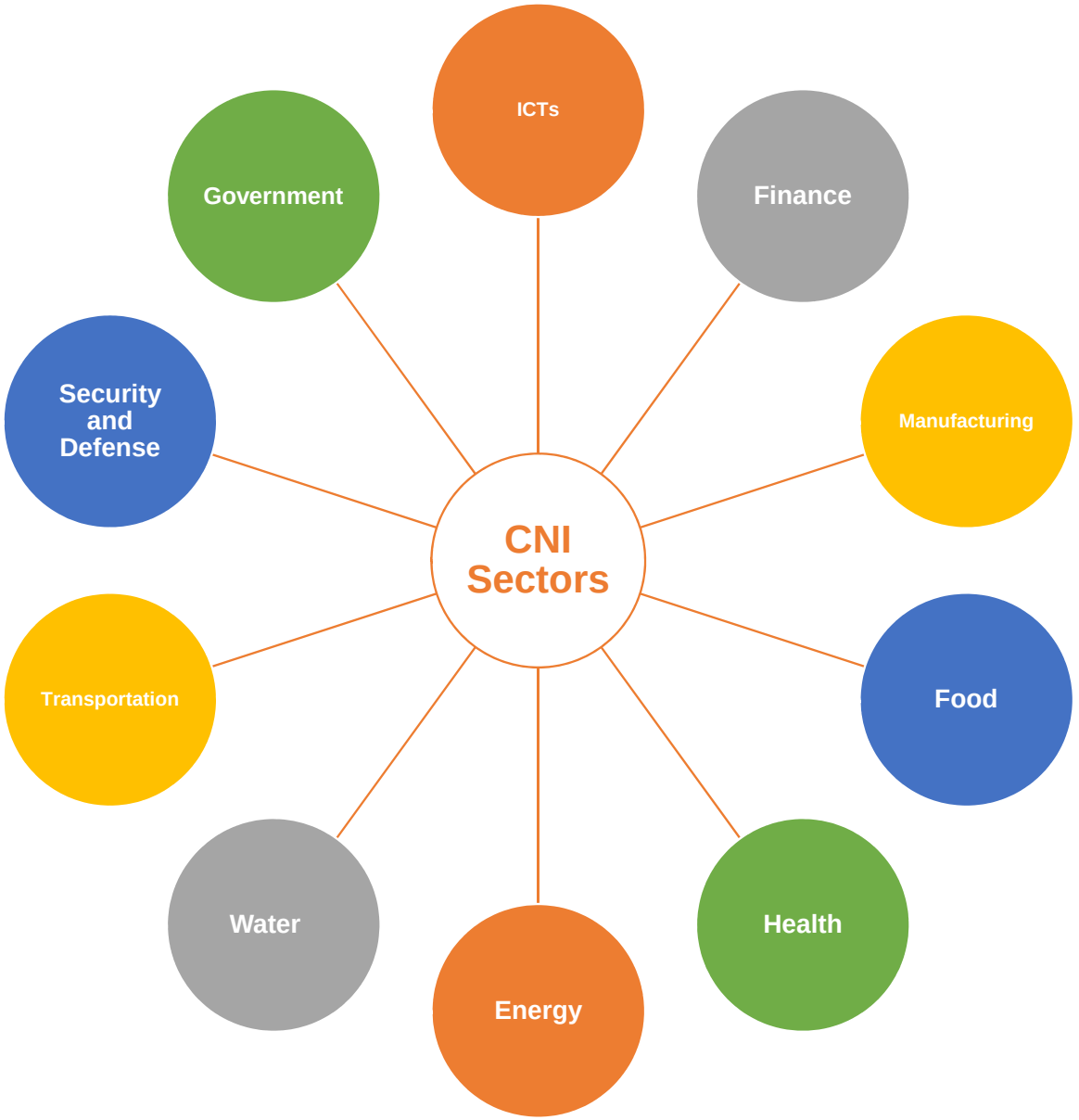
…and generally (at the national level)

- 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



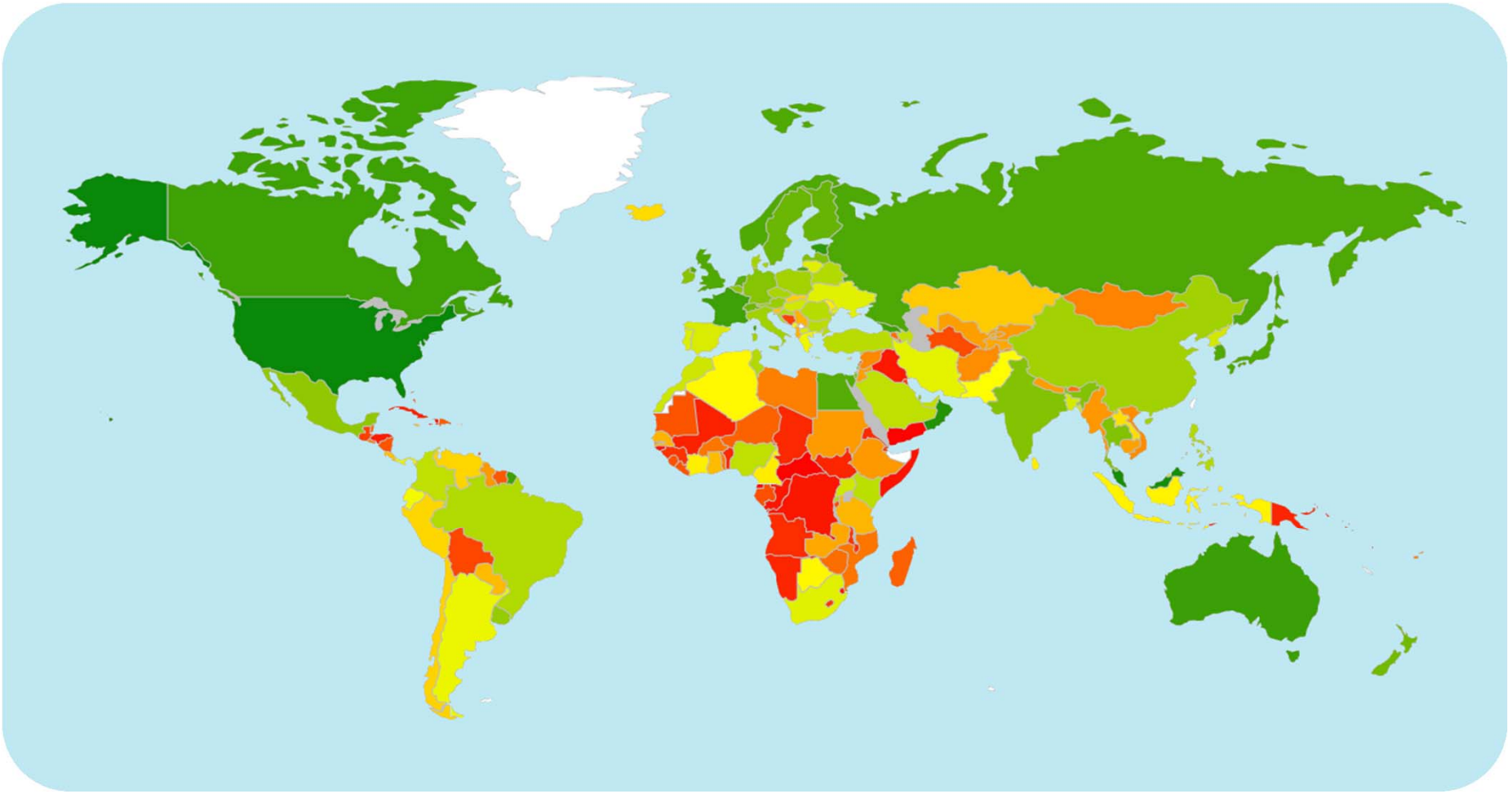
ITU Global Cybersecuirty Index (GCI)

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

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

Source : ITU GCI

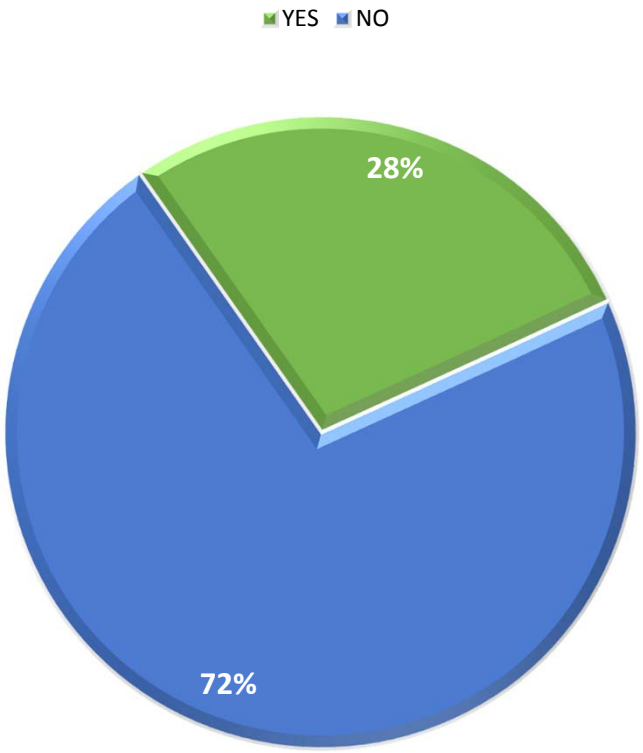
Heat Map (CGI)



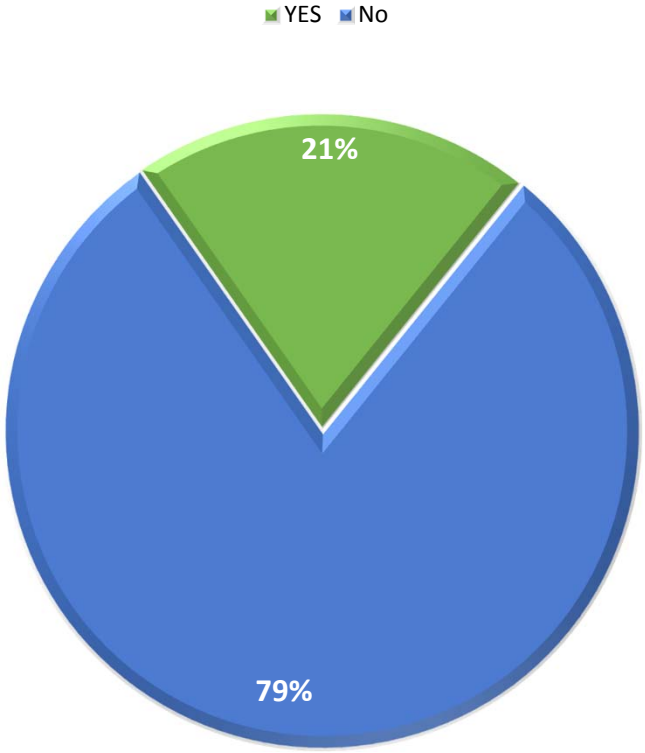
Commitment levels High Medium Low

Source : ITU GCI

Key Findings of GCI 2017 on CIP



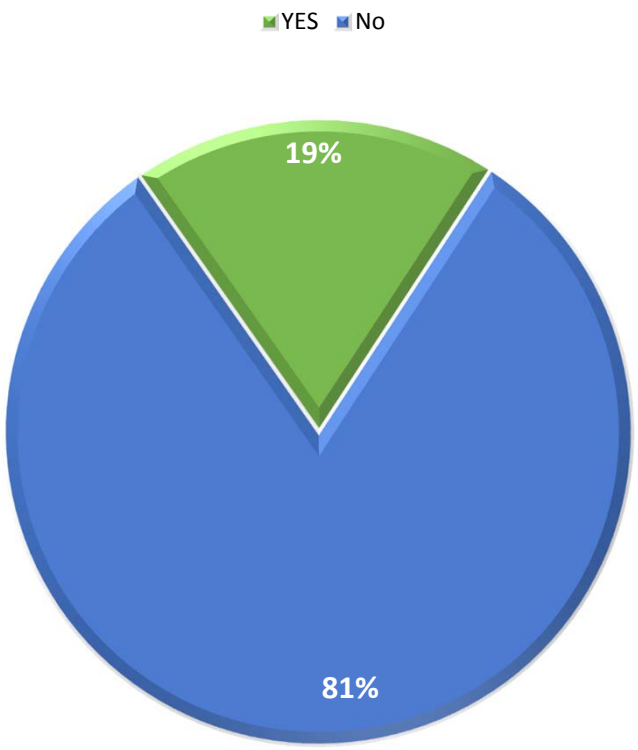
Does the legislation or regulation impose the implementation of cybersecurity measures on the critical infrastructure operators?



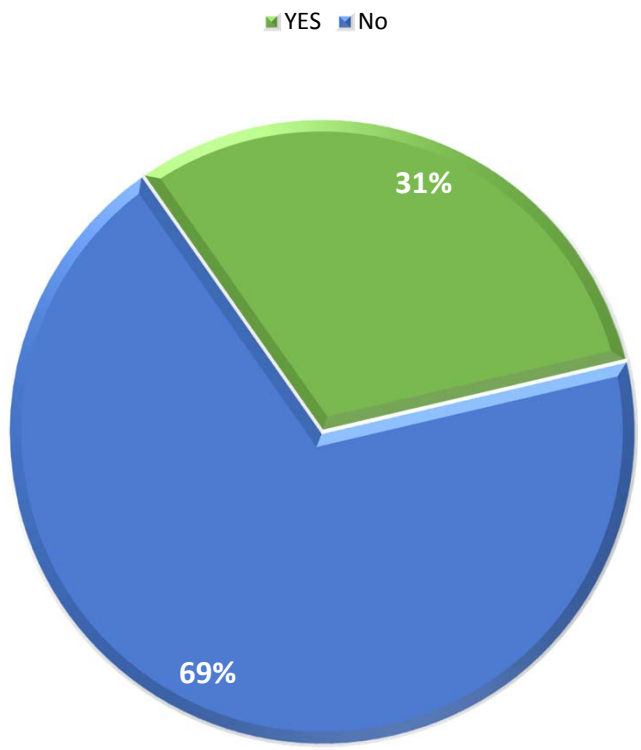
Does the legislation or regulation impose cybersecurity audits on the critical infrastructure operators ?

Source : ITU GCI

Key Findings of GCI 2017 on CIP



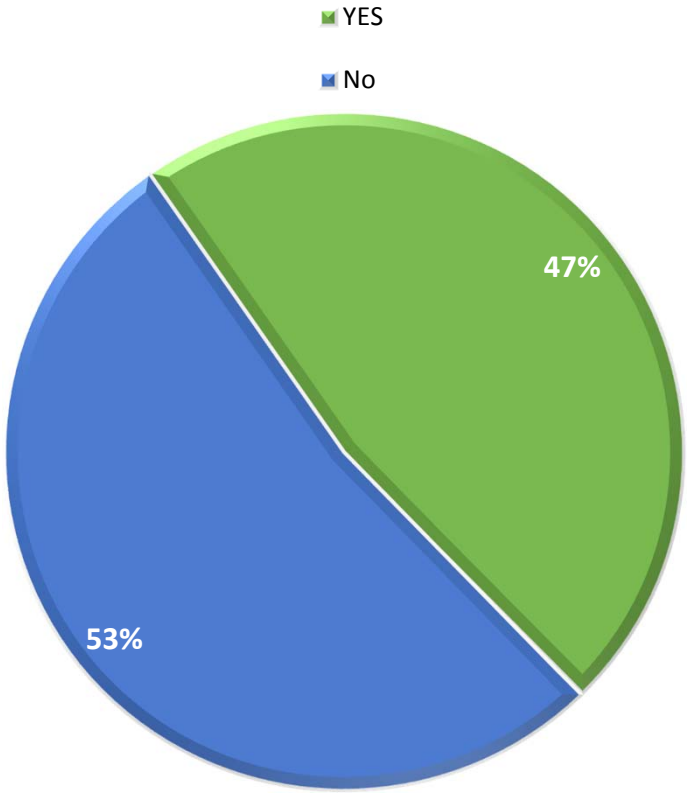
Does national cybersecurity strategy include a national resilience plan ?



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



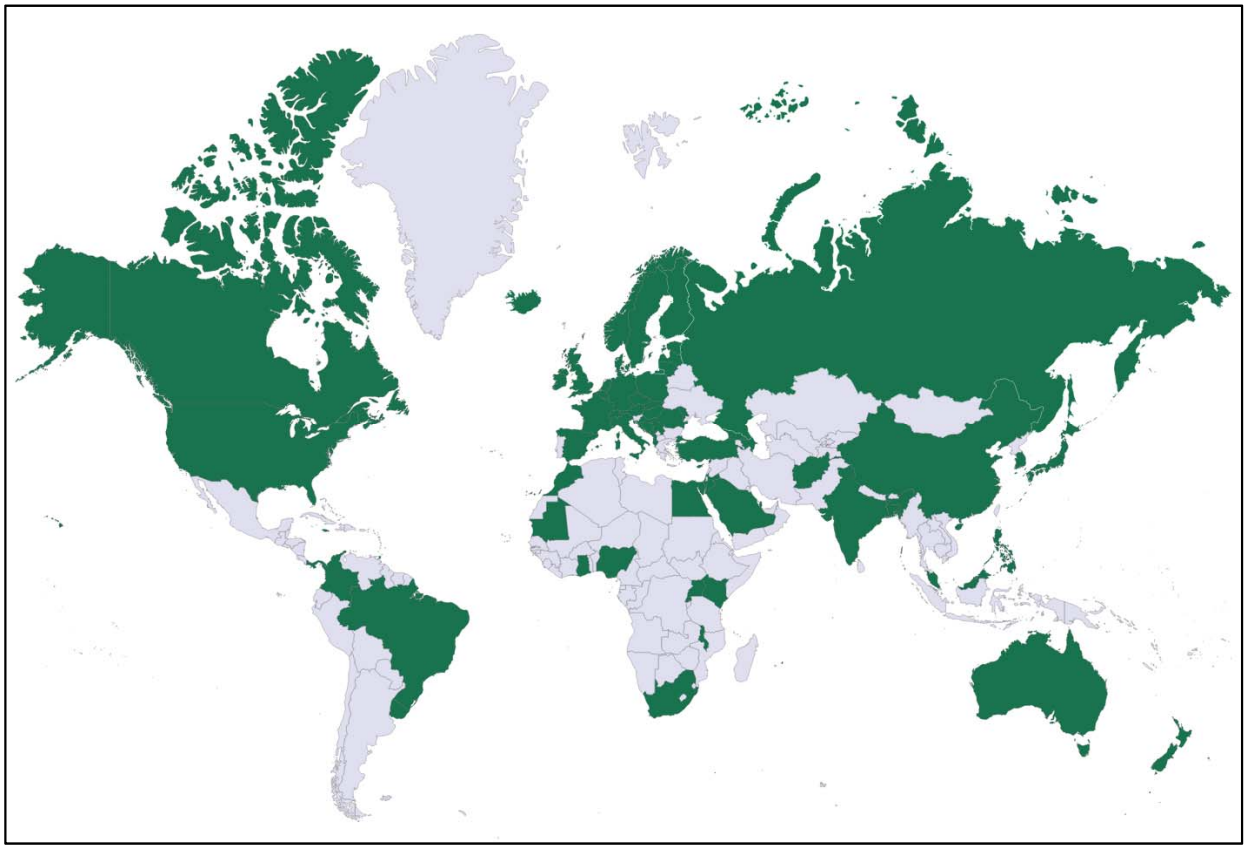
Do you have an responsible agency responsible for critical information infrastructure protection?

- 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.

Source : ITU GCI

National Cybersecurity Strategies

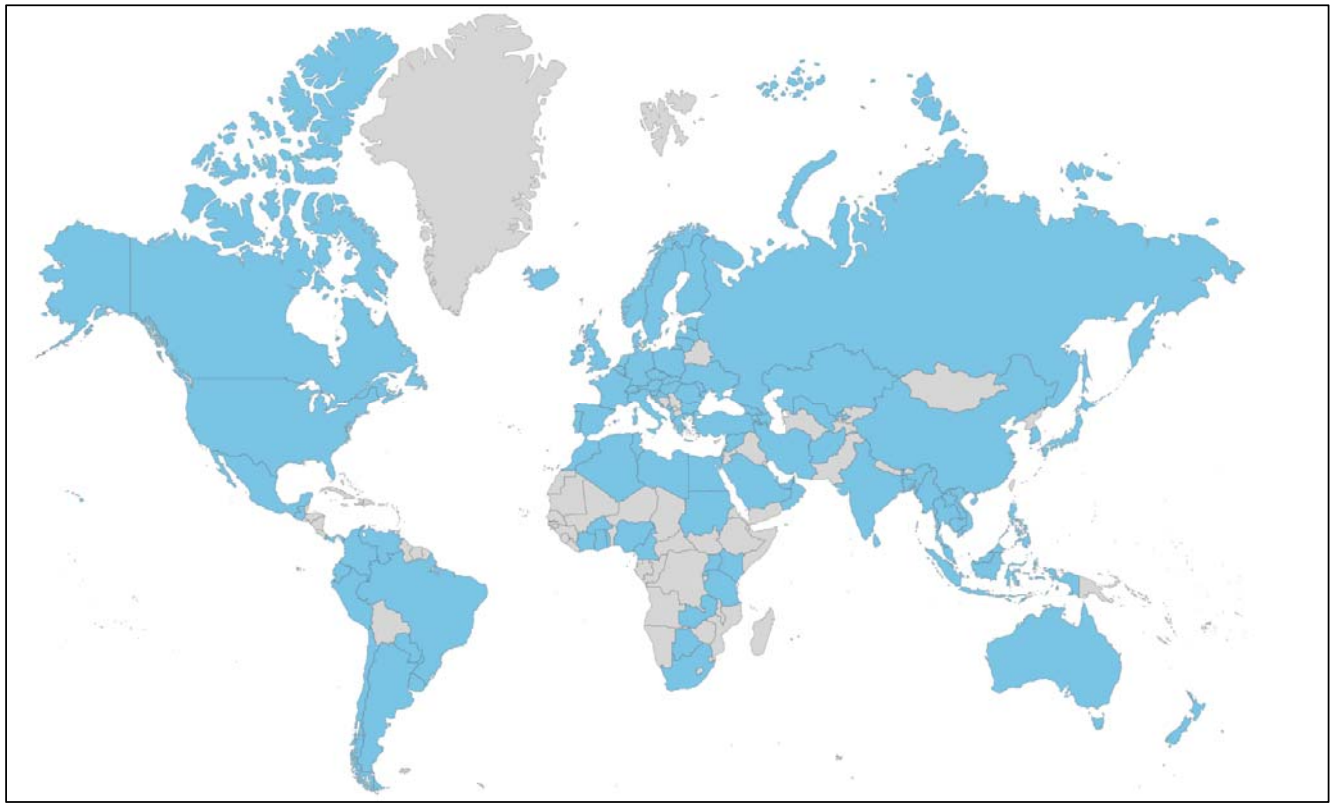
Currently around 72 countries have published National Cybersecurity Strategies



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