Cyberthreat Spawns New Era Of Public-Private Collaboration

Interactive Roundtable

4:30-5:30, Tuesday
15 September 2015

WORLD BANK GROUP

OASIS

Introduction

- ***Session Facilitator:*** **Alexander Howard**
  Senior Editor, Technology and Society, Huffington Post
- **Marco Obiso**
  Cybersecurity Coordinator, ITU
- **Eric Hibbard**
  CTO Security & Privacy, Hitachi Data Systems, INCITS, IEEE
- **Scott Algeier**
  Founder, President & CEO, Conrad, Inc. & Executive Director, IT-Information Sharing & Analysis Centers (IT-ISAC)

Borderless Cyber 2015

Cyberthreat Spawns New Era Of Public-Private Collaboration

Marco Obiso
Cybersecurity Coordinator

Global Cybersecurity Index (GCI)

Objective

The GCI aims to measure the level of commitment of each nation in cybersecurity in five main areas:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- National and International Cooperation

Goals

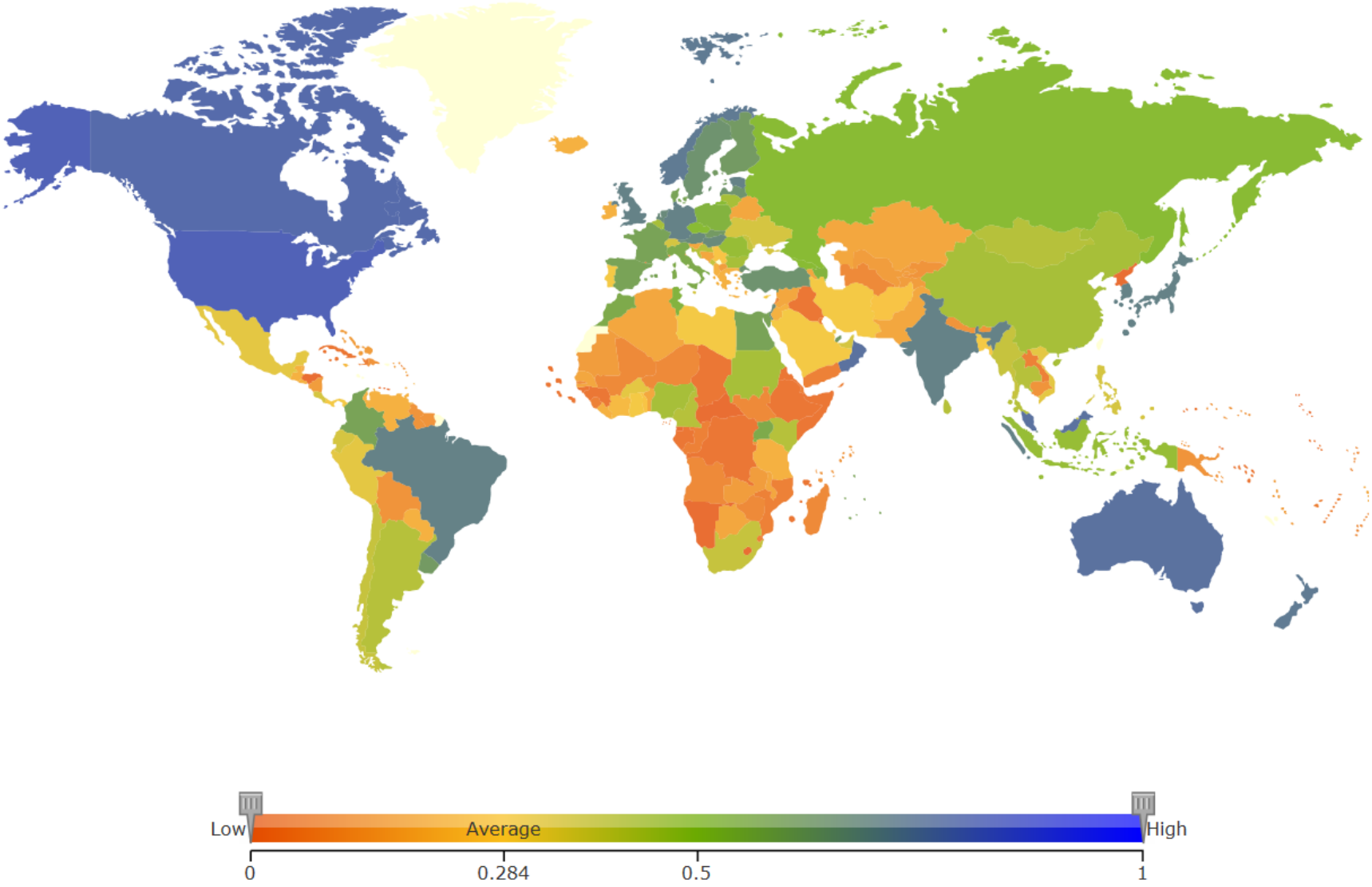
- Promote cybersecurity strategies at a national level
- Drive implementation efforts across industries and sectors
- Integrate security into the core of technological progress
- Foster a global culture of cybersecurity

105 countries have responded

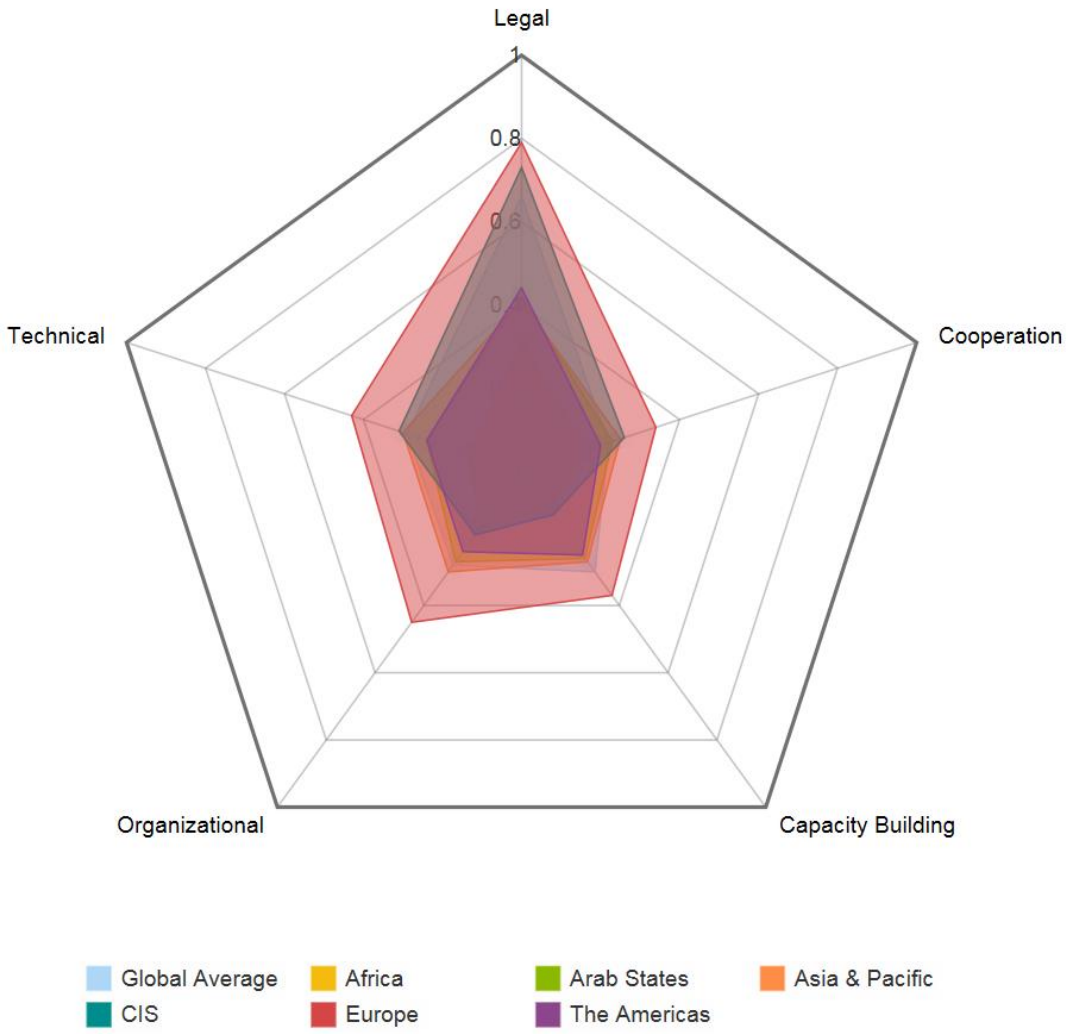
Final 2014 Results are on ITU Website

Next iteration in progress

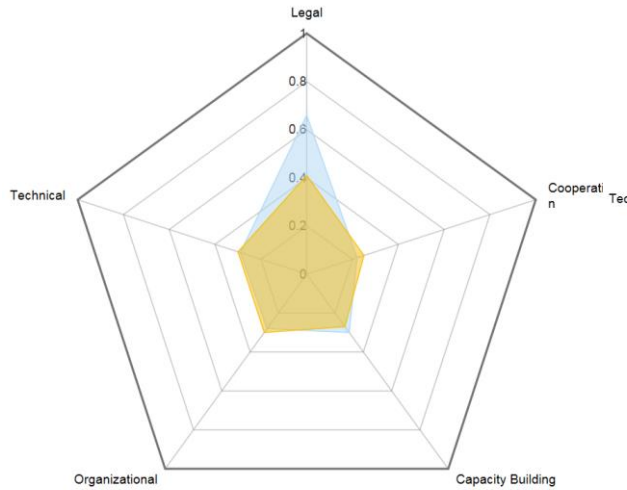
GCI 2014 World distribution



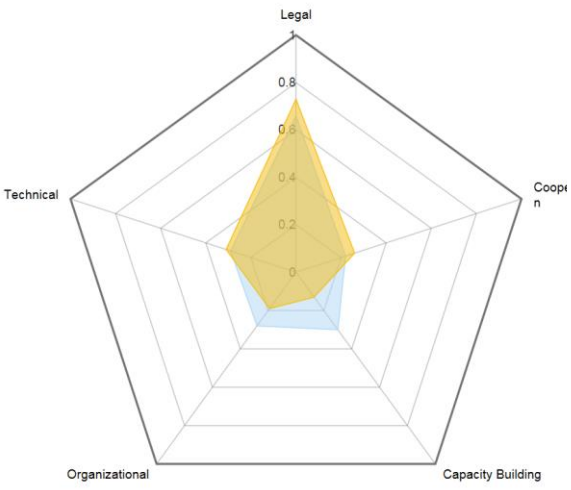
GCI 2014 World comparison



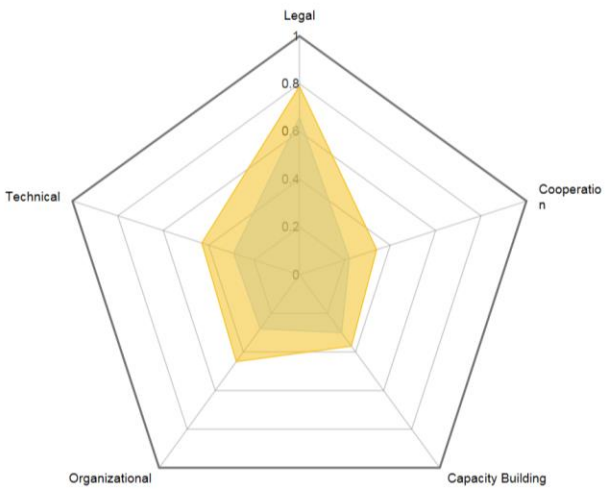
Regional Comparison



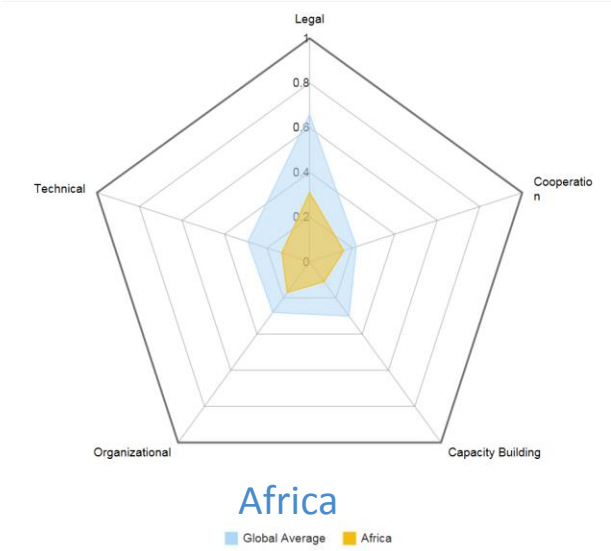
Asia & Pacific

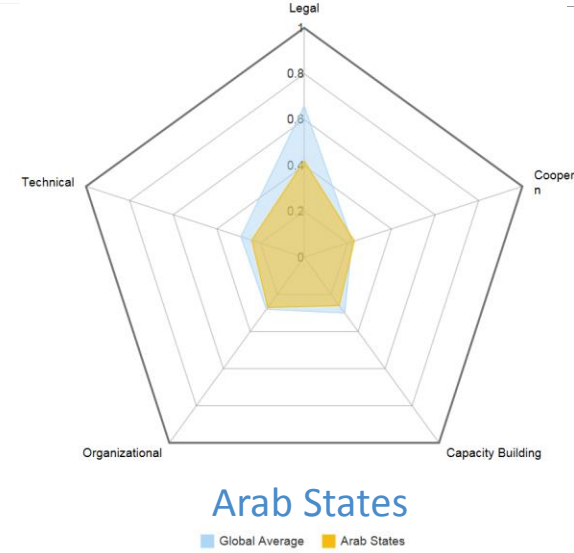


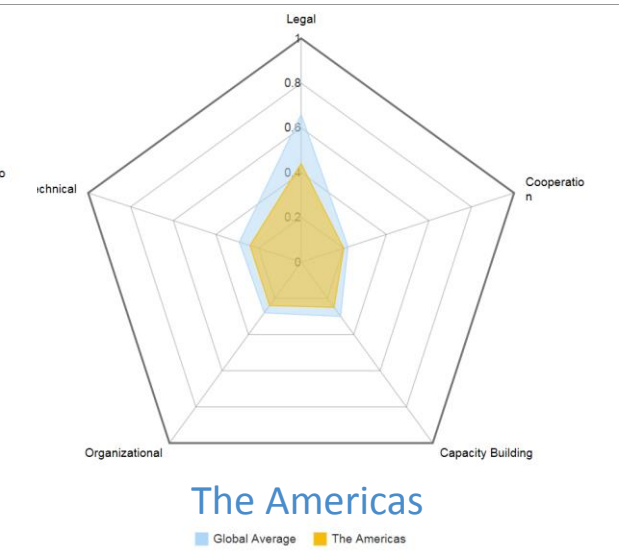
CIS



Europe







Africa

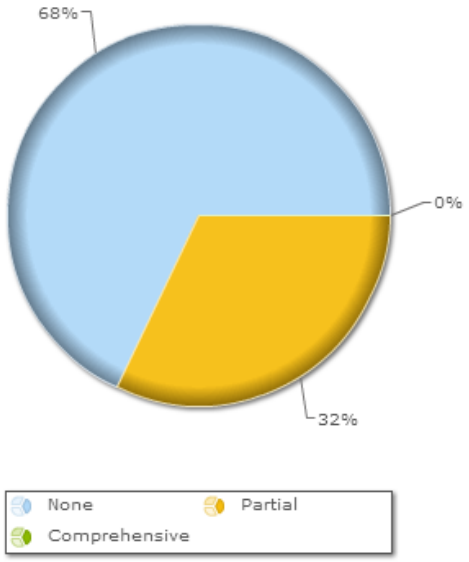
Arab States

The Americas

INTER-AGENCY COOPERATION

Inter-agency cooperation refers to any officially recognized national or sector-specific programs for sharing cybersecurity assets (people, processes, tools) within the public sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and/or resources between departments and agencies). This includes initiatives and programs between different sectors (law enforcement, military, healthcare, transport, energy, waste and water management, etc.) as well as within departments/ministries (federal/local government, human resources, IT service desk, PR, etc.).

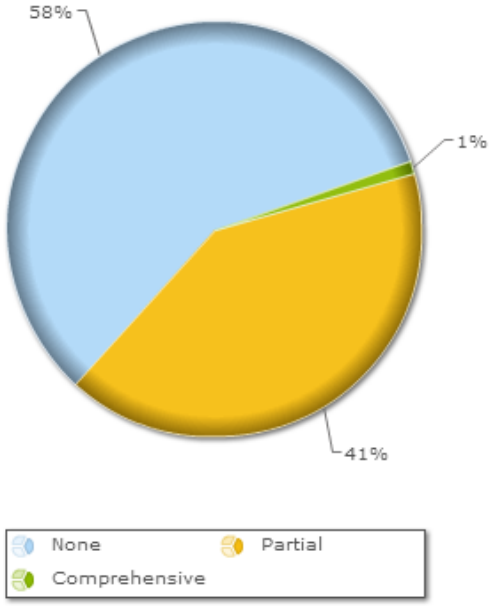
Countries that have officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.



INTER-STATE COOPERATION

Inter-state cooperation refers to any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states (i.e. signed bi-lateral or multi-lateral partnerships for the cooperation or exchange of information, expertise, technology and/or resources). Inter-state cooperation also includes regional level initiatives.

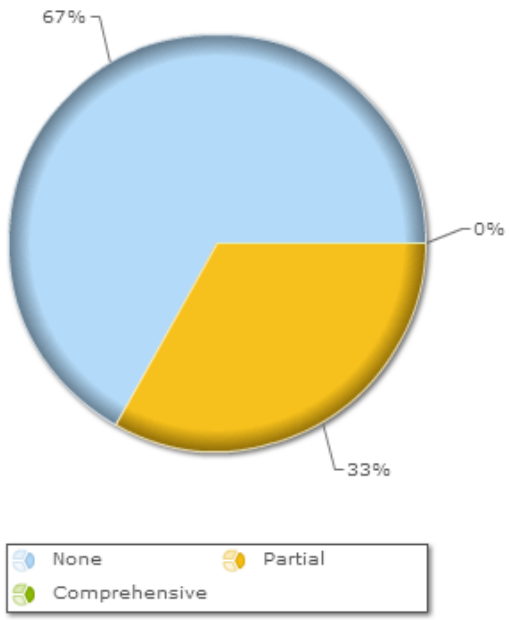
Countries that have officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states.



INTERNATIONAL PLATFORMS AND FORUMS

This is a measure of officially recognized participation in international cybersecurity platforms and forums. Such cooperative initiatives include those undertaken by (but not limited to): United Nations General Assembly; International Telecommunication Union (ITU); Interpol / Europol; The Organisation for Economic Cooperation and Development (OECD); UN Organizations on Drug and Crime Problems (UNODC), etc.

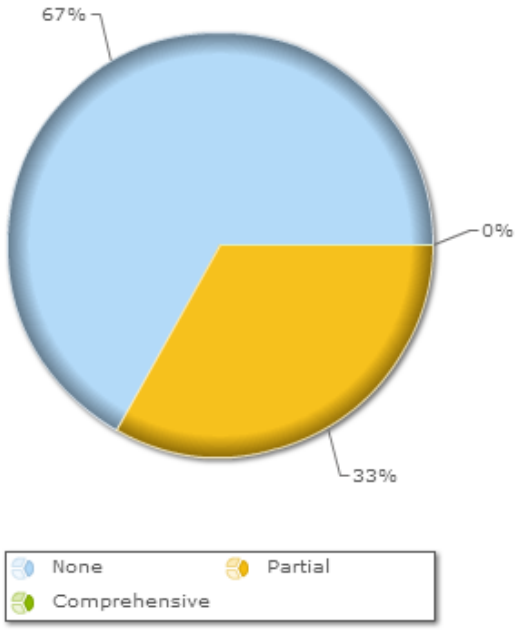
Countries that have officially recognized participation in regional and/or international cybersecurity platforms and forums.



PUBLIC-PRIVATE PARTNERSHIPS

Public-private partnerships (PPP) refer to ventures between the public and private sector. The number of officially recognized national or sector-specific PPPs for sharing cybersecurity assets (people, processes, tools) between the public and private sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and/or resources) is measured.

Countries that have officially recognized national or sector-specific programs for sharing cybersecurity assets between the public and private sector.



Some Best Practices

Moldova

- In 2013, the **e-Governance Academy of Estonia and the e-Government Center of the Republic of Moldova** implemented a cyber security project with 3 main components:
  - The first component consists in developing a **Cyber Security Roadmap** for Moldovan government institutions
  - The second component consists in developing **minimum requirements for digital information security** for government institutions, or what governments should do in order to secure digital information
  - The third component is more general, **raising awareness** among government officials and Moldovan citizens on current risks and threats in relation to cyber security

Recommendations (some of them)

- Do not take things for granted; have open mind; do not assume you are the first undertaking this work; most of the work is already out there, use it instead of criticize it
- Adopt a logical sequence, for instance:
  - ✓ intra-agency - inter-agency (nation as-a-whole) - regional – international
  - ✓ can also be undertaken in parallel, with clear identified interdependencies
- Identify foundation work to start with, as way to get management support and buy-in, for instance:
  - ✓ CSIRT/CIRT establishment
  - ✓ National cybersecurity strategy
  - ✓ Nation wide exercise (such as cyberdrills)

How to apply them

Outreach and information sharing activities with international partners as integral part of any National Cybersecurity Strategy (NCS).

- Progressive programs to formalize international trusted relationships and information sharing mechanisms through multilateral agreements and organizations including technical topics (measures, mechanism, CERT, …)
- Plan to outline how to manage international collaboration across multiple strategic areas (e.g. law enforcement, incident response, and R&D)
- Complement NCS with international strategy to address key areas as information sharing, mutual support in Incident Detection/Response, cooperation in fighting cyber crime, Research, training, etc.

Thank You

www.itu.int/cyb

cybersecurity@itu.int

Incentives and Barriers for Cyber Information Sharing

ERIC A. HIBBARD, CISSP, CISA

WORLD BANK GROUP

OASIS

Standardization

- Consensus-based cyber standards
  - Respond to known threats (real and perceived)
  - Take significant time and effort to develop
  - Can involve significant compromises/negotiations
  - New and emerging technology may be missed
  - Are common knowledge (attackers know too)
- Can serve as a basis for due care/diligence
- May be a rallying point (e.g., PCI DSS)

Legal Implications

- There are no guarantees that shared information will remain secret
  - Hard to establish/maintain “trusted” players
  - Attackers have a special interest in info sharing
- Can shared info result in prosecution?
- Are there liabilities/penalties for withholding or incomplete sharing (accidental/intentional)?
- Acknowledgement of info sharing could result in litigation

Automation

- The threat landscape changes rapidly, so time is of the essence
- Actionable information is critical
- The sheer volume of information makes in almost impossible for security personnel to keep up (assuming you have personnel)
- Domestic and international standards are needed to facilitate automated responses

Government as a Partner

- Industry drives the accelerating pace of change in cyberspace, not government.
- Governments have a critical shortage of cybersecurity professionals.
- Cybersecurity is often part of the competitive landscape
  - Between governments
  - Between companies

IT-ISAC OASIS Conference

September 15, 2015

WORLD BANK GROUP

OASIS

About the IT-ISAC

- Established in 2000, Operational in 2001.

- Mission is to:
- 1. Report, exchange and analyze across the IT Sector, and partner industries, information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures,
- 2. Establish a mechanism for systematic and protected exchange and coordination of such information and trusted collaboration; and
- 3. Provide thought leadership to policymakers on cyber security and information sharing issues.

Effective Practices in Public Private Partnerships (PCIS and IT SCC)

- Senior level commitment to the partnership process communicated to staff and upper echelons
- Involvement at the priority/goal and objectives phases of projects, not just implementation
- Use of the process identified in the NIPP for involving industry
- Reaching out to stakeholders early on, ideally at the “blank page” stage
- Continuous and regular interaction between government and industry stakeholders
- Providing adequate time for stakeholder review (equal to government review)

Effective Practices in Public Private Partnerships (PCIS and IT SCC) Cont.

- Establishing co-leadership of programs
- Consensus partnership decision making
- Communicating genuine interest in stakeholder input; e.g. via co-drafting
- Adequate engagement from federal agencies beyond DHS
- Government follow through on partnership related decisions
- Adequate and competent support services

Contact Information

Scott C. Algeier

Executive Director, IT-ISAC

President and CEO, Conrad, Inc.

salgeier@it-isac.org

scott@conradinc.biz

703-385-4969

WORLD BANK GROUP

OASIS

#BorderlessCyber

Questions ?