RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Can Government Cybersecurity Policies Balance Security, Trade & Innovation?

SESSION ID: PNG-T07

Moderator: Danielle Kriz
Director, Global Cybersecurity Policy
Information Technology Industry Council (ITI)

Panelists:

Allan Friedman, PhD
Visiting Scholar, Cyber Security Policy Research Institute School of Engineering, George Washington University

Masahiro Uemura
Director, Office of IT Security Policy
Ministry of Economy, Trade and Industry, Government of Japan

Jon Boyens
Senior Advisor for Information Security
U.S. National Institute of Standards and Technology

Alexander Dewdney
Counselor for Cyber
British Embassy, Washington DC

Danielle Kriz (ITI): *Panel overview*

- Governments are increasingly prioritizing cybersecurity
- Governments are proposing or enacting strategies, policies, laws, and regulations related to cybersecurity (mandates on cryptography, security standards, CIIP, supply chain risk management, etc)
- Some policies focus on governments' own use of IT (e.g. gov't procurement), and others on regulating their commercial markets
- Governments have important roles to play in cybersecurity
- But some policies interrupt trade and innovation
- Can we come to an appropriate balance?

Allan Friedman (GWU): *Cybersecurity and Trade- National Policies, Global and Local Consequences* [Sept. 2013]

- *WHY?* Cybersecurity is different from other trade issues
- *CONTEXT:* Lessons from similar issues
- *CONSEQUENCES*
    - Technical standards matter a lot
    - Acronyms for economists: FDI, LDCs, IP, etc
    - National Security Exceptions = Mutually Assured Destruction
- *SO WHAT?* 4 Recommendations and 7 Research Questions
- Full report: http://v.gd/cybertrade

Jon Boyens (NIST): *Enabling innovation, competitiveness and security*

- ROLE: Current and evolving
- APPROACH: Public-Private Partnership; science-based, not geopolitical
- PROCESS: Engage stakeholders early and throughout

Masahiro Uemura (METI): *Japan’s experience*

- IT systems security: Utilize more universal standards

  - Government : Change from individual guidelines in ministries to current unified standards

  - Industry: Change from domestic criteria to international standards, ISMS

- Critical infrastructure: Public-private partnership

  - Voluntary information sharing scheme, J-CSIP operated by IPA

  - EDSA & CSMS [IEC 62443], Enhance the export of Japanese ICSs, raise awareness

- Japan's 2013 cybersecurity national strategy

□ - Enhance the utilization of international standards, int’l cooperation

  - Viewpoint about trade and information security

Presenter’s Company Logo – replace on master slide

Alex Dewdney (British Embassy): *UK experience*

- The UK’s National Cyber Security Strategy: security and prosperity
- International, EU, and national dimensions
- Government and industry in coalition