

September 5, 2016

Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

Input to the Commission on Enhancing National Cybersecurity

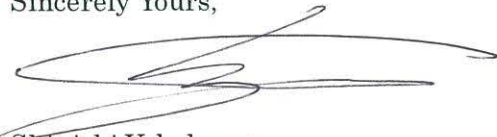
Dear Nakia:

NTT appreciates the opportunity to submit comments on the current and future state of cybersecurity in the digital economy. Our comments are on the “International Market”.

Cybersecurity has a dual mission in NTT. One is to protect ourselves, and the other is to provide security services to clients. For protecting ourselves, since we run our businesses in more than 80 countries, internationally harmonized security requirements and regulations are very important. For serving clients, we launched NTT Security in August 2016, a new company that provides a managed security service platform globally. A sound international cybersecurity market is foundational to deliver our service effectively to clients.

Our comments, described in the attachment, are based on our commitments to contribute to building global cyber resiliency. We welcome the opportunity to answer any questions regarding this document and thank you for this opportunity.

Sincerely Yours,



Shinichi Yokohama
Head, Cybersecurity Integration
NTT Corporation

Attachement (2)

Executive Summary - International Market

Trends and challenges

To meet pressing needs to ensure robust cybersecurity for its constituencies, each country/region government is setting up baseline requirements. At the same time, governments recognize the importance of policy harmonization, and it is pursued at bi-lateral and multi-lateral fora. However, agreements often lack operational specifics and stay at a high level, such as respect for multi-stakeholder approaches and encouraging the free flow of information.

Progress and promising approaches

Industries, both individually and as a group, have started providing opinions for international policy alignment, based on their operational experiences. At the same time, governments have also started inviting industries to governmental dialogues. Inputs from industries to governmental fora, based on their field level operation, appear to be a promising approach to ensure practical and tangible linkage between policy and operational reality and ensure effectiveness and practicality of policy alignment.

Suggestion for the next 1-2 years

Ask industries to identify specific policy items that require international harmonization by talking among companies within each sector. Items, if not harmonized, that will become barriers for 1) cost efficiency, 2) capability enhancement, and 3) innovation, should be identified based on industry experiences. In parallel, establish an international government forum to consider these industry voices, and to promote international harmonization. Given the breadth and complexity of the issues to be discussed, a phased approach is suggested, i.e. start from a small set of sectors and small number of governments.

Future challenges and suggestion for the next decade

Complexity around international markets will exponentially increase. The number of countries/regions concerned will increase as will the diversity of interests. Policy items that require harmonization will also increase as technologies and innovations advance. We should position the next 1-2 years as a window of opportunity to establish a mechanism that nurtures international markets. For the success over a decade, we need to continuously position industries and their operational experience as lead for policy harmonization and link operational reality to policy formulation.

Comments on “International Market”

Trends and challenges

To meet pressing needs to ensure robust cybersecurity for its constituencies, each country/region government is setting up baseline requirements. At the same time, governments recognize the importance of policy harmonization, and it is pursued at bi-lateral and multi-lateral fora. However, agreements often lack operational specifics, and stay at a high level, such as respect for multi-stakeholder approaches and encouraging the free flow of information.

- In Japan, the government issued “National Cybersecurity Strategy” (Sept 2015), followed by a series of new guidelines such as “Cybersecurity Management Guidelines” (Dec 2015), “General Framework for Secured IoT Systems” (June 2016).
- The European Commission issued “Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry” and the European Parliament adopted “Network and Information Security Directive” (July 2016)
- In parallel, each government recognizes the necessity and values of policy harmonization. In 2016, the G7 Summit addressed, in its Leaders Declaration, a proposal to develop a follow-up Working Group for cyber security policy harmonization. Bi-lateral discussions are also undertaken between countries such as US-Japan. For example, the US-Japan Cyber Dialogue and Internet Economy Dialogue.
- While some of these international dialogues address specific and operational challenges, such as the EU-US Privacy Shield, most of agreements stay at a high-level and linkage to field-level operation is not clearly identifiable.
- This “missing link” between policy and operations is a big challenge to make international harmonization effective and eventually develop a sound international market.

Progress and promising approaches

Industries, both individually and as a group, have started providing opinions for international policy alignment, based on their operational experiences. At the same time, governments have also started inviting industries to governmental dialogues. Inputs from industries to governmental fora, based on their field level operation, appear to be a promising approach to ensure practical and tangible linkage between policy and operational reality and ensure effectiveness and practicality of policy alignment.

- For the NIST's workshop on Cybersecurity Framework in April 2016, multiple international companies, including NTT, contributed use cases, lessons learned, and suggestions for Framework's future. Those inputs became a foundation for the international harmonization agenda.
- Another example is US-Japan Cyber Dialogue in July 2015. For the first time industry leaders were invited to share their experience to this bi-lateral government discussion. Also, a multi-stakeholder conference was organized preceding the 2016 G7 Summit in Japan where business leaders from G7 countries shared their experiences and commitments to international collaboration.

Suggestion for the next 1-2 years

Ask industries to identify specific policy items that require international harmonization by talking among companies within each sector. Items, if not harmonized, that will become barriers for 1) cost efficiency, 2) capability enhancement, and 3) innovation, should be identified based on industry experiences. In parallel, establish an international government forum to consider these industry voices, and to promote international harmonization. Given the breadth and complexity of the issues to be discussed, a phased approach is suggested, i.e. start from a small set of sectors and small number of governments.

- Today, each sector has international fora where cross-border topics are addressed. Challenges caused by inconsistent international cybersecurity requirements and regulations will be different by sectors. So, asking each sector to consolidate sector-specific requests for policy harmonization will be a practical first step. Recommendations from each sector shall be aggregated into industry-wide opinions.
- From NTT's experience of trying to implement global internal security practices and developing global ICT services, challenges caused by inconsistent policy

requirements fall into the following three categories::

1) Cost increase

Meeting country-by-country requirements will drive up security implementation cost. For example, if countries have very restrictive data residency requirements, multi-tenant data storages and solutions are difficult.

2) Capability inefficiency

Cross-border synergies of security knowledge will be limited. For example, success of security data analytics by aggregating data from different geography will be difficult if countries have strong data residency requirements. Workforce development efforts and resource allocation could be also duplicated.

3) Barriers for service innovation

Security is an important feature in most of ICT service developments. If different countries have different security requirements, innovation efforts need to accommodate different features.

- On the government side, countries should select one venue to listen to voices from industry. Specifying a single multi-lateral forum (such as G7) to listen to voices from industry representatives and examine their viabilities will reduce the burden caused by duplicated meetings and gatherings.

Future challenges and suggestion for the next decade

Complexity around international markets will exponentially increase. The number of countries/regions concerned will increase as will the diversity of interests. Policy items that require harmonization will also increase as technologies and innovations advance. We should position the next 1-2 years as a window of opportunity to establish a mechanism that nurtures international markets. For the success over a decade, we need to continuously position industries and their operational experience as lead for policy harmonization and link operational reality to policy formulation.

- In the next decade, billions of additional people will equip themselves with smart phones that are connected to the Internet. Most of them are in emerging markets where interests by countries and governments are diverse. Beyond people, a much larger number of items will be connected to the Internet and the IoT society becomes reality. Topics that will require international harmonization will increase in breadth, complexity and inter-dependency.
- If we do not succeed in developing a mechanism to develop and maintain sound international markets in the next 1-2 years, we face a risk of falling into endless discussion and negotiation on interlinked but fragmented issues. Discussion and negotiation would take place at different fora by different participants, but unfortunately leading us nowhere.
- What is essential is to persistently respect experience and wisdom gained from field operations, and to bring them into policy formulation process. Doing it internationally is a big challenge, but now is the time for us so scope our views and efforts beyond individual country.