RSAConference2019 Asia Pacific & Japan

Singapore | 16–18 July | Marina Bay Sands



SESSION ID: PGR-R03

How To Make Successful Cybersecurity Public-Private Partnerships

Mihoko Matsubara

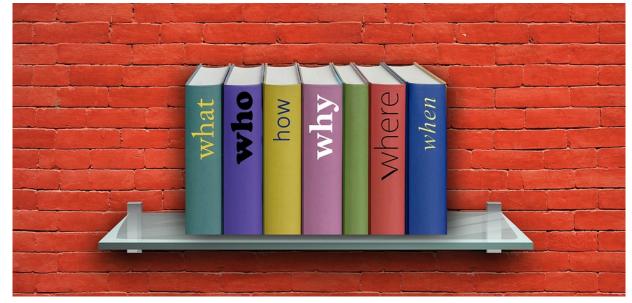
Chief Cybersecurity Strategist NTT Corporation
@M Miho JPN

Yuji Furusawa

Manager, R&D Planning Department NTT Corporation

Today, we will talk about

- What, why, and how
- Lessons leaned from Japanese cybersecurity Public-Private Partnerships (PPPs)
- How to make successful PPPs





Hurdles for public-private partnerships

- Free riders
- Liabilities
- Overlapped request
- Waiting for substantial cyber threat intelligence to provide
- What else?





RSA°Conference2019 Asia Pacific & Japan

What constitutes Public-Private Partnerships

Types of Cybersecurity Public-Private Partnerships

- Cyber threat intelligence sharing
 - ISACs
- Guidance, best practices
 - Technology
 - Business management, corporate governance
- Joint operations
 - Anti-Botnet, IoT security, critical infrastructure protection
 - Counter-cybercrime



Why Public-Private Partnerships?

- "Private" aspect
 - Industry owns majority of ICT assets, e.g., 90% in Japan
 - Cybersecurity as business management
- "Public" aspect
 - Fundamentals for citizens' lives, welfare, and national economic growth
 - Cybersecurity as national security
- Cybersecurity requires both technology and policy



Models of Public-Private Partnerships

- Government-led
- Industry-led

- National/local
- International/global



RSA Conference 2019 Asia Pacific & Japan

Government-led examples

Government-led examples in Japan

- Cyber threat intelligence sharing
 - CEPTOAR
 - NISC Cybersecurity Council
- Joint operations and exercises
 - Revised Telecommunication Act and NOTICE
 - Annual national joint exercises since 2009



CEPTOAR

- NISC launched it in 2009
- Sector-specific cyber threat intelligence sharing
- 18 CEPTOARs in 14 critical infrastructure industries

CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response

NISC: National center of Incident readiness and Strategy for Cybersecurity



NISC Cybersecurity Council

- Launched in April 2019
- Bottleneck: free riders
 - Give and take
- Tiered structure
 - 1st tier members (cybersecurity companies) can exchange early-phase information with their peers and government without worrying about disseminating false positive information.
 - 2nd tier members, who are required to provide feedback to cybersecurity companies, can receive early-phase information.
 - General members can receive advice from 1st tier members.



Lessons learned 1

- Baby steps to take forward
 - Information sharing of "what"?
 - One-way feeds → Mutual feedback



Same request by different agencies to industry



RSA Conference 2019 Asia Pacific & Japan



Industry-led examples

- Sector-based
 - Invite a relevant government agency as an observer
- Cross-sectoral
 - Can advocate influentially thanks to the size and compehensiveness
 - Focuses can be defused
- International initiatives
 - Multinational companies form partnership beyond national borders
 - Can be "bought-in" for local community



Industry-led examples in Japan

- Sector-based
 - Over ten ISACS such as ICT, Financials, and Auto
- Cross-sectoral
 - Kei Dan Ren (The Japan Business Federation)
 - Cyber Risk Information Center's Cross-Sector Forum (CRIC-CSF)
- International initiatives
 - Council to Secure the Digital Economy (CSDE)



ICT-ISAC Japan

- The first ISAC in Japan (as Telecom-ISAC Japan in 2002)
- Ministry of Internal Affairs and Communications as an observer
 - c.f., NCC/Comm-ISAC in the United States
- Cyber Clean Center with GOJ and JPCERT/CC
 - Joint operations to tackle with botnet





Cross-Sector Forum

- "Circle of Trust" of 44 major Japanese companies
 - GOJ as an observer
- Crafted cybersecurity capacity building model and strategy
 - GOJ refers to Forum documents in its policy and strategy
- Proactive participation to shape policy
- Speaking at NIST conferences in the US to share how the Forum adopted the NIST Cybersecurity Framework



CSDE's International Anti-Botnet Guide

- Alliance of tech companies in Americas, Europe, and Asia
 - Joint initiative by ITI and USTelecom



- Published "International Anti-Botnet Guide" as reference for ISPs, manufacturers, etc.
 - In alignment with EO 13800 of the POTUS
- In Japan
 - Shared with the Ministry of Internal Affairs and Communications
 - Disseminated through ICT-ISAC Japan



Lessons learned 2

- Start small (sector-specific) → Cross-sectoral → government
- Learn from competitors, which have same challenges
- Industry-driven → two-way discussion
- Leverage international initiative to mobilize local community



RSAConference2019 Asia Pacific & Japan

Conclusion and what you can do

Conclusion: How to make successful cybersecurity PPP?

- Industry-driven discussions for national/international resiliency
 - Individual, sectoral, and national/international support
- Build "Circle of Trust" with clear objectives and mutual benefits
 - ISAC for cyber threat intelligence sharing
 - Cross-Sectoral Forum for sharing best practices
 - Joint cyber exercises with government and industry
- Make discussions relevant to key stakeholders



And what you can do

- Today or this week, you should
 - Identify 2-3 peers in your industry to start periodic meet-ups
- In the first three months, you should:
 - Set agenda to discuss
 - Identify hurdles for two-way discussions
 - Organize informal discussions with industry peers
- Within six month, you should:
 - Launch a formal framework
 - Invite relevant government agencies to the industry-led initiative

