Cyber Security in Japan (v.2)

Ryusuke Masuoka (masuoka@cipps.org) and Tsutomu Ishino (ishino@cipps.org)

Cyber Security Policy Research Team
Center for International Public Policy Studies (CI PPS)

December 2012
Outline

• Japanese Government’s Approach
• Situation in Japan
• NISC and Four Key Agencies
• Cyber Incidents
• Cybercrime Trends in Japan
• References
JAPANESE GOVERNMENT’S APPROACH
Approach by Japanese Government

**Cross-sectional Framework Lead by Cabinet Secretariat**

**IT Strategic Headquarters**
- **Director-General:** Prime Minister
- **Vice Director-Generals:**
  - Minister of State for Science and Technology Policy
  - Chief Cabinet Secretary
  - Minister of Internal Affairs
  - Minister of Economy, Trade and Industry
- **Members:**
  - National Public Safety Commission Chairman
  - Minister of Internal Affairs
  - Minister of Economy, Trade and Industry
  - Minister of Defense
  - Members from the private-sector (6)

**Secretariat**
- **Cabinet Secretariat IT Dep’t:**
  - **Chief:** Assistant Chief Cabinet Secretary (Domestic affairs)

**Information Security Policy Council**
- **Chairman:** Chief Cabinet Secretary
- **Deputy Chairman:** Minister of State for Science and Technology Policy
- **Members:**
  - National Public Safety Commission Chairman
  - Minister of Internal Affairs
  - Minister of Economy, Trade and Industry
  - Minister of Defense
  - Members from the private-sector (6)

**Secretariat**
- **CISO Conference**
- **Special Committee on Critical Infrastructures**
- **Special Committee on Technological Strategy**
- **Special Committee on Edification and Education**

**National Information Security Center (NISC)**
- **Director:** Assistant Chief Cabinet Secretary (Risk & Security)
- **Deputy Director:** Councillor, Cabinet Secretariat (2)
- **Cabinet Counsellors** (6)
- **Advisors on Information Security** (3)

**Agencies in charge of critical infrastructures**
- Financial Services Agency: Financial Institutes
- Minister of Internal Affairs: Municipal, Communication
- Ministry of Health, Labour and Welfare: Hospitals, Water
- Ministry of Economy, Trade and Industry: Electric Power, Gas
- Ministry of Land, Infrastructure, Transport and Tourism: Railways, Airlines, Distribution

**Other agencies**
- Ministry of Education, Culture, Sports, Science and Technology: Cyber Security Education

**Four Key Agencies**
- National Police Agency
- Ministry of Internal Affairs and Communications
- Ministry of Economy, Trade and Industry
- Ministry of Defense

**Critical Infrastructures**
- Financial Institutes
- Municipal, Communication
- Hospitals, Water
- Electric Power, Gas
- Railways, Airlines, Distribution

**Governmental Agencies**
- Businesses
- Individuals
NISC and Four Key Agencies

- National Information Security Center (NISC)
  - Coordinating government efforts

- National Police Agency (NPA)
  - Fighting Cybercrimes

- Ministry of Internal Affairs and Communications (MIC)
  - Communication and Network Policies

- Ministry of Economy, Trade and Industry (METI)
  - IT Policies

- Ministry of Defense (MOD)
  - National Security
SITUATION IN JAPAN
Situation in Japan

- Started bearing fruit, but still a long way to go

• Wake up call – Mitsubishi Heavy Industries (MHI), Sep. 2011
  - Cyber security particularly hot after a cyber attack on MHI revealed
  - Anonymous hits Japan – July 2012 (Sony in 2011)
  - Stuxnet raised awareness for cyber attacks on critical infrastructures
  - Many relevant books published

• “Information Security 2012” – July 2012

1. Strengthening Measures for Sophisticated Threats to Companies and Organizations Handling Important National Information on Security
2. Maintaining a Safe and Secure User Environment for Addressing the Emerging Risks Associated with the Proliferation of New Information and Communications Technology Including the Full-Fledged Widespread Use of Smart Phones
3. Reinforcement of International Alliances
Situation in Japan

- Progresses and Setbacks

• Progresses
  - Laws are being updated
  - Cybercrime Convention into force – 1 Nov. 2012
  - MOD stands up to meet the challenges beyond its IT infrastructure
  - Control System Security Center (CSSC) – Mar. 2012

• Setbacks
  - PC Hijack Case
  - Concern of too many pilots
NI SC AND FOUR KEY AGENCIES
- Coordinating government efforts


1. Strengthening Measures for **Sophisticated Threats** to Companies and Organizations Handling Important National Information on Security
2. Maintaining a Safe and Secure User Environment for Addressing the Emerging Risks Associated with the Proliferation of New Information and Communications Technology Including the Full-Fledged Widespread Use of **Smart Phones**
3. Reinforcement of **International Alliances**

- FY2013 – 31.5B JPY Planned (Japanese Government Total)
National Police Agency (NPA) – Fighting Cybercrimes

• Cyber-Security Activities
  1. “Cyber Force Center” (Reorganized 140 IT Staffs of NPA)
  2. Information sharing with CCI-Designated Companies
  3. “Council to Prevent Unauthorized Communications to Counter Cyber-Intelligence” (with 4,800 companies all over Japan)

• FY 2013 – 2.4B JPY Planned
  1. Improve response capability against cybercrimes
  2. Improve response capability against cyber attacks to state secrets and critical infrastructures
  3. Extend international collaboration
  4. Keep analysis and law enforcement capabilities up to date with changing IT technologies and laws

CCI: Counter Cyber Intelligence
- Communication and Network Policies

• Cyber Security Activities
  – Cyber Attack Analysis Council, jointly with METI
    • IPA, JPCERT/CC, NICT, Telecom-ISAC Japan
  – Smart Phone Information Security

• FY2013 – 3.66B JPY Planned
  – Comprehensive security environment ready for new types of cyber attacks – 2.62B JPY

IPA: Information-technology Promotion Agency, Japan
JPCERT/CC: Japan Computer Emergency Response Team Coordination Center
METI: Ministry of Economy, Trade and Industry
NICT: National institution of information and communications technology
Telecom-ISAC Japan: Telecom Information Sharing and Analysis Center Japan
• **Cyber Security Activities**
  
  - Initiative for Cyber Security Information sharing Partnership Japan (J-CSIP)
    - Information sharing of cyber attacks
  
  - Cyber Attack Analysis Council, jointly with MIC
    - IPA, JPCERT/CC, NICT, Telecom-ISAC Japan
  
  - Building a pool of advanced information security experts
    - National security competitions, etc.
  
  - Securing control systems
    - Cyber security exercises, etc.
  
  - Control System Security Center (CSSC) – Mar. 2012
    - Established in Tokyo and Tsunami-affected area (Miyagi Reconstruction Park)

• **FY 2013 - 2.15B JPY Planned**
  
  - Information security promotion projects - 1.6B JPY
  
  - Hubs for security verification and education
    - Control systems test beds at CSSC - 0.55B JPY

IPA: Information-technology Promotion Agency, Japan  
JPCERT/CC: Japan Computer Emergency Response Team Coordination Center  
MIC: Ministry of Internal Affairs and Communications  
NICT: National institution of information and communications technology  
Telecom-ISAC Japan: Telecom Information Sharing and Analysis Center Japan
• Cyber Security Activities – 6 core approaches
  1. Improve information and telecommunication systems security
  2. Reinforce protection systems
  3. Prepare rules and regulations
  4. Develop Human resources
  5. Promote information sharing
  6. R&D of latest technologies

• FY 2013 – 21.2B JPY Planned
  - “Cyberspace Guard” (tentative name)
    • ~100 members, 10B JPY
  - MOD Cyber Range – 1.59B JPY
  - Add network monitoring equipment
  - Training through Japan-U.S. joint exercises
CYBER INCIDENTS
Case: Advanced Persistent Threat (APT)

(0) Preliminary Investigation
(1) Initial Penetration
(2) Building Attack Infrastructure
(3) System Survey
(4) Final Attack Execution

Attacker Spear Phishing Email
Confidential Info Obtained

Based on a Fujitsu slide, Modified by CIPPS
CYBERCRIME TRENDS IN JAPAN
Networking Crimes Cleared in 2011 - Details

- Unauthorized Access Violations: 4%
- Crimes Targeting Computers / Electronic Records: 2%
- Frauds: 16%
- Copyright Infringements: 7%
- Violations of Youth Protection Laws: 8%
- Child Prostitution Offenses: 8%
- Violations of Dating Site Regulation Act: 8%
- Distribution of Obscene Materials: 12%
- Child Pornography Offenses: 15%
- Others: 16%

Source: NPA
Calls to Internet Hotline Center (IHC)

- **Calls**: 91,769, 143,280, 140,391, 189,388, 182,757
- **Forwarded to Police**: 8,310, 8,221, 20,659, 22,964, 23,846

<table>
<thead>
<tr>
<th>Year</th>
<th>Calls</th>
<th>Forwarded to Police</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>91,769</td>
<td>8,310</td>
</tr>
<tr>
<td>2008</td>
<td>143,280</td>
<td>8,221</td>
</tr>
<tr>
<td>2009</td>
<td>140,391</td>
<td>20,659</td>
</tr>
<tr>
<td>2010</td>
<td>189,388</td>
<td>22,964</td>
</tr>
<tr>
<td>2011</td>
<td>182,757</td>
<td>23,846</td>
</tr>
</tbody>
</table>

- **Calls about Illegal/Harmful Information**: 1,6418, 20,333, 33,968, 44,683, 41,400
- **Illegal Information**: 12,818, 14,211, 27,751, 35,016, 36,573
- **Harmful Information**: 3,600, 6,122, 6,217, 9,667, 4,827

Source: NPA
REFERENCES
References

• Documents

• Organizations
  - CIPPS: Center for International Public Policy Studies http://cipps.org/english/
  - JPCERT/CC: Japan Computer Emergency Response Team Coordination Center http://www.jpcert.or.jp/english/
  - NICT: National institution of information and communications technology http://www.nict.go.jp/en/