Cybersecurity Response and Industry Promotion Policy

Jung Su Song
Director General, Cyber Security Policy Bureau
Contents

- Korea’s Cyber Threat Response
- Cybersecurity Industry Promotion
Korea’s Cyber Threat Response
Korea Cyber Security Policy

Internet Incidents Prevention
- Critical Information Infrastructure Protection
- Security Assessment for Readiness
- Information Security Management System (ISMS)

Research & Development
- Develop a Easy-to-Use Security Technology
- Develop Innovative Technologies
- Reinforce Smart Security Recognition Tech

Human Resource Management
- Promote a Career Path for Security Experts
- Support Infrastructure to Foster Top Security Experts

Cyber Threat Response
- Share Cyber Incidents Information with Relevant Stakeholders
- Respond promptly to Cyber Incidents
# Cyber Incident Response (Framework)

<table>
<thead>
<tr>
<th>Warning Level</th>
<th>When to issue warnings</th>
<th>Measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>• Issue Critical</td>
<td>• Organize a crisis center</td>
</tr>
<tr>
<td></td>
<td>• Subject: MSIP</td>
<td>• Create a private-public joint investigation group</td>
</tr>
<tr>
<td></td>
<td>• Prior consultation with the National Crisis Management Office</td>
<td>• Block a specific service ※ Overall response</td>
</tr>
<tr>
<td>Severe</td>
<td>• Issue Severe</td>
<td>• Notify a specific service control team</td>
</tr>
<tr>
<td></td>
<td>• Subject: MSIP</td>
<td>• Make a public announcement (media)</td>
</tr>
<tr>
<td></td>
<td>• Prior consultation with the National Crisis Management Office</td>
<td>• Start an emergency work system ※ Rapid response</td>
</tr>
<tr>
<td>Substantial</td>
<td>• Issue Substantial</td>
<td>• Assess damage and report</td>
</tr>
<tr>
<td></td>
<td>• Subject: MSIP</td>
<td>• Start an emergency work system ※ Tighten security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Increased possibilities to have a serious security incident and damage</td>
</tr>
<tr>
<td>Moderate</td>
<td>• Issue Moderate</td>
<td>• Make a public announcement</td>
</tr>
<tr>
<td></td>
<td>• Subject: MSIP</td>
<td>• Tighten monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Start an emergency work system ※ Observe signs</td>
</tr>
<tr>
<td>Normal</td>
<td>• Normal Situation</td>
<td>• Follow protocols as usual</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Consult with the NIS and MND, and report to the BH National Crisis Situation Center</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyze causes, prevent spread of accident and support recovery</td>
</tr>
</tbody>
</table>
KISC cooperates with the National Police, NIS, and the Ministry of National Defense to respond to cyber threats and provides related information to private companies.
Cyber Incidents Response (Process)

**Prevention**
- Security Prevention
- CII Protection
- ISMS-PIMS
- Security Guide
- Cyber Safety Diagnosis
  - CII
  - Public Online Services
  - Web Hard
  - ISMS Certification
- Awareness Enhancement
  - Media, KrCERT Website
  - Domestic, International Drill

**Collection & Detection**
- 24/7 Monitoring
- Domestic Internet Traffic
- DNS, Major Websites
- New MC, Vulnerabilities
- Cyber Hot Line 118
- DDoS at IX Node
  - Installed a DDoS Defense System at 11 ISPs
  - Web-embedded MC
  - Monitor 3.2 million Domestic Websites
- Bug Bounty Program

**Analysis & Measures**
- MC & Vulnerability Analysis
- Block Harmful URL/IP
- DDoS Shelter Service
- Cyber Curing Service
  - Notify Malware Infection (PC, Smartphone Users)
  - Provide a Dedicated AV
- Cyber Fraud
  - Phishing
  - Pharming,
  - Smishing
  - Voice phishing
- Bilateral Cooperation

**Sharing & Recovery**
- C-TAS
  - Cyber Threat Information
- Gathering
- Analysis
- Exchange
- Technical Support
  - On-spot Investigation
  - Provide Countermeasures
- Cyber Threat Warning Level
  - Normal
  - Moderate
  - Substantial
  - Severe
  - Critical
Prevention

**ISMS** (Information Security Management System)

**CIIP** (Critical Information Infrastructure Protection)

- Energy
- Banking
- Defense
- Transportation
- Internet Data Center
- Major Companies
- Internet Service Provider
- ICT Service Provider
- Clinics
- Pharmacies
- Small Companies
- Internet Cafe
- SMEs
Prevention: CIIP (Critical Information Infrastructure Protection)

- Protect CIIP from various cyber attacks in the areas of communications, finance, and energy
  * ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

**Committee on Protection of Information and Communications Infrastructure**

- Ministry of Science, ICT and Future Planning: Support the Private Sector
- Prime Minister’s Office: Prime Minister (Chairperson)
- NIS: Support the Public Sector

**Infrastructure Protection Procedures**

1. Analyze and evaluate vulnerabilities
2. Establish cyber security measures
3. Draw a cyber security plan
4. Deliberate and make a decision

Prevention: ISMS & SECU-STAR

- **ISMS**: Grant a certification by examining an information system which is constructed and operated in accordance with the criteria predetermined by the law
  - Subject: Major ISPs, IDC, ICT Service Providers (Check 104 criteria including managerial, technical, physical protection measures)
  - Terms of Validity: 3 years (annual evaluation)

- **SECU-STAR**: A method used to rate information security readiness
  - Primary Subject: SMEs
  - Measures: Rating agencies evaluate information security readiness and rate accordingly
  - Check 30 criteria such as infrastructure, activities, etc.
  - 27 enterprises received certification (‘14.11 ~ ’16.1)
Collection & Detection : 24/7 Monitoring

Monitor Abnormalities of Domestic Internet Networks for 24/7

- **Traffic**: Local Internet Service Provider, Ports, Protocols, Attacks
- **Web Servers**: 900+ Major Domestic Web Servers
- **DNS**: 13 Root DNS, 6 KOR DNS, 12 Major Domestic ISP DNS
- **Security Information**: Major Anti-Virus, System/Software/Security Company Sites
- **Monitor Web-embedded Malicious Codes**
- **Hotline**: ISPs, Anti-Virus Vendors, NCSC, and etc.
Collection & Detection: Malicious Code Detection System

- Monitor web-embedded malicious codes (3.2 million domestic websites)
- Enhance security of domestic websites and Internet users
Analysis & Measures: DDoS Defense System

- Early Detection of DDoS Attacks at Internet Exchange (IX) Node
Analysis & Measures: Mobile Cyber Curing System

- Provide a Cyber Curing Service to Smartphone Users
  - **KISA**
    - Analyze malicious applications and get malicious URLs
  - **Telecom.**
    - Find infected smartphones, notify and delete malwares

**Collectors**
- Smishing Messages
  - Malware Report

**KISA**
- 1. Collect Malicious Apps
- 2. App Analysis
- 3. Sending Malicious URLs
- Mobile Cyber Curing System

**Telecom. Company**
- 4. Find Infected Phones Accessing Malicious URLs

**Infected Phone Users**
- 5. Send Push Messages
- 6. Delete Malicious Apps

Ministry of Science, ICT and Future Planning
Sharing & Recovery: Cyber Threat Analysis & Sharing System (C-TAS)

- C-TAS was developed for rapid incident response with systematized processes of cyber threat information gathering, analysis and exchange.

### Information Gathering
1. Cyber Threat Incident Info.
2. Detection Log
3. Malware
4. Malicious Domain
5. Vulnerability

### Storage
Integration & Profiling

### Comprehensive Analysis
Correlational Analysis

### Information Exchange
- Make Anti-virus
- Patch Vulnerability
- Block Malicious Site
- Share Analysis Report
Sharing & Recovery: Global CSIRT Communities

Actively Participate in CSIRT Communities as a Global Leader in Cybersecurity

To Create Safe, Clean and Reliable Cyber Space in the AP Region through Global Collaboration

Regional CSIRT Community In Asia-Pacific

- National CSIRTs in the Asia-Pacific Region
  - 28 teams from 20 countries
- Founding Members
- Steering Committee
  - Vice Chairperson in 2014~2015
- Membership Working Group Convener
  - Encourage a membership in the region
- Annual Conference, Annual Drill
  - 2011 Annual Conference in Jeju
  - Participated in drills and led drills in 2004~2006

Global CSIRT Community

- All CSIRTs (national, vendor, academy, etc.)
  - over 350 teams from more than 70 countries
- Real-time information sharing via mailing
  - Trends, vulnerabilities, and etc.
- Discussions, Standard, Special Interest Groups
  - CVE, TLP, Malware Analysis, and etc.
- Annual Conference and Technical Seminars
  - 28th Conference in Seoul (2016)
- 8 Full Members in Korea
  - KrCERT/CC supports applicants in Korea
Cybersecurity Industry Promotion
Nurturing Global Startups

Laying the Foundation

< Information Security Cluster >

Response Facility
(Internet Incident Response Center)

R&D Center

Manpower Development Center

Create Synergy Effects

Seeking Startups

< Startup Support Programs >

✓ K-Global Project
✓ Information Security Specialized College
✓ Employment-based Masters Program
✓ ITRC
✓ Information Security College Organizations
✓ Military Specialists and Cyber Conscripted Policemen

Collaboration with Partners

Nurturing & Supporting

<Global Incubator and Accelerator>

Link to Global Incubators
* Global fund (ex. Yozma Group)

Link to Global Accelerator*
* Mach37, Mass Challenge, and etc.

Provide a Mentoring Service to be a Part of Global Ecosystem

Nurture Globalized Startups
Technology Sharing Platform

Constructing a R&D Cooperation System

Integrate and share a trend of cybersecurity technology development and product and service information to support commercialization of R&D results

- Support enterprises by sharing results of a government-funded R&D in the cybersecurity area to enhance technical skills of SMEs and strong SMEs which lack internal financing capability and R&D competence
## Investment in Cybersecurity

### Expand investment demand & Improve fundamentals

<table>
<thead>
<tr>
<th>Expand Investment in the Public Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Gradually increase cybersecurity budget as one of the top investment priorities</td>
</tr>
<tr>
<td>(2016: 6% → 2020: 15%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encourage Investment in the Private Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide more incentives to encourage voluntary investment from the private sector</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Diffuse a Culture of Receiving Proper Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Raise a price level of security continuity service comparably with commercial SW maintenance service</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Improve Industry Fundamentals</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Make tailored policies by diagnosing current status of local industry and improve fundamentals with focus on excellent information security technologies and companies</td>
</tr>
</tbody>
</table>
Regional Offices for Cooperation

**Regional Offices**

**Networking Platform**

**Expand Partnership**

**SOUTH AMERICA** (Costa Rica)
- E-gov’t, expert training, incident response model
- Peru, Nicaragua, Paraguay, and more

**MIDDLE EAST** (Oman)
- Digital forensics and incident response model
- UAE, Qatar, Iran, and more

**AFRICA** (Tanzania)
- KISC model (Best practice: Rwanda)
- EAC, Gabon, Senegal, Botswana, and more

**SOUTHEAST ASIA** (Indonesia)
- Expert training, mutual industry exchange
- India, Vietnam, Cambodia, and more
Cybersecurity Capacity Building

Cybersecurity Capacity Building Initiative

APISC CSIRT Training Program

Needs based Assistance

- Invitation-based training or local workshops
- Security Policy and Technology courses
- Tailored to a recipient country
- Held cybersecurity workshops

Form a Trust-Worthy Relationship

- 5-Day training program
- CSIRT operation and establishment
- Know-how sharing
- 237 participants from 47 countries since 2005
Thank you