Cyber attack and incident response

Private sector's perspective for public/private information sharing

6 June 2012
Octopus Conference at Strasbourg
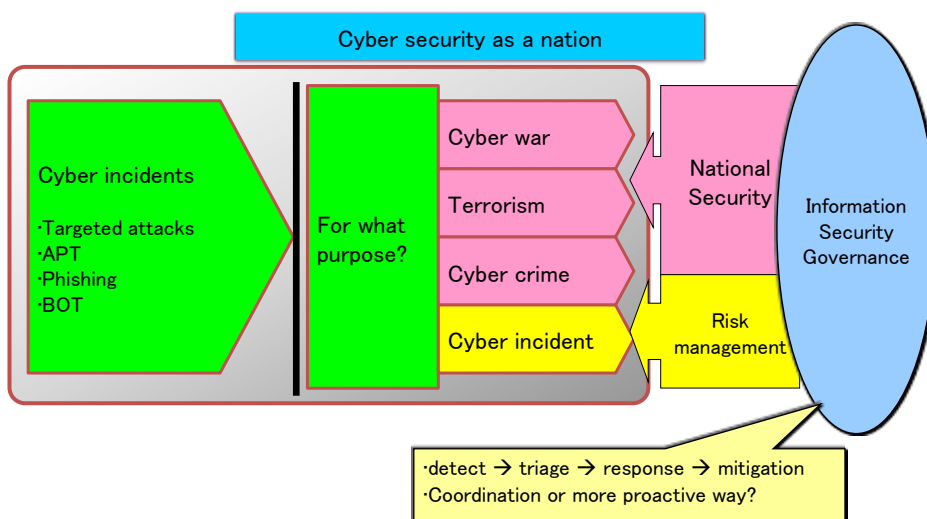
Tomohiko Yamakawa

Information security or cyber security?

·Information security is for company itself
· (compliance, data protection, risk management, etc.)
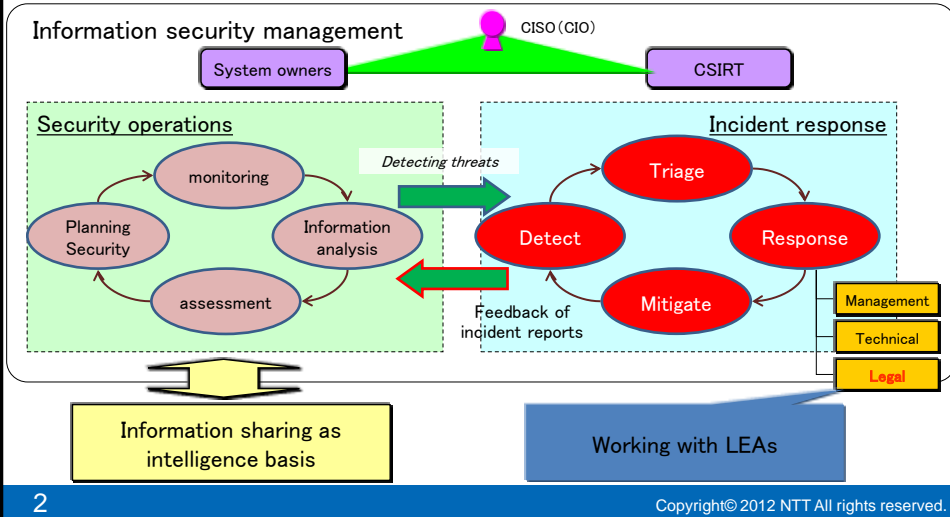·Cyber Security as a nation (National Security)

For newest threats... (just personal opinion ;)

·Process of information security management is separated into two parts; "security operation" and "incident response"
·Traditional style of working with LEA would be recognized as a process of "legal response" of incident response.
•"Information sharing as intelligence basis" should be recognized as another process.

Information security management

CISO（CIO）

System owners — CSIRT

Security operations
- monitoring
- Planning Security
- Information analysis
- assessment

Detecting threats →

Incident response
- Triage
- Detect
- Response
- Mitigate

Feedback of incident reports

Management
Technical
Legal

Information sharing as intelligence basis

Working with LEAs

Issues for discussion

► What are the cybersecurity challenges you have been facing as industry (Botnets? Phishing attacks ? Targeted attacks?)

- ► All kinds of incidents and attacks should be "challenges"
- ► Especially against *targeted attacks* new style "information sharing is expected. (not the same as those of DDoS and Botnets)
- ► Not only as just "coordination" by CSIRT but "intelligence base" knowledge should be shared.
- ► Issue of "compliance" remains.

Issues for discussion (continued)

- What are the innovative approach we have developed in Japan to respond to these challenges (did you start collecting data on online threats in new ways? Did you start to share data or intelligence in new ways?)

  - Just started the discussion about new scheme for information sharing between public and private sectors
  - Amendment of "Act on the Prohibition of Unauthorized Computer Access"

- Sharing information with organizations in other countries

  - Within a scope of "Due Process"
  - Appropriate legal framework is expected
  - Issue of information sharing for private sector

4

Just FYI...

5

About NTT Group

NTT group develops businesses in broad fields as a forerunner of the ubiquitous broadband era.

NTT's Voting Rights Ratio: 100%
NIPPON TELEGRAPH AND TELEPHONE EAST CORPORATION
(Regional Telecommunications Services)

Total Assets: ¥3.765 trillion   Number of Employees: 5,900
Operating Revenues: ¥1.9571 trillion   Paid-in Capital: ¥335 billion

NTT's Voting Rights Ratio: 100%
NIPPON TELEGRAPH AND TELEPHONE WEST CORPORATION
(Regional Telecommunications Services)

Total Assets: ¥3.4077 trillion   Number of Employees: 5,500
Operating Revenues: ¥1.758 trillion   Paid-in Capital: ¥312 billion

NTT's Voting Rights Ratio: 100%
NTT Communications Corporation
(Domestic long-distance and International Telecommunications Services)

Total Assets: ¥1.1637 trillion   Number of Employees: 8,150
Operating Revenues: ¥1.334 trillion   Paid-in Capital: ¥211.7 billion

NTT's Voting Rights Ratio: 54.2%
NTT DATA Corporation
(Data Telecommunications Services)

Total Assets: ¥1.4686 trillion   Number of Employees: 50,000
Operating Revenues: ¥1.1619 trillion   Paid-in Capital: ¥142.5 billion

NTT's Voting Rights Ratio: 66.4%
NTT DOCOMO, INC.
(Mobile Telecommunications Services)

Total Assets: ¥6.7916 trillion   Number of Employees: 22,950
Operating Revenues: ¥4.2243 trillion   Paid-in Capital: ¥949.7 billion

NTT

NIPPON TELEGRAPH AND TELEPHONE CORPORATION
(Holding Company)

Total Assets: ¥7.5702 trillion   Number of Employees: 2,900
Operating Revenues: ¥390.3 billion   Paid-in Capital: ¥937.9 billion

Major Businesses:
Planning management and strategies for the NTT Group;
Encouraging fundamental R&D efforts

Total Assets: ¥19.6656 trillion
Operating Revenues: ¥10.1814 trillion
Number of Employees: 219,350
Number of Consolidated Subsidiaries: 756

(The above figures are as of FY2010 year-end.)

6

"Information Security" as Corporate Social Responsibility

7

NTT Group CSR Charter

Our Commitment

As a leader of the information and telecommunications industry, the NTT Group is committed to providing reliable, high-quality services that contribute to the creation of a safe, secure and prosperous society through communications that serve people, communities, and the global environment.

Our CSR Goals

· Communication between people and their communities
   1. We shall strive to create a richer and more convenient communications environment, and utilize our technology to contribute to the resolution of the various issues faced by societies with aging and declining populations.

· Communication between people and the global environment
   2. We shall strive both to reduce our own environmental impacts and build environment-friendly forms of communications, and to provide information and communications services that help to reduce the impact of society as a whole on the global environment.

   Safe and secure communication
   3. While striving earnestly to ensure information security and resolve telecommunications-related social issues, we shall do our utmost to provide a safe and secure user environment and contribute to the creation and future development of communication culture.
   4. Fully recognizing the role that telecommunications plays as critical infrastructure supporting society and protecting our livelihoods, we shall strive to offer secure and reliable telecommunications services fortified to withstand disasters and capable of connecting people irrespective of time, location and other circumstances.

· Team NTT communication
   5. As Team NTT, we pledge to apply the highest ethical standards and awareness of human rights to our business duties, striving to fulfill our mission to society by working for the creation of pleasant workplaces, personal growth, and respect for diversity, and for the further development of a flourishing and vibrant community.

− Team NTT comprises all NTT Group employees, including temporary employees, contract employees, employees of our corporate partners, and also former employees who endorse the NTT Group's CSR activities.

From NTT Group CSR report 2011

NTT CERT: Supporting security across the NTT Group

NTT Group

A computer security incident response team (CSIRT) is an organization that gathers information on computer security threats, investigating them, and implementing appropriate response activities. NTT-CERT, operated by the NTT Information Sharing Platform Laboratories, is the CSIRT for the NTT Group.

In addition to handling inquiries regarding NTT Group information security, NTT-CERT also works with security managers and system administrators of group companies to minimize security threats. It helps, for example, to test the security of Web servers used by group companies, as well as conducting experiments and providing consulting support related to the security of the next-generation network (NGN) provided by NTT East and NTT West.
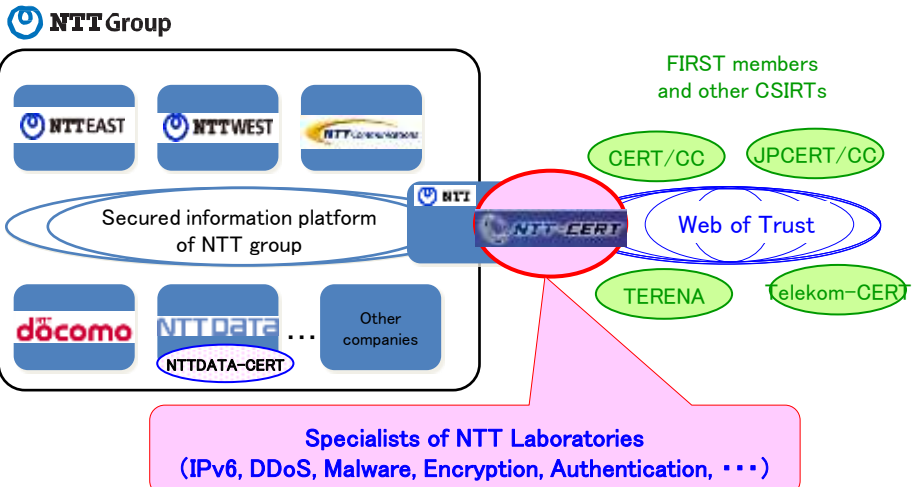
In fi scal 2011, it assisted in countering VoIP phone highjacking-based international call transmission and other attacks, and also helped around the clock with the NTT Group's cyber attack countermeasures during the APEC conference held in Yokohama. It has also begun to research technologies for enhancing the security of smartphones, which are now spreading rapidly in Japan.

NTT-CERT contributes to improving the security level not only of the NTT Group, but also of Japan as a whole by helping to recruit members to the Nippon CSIRT Association∗ and promoting its activities, including the introduction of a program for building and operating CSIRTs.

∗A Japanese CSIRT organization established in April 2007 by NTT-CERT, JPCERT/CC, and others

Coordination for security incident response as NTT Group

- · "Web of Trust" with other CSIRTs globally
- · As centre of excellence of information security for NTT group
- · Providing knowledge to NTT group companies

NTT Group

NTT EAST NTT WEST NTT Communications

Secured information platform of NTT group

NTT

NTT-CERT

docomo NTT DATA ... Other companies

NTTDATA-CERT

FIRST members and other CSIRTs

CERT/CC JPCERT/CC

Web of Trust

TERENA Telekom-CERT

Specialists of NTT Laboratories
(IPv6, DDoS, Malware, Encryption, Authentication, ···)

10

Thank you !

The Government of Japan supports the CoE Global Project on Cybercrime.

Between 6th to 8th in the Foyer of the Committee of Ministers, an exhibition "Tsunami in Japan, towards a better future" is organized.
All participants are welcomed.

11