International Cooperation:
Opportunities & obstacles of sharing of information across borders

2:30-4:00, Tuesday
15 September 2015
Introduction

• **Session Facilitator:** Jamie Clark
  General Counsel, OASIS

• Ken Ducatel
  Chief Information Security Officer, European Commission

• Ryuichi Hirano
  Counsellor, National center of Incident readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat, Government of Japan

• Adam Sedgewick
  Senior Information Technology Policy Advisor, National Institute of Standards and Technology
Information Sharing & Reporting for Cybersecurity in the EU context

Ken Ducatel
European Commission - CISO
The EU Context

• Legislative requirements for breach notification
  • Breach notifications for telcom providers (already law since 2009 Art 13a Framework Dir and Art 4 of e-privacy Dir)
  • eIDAS Art 15 for trust service providers
  • NIS Directive and General Data Protection Regulation proposals still under discussion

• Information sharing
  • Member States (NIS Directive proposals)
  • ENISA: providing cyber threat intelligence and capacity building
  • Between EU institutions (CERT-EU)
  • Inside the European Commission
Breach notifications by law (NIS directive):

- operators of critical infrastructures in some sectors (financial services, transport, energy, health),

- enablers of information society services (app stores e-commerce platforms, Internet payment, cloud computing, search engines, social networks)

- and public administrations

must adopt risk management practices and report (notify) national authorities major security incidents on their core services.
Exchange of threats, know-how and incidents

a) NIS Directive: creation of a cooperation mechanism among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure, cooperate and organise regular peer reviews.

b) European Commission: CISO/DG DIGIT; the Directorate for Security and other Local IS Officers

c) ENISA (European Union Network and Information Security Agency):

d) CERT-EU: Works for the 60+ EU Institutions and Agencies
National/governmental CERTs

ESTABLISHED IN 2005:
- Finland
- France
- Germany
- Hungary
- The Netherlands
- Norway
- Sweden
- United Kingdom

SITUATION IN 2014:
- Armenia
- Austria
- Belgium
- Bulgaria
- Croatia
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Georgia
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Israel
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- Turkey
- Ukraine
- United Kingdom
- EU Institutions

IT Security in the EU Institutions: Organisationally complex
(source RAND for the EP 2013)
The next 5 years: ENISA activities
EU Institutions’ own CERT
Created 6/2011, operational four months later
Supports 60+ entities
Supporting defense against targeted cyber threats
Single point of contact
1. **General Provisions**
   - Purpose/Definition/Basic Principles/Responsibility...

2. **Cybersecurity Strategy**
   - Comprehensive and effective promotion of cybersecurity policy
   - Cabinet decision/Report to the Diet

3. **Basic Policy**
   - Assurance at Administrative Organs
   - Assurance at Critical Infrastructure Operators
   - Facilitation of voluntary activity of Private enterprises
   - Cooperation with multiple stakeholders
   - Crackdown on cybercrime and prevention of damage
   - Action for matters which may critically affect the National security
   - Enhancement of Industrial development
   - Promotion of R&D, Education, International Cooperation
   - Development of Human resources

4. **Cybersecurity Strategic Headquarters**
   - The Headquarters shall be established under the Cabinet
   - National cybersecurity strategy, evaluation, coordination

---

**Government Organization**

- **Cabinet of Japan**
  - IT Strategic Headquarters (Director-General: Prime Minister)
  - NSC (Chair: Prime Minister)
  - Information Security Policy Council

---

- **Cybersecurity Strategic Headquarters**
  - (Director-General: Chief Cabinet Secretary)

---

**National Information Security Center (NISC)**

- National center of Incident readiness and Strategy for Cybersecurity
New “Cybersecurity Strategy of Japan” (Outline)

1 Understanding of Cyberspace
- Blessings of Cyberspace: Generating infinite values, essential foundation for our socio-economic activity
- “Hyper-connected and converged society” is coming
- Cyber threats are becoming more serious and being perceived as national security matters

2 Objective
- Develop and advance free, fair, and secure cyberspace subsequently contribute to:
  1) Socio-economic vitalization
  2) Safe and secure society
  3) International Peace and Stability

3 Principle
- 1. Free Flow of Information
- 2. Rule of Law
- 3. Openness
- 4. Self-governance
- 5. Cooperation among Multi Stakeholders

4 Policy Measure

1) Socio-Economic Vitalization and Sustainable Development
- From Cost to Investment
  - Creating Secure IoT System
  - Promoting Management with cybersecurity mindset
  - Improving Business Environment

2) Realizing a Safe and Secure Society for the People
- Foundation for 2020, further
  - Protecting People and Society
  - Protecting CII
  - Protecting Governmental Agencies

3) Peace and Stability of International Community and Japan’s National Security
- Proactive contribution to peace in cyberspace
  - Ensure Japan’s National Security
  - International Peace and Stability
  - International Partnership

CrossCutting
- R&D
  - Improving detection and protection capabilities
- Human Resources
  - Developing multi-talent, practical training, promoting skill standards

5 Organization
- Enhancement cooperation with public and private sector, Institution building toward the Tokyo Olympic and Paralympic Games in 2020
International Cooperation in Cybersecurity and Standards

15 September 2015

Adam.Sedgewick@nist.gov
Obama Administration’s Priorities on Cyberspace

1. Protecting the country's critical infrastructure — our most important information systems — from cyber threats.
2. Improving our ability to identify and report cyber incidents so that we can respond in a timely manner.
3. Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.
4. Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.
5. Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.
Cybersecurity at NIST

• Non-Regulatory role in cybersecurity began in 1972 with the development of the Data Encryption Standard – began when commercial sector also has a legitimate need for cryptography, including in ATMs.

• Using widely-accepted standards helps create competitive markets around market need through combinations of price, quality, performance, and value to consumers. It then promotes faster diffusion of these technologies throughout industry.

  • Ensure timely availability of standards, and associated testing, that address identified NIST IT Laboratory priorities, including national priorities established in statute or administration policy;
  
  • Achieve cost-efficient, timely and effective solutions to legitimate regulatory, procurement and policy objectives;
  
  • Promote standards and standardization systems that enable innovation and foster US competitiveness; and
  
  • Facilitate international trade and avoid the creation of unnecessary obstacles to trade.
Key NIST Information Sharing Projects

• NIST has worked on security automation and continuous monitoring standards and test tools. The standards support:
  • Identification of IT Assets
  • Awareness of the operational state of computing devices
  • Standardized security reference data
  • Analysis of security control effectiveness measures

• NIST helped develop Security Content Automation Protocol (SCAP) and move it to the IETF standards body.

• NIST hosts the National Vulnerability Database (NVD) to maintain a database of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

• Draft SP 800-150, Guide to Cyber Threat Information Sharing to provide organizations with guidance on establishing, participating in, and maintaining information sharing relationships throughout the incident response life cycle.
“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”

President Barack Obama
Executive Order 13636, Feb. 12, 2013

- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work
International Aspects, Impacts, and Alignment of the Cybersecurity Framework

- Because the Framework references globally accepted standards, guidelines, and practices, organizations inside and outside of the United States can use the Framework to efficiently operate globally and manage new and evolving risks.

- "Cybersecurity risks and threats are a global problem, and the more the Framework can be socialized globally, especially among governments and those agencies that deal with cyber issues, the better." - ISACA

- We are working with standards developing organizations, industry, and sectors to ensure the Cybersecurity Framework remains aligned and compatible with those existing and developing standards and practices.
• To ensure cybersecurity and resiliency of U.S. information and communications systems and supporting infrastructures, we must develop and use robust cybersecurity standards and assessment schemes
• Four key (and interrelated) objectives for standards and assessment:
  • Enhancing national and economic security and public safety
  • Ensuring standards and assessment tools are technically sound
  • Facilitating international trade
  • Promoting innovation and competitiveness
• Standards developing bodies that develop standards through open, transparent, impartial, and consensus-based processes and are globally relevant are strongly preferred
Resources
Where to Learn More and Stay Current

The National Institute of Standards and Technology Web site is available at http://www.nist.gov


The Framework for Improving Critical Infrastructure Cybersecurity and related news and information are available at www.nist.gov/cyberframework

For additional Framework info and help cyberframework@nist.gov
#BorderlessCyber

Questions ?