Overview of Information Security Management Activities Undertaken within ITU-T SG 17 and ISO/IEC JTC1/SC 27

KDDI Corporation
NICT Incident Response Group Leader
Rapporteur of ITU-T SG17 Question 7
ISO/IEC SC27/WG1 National Convener

Koji NAKAO
Network dependency and Security Incidents now co-relatively getting bigger and bigger

- Popularization of Broadband communication environment

- Network dependency is getting higher and higher
  - Various and advanced use of internet

- Increasing Security Threads
  - Security Incidents are getting serious by Slammer, Blaster, Sasser worms, Botnets.

  - Malignant worms are getting skillful and integrated.
  - A lot of internet users do not care to apply Security Patches.
  - Network itself is now included as a target of attacks.
Threats in our surroundings

ICT Security Incidents:
1) Scans & Probes, 2) Computer Intrusions, 3) Malicious Software (Viruses, etc.), 4) Computer Sabotage & Damage (e.g. by DoS attacks), 5) Information theft and Espionage, 6) Impersonation
Threats: Internet Attacks

- Botnet
- Online Business Botnet Controller (IRC Servers)
- DNS Servers (Pharming Attacks)
- Virus/Worms
- Authors
- Organized Crimes Syndicates

Internet Attacks
- Social Engineering (IM/Emails/P2P/In-person)
- Web Defacements
- Denial of Service
- Open Proxies
- Open Mail Relays
- Phishing Web Sites
- Phishers' "Safe Houses"
- Spammers
- Open Proxies
- Open Mail Relays
- Phishers
- Phishing Web Sites
- Organized Crimes Syndicates
- Producing Sypware/Trojans/Rootkits
- Viruses/Worms
- Botnet Herders
- Botnet Controller (IRC Servers)
- DNS Servers (Pharming Attacks)
- Spammers
- Social Engineering (IM/Emails/P2P/In-person)
- Virus/Worms
- Authors
Real-time packet source visualization

Visualizing source of incoming packets at our darknet
3-D display of real-time incoming packet flow
If there are no appropriate security countermeasures in the organization, the following RISKs can be assumed for example:

- **Loss of**
  *customer services, sales and market share
  *revenue, income and financial stability
- **Damage to**
  *customer trust and confidence
  *image, reputation and brand name
- **Non-compliance with legislation**
First, what do we have to **PROTECT**?

→ **Information Assets in Organization**

**Information Assets:**
- Anything related to “Information” that has value to the organization
Example of a Security Incident

Leakage of 560,000 **Customer Information** was detected in 2003.

- Lack of Confidence
- Apology to the customers,
- Sent Gift Coupons to the customers (damage: 5 million $)
Risk is assessed by using Threats, Vulnerability, and Assets. Risk can be calculated by "Threats" x "Vulnerability" x "Importance of Assets". Security Controls are indispensable!
Risks in Organizations: Risk Analysis

1st Step: Identification of all information assets

- Customer Information
- Human affairs information
- Management strategy information
- New service information

2nd Step: Risk Assessment

- Implementing controls selected to reduce risk for example,

3rd Step: Risk Treatment

- Risk acceptance level
Information Security Management System (ISMS) is necessary; PDCA model.
Information Security Management System (ISMS) established and maintained in Organizations

1. Security policy
2. Security organisation
3. Asset classification & control
4. Personnel security
5. Physical & environmental security
6. Communications & operations management
7. Access control
8. Systems development & maintenance
9. Business Continuity
10. Compliance
The 27000 Family of ISMS Standards in ISO/IEC
Hierarchical Security Management Model
(SC 27 View)

- **Terminology**
- **Principles**
  - provide generally accepted high-level basic rules used as a foundation to guidance
- **Frameworks**
  - provide a simplified description of interrelationships used to organize concepts, methods and technologies
- **Element Standards**
  - provide specific requirements that apply to a defined area of security management
- **Application Guides and Supplements**
  - provide detailed descriptions offering guidance on how element standards may be applied in specific situations
- **Toolbox of Techniques**
Hierarchical Security Management Model
(SC 27 View discussed in WG1)

Terminology
- ISO Guide 73
- SC 27 SD 6 Updated and harmonized
- Vocabulary & concepts (27000)

Principles

Frameworks

Element Standards
- Code of Practice for (27002/17799)
- ISMS Implementation Guidance (27003)
- ISM Measurements (27004)
- Risk management (27005)

Application Guides and Supplements
- Accreditation (27006)
- Financial ISMS Guide (TC 68)
- Telecom ISM Guide (27011) (ITU-T X.1051)
- Healthcare ISMS Guide (TC 215)

Toolbox of Techniques
- Info Security Incident Management (TR 18044)
- IT Intrusion Detection Framework (TR 15947)
- IT Network Security (IS 18028 / ITU-T X.???)
- Guidelines for TTP Services (IS 14516 / ITU-T X.842)
Evolution on Information Security Management (Guideline)

- BS 7799-1:1995
- BS 7799-1:1999
- ISO/IEC 17799:2000
- ISO/IEC 17799:2005
- BS 7799-2:1998
- BS 7799-2:1999
- ISO/IEC 27001:2005

Code of practice for information security management
15th June 05

ISMS requirements
15th Oct 05
Structure of ISMS Standards in ISO

- **27000 Family**
  - **27001**: ISMS requirements
  - **27002**: ISMS implementation guidelines
  - **27003**: ISMS Accreditation Guidelines
  - **27004**: ISM measurements
  - **27005**: ISMS Risk Management
  - **27006**: Code of practice

- **Fundamentals and vocabulary**

- **17799**: Code of practice
ISO/IEC 27001 Information security management system requirements

- **Fact Sheet**
- This was published on the 15\textsuperscript{th} Oct 05
- It is a certification and auditable standard and it replaces BS 7799-2:2002
- Based on a mandatory risk based approach and aims at achieving effective information security through continual improvement process
- Includes an Annex (Annex A) which lists the controls from 17799 with the ‘should’ replaced with the mandatory ‘shall’
- Uses the same PDCA management systems process model as ISO 9001 (QMS) and ISO 14001 (EMS)
ISO/IEC 17799 Code of practice for information security management

**Fact Sheet**

- The revised 2000 version of this standard was published on the 15th June 05
- This is **NOT a certification and auditable standard** – it is a code of best practice
- It aims is to provide a catalogue of **non-mandatory best practice** with some implementation guidelines – the controls in 17799 are contained in ISO/IEC 27001 Annex A as mandatory ‘shall’ statements.
- From April 2007 ISO/IEC 17799 is expected to be renumbered as 27002
ISO/IEC 27002 (17799)
Policies, Procedures, Technical & non-technical controls

• **11 Management Domains**

<table>
<thead>
<tr>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security policy</td>
</tr>
<tr>
<td>Organising information security</td>
</tr>
<tr>
<td>Asset management</td>
</tr>
<tr>
<td>Human resources security</td>
</tr>
<tr>
<td>Physical &amp; environmental security</td>
</tr>
<tr>
<td>Communications &amp; operations management</td>
</tr>
<tr>
<td>Access control</td>
</tr>
<tr>
<td>Information systems acquisition, development and maintenance</td>
</tr>
<tr>
<td>Information security incident management</td>
</tr>
<tr>
<td>Business continuity management</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
</tbody>
</table>

- **Information**
- **People**
- **Services**
- **Applications**
- **Physical**
- **ICT**
- **Business processes**
Standardization Overview on Security Management for telecommunication in ITU-T SG17 WP2
Study Group 17 Security Questions 2005-2008

Security Management
*ISM-Guidelines for Telecom
*Incident Management
*Risk Assessment Methodology
*etc…
*X.1051

Telecom Systems Users

Telebiometrics
*Multimodal Model Framework
*System Mechanism
*Protection Procedure
*X.1081

Q7/17

Secure Communication Services
*Mobile Secure Communications
*Home Network Security
*Security Web Services
*X.1121, X.1122

Q9/17

Cyber Security
*Vulnerability Information Sharing…
*Incident Handling Operations
*Security Strategy
*Countering SPAM

Q6/17

Communications System Security
*Vision, Project Roadmap, Compendia, …

Q4/17

Security Architecture & Framework
*Architecture, Model, Concepts, Frameworks, etc…
*X.800 series
*X.805

Q5/17

Q8/17

Q17/17
Designs and Specifications of Secure Application Services and Protocol

Techniques of Telebiometorics for any applications

Techniques of Cyber-Security for any applications

Security Architecture and Framework on Telecommunications Services

Security Management Guidelines for Telecommunications
Security Management working scopes in Q7

**Information Security Management Guidelines for telecommunications**
(Existing X.1051, Information security management system – Requirements for telecommunications (ISMS-T) )

- Jointly develop a guideline of information security management with ISO/IEC JTC 1/SC 27.

**Risk Management Methodology**

- Study and develop a methodology of risk management for telecommunications in line with Recommendation X.1051.
- Produce and consent a new ITU-T Recommendation for risk management methodology.

**Incident Management**

- Study and develop a handling and response procedure on security incidents for the telecommunications in line with Recommendation X.1051.
- Produce and consent a new ITU-T Recommendation for incident management methodology and procedures.
Revised Recommendation X.1051

Information Security Management Guidelines for telecommunications based on ISO/IEC 27002 under Question 7/SG17
Introduction of Information security management guidelines for Telecommunications (Revised X.1051)

Revised X.1051

- Security policy
- Organising information security
- Asset management
- Human resources security
- Physical & environmental security
- Communications & operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Figure 1 – PDCA model applied to ISMS processes
Approach to develop the revised Recommendation X.1051

ISO/IEC 17799 (2005)  | Revised X.1051  | Existing X.1051
Brief Introduction of revised X.1051

Main elements of information security management guideline for telecommunications

① ISO/IEC 17799 (2005)
② ITU recommendations ISMS-T (X.1051)
③ Legal requirements for telecommunications

① ISO/IEC 17799 (2005)
→ Strategies in 11 areas for general business

Control
1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance


③ Legal requirements for telecommunications organizations

Telecommunications Business Law
① Protecting the confidentiality of communications
② Priority treatment for important communications
③ Delineation of responsibilities

Other legislation relevant to telecommunications

Information Security Management Guidelines for Telecommunications based on ISO/IEC 27002
Importance of information security management in telecommunications organizations

Considerations on Information security for telecommunications organizations

Ex 1: Telecommunications organizations should consider that telecommunications equipment and facilities are used by users of telecommunications services outside the organization, in addition to consider that information processing facilities are used by employees and subcontractors internal the organization.

Ex 2: Telecommunications organizations provide telecommunications services by means of interconnecting, sharing telecommunications equipments with other telecommunications organizations, and by means of using telecommunications business of services of other telecommunications organizations. The information security of telecommunications organizations is mutually dependent.

Ex 3: Business continuity plan is strongly required for telecommunications organizations since threats such as cyber attacks, viruses and worms are increasing on the Internet. Additionally, they should ensure compliance and prevent violation of the relevant legislative requirements with respect to ensuring the confidentiality of communications and protecting personal information.

Telecommunications organizations are required to consider additional considerations with ISO/IEC 17799 to further ensure their information security.
### Structure of Descriptions in revised X.1051

#### 11 Security Management Areas

<table>
<thead>
<tr>
<th>No.</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Security Policy</td>
</tr>
<tr>
<td>6</td>
<td>Organization of Information Security</td>
</tr>
<tr>
<td>7</td>
<td>Asset Management</td>
</tr>
<tr>
<td>8</td>
<td>Human Resources Security</td>
</tr>
<tr>
<td>9</td>
<td>Physical and Environmental Security</td>
</tr>
<tr>
<td>10</td>
<td>Communications and Operation Management</td>
</tr>
<tr>
<td>11</td>
<td>Access Control</td>
</tr>
<tr>
<td>12</td>
<td>Information systems acquisition, development and maintenance</td>
</tr>
<tr>
<td>13</td>
<td>Information security incident management</td>
</tr>
<tr>
<td>14</td>
<td>Business continuity management</td>
</tr>
<tr>
<td>15</td>
<td>Compliance</td>
</tr>
</tbody>
</table>

#### Objectives

- Objective
- Controls
- Implementation guidance
- Related information

- Add “objective” for telecommunications
- Add “controls” for telecommunications
- Add “implementation guidance” for telecommunications
- Other information

(Same structure as ISO/IEC 17799(2005))
0. Introduction
1. Scope
2. Terms and definitions
   2.1 Terms and definitions for information security in general
   2.2 Terms and definitions for information security in telecommunications organizations
3. Structure of this Guideline
4. Information security management systems in the telecommunications industry
   4.1 Goal
   4.2 Information assets to be protected
   4.3 Establishment of information security management
5. Security policy
   5.1 Information security policy
6. Organization of information security
   6.1 Internal organization
   6.2 External parties
7. Asset management
   7.1 Responsibility for assets
   7.2 Information classification
8. Human resources security
   8.1 Prior to employment
   8.2 During employment
   8.3 Termination or change of employment
9. Physical and environmental security
   9.1 Secure area
   9.2 Equipment security
   9.3 Security under the control of other parties

*Underlines indicate the newly described area compared with ISO/IEC17799.
10 Communications and operations management
   10.1 Operational procedures and responsibilities
   10.2 Third party service delivery management
   10.3 System planning and acceptance
   10.4 Protection against malicious and mobile code
   10.5 Back-up
   10.6 Network security management
   10.7 Media handling
   10.8 Exchange of information
   10.9 E-commerce service
   10.10 Monitoring

11 Access control
   11.1 Business requirements for access control
   11.2 User access management
   11.3 User responsibilities
   11.4 Network access control
   11.5 Operating system access control
   11.6 Application and information access control
   11.7 Mobile computing and teleworking

12 Information systems acquisition, development and maintenance
   12.1 Security requirements of information systems
   12.2 Correct processing in applications
   12.3 Cryptographic controls
   12.4 Security of system files
   12.5 Security in development and support processes
   12.6 Technical vulnerability management

13 Information security incident management
   13.1 Reporting information security events and weaknesses
   13.2 Management of information security incidents and improvements

14 Business continuity management
   14.1 Information security aspects of business continuity management

15 Compliance
   15.1 Compliance with legal requirements
   15.2 Compliance with security policies and standards, and technical compliance
   15.3 Information systems audit considerations
Recommendations planned to develop in Q7/17 (Security Management)

X.1050: To be proposed

X.1051: In revision process
Information Security Management Guidelines for Telecommunications based on ISO/IEC 27002

X.1052: To be proposed

X.1053: To be proposed
(Implementation Guide for Telecoms)

X.1054: To be proposed
(Measurements and metrics for Telecommunications)

X.1055: In the first stage of development
Risk Management Guidelines for Telecommunications

X.1056: In the first stage of development
Security Incident Management Guidelines for Telecommunications

X.1057: To be proposed
(Identity Management for Telecoms)
Future Schedule

*2007 September – **ITU-T SG17** meeting  
Draft Rec.X.1051 : Final Review in ITU-T

*2007 October – **ISO/IEC SC27** meeting  
Draft ISO/IEC 27011(X.1051) : FCD process (Final Technical Review)

*2007 December – **ITU-T SG17 WP2** meeting  
Draft Rec.X.1051 : Finalizing process  
Consent in ITU-T and FDIS process in ISO

**R.1051 = ISO/IEC 27011**
Information Security Management should be established and maintained to consider in overall environments not only for **Organizations**, but also for **Network Providers** (telecommunications organizations) and **Customers**.

**Final Remark**

ISMS is also a common language