

ITU Regional Development Forum 2008
"Bridging the Standardization Gap in Developing Countries"
Accra, Ghana, 26-28 May 2008

**Cybersecurity, Combatting spam
and Identity Management**

Dr Tim Kelly,
Head, Standardization Policy Division
(ITU-T)

Agenda

- **Cybersecurity**

- **PP-06 & WTSA-04 Resolutions related to security**
- **ITU's role as coordinator for WSIS action line C5**
- **ITU-T work on cybersecurity**
- **ITU-D work on cybersecurity**

- **Combatting spam**

- **Current level of threats**
- **Stop Spam Alliance**

- **Identity management**

- **Towards federated identity management**
- **Work of ITU-T Focus Group**

PP-06 Resolutions related to security

- **Resolution 130: Strengthening ITU's role in building confidence and trust in use of ICTs**
 - **Resolves to give this work a high priority in ITU**
 - **Requests a review of current work and progress**
 - **Instructs to facilitate access to tools and to continue cybersecurity gateway**
- **Resolution 149: Study of definitions and terminology relating to Res 130**
 - **Establishes a working group (chair: Nabil Kisrawi, Syrian Arab Republic)**
 - **Report to PP-2010**

WTSA-04 Resolutions related to cybersecurity and combatting spam

- **Res. 50: Cybersecurity**

- **Calls on ITU-T to evaluate Recs with respect to cybersecurity threats and to raise awareness**

- **Res. 51: Combating spam**

- **Calls on the ITU-T Director to report to Council on relevant initiatives for combating spam**

- **Res. 52: Countering spam by technical means**

- **Instructs relevant Study Groups, in collaboration with IETF, to develop technical Recs, including definitions, on countering spam**

Cybersecurity and WSIS



- **World Summit on the Information Society**

- “Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. “

WSIS Geneva Declaration of Principles, Para 35

- “**We reaffirm** the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cyber-security, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks.”

WSIS Tunis Agenda, Para 39

ITU's role as WSIS C5 Coordinator

- **Annual facilitation meetings**

- **15-16 May 2006, Geneva**
- **14-15 May 2007, Geneva**
- **22-23 May 2008, Geneva**

- **Focus Areas**

- 1. National strategies**
- 2. Legal frameworks**
- 3. Watch, warning and incident response**
- 4. Spam and related threats**

<http://www.itu.int/wsis/c5/index.html>



Cybersecurity Gateway

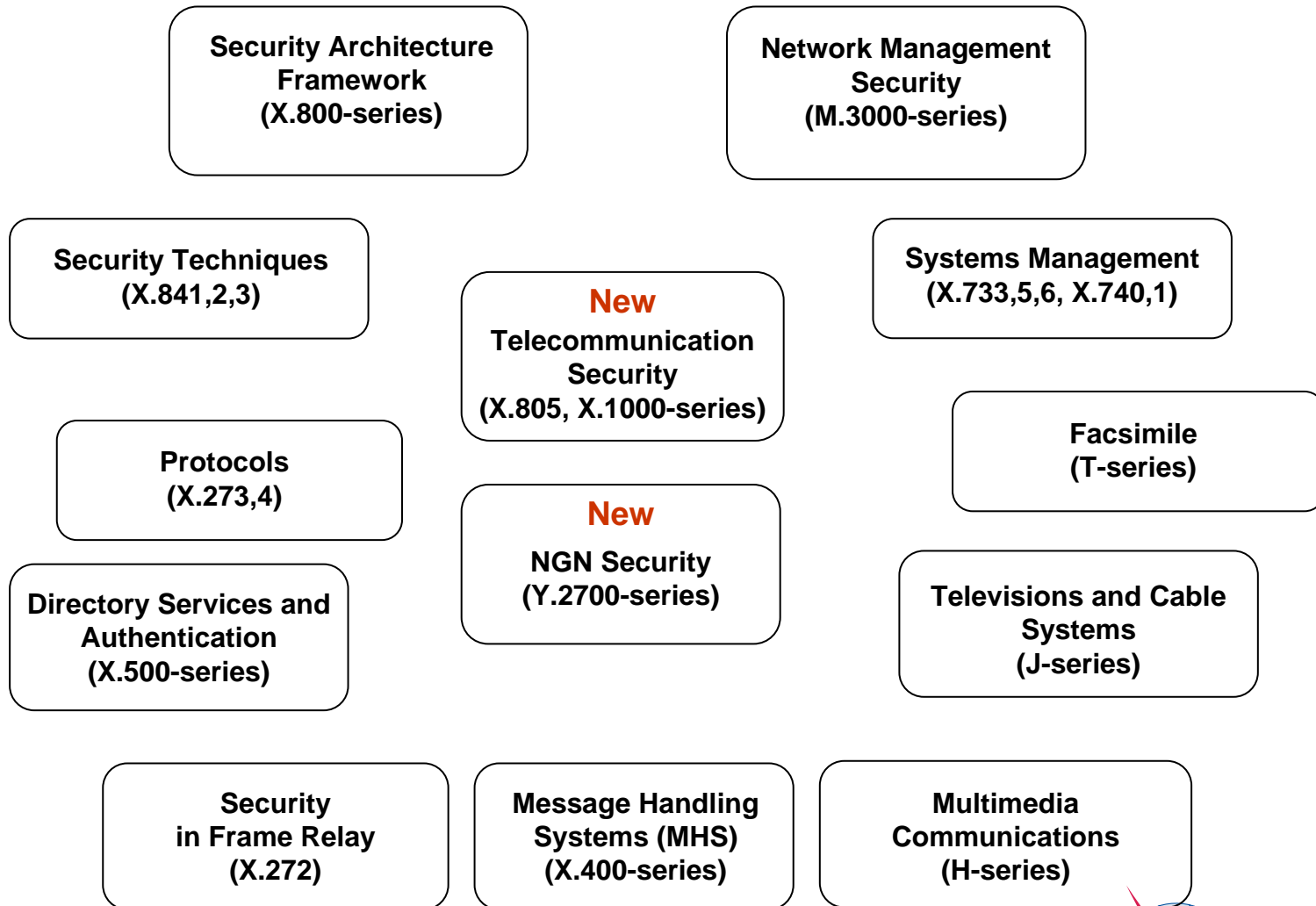
- Provides an easy-to-use information resource on national and international cybersecurity related initiatives worldwide
- Separate portals for:
 - Citizens
 - Governments
 - Businesses
 - International organizations
- Interactive map for country-specific data
- www.itu.int/cybersecurity/gateway



Global Cybersecurity Agenda

- **New initiative to develop a framework for international cooperation in cybersecurity**
- **Establishes a high-level experts group**
- **Five pillars**
 - **Legal framework**
 - **Technical measures**
 - **Organizational structures**
 - **Capacity-building**
 - **International cooperation**
- **<http://www.itu.int/osg/csd/cybersecurity/gca/>**

ITU-T Security Building Blocks



Study Group 17: Security, languages and telecommunication software

- **SG 17 is the Lead Study Group on telecommunication security - It is responsible for coordination of security across all study groups.**
- **Subdivided into three Working Parties (WPs)**
 - *WP1 - Open systems technologies;*
 - *WP2 - Telecommunications security; and*
 - *WP3 - Languages and telecommunications software*
- **Most (but not all) security Questions are in WP2**
- **Summaries of all draft Recommendations under development in SG 17 are available on the SG 17 web page at:**
<http://www.itu.int/itu-t/studygroups/com17>

SG17 Study Questions on Security

- **Q4/17: Communication Systems Security**
 - **Vision, project roadmap etc**
- **Q6/17: Cybersecurity**
 - **Vulnerability info-sharing, Incident handling**
- **Q5/17: Security Architecture and Framework**
 - **Architecture, model, concepts, frameworks**
- **Q7/17: Security Management**
 - **ISMS-T, Incident management, Risk assessment**
- **Q8/17: Telebiometrics**
 - **Multimodal model framework, System mechanism**
- **Q9/17: Secure communication services**
 - **Security for mobile networks, home networks, web services**
- **Q17/17: Countering spam by technical measures**
 - **Technical anti-spam measures**

Examples of recently approved security Recommendations

M.3016.0 1, 2, 3, 4	Security for the management plane: Overview, Security requirements, Security services, Security mechanism, Profile proforma
X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
X.805	Security Architecture for Systems Providing End-to-End Communications
X.893	Information technology – Generic applications of ASN.1: Fast infosec security
X.1035	Password-authenticated key exchange (PAK) protocol
X.1051	Information security management system - Requirements for telecommunications (ISMS-T)
X.1081	The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics
X.1111	Framework for security technologies for home network
X.1121	Framework of security technologies for mobile end-to-end communications
X.1122	Guideline for implementing secure mobile systems based on PKI
X.1141	Security Assertion Markup Language (SAML 2.0)
X.1142	eXtensible Access Control Markup Language (XACML 2.0)
Y.2701	Security requirements for NGN release 1

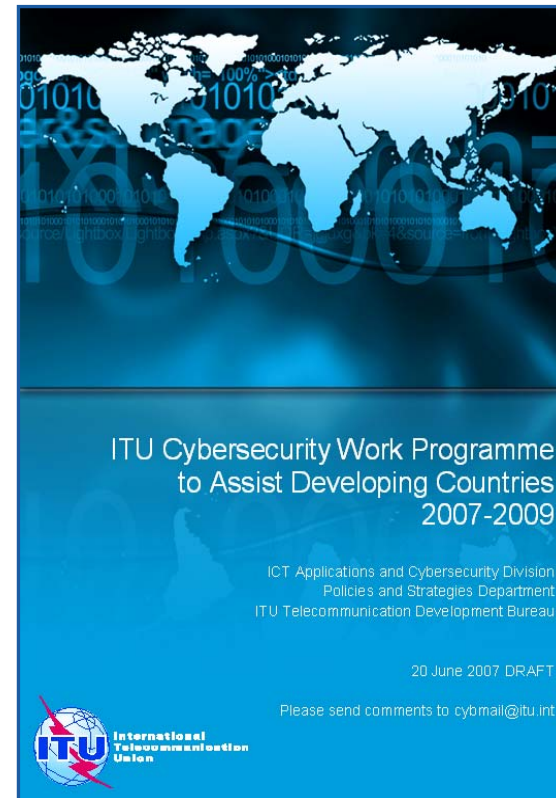
ICT security standards roadmap (2nd edition: May 2007)

- Part 1 contains information about organizations working on ICT security standards
- Part 2 is a database of existing security standards
- Part 3 will be a list of standards in development
- Part 4 will identify future needs and proposed new standards
- Part 5 is now being developed and includes Security Best Practices



ITU-D Cybersecurity Work Programme to Assist Developing Countries

- Most countries have not formulated or implemented strategies for cybersecurity and/or Critical Information Infrastructure Protection (CIIP)
- ITU Work Programme scopes a set of high level assistance activities
- Also scopes detailed activities planned in the 2007-2009 period by the [ITU Development Sector's ICT Applications and Cybersecurity Division](#)
- Used to develop detailed operational plan for 2008-2009



www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

High-level elements in ITU-D work programme

- Assistance related to Establishment of National Strategies/Capabilities for CIIP
- Assistance related to establishment of appropriate cybercrime legislation and enforcement mechanisms
- Assistance related to establishment of Watch, Warning and Incident Response (WWIR)
- Assistance related to Countering Spam and Related Threats
- Assistance in Bridging the Security-Related Standardization Gap
- Establishment of an ITU Cybersecurity/CIIP Directory, Contact Database and Who's Who Publication
- Cybersecurity Indicators
- Fostering Regional Cooperation Activities
- Information Sharing and Supporting the ITU Cybersecurity Gateway
- Outreach and Promotion of Related Activities

Regional cybersecurity forums and workshops:

- Sofia, Bulgaria, 7-9 October 2008
- Brisbane, Australia, 14-17 July 2008
- Doha, Qatar, 18-21 February 2008
- Praia, Cape Verde, 27-29 November 2007
- Buenos Aires, Argentina, 16-18 October 2007
- Hanoi, Vietnam, 28-31 August 2007

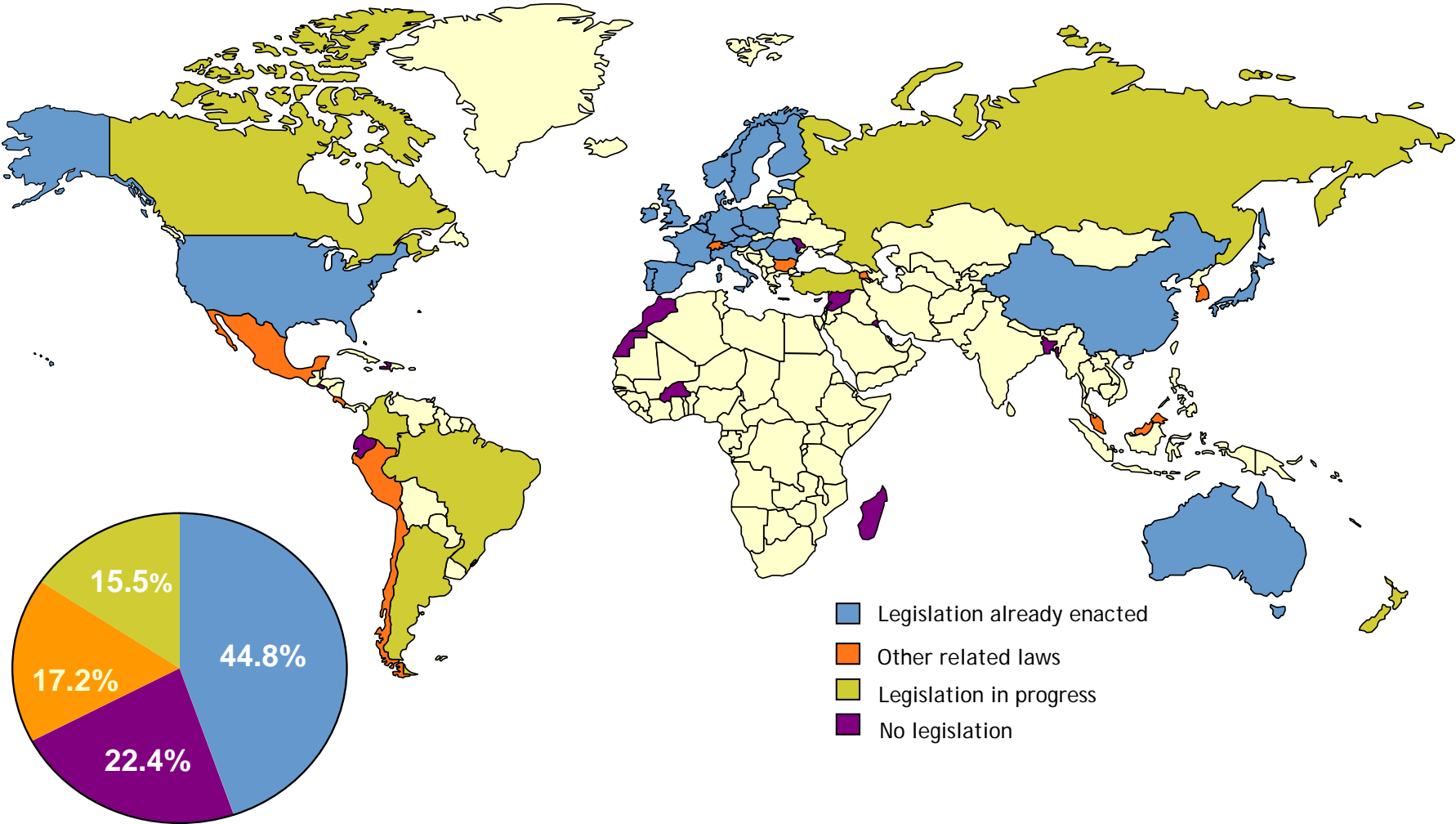
Combatting spam: Current threat level

Spam as a % of all email, worldwide



Source: MessageLabs.

ITU survey on anti-spam regulation



StopSpamAlliance

- We call upon **all stakeholders to adopt a multi-pronged approach to counter spam that includes, *inter alia*, consumer and business education; appropriate legislation, law enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation.**
 - ***Tunis Agenda for the Information Society, para 41***
- **StopSpamAlliance.org is an informal alliance of:**
 - **international organisations including ITU, OECD, APT, ISOC etc)**
 - **governments (UK, Australia, Malaysia etc)**
 - **open to all WSIS stakeholders**

What is Identity Management?

- **Management of digital identity**

- **All trusted ICT and network capabilities and resources for**

- Authentication (e.g., certificates)
 - Identifiers (e.g., E.164 nos., URIs, IP addresses, domain names)
 - Attributes (e.g., names, location)
 - Patterns and reputation

- **For entities of any kind**

- People
 - Organizations
 - Objects (e.g., devices, SIMs, RFIDs, content..)

- **Common global needs for interoperability**

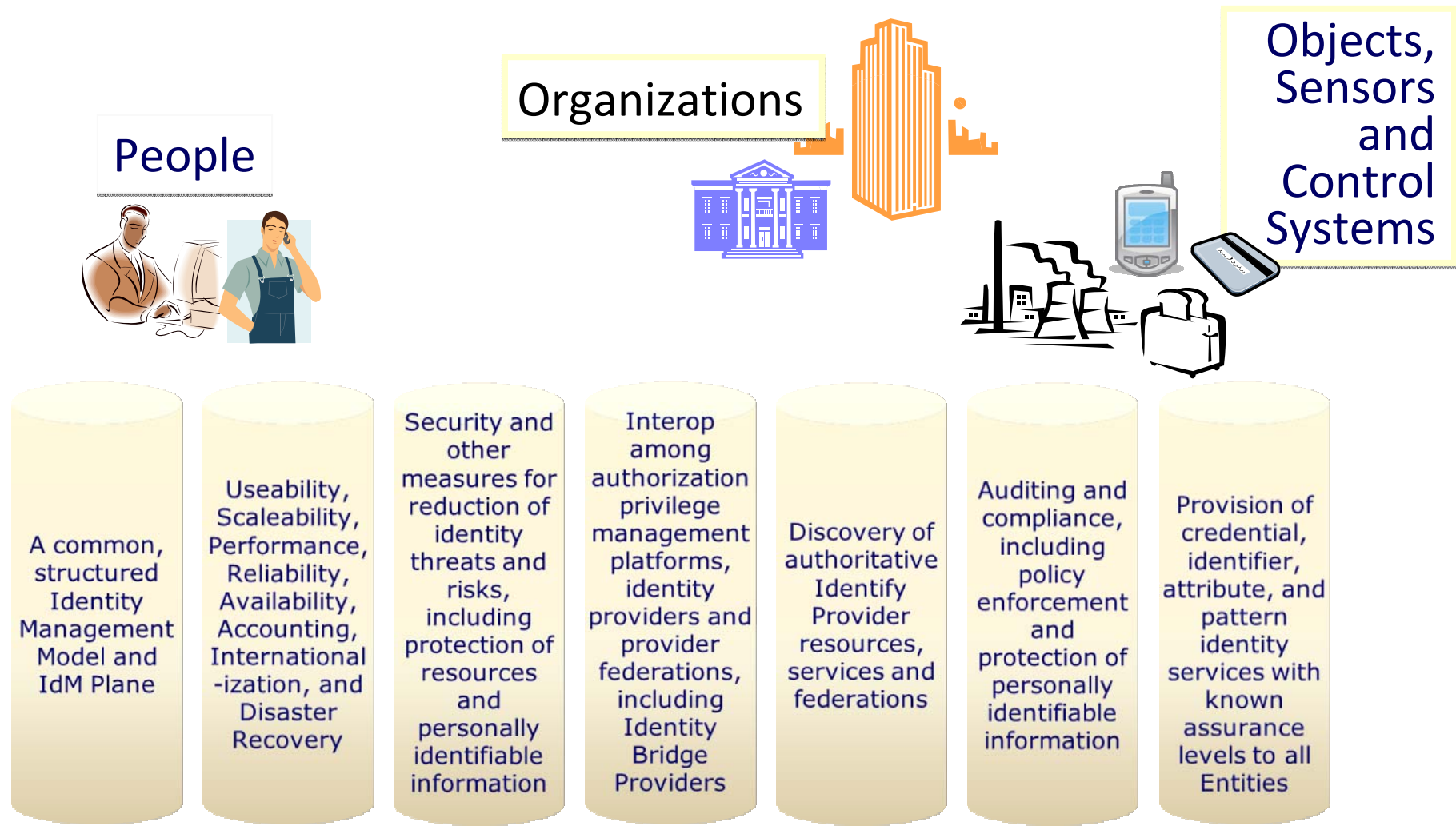
- **Essential for network/cybersecurity and eCommerce**

- **Essential for an increasingly “always on” world**

Focus Group on Identity Management

- **Created in December 2006, by TSAG**
- **Six meetings in Geneva (x3), Mountain View, Tokyo and Cambridge; workshop in Lucerne**
- **Focus Group products**
 - **Requirements structure and provisions**
 - **Use cases, platforms, gaps**
 - **Draft framework(s)**
 - **Reference materials, including a lexicon and a legal/regulatory compendium**
- **Inputs to Study Groups 13 and 17**

The “seven pillars” for globally interoperable Identity Management



For more information:

- **ITU-T Study Group 17 at:**
www.itu.int/ITU-T/studygroups/com17
- **ICT Security Standards Roadmap:**
<http://www.itu.int/ITU-T/studygroups/com17/ict/index.html>
- **ITU-T Focus Group on Identity Management:**
www.ITUwiki.com
- **ITU-D work on cybersecurity:**
www.itu.int/ITU-D/cyb

Glossary of terms used

APT	Asia-Pacific Telecommunity
CIIP	Critical Information Infrastructure Protection
ENISA	European Network and Information Security Association
ISMS-T	Information Security Management Systems, requirements for Telecoms
ICT	Information and Telecommunication Technology
IP	Internet Protocol
ITU	International Telecommunication Union
ITU-D	ITU Development Sector
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
NGN	Next Generation Networks
NISSG	Networks and Information Security Steering Group
OECD	Organisation for Economic Cooperation and Development
PAK	Password-authenticated Key exchange
PKI	Public Key Infrastructure
PP-06	ITU Plenipotentiary Conference 2006
RFID	Radio Frequency Identification
SG	Study Group
SIM	Subscriber Identification Module (on mobile phone)
TSAG	Telecommunication Standardization Advisory Group
URI	Universal Resource Identifier
UNGA	United Nations General Assembly
WCIT	World Conference on International Telecommunications
WP	Working Party
WSIS	World Summit on the Information Society
WTSA	World Telecommunication Standardization Assembly
WWIR	Watch Warning and Incident Response