New Horizons for Security Standardization

Report of the security workshop hosted by the International Telecommunications Union/Telecommunication Standardization Bureau in Geneva on 3-4 October 2005

Table of Contents

Background and Objectives

The workshop was planned and coordinated by ITU-T Study Group 17 (SG 17) as part of its Lead Study Group mandate to coordinate the security work in the ITU Telecommunications Standardization Sector (ITU-T).

The overall objectives of the workshop were to help advance the ITU-T's ICT security standardization work and to promote increased cooperation between organizations engaged in the development of security standards. In particular, the workshop aimed to:

- Provide an overview of key security standardization activities in international standards development organizations (SDOs); consortia and regional SDOs;
- Seek to find out from stakeholders (e.g., network operators, system developers, manufacturers and end-users.) their primary security concerns and issues (including possible issues of adoption or implementation of standards);
- Try to determine which issues are amenable to a standards-based solution and how the SDOs can most effectively play a role in helping address these issues;
- Identify which SDOs are already working on these issues or are best equipped to do so; and
- Consider how SDOs can collaborate to improve the timeliness and effectiveness of security standards and avoid duplication of effort.

This report, which will be shared with all organizations that participated in the Workshop as well as other organizations with an interest in security standardization, has been prepared to provide a record of the findings of the Workshop. These findings provide valuable guidance that can contribute to future standards development work.

Participation

The workshop attracted 76 participants and was rated "very satisfactory" by the returned evaluation forms (Annex C). Presentations were made by representatives ITU-T, ISO/IEC, IETF, ATIS, ETSI, 3GPP, ETNO, OASIS and the RAISS Forum. The participation of external SDOs and user forums was particularly welcome and indicated broad interest in the workshop objectives. Representatives of several other ITU-T Study Groups participated as speakers, panellists and delegates.

Program

The workshop provoked very lively discussions and generated many very useful ideas and proposals. Since the results of the workshop are most important, this report concentrates, for the most part, on reporting the key points and ideas from the presentations and the discussions.

A summary of the program and agenda is appended to this report as Annex A. The workshop

was webcast and audio archives along with the slides of all presentations, abstracts and speaker biographies, are available on the SG17 web site at the workshop web page: http://www.itu.int/ITU/worksem/security/200510/avprogram.html

Key points and results of the Workshop discussions

Key points discussed during the workshop included:

- the possible creation of a Security Experts Network (SEN), gathering security experts from all SDOs, and meeting once a year, to share information and improve collaboration;
- using the ITU-T SG 17 *Security Standards Roadmap*[1] to increase collaboration and avoid duplication of work among SDOs;
- the need for a global standards framework providing for international agreements on acceptable levels of security;
- the need for security standards to respond to business needs while recognizing that there will be differences in requirements as a result of variations in user, regional and national needs;
- the need to help users articulate their security needs and understand what standards can and cannot offer;
- the need to improve the responsiveness of security standards to technological change and to emerging threats;
- the need for better metrics to quantify the threat and risk and the effectiveness of controls;
- sharing priorities among SDOs to identify where best to develop standards; and
- exploring the possibility of funding from international organizations (UN, APEC, OECD, etc) for security standardization.

Key observations and findings from the presentations and discussions are summarized in Annex B. However, it must be stressed that a summary of key points cannot do justice to the excellent and thought-provoking quality of the presentations. Readers are urged to review the presentations in addition to the summary of key points and ideas presented here.

Follow-on actions

The key findings will be used by ITU-T SG 17 to try to determine how best to shape the future security standards work and improve collaboration.

SG 17 completed a review of the initial draft of this report during the October 2005 SG 17 meeting and proposed some immediate actions to respond to some of the suggestions. Specifically, SG 17 agreed to:

a) Immediately begin to implement the proposal for a security expert's network, initially by establishing links with the external SDO representatives who attended the Workshop.
b) Publish the first version of the *Security Standards Roadmap* as soon as possible.
c) Consider how to establish interworking with other organizations such as ENISA. (As a

[1] A first edition of the *ICT Security Standards Roadmap* which is under development by ITU-T SG 17 is expected to be released in November 2005.

first step a copy of the workshop report will be sent to ENISA).

d) Ask external organizations what follow-up steps they would recommend.

In addition, we have had the suggestion that a one-day workshop on Identity Management be organized in collaboration with other groups that are working on this topic.

SG 17 will give further consideration to the workshop findings over the next few months and at its next meeting in April 2006.

Report development and review

This report was prepared by the Workshop Drafting Committee (Mr Adam Golodner, Mr Mike Harrop, Mr Meng Chow Kang, Mr Julian Minard, Mr Lewis Robart, Mr Georges Sebek, Mr Fabrice Stevens), and reviewed by workshop speakers, chairs and panellists before being finalized.

Acknowledgement

Thanks are due to all SG 17 and ISO/IEC representatives who participated in the planning of the workshop, ITU-T staff for their participation in the planning process and for taking care of organization and administration, the speakers, panellists and chairs, and all the participants who contributed so actively to the discussions and to the success of the workshop.

Annex A: Workshop Program and Agenda

First day

Workshop opening

Opening remarks by Workshop Chairman**,** Herb Bertine, Chair ITU-T SG 17

Welcome by Houlin Zhao, Director, Telecommunications Standardization Bureau, ITU

Session 1 – The role of standards in telecommunications and IT security

Chair: Yu Watanabe, KDDI, Japan

Security standardization in an evolving threat environment – Bill McCrum, Industry Canada

This session provided a context for the workshop by providing some background on how the security standardization work began and how it has evolved to meet a changing threat environment as Internet use has become pervasive. A summary of the current threat environment was included.

Overview of security standards work

ITU-T – Koji Nakao (Japan)
ISO/IEC – Ted Humphreys (UK)
IETF – Russ Housley (USA)

These presentations were high-level and broad-ranging and provided an overview of the security standards work in each organization, existing collaboration, plus the major achievements and the key standards produced. Mention was made of how requirements for standards are determined and evaluated, how standards are marketed, how they are assessed for success and who the targeted users are for each organization's standards. Possible gaps were indicated along with some of the respective strengths and weaknesses of each organization's processes.

Session 2 – Key areas of security standards focus.

Chair: Byoung-Moon Chin, TTA, Korea

Representatives of ITU-T, ISO/IEC JTC 1 and ETSI each highlighted what they consider to be a key topic of current focus and reported on the challenges and issues associated with that topic.

ISO/IEC JTC 1/SC 27 perspective - Marijke De Soete, Vice-chair ISO/IEC JTC 1/SC 27

- Security techniques standards within SC 27
- Signature and authentication standards for secure e-business
- Focus on future 'diversions' biometrics and identity management

ITU-T SG 16 perspective – Martin Euchner, Rapporteur Q.25/16

- NGN Multimedia Security

ESTI perspective - Charles Brookson, Dept. Trade and Industry, UK

- Overview and ETSI security program
- Update on GSM standards

Session 3 – Emerging Technical Issues

Chair: Jianyong Chen, ZTE, China

In this session, experts addressed a number of technical topics that have network security implications

Wireless security: can wireless and wireline security be unified? – Zhi Zhou, China Mobile

RFID and Ubiquitous Sensor Network – Kyoil Chung, ETRI

Trusted computing platform (including trusted mobile platform) – Abbie Barbir, Nortel Networks

Session 4 – Stakeholder perspectives

Chair: Charles Brookson, Dept. of Trade and Industry, UK

A panel of stakeholders representing standards users addressed some of the key questions concerning development and use of security standards. Who are the security standards stakeholders (i.e. the organizations who use the standards) and are the SDOs responding adequately to their needs? If not, why not? What needs to change? What are the economic implications of security standards? Can security standards be implemented cost-effectively in a way that provides "good-enough security" while ensuring cost-competitiveness of the product/service?

Each panellist made a short opening presentation following which there was a moderated discussion with questions and contributions from the audience.

Panellists:

Luis Sousa Cardoso, Portugal representing ETNO
Eric Wiatrowski, Chief Security Officer, France Telecom
Lewis Robart, Senior Project Officer, Industry Canada
Adam Golodner, Cisco
Mirek Kula, GTECH, USA

Wrap-up of Day 1

The Workshop Chairman and Rapporteur provided a brief summary and identified issues for overnight discussion/review.

Second day

Session 5: Day 2 Introduction

The Workshop Chairman provided an introduction to Day 2 and reported on results of after-hours discussions. Feedback was invited from participants.

Session 6: Key network security issues – some regional and consortia perspectives

Chair: Arkadiy Kremer, RANS, Russia

Representatives from regional SDOs and user groups provided their perspectives on key issues affecting network security.

OASIS - Jamie Clark, Director, Standards Development, OASIS
3GPP - Rajesh Talpade, Telcordia, France
ATIS - Francois Cosquer, Alcatel, North America
RAISS Forum - Meng Chow Kang, Microsoft, Singapore

Session 7: Overview of some specific areas of current interest for security standardization

Chair – Lewis Robart, Industry Canada

This session covered 3 key areas of technical focus for security standardization.

Information Security Management for Networks **–** Angelika Plate, SC 27, Germany and Ted Humphreys SC27, UK

SS7 and the vulnerability of the networking infrastructure – Michel Leber, Tekelec France

Security of voice in an IP environment – Xiaofeng Huang, France Telecom

Session 8 – Security Standards for the Developing Countries and Countries with Economies in

Transition

Chair: Abbie Barbir, Nortel Networks, Canada

Raphael Nlend, Ministry of PTT, Cameroon

This session responded to a growing need to address network security in the developing countries and countries with economies in transition. The presentation reviewed the particular situation in these countries and special needs for DCs/CETs that are not already being addressed by the current security standards work.

Session 9 – Refining the focus and the processes for security standardization

Chair: Ted Humphreys, Convenor, ISO/IEC JTC 1/SC 27/WG 1

This panel discussion and interactive session provided an opportunity for all workshop participants to join in the discussion to try to find answers to the problems facing standards development organizations.

Questions included: What are the crucial problems in ICT security and which of these can/should be addressed by standards? What areas should standardization avoid? Are there differences in security standards needs (or differences in emphasis) in the different regions? How can standards bodies respond most quickly and effectively to emerging threats? How can the work be funded and resourced? And how can SDOs address evolving threats?

Panellists: Charles Brookson, ETSI
Luis Cardoso, ETNO
Mirek Kula, GTECH
Francois Cosquer, Alcatel, North America.

Session 10 – Improving the effectiveness of the security standards process - next steps and conclusions

Chair: Bob Thornberry, Lucent Technologies

The purpose of this panel session was to identify those areas of focus in which the standards organizations (and the ITU in particular) can be most effective in developing security standards, to prioritize security standards needs/activities and to improve collaboration. There was also significant interaction with delegates during this session.

Questions addressed during this session included: how can we increase collaboration and leverage the respective strengths of the formal and informal processes? What can be done to improve alignment of the needs and the work? How can we avoid redundant and conflicting efforts? How do we validate new work proposals and ensure on-going cooperation and

coordination?

Panellists: Angelika Plate, ISO/IEC
Herb Bertine, ITU-T
Jamie Clark, OASIS
Russ Housley, IETF
Tim Kelly, ITU Strategy and Policy Unit
Koji Nakao ITU-T and ISO/IEC

Session 11– Summary and closing remarks

The Workshop Chair and Rapporteur reviewed and summarized the results of the workshop and indicated the steps to be taken to capture the discussion in a report that will be published following review by the drafting committee and all speakers, chairs and panellists.

Annex B: Key observations and findings from the presentations and discussions

This Annex reports the key observations arising from the workshop presentations and discussions. Included here are some diverging views. Although there was considerable agreement on many of these points, this report is not intended to imply consensus or general agreement on every statement. Support for these points will be indicated by actions taken by workshop participants to follow-up on the suggestions and issues they regard as most important.

1. General Objectives and comments from Session 1

The challenge is to establish effective collaboration and cooperation within the security standards community and to build on the cooperation and goodwill of this workshop and the collective experience of our respective SDOs to address these problems in the future.

How can we learn from each other? How can we avoid making mistakes that have been made previously?

2. What are the crucial problems in ICT security standardization?

Standards processes cannot react fast enough to emerging threats.

We need a structure/organization to help gather, categorize and classify security standards and relevant standardization activities. (See also points made in section 3 on Standards Proliferation.)

We currently do not have a process for assessing the adequacy and completeness of the existing standards from a security perspective.

We need to encourage stakeholder interest in the standards process.

<u>Lack of understanding of standards and lack of expertise in applying them</u>

The point was made that standards are difficult to understand and implement. For example, there is often a need to explain to regional experts/entities how to deal with security standards issues and how to apply the security functionality. That suggests that standards bodies should pay more attention to developing some kind of umbrella documentation to explain how standards cover certain requirements (e.g. handbooks, technical reports, user guides).

<u>The robustness of security standards</u>

There were a number of somewhat divergent views on this topic.

One view suggests that, with respect to the ability to deploy solutions outside the operating system kernel (Layer 3 vs Layer 4), ease of deployment is more important than offering an all-

encompassing set of security services.
Pressure to get products to market can result in problems in implementation regardless of any inherent problems in the standards. Some standards have gone forward even though some people believed that there were inherent flaws at the time they were developed – again a problem of speed versus quality.

It was suggested that we may need two kinds of security standards: those that are carefully reviewed and field tested prior to ratification; and those that have to be developed and deployed quickly, without robust review and testing, in order to get something into place quickly (rough and running code versus formal review and test processes).

3. Meta issues

Standards proliferation

Comment from floor: "I didn't realize there was so much security standards work going on." Clearly, if people don't know what standards exist, what standards are under development, who is involved or what work is planned, there is a much greater risk of duplication of effort. (This links to the point made in section 2 above pointing out the need for some identification and categorization of the standards and standards work.)

We need to harness activities or we will be smothered in standards.

There are lots of standards but maybe, in fact, there are too few. Different interests and perspectives are shared in different groups. There will always be a large number of standards. We need to define a common classification to help differentiate the work and avoid duplication.

There is a need for better understanding of standards and processes and a need for categorization of SDOs and standards that will allow people to understand roles and responsibilities.

The SG 17 *Security Standards Roadmap* (which will include non-ITU-T work) could help overcome this problem if it is shared widely.

There is also a need for classification of standards in terms of functionality, applicability, complexity and cost. (This again links back to the point made in section 2).

Need for a global framework

Without an international framework, standards are developed in a vacuum. Until there is a framework that provides both market incentives for implementation and sanctions for failure to implement, and which provides for international agreement on acceptable levels of security, then our impact will be limited. But national and even regional initiatives are not enough on their own. They need to be part of a larger, global framework. ENISA is helping to coordinate European security initiative. Other regional/national efforts are also underway. But we need an

international framework.

4. Standards Requirements and Priorities

What are the business requirements for security standards?

Standards are needed to address privacy, governance, e-business requirements, accessibility and tools for customers.

From an economical perspective, standards are driven by market needs. Vendors put a lot of effort into standards for competition, interoperability, etc. Operators want to interoperate with other domains.

When we reach the domain boundary, we are likely to encounter different standards but for quality of service (QoS) reasons, we need a sound (i.e. robust and secure), end-to-end communication link. (Note, however, that the end points may vary according to the service being provided and the particular viewpoint e.g. client, service provider. In some cases, end-to-end may refer to desktop-to-desktop or handset-to-handset; in other cases it could refer to end-points of sub-networks.)

We need to be discriminating about where we focus the network security efforts. objective standards for quality.

Differences in security needs

Different customers and industries all come with their own set of concerns and requirements. Profiles could help

Different needs are sometimes dictated by national and regional differences in legislation s (e.g. privacy)

Keep security as simple as you can to meet the needs (or an acceptable compromise) and no more (i.e. just-enough security)

Priorities for security standards

We need some way to address the issue of priorities for standards. Perhaps we could share priorities among the groups represented at the workshop.

To what extent does the urgency of the requirement impact or influence the acceptable rigorousness of the standard? (See above notes on business requirements and robustness of security standards.)

ISO/IEC and ITU-T have fast track processes but these require that the specification presented be reasonably stable and have a good measure of agreement within the submitting community.

In identifying candidates for security standardization, we might consider encouraging the consortia processes or some Focus Group review process in some cases, rather than launching some Questions / New Work Items (NWIs) directly into the formal standards processes.

5. Liaison and information sharing

Steps to improve collaboration and interworking

There are many different ways of collaborating. Liaison is working well between ITU-T and ISO/IEC. Processes are formalized and it is unclear what could be done to improve formal liaison arrangements.

To a large extent, liaison is better used only for information sharing but we need not just liaison but active participation in processes. We need to coordinate the work at the working level. It is important that stakeholders participate actively in developing the output and ensure requirements are met.

Simple exchange of documents is not very effective. However, a Point of Contact Network linking primes from all SDOs maybe useful. We could consider establishing a Security Experts Network (SEN) (see proposal below).

The standards meetings need to be more inclusive, and to draw in policy-makers, regulators, and those from the insurance industry and from civil society. Without standards, there will be no "solutions" for the policy people to discuss.

We should co-locate meetings or hold joint meetings where possible to help resource scheduling and active liaison.

Some new tools to help share information will soon be available from the ITU-T (e.g. the *Security Standards Roadmap*).

OASIS uses the fast track process and has had success with elevating standards to ISO. However, submitting organizations must be willing to surrender control of their products (freely available, open, etc.). The lifecycle of standards products is longer than people generally expect. The growth and development of the standards results in feedback to the ongoing maintenance of standards products over decades.

The IETF uses email lists to announce new work that is being considered. They encourage all interested parties to get on the mailing list.

The IETF maintains the standards they develop but they need to understand requirements for improving products to work with new technologies. The IETF relies on participants to make requirements clear and well known, and then to work within the IETF to develop the protocols and other documents.

Information sharing issues of specific concern to ITU-T

Technical tracks during the workshop highlighted a number of new/emerging technologies. There seem to be two areas where immediate coordinated action would be beneficial: (tele)biometrics and RFID. There are contributions to SG 17 that indicate the likely value of cooperation. (These are focussed mainly on collaboration with ISO/IEC.)

Another topic frequently referred to was identity management and anonymity, an area that ITU-T has not yet begun to address specifically, but which is certainly of relevance. (ISO and others are working on this topic (see, for example, ISO/IEC JTC 1/SC 27 NP 24760 – Information technology – Security techniques – A framework for identity management).

Several expressions of interest were received from people willing to work on specific issues including common language and VoIP security. This encompasses interworking issues between SIP-based and SS7-based signaling protocols. ITU-T needs to capitalize on this interest.

There are opportunities for additional cooperation with ISO/IEC JTC 1/ SC 27 in ISMS projects.

Re-use of standards

There is a big challenge in the integration of the existing security protocols with existing and emerging applications. Interconnecting existing protocols with IP changes a great deal from a security standpoint. If we re-use existing protocols we may discover a whole new world of threats.

Questions that must be considered include the extent to which existing protocols can be reused as opposed to developing new protocols. What compromises have to be made to reuse a security standard? How is the issue evaluated? Who decides? Traditionally there has been a tendency to reinvent rather than re-use (and not just in standards).

Some security requirements are applicable to all networks, some depend on what you want to do on the network.

(SG 16 seems to have some useful experience here. The mandate of SG 16 is Multimedia, not security but, as a developer of application standards, SG 16 has not only recognized the need for security to be built-in, but has gone ahead and developed security standards to protect their applications. Security expertise is scarce but SG 16 found the expertise to develop their own security standards by drawing on expertise and standards from elsewhere).

Proposal for establishment of Security Experts Network (SEN)

Without active participating experts, security standards cannot be developed successfully. We should consider creating a SEN as a result of this workshop and invite participants to designate

initial SEN contacts.

1) Designate a point of contact (POC) (Security Experts) in each environment (SDO);

2) Define a procedure for communication including:
   - Protocol
   - Content (including formats) and

3) Hold a SEN meeting each year to share overall experiences.

6. User issues

Managing Expectations

There seems to be an expectation from some users that security standards should stop or prevent new attacks in the future, after their deployment. In reality, most security standards are able to address only known risks or security issues in existing technology, or anticipated security issues in new technology. New attacks, exploits, and vulnerabilities will emerge when technology is deployed in real-world environment, often from venues that were not anticipated or visualized during the technology design or security standards specification stages.

As such, we probably need to adjust expectations for what security standards can achieve. The purpose of security standards should perhaps be clarified and re-instated - for improving security interoperability, and raise the security baseline.

Risk management can help identify untrustworthy elements and implementation of trusted functionality may be able to offer users a clearer indication of the security they can expect and an indicated level of confidence.

Addressing the invisible stakeholders

Questions were raised about the extent to which we are considering the requirements/needs of the forgotten stakeholders (consumers, research orgs, educational orgs, NGOs, regulators, administrations), some of whom may not be able to articulate their requirements in technical terms.

Should we leave it to market forces or is there some way of representing those stakeholders who are not directly involved in standards processes?

Issues for Developing Countries / Countries with Economies in Transition (DC-CET)

Cost effectiveness: Telecommunication security product and services must be affordable.

Harmonization of security products at a global level can go along way to reduce costs.

A guidance document for is needed for telecommunications security for DC-CET.

Standards are needed for secure e-application aimed at delivering services for various sectors.

Cross recognition of digital credentials across geopolitical boundaries is important.

7. Technology and threat issues

Addressing the gaps and dealing with technology developments

We need to consider how to address the security standardization gaps. There seems to be no consistent, established process for addressing the gaps in security standards. Are we just waiting for someone to propose a new work item? Are the new Questions/New Work Items truly responding to market priorities for security standards? (Note: in the past, much effort has sometimes been spent on standards that have failed when subjected to the test of the market place.)

The technology tracks of the workshop raised some major security implications. Given the rate of change of technology, if we are to avoid wasted effort, will need to consider what we should standardize and what we should avoid standardizing. In some cases technology just bypasses the standardization process. Should there, perhaps, be some process that allows for recognition of interim standards or best practices where technology may change in the short term?

For a topic like RFID, where the security implications are very broad, how do we begin to identify which SDOs should be involved? How will the work be divided up without duplicating effort? Which SDO is in the best position to respond to the need for the various security standards and how can that be determined?

What are the emerging threats and how can they be addressed?

Spyware, bots, spam-related threats, phishing and cyber crime were identified as the primary concerns.

How can the response to emerging threats be improved?

Understanding the issues involved is crucial.

Industry groups are often faster in specification development and industry can respond more quickly than SDOs to develop fixes for emerging threats in the short term. Formalized standards can help in the longer term.

Liability must be assigned for bad behaviour on the network. Users should be made liable for failure to secure their platforms before they to use the services.

More secure network interconnections can reduce the impact of emerging threats.

We need better capability to trace-back attacks. (However, network and service operators are constrained by laws governing interception.)

Premium video (IPTV) is raising the bar for networks. There are a lot of good standards available already – we should make use of them.

8. Focus for future standardization work

What areas should be avoided for security standardization?

We should not standardize security policy per se. (However, guides to developing policy are OK.) There are structured data methods for expressing policy constraints generically and perhaps we can determine how to reflect policies in standardization efforts.

Which topics can/should be addressed by standards?

Topics should be contribution-driven but contribution-driven development can lead to duplication of effort.

ETSI takes a proactive approach to urgent issues (see below under *standards funding*).

We need common terminology to help progress the work. There are several "languages" in the area of security. We need to harmonize a common language for security infrastructure. The ITU can provide leadership in this area.

A standards roadmap map (i.e. a guide to the standards organizations (who they are and what they do), their activities and their standards) would be useful.

9. Process issues

General concerns

We need to understand how security is applied/implemented and fed back into the standards process.

Security is like any other utility and should be provided to most (perhaps not all) users transparently, without any specific knowledge requirements on the part of the user. Usability and security should not be a trade-off. They should go together and work together.

Real-world implementations consist of multiple standards.

We need to be aware of the risk of introducing new vulnerabilities when developing/implementing standards.

Should standardization be step 1 or step 2, i.e. should we be developing standards or finding solutions? Standardization bodies should focus on finding the best solutions but must remember the installed base.

We should write standards for the long haul and be prepared to revise them.

A caution was sounded with respect to open architectures, use of which can result in varied interpretations.

Division of labour is a noble goal, but traditional layered frameworks are becoming less relevant. For example, Java has no layers. Until there is a new paradigm, it will be difficult to share the work across SDOs. However, we should not ignore layered architectures or discard older taxonomies if they work unless there is a suitable replacement and it is validated. It is necessary to find which pieces do and do not fit.

Metrics

Several comments addressed the issue of metrics and of being able to measure the effectiveness of security controls and ISMS implementations. Without standards, there can be no reliable metrics.

Until we can quantify the size of the Cybersecurity problem accurately, and show how it is growing, we will not succeed in gaining the attention of policy-makers, which is essential for creating a global framework.

We need better metrics, particularly on the threat/risk trade-off (similar to the cost/benefit trade-off approach taken by insurance companies). To some extent, risk management is in conflict with security control. In some cases we need less control but more security management. Guidance in this area would be useful. This balance is main aim of ISMS standard. Use risk assessment to assess the current situation and where things are expected to go; use controls to fill the gaps; then, over time, check implementations with metrics and measurements.

We also need to try to measure the impact of this workshop.

How can work be funded?

Contribution-driven seems to work. But if contributions dry up, so will the security work.

There is often little incentive for service providers to undertake or contribute to security work. Getting incentives for service providers to do that is important.

In ETSI, urgent issues are considered by Special Task Forces, i.e., groups of experts selected and paid by ETSI to develop a standard under the supervision of a technical body.

The interest of international organizations (UN, APEC, OECD, etc.) in security should be explored.

ITU-T-specific process issues

ITU-T must scope its activities. Network security and information security tend to get confused. ITU-T must address the former. E.g. securing the global telecom infrastructure, ensuring it is not vulnerable to attacks, ensuring that it employs good deployment techniques, ensuring that management and administration of the network are done securely, and ensuring that NGN (converged) network security issues are addressed. (But where are the network endpoints?)

Note that ITU-T does not need to collaborate with everyone – just SDOs involved in security work in the ITU-T space of network security.

Note also that there is more than one solution to telecom security issues, and that NGN means different things to different people.

Proposed process for development of security controls

The following process was proposed for development of security controls:

1) Identify the business, service and application requirements first (independent of security) in each area;

2) Consider how to construct the requirements for the environment (design and implementation);

3) In the process of construction, conduct a threat analysis and risk assessment and identify the security requirements;

4) To meet the security requirements:
- use the existing security technologies, and standards without any modifications if they fit;
- use them and consider them in combination with other standards; and
- develop the security controls and technologies.

5) Judge whether the security controls should be standards or guidelines, etc.

10 Follow-on issues

At its meeting immediately following the workshop, Question 4 of SG17 approved the following

steps:

a) Immediately begin to implement the proposal for a security expert's network, initially by establishing links with the external SDO representatives who attended the Workshop.
b) Publish the first version of the *Security Standards Roadmap* as soon as possible.
c) Consider how to establish interworking with other organizations such as ENISA. (As a first step we will send a copy of the workshop report when it is finalized.)
d) Ask external organizations what they would recommend as the next steps for this activity.

In addition, we have had the suggestion that a one-day workshop on Identity Management be organized in collaboration with other groups that are working on this topic.

Annex C: Workshop Evaluation

Of 78 participants, 31 returned the filled evaluation form. From the respondents, 35% indicated an overall ranking for the Workshop as “very satisfied”, 52 % as “satisfied.

1= very dissatisfied, 2= dissatisfied, 3= neutral, 4= satisfied, 5= very satisfied

The average overall ranking of the Workshop was: 4.2

58 % of respondents would welcome another ITU-T workshop on the same subject in the next 1-2 years