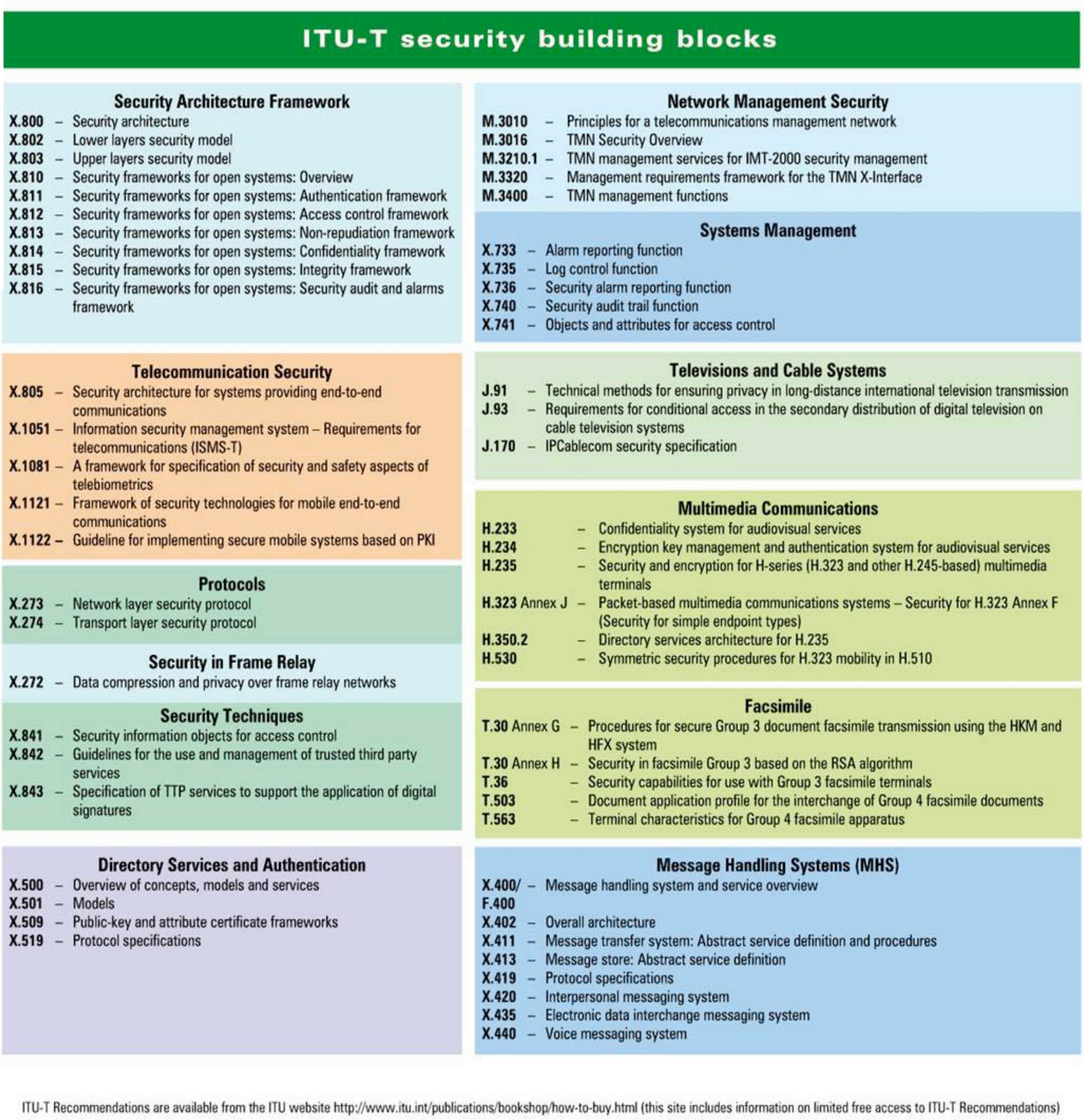
Security Baseline for Network Operators

Arkadiy Kremer

Vice Chairman ITU-T SG 17



ITU-T security building blocks

Security Architecture Framework

X.800	Security architecture
X.802	Lower layers security model
X.803	Upper layers security model
X.810	Security frameworks for open systems: Overview
X.811	Security frameworks for open systems: Authentication framework
X.812	Security frameworks for open systems: Access control framework
X.813	Security frameworks for open systems: Non-repudiation framework
X.814	Security frameworks for open systems: Confidentiality framework
X.815	Security frameworks for open systems: Integrity framework
X.816	Security frameworks for open systems: Security audit and alarms framework

Telecommunication Security

X.805	Security architecture for systems providing end-to-end communications
X.1051	Information security management system – Requirements for telecommunications (ISMS-T)
X.1081	A framework for specification of security and safety aspects of telebiometrics
X.1121	Framework of security technologies for mobile end-to-end communications
X.1122	Guideline for implementing secure mobile systems based on PKI

Protocols

X.273	Network layer security protocol
X.274	Transport layer security protocol

Security in Frame Relay

X.272	Data compression and privacy over frame relay networks

Security Techniques

X.841	Security information objects for access control
X.842	Guidelines for the use and management of trusted third party services
X.843	Specification of TTP services to support the application of digital signatures

Directory Services and Authentication

X.500	Overview of concepts, models and services
X.501	Models
X.509	Public-key and attribute certificate frameworks
X.519	Protocol specifications

Network Management Security

M.3010	Principles for a telecommunications management network
M.3016	TMN Security Overview
M.3210.1	TMN management services for IMT-2000 security management
M.3320	Management requirements framework for the TMN X-Interface
M.3400	TMN management functions

Systems Management

X.733	Alarm reporting function
X.735	Log control function
X.736	Security alarm reporting function
X.740	Security audit trail function
X.741	Objects and attributes for access control

Televisions and Cable Systems

J.91	Technical methods for ensuring privacy in long-distance international television transmission
J.93	Requirements for conditional access in the secondary distribution of digital television on cable television systems
J.170	IPCablecom security specification

Multimedia Communications

H.233	Confidentiality system for audiovisual services
H.234	Encryption key management and authentication system for audiovisual services
H.235	Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals
H.323 Annex J	Packet-based multimedia communications systems – Security for H.323 Annex F (Security for simple endpoint types)
H.350.2	Directory services architecture for H.235
H.530	Symmetric security procedures for H.323 mobility in H.510

Facsimile

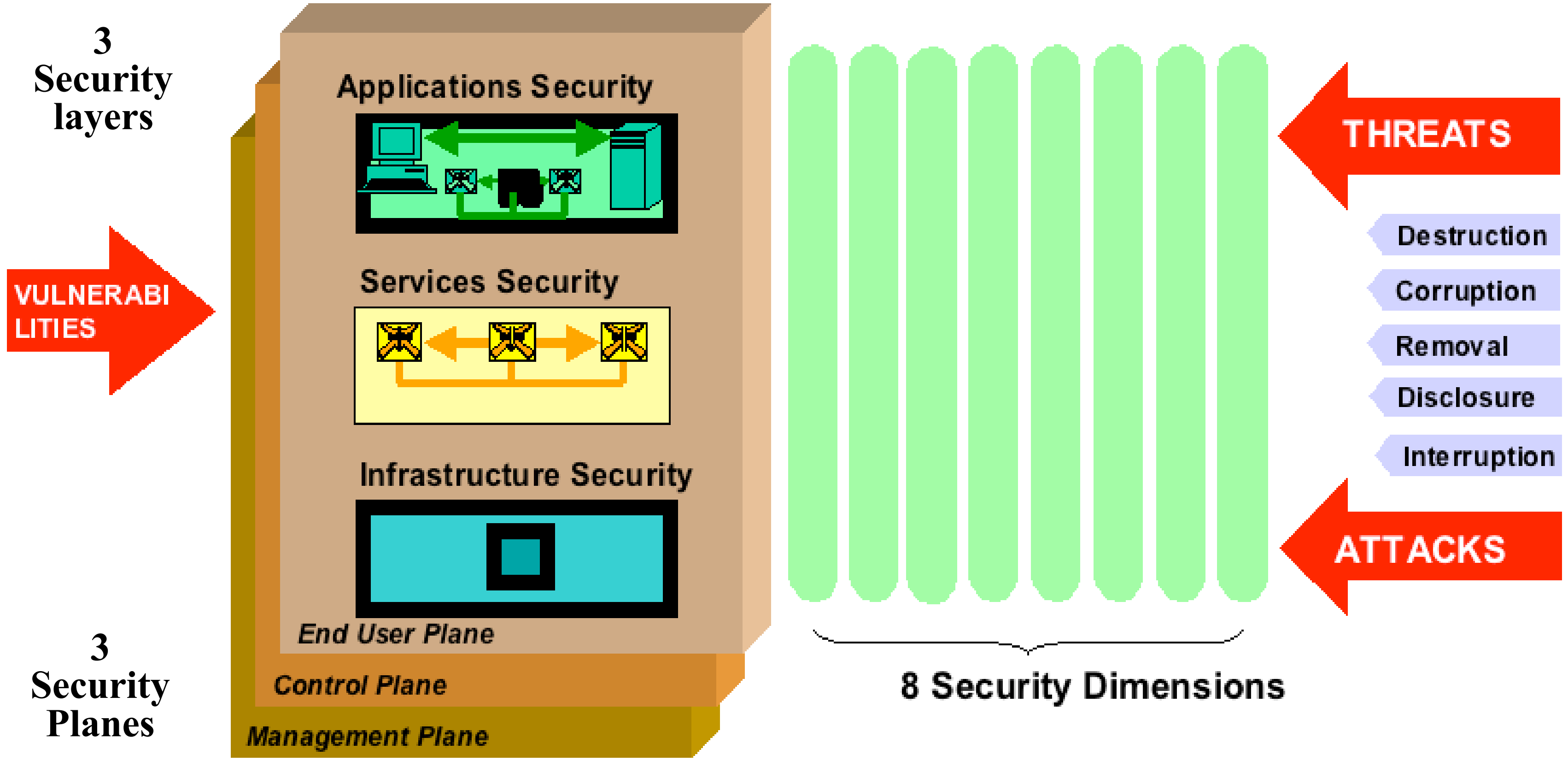
T.30 Annex G	Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system
T.30 Annex H	Security in facsimile Group 3 based on the RSA algorithm
T.36	Security capabilities for use with Group 3 facsimile terminals
T.503	Document application profile for the interchange of Group 4 facsimile documents
T.563	Terminal characteristics for Group 4 facsimile apparatus

Message Handling Systems (MHS)

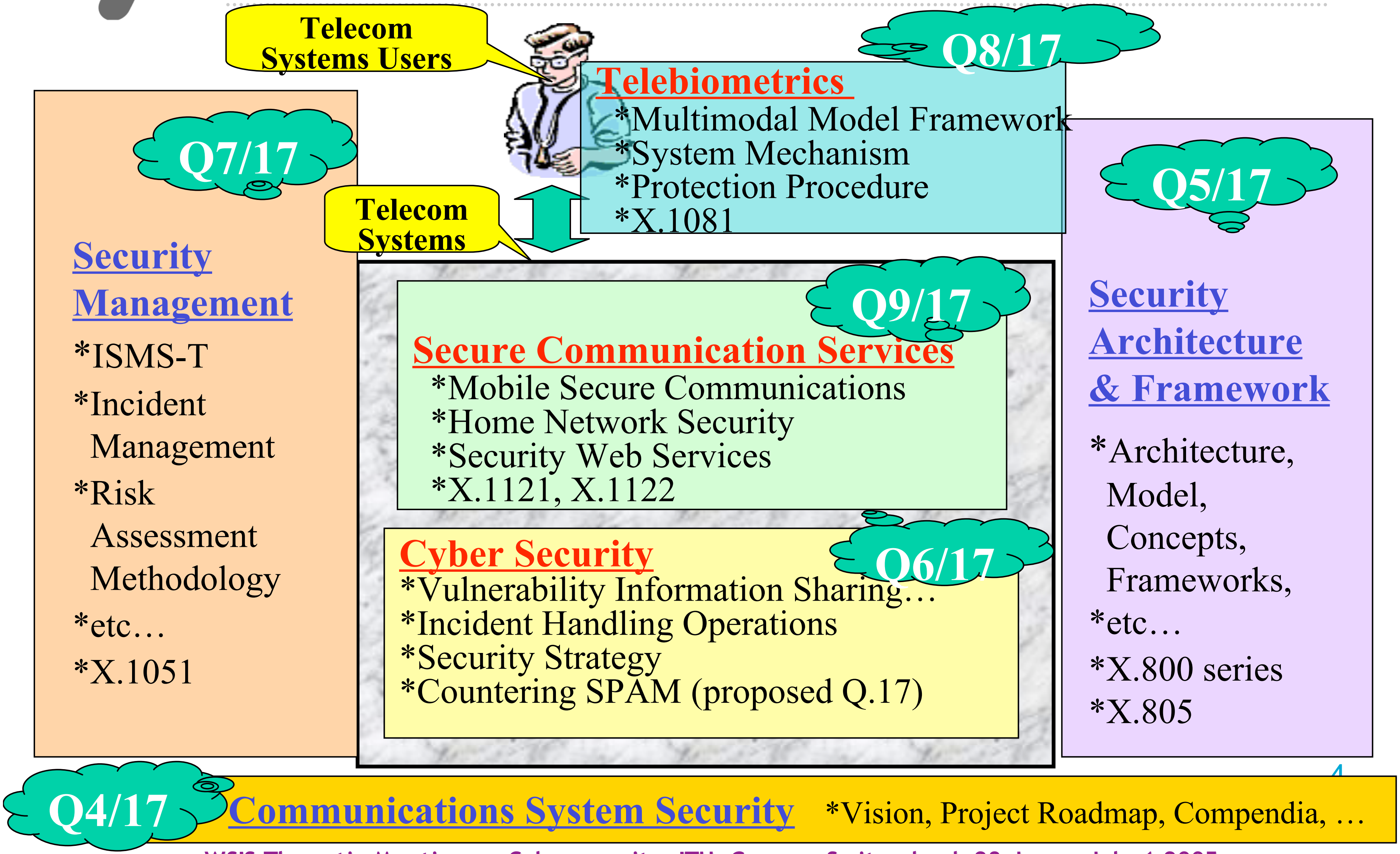
X.400/ F.400	Message handling system and service overview
X.402	Overall architecture
X.411	Message transfer system: Abstract service definition and procedures
X.413	Message store: Abstract service definition
X.419	Protocol specifications
X.420	Interpersonal messaging system
X.435	Electronic data interchange messaging system
X.440	Voice messaging system

ITU-T Recommendations are available from the ITU website http://www.itu.int/publications/bookshop/how-to-buy.html (this site includes information on limited free access to ITU-T Recommendations)

X.805



- Vulnerabilities can exist in each Layer, Plane and Dimension
- 72 Security Perspectives (3 Layers ✖ 3 Planes ✖ 8 Dimensions)



Telecom Systems Users

Q8/17

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

Q7/17

Security Management
- *ISMS-T
- *Incident Management
- *Risk Assessment Methodology
- *etc…
- *X.1051

Telecom Systems

Q9/17

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

Q6/17

Cyber Security
- *Vulnerability Information Sharing…
- *Incident Handling Operations
- *Security Strategy
- *Countering SPAM (proposed Q.17)

Q5/17

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

Q4/17 Communications System Security *Vision, Project Roadmap, Compendia, …

The first SG 17 meeting in 2005-2008 study period

Moscow (Russia), 30 March – 8 April 2005

Three areas of research were discussed:

- question-answering system and other aspects of OSI,
- security in telecommunication systems,
- formal languages and software for telecommunications.

92 delegates from 17 countries presented more than 70 contributions with offers for Recommendations development in the SG 17 responsible areas.

General project overview

The project proposes a security baseline for network operators that will provide meaningful criteria against which each network operator can be assessed if required.

Use of these criteria depends from regulatory regime and from type of the operator depending on the underlying network technology.

The project objective is to develop a baseline requirement specification, based on international security standards, that defines a basic level of security for network operators.

The resulting baseline requirement specification should provide a "floor" of security.

As a result of project implementation by 2008 ITU-T Recommendations will be developed for network operators. Recommendations development must become the outcome of finding the balance between:

- costs and value,
- freedom and security,
- national legislations and self-regulatory practices,
- interests of consumers, operators and regulators,
- bring to the creation of evidence base and ad hoc law enforcement.

A comprehensive international cooperation is offered.

The efforts to generalize and find phrasing equally good for all types of operators lead to such abstract statements that it is virtually impossible to apply them in practice.

Therefore, for typical network services general requirements will be elaborated.

Particulars of ISP operation

1. Apart from a specific set of threats ISP is different from other network operators in that it always works in the global information space and interacts with all providers in the world.

2. In the Internet it is difficult to separate information exchange into international and national and it is easy to violate the legislation of one country from the other.

3. Historically, due to intrinsic globality of the Internet and difficulty of its legal regulation, self-regulatory norms evolved and are practiced which by far not always comply with national legislations.

4. Quite often situations occur when protection violation of a certain network resource affects not so much its owners as much as it affects other individual having nothing to do with the said violation.

Anti-viral protection

To protect against the mail virus it is not sufficient to install anti-viral software into the majority of servers. It is required to install it to all mail servers.

In operator service agreements with consumers there has to be foreseen an obligation on the part of consumer to install antiviral software on its email servers.

For creation of complex anti-viral protection systems able to withstand contemporary harmful codes and tools it is reasonable to install software from various vendors.

When selecting the anti-viral software vendors it is required to take into account the number of released updates and their consistency, the speed of reaction towards new threats and availability of complete line of solutions for various network elements.

Counteraction to SPAM dissemination

- completeness – the filter has to reveal as much SPAM as possible,
- preciseness – the filter has to make as few errors as possible and avoid assigning a regular mail to SPAM,
- resilience – complete analysis of messages should not allow access to new, previously unknown type of SPAM,
- “up-to-date” -ness – the decision-making filter should apply the latest knowledge of SPAM,
- the filter has to be set-up to the linguistics of particular language,
- the protection against SPAM has to be less costly than its receipt.

Resource protection

Attackers very seldom use own resources for attacks. As a rule, they use other servers.

It is unrealistic to demand that network operators and their customers eliminate all vulnerabilities. At the same time the recommendations eliminating the emergence of new vulnerabilities are useful.

Network operator has to prevent situations when equipment connected to public network can be remotely accessed without authorization, or by a default password.

In the communication service agreements a similar obligation has to be foreseen for consumers to meet the same requirement.

Protection against side damage

Three types of damage incurred during protection:

- damage to the attacker,
- damage to oneself or a protected resource,
- damage to third parties or to their resources.

We do not only protect the Internet, but also exist within it, we must protect it without interfering with this existence.

Reaction to incidents

Very seldom cases are observed when both the source and the target of network attack are located within a single operator’s network.

As a rule the target (targets) and the source (sources) of attack are far from each other.

As a rule, in-between two operators chosen at random there is no interconnect agreement.

Every network operator has to establish information security incidents reaction department.

Conclusion

1. We need to standardize and learn information security much more as a system which is required to be created and managed rather than a subject of sale or service which it is possible to buy.

The ITU might be the leader in such a systematic understanding and standardizing of the information security.

2. There are number of different languages in which people talk about information security.

The ITU might be the leader in creating such a common language for better understanding and creation of cybersecurity infrastructure.

Conclusion

3. There is a number of standards in the field of information security. But a standard is the real standard when it has the applications.

The ITU might be the leader in joining efforts of different standardization bodies in preparing reports on information security standardization processes from the point of view of their business applications.

4. Participation in the project is open to all ITU members. I would like to invite interested bodies to become members of the project team and join our efforts in such an interesting collaboration.

Thank You!

kremer@mail.rans.ru
www.rans.ru