



4 November 2004

SESSION 4

SECURITY: CONFLICT AND CONVERGENCE

1



4 November 2004

SESSION 4

SECURITY: CONFLICT AND CONVERGENCE

Chairman: Peter Van Roste, European Policy Director, eBay International, **USA**

Moderator: Sergio Antocicco, President ANUIT Italian Telecommunications Users Association, **Italy**

Speakers:

- Tracey Pitt, Chief Executive ETR2A/eBusiness Centre, Northumbria University, **United Kingdom**
- Arvo Ott, Head of Department of State Information Systems, Ministry of Economic Affairs and Communications, **Estonia**
- Patricia Cooper, Chief Regional & Industry Analysis Branch, Federal Communications Commission (FCC), **USA**
- Jens Sörvik, Project Officer, International Organisation for Knowledge Economy and Enterprise Development, **Sweden**
- Neil Edwards, Managing Partner, XianGroup, **USA**
- Maury D. Shenk, Managing Partner, London Office, Steptoe & Johnson, **United Kingdom**

2

eBAY contribution:

Privacy in an online environment

The goal: Provide a global online trading platform where practically anyone can trade practically anything

3

Some interesting facts... (Q3 2004)

125 Million Registered users

348 Million Listings

USD 8,3 Billion Gross Merchandise Value

430.000 people in the US make a full-time or part-time living selling on eBay

4

eBay Privacy Vision

- Provide an open environment that facilitates online trade through trust
- Trust is facilitated by the fair information principles, and by providing users with:
 - notice and communication
 - choice and control
 - security, authentication and enforcement
- Trust is earned with integrity and time

5

Privacy & Security

- ***Privacy and Security go hand in hand***
- ***Protecting privacy is not possible without processing personal data***
- ***Fighting online identity theft is not possible without processing IP addresses***
- ***Existing privacy laws should be enforced, introducing new laws does not necessarily add protection.***

6

ETR²A* contribution:

**The importance of Information
Sharing in the protection of Critical
Information Infrastructure**

* European Telecommunications Resilience & Recovery
Association

7

Critical Information Infrastructure

Information Infrastructure is a critical cross cutting factor, which other Critical Infrastructures depend upon.

The evolving Information Infrastructure is as vital as power¹.

Telephone networks

- Internet
- Terrestrial and
- Satellite Networks

¹ National Academy of Sciences

8

Information Sharing

- What information
- When
- How
- Why
- With Whom

9

What ETR²A is doing

- Warning, Advice, Reporting Point (WARP)
- Trusted Information Sharing environment
- UK Government initiative
- Links to international communities
- Low cost
- No threat

10

Warning Advice and Reporting Point

- Reported incident (attacks, problems, vulnerabilities)
- Anonymised
- Sanitised
- Shared experiences
- Best Practice
- Increase awareness
- Increase resilience

11

Contribution of the Ministry of Economic Affairs and Communications - Estonia:

Trust and e-security in the framework of national ICT architecture

12

Some statistics on Estonia

- **54% of population uses Internet**
- **35 % have their own home computer**
- **100 % of public employees have computerized workplace with Internet connection**
- **More than 740, 000 Internet-banking clients**
- **More than 600, 000 ID-cards issued**
- **59% tax declarations were filled online**

(whole population – 1,356 mil.)

13

Trust and e-security in the framework of national ICT architecture

- **Organizational means, technical means, IT-means – what is the key factor for e-security?**
- **Implementation of enterprise architecture – ID-cards and internet bank identification, secure environment for e-services**
- **Unified identification and authorization mechanisms – is it additional risk for e-security**
- **e-gov services - internal and external risks, methods for secure personal data protection rules**

14

National chip-based Identity Card

Issuing authority:
Estonian Citizenship and
Migration Board

Service contractor:
TRÜB Switzerland

Start of issue: January 1, 2002



Conformance with:
ICAO Doc. 9303 part 3

Inside 16 Kb RSA crypto chip are :
2 private keys; authentication certificate;
digital signature certificate;
personal data file

15

Contribution of FCC:

Network Security Policy: The U.S. Experience

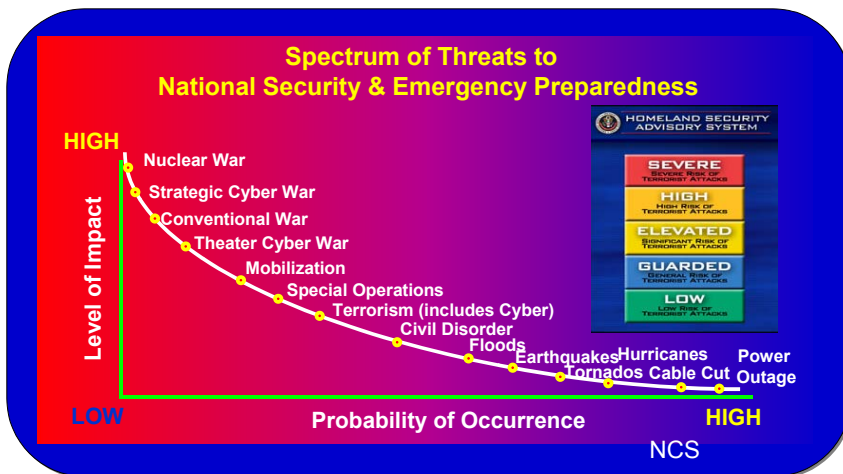
16

Network Security: Definitions

- Addresses the security and reliability of the physical U.S. telecommunications and media networks from natural disasters or man-made attacks
- Part of larger “Cybersecurity” Issue
 - Includes information security, privacy, data protection and law enforcement, among others

17

The Need to Address Physical Security and Reliability



18

Federal Advisory Committees chartered by the U.S. FCC

- **TELECOM: Network Reliability and Interoperability Council (NRIC)**
- **MEDIA: Media Security and Reliability Council (MSRC)**
















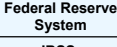



















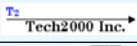



19

NRIC: Mission

- “Partner with the Federal Communications Commission, the communications industry and public safety to facilitate enhancement of emergency communications networks, homeland security, and best practices across the burgeoning telecommunications industry.” (NRIC VII)
- Accomplished through development and deployment of industry **Best Practices** to promote network reliability and interoperability
- www.nric.org

20

NRIC: A Partnership with Industry

Service Providers & Network Operators	Equipment & Software Suppliers	Government & Other Entities
 		
 		Eric Guerrino Jennifer Dickerson Heather Wyson 
 		
 		Ken Buckley 
 		
 		New York Clearinghouse 
 		
 		
 		
		John L. Clarke III 

MSRC: Objectives

- Ensure the security and sustainability of broadcast and multichannel video programming distribution (MVPD) facilities.
- Ensure the availability of adequate transmission capability during natural disasters or man-made attacks.
- Facilitate the rapid restoration of broadcast and MVPD services in the event of significant disruptions.
- Ensure that critical communications is available to the public during and after a disaster while protecting the means to do so.

MSRC: Membership

- Harris Broadcast Communications
- National Association of Broadcasters
- Association of Public Television Stations
- National Public Radio
- National Cable and Telecommunications Association
- MSTV, Inc.
- Tribune Company
- NBC
- Walt Disney Company
- Univision Communications, Inc
- Belo Broadcasting
- Hearst-Argyle Television, Inc.
- Emmis Communications Corp.
- Pegasus Communications Corp
- Thirteen/WNET
- Clear Channel Communications, Inc.
- Cumulus Radio
- Radio One, Inc.
- Hispanic Broadcasting Corp
- WETA
- Sellers Broadcasting, Inc.
- Time Warner Cable
- T&T Broadband Services
- Comcast Corporation
- Cox Enterprises, Inc.
- usquehanna Communications
- Armstrong Utilities
- DirecTV, Inc.
- EchoStar Communications Corp.
- XM Satellite Radio, Inc.
- SES Americom, Inc.
- PanAmSat Corporation
- Intelsat Global Service Corporation
- VerestarAmerican Tower Corporation
- International Association of Chiefs of Police
- National Translator Association
- American Planning Association
- National Captioning Institute
- News Corp.

23

Guiding Principles for Developing Best Practices

- **“People** Implement Best Practices”
- **Do not endorse** commercial or specific "pay for" documents, products or services
- Address **classes** of problems
- Look for solutions **that have already been implemented/tried**
- Developed by **industry consensus**
- Best Practices are verified by a **broader set** of industry members
- **Sufficient rigor and deliberation**

24

Caveats for Best Practices

- Current list of best practices are constrained by what can be implemented
- Not all best practices are appropriate for all service providers or architectural implementations
- The best practices are not intended for mandatory regulatory efforts
- **Best Practices will require *continual* refinement, additions and improvement**

25

Network Security: International Initiatives

- **Europe:** Formation of ENISA adds to ongoing individual network operators' security efforts
- **Latin America:** Organization of American States initiative on Cybersecurity includes network security component, through CITEL
- **Asia:** APEC drafting recommendations on cybersecurity (hacking, encryption, spam) through APEC-Tel
- **ITU:** Next Generation Networks Study Group under ITU-T developing standards for network security

26

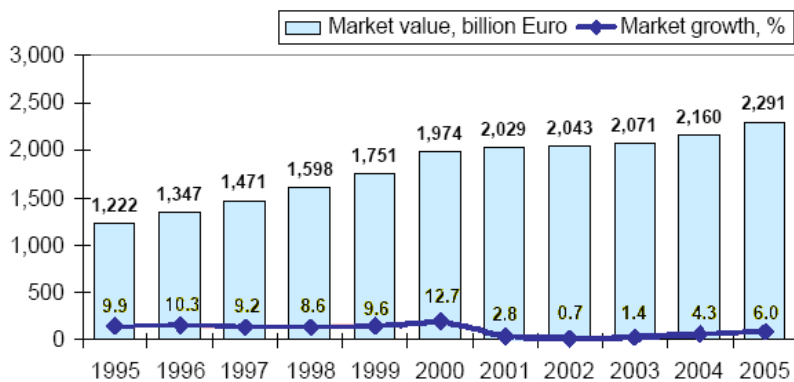
Contribution of IKED*:

The Global Trust Center

*International Organisation for Knowledge Economy and Enterprise Development

27

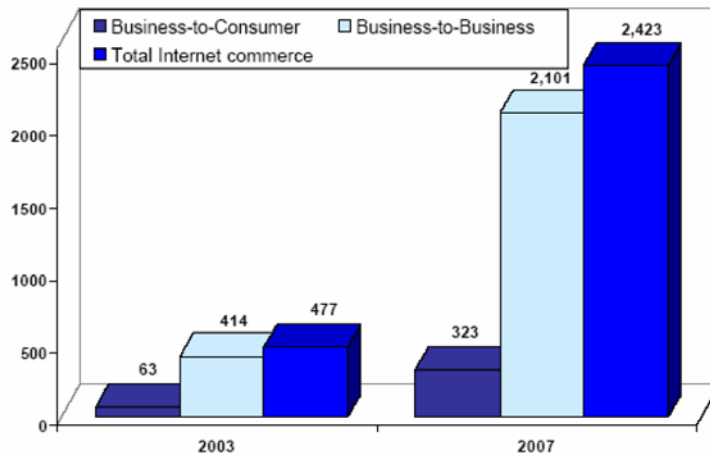
Worldwide ICT Market annual growth, 1995-2005, in %



Source: EITO (2004)

28

Internet Commerce in Western Europe, 2003 and 2007, in billion Euro



Source: EITO (2004)

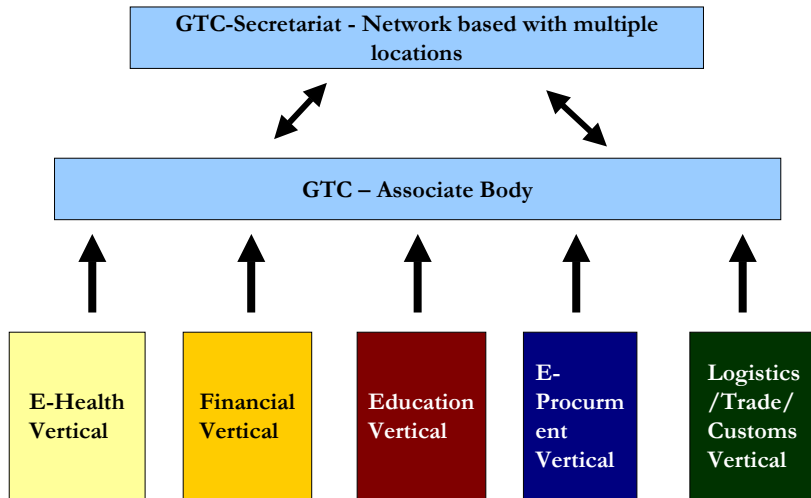
29

Risks

- Data confidentiality, availability and integrity;
- Consumer and merchant authentication;
- Non-repudiation and liability in the case of fraud;
- Costs from failure;
- Interoperability requirements.

30

Possible Global Trust Center Set-Up



31

Malmö, 04-11-2004

Contribution of Xian Group:

**Will Traditional Security
Companies Survive the Wired to
Wireless Convergence Revolution?**

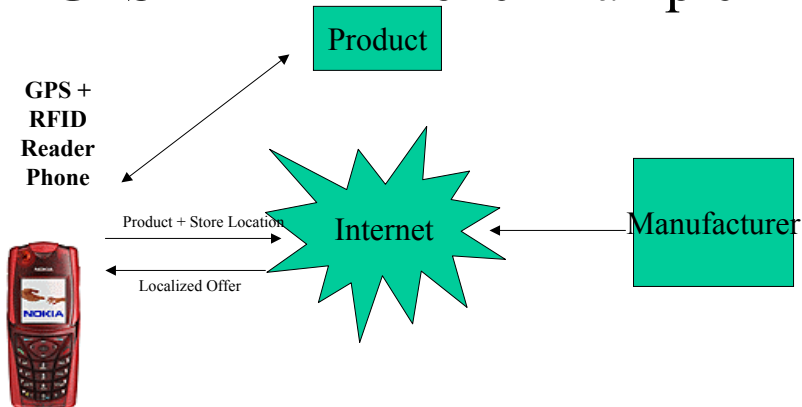
32

Security Providers Have Not Delivered The Same Level of Services to Wireless Devices

Core Security Services	PC	Wireless Devices
Password Protection	Yes	Yes
Personal Firewall	Yes	No
Intrusion Detection	Yes	No
Antivirus	Yes	No
Privacy Control	Yes	No
Ad blocking / Anti spyware	Yes	No
Anti spam	Yes	No
Parental Control	Yes	No
Encryption	Yes	Limited
Authentication (Certificate / Token)	Yes	Limited
Trusted Internet / Carrier Network Security Platforms	Yes	Yes

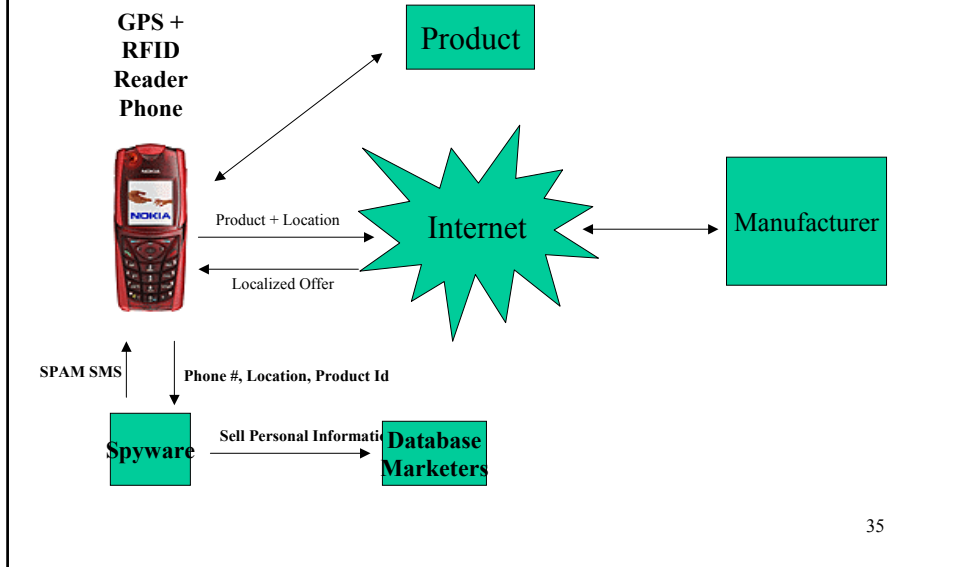
33

GPS + RFID Phone Example



34

Infected GPS + RFID Phone Example



35

Security Industry Trends To Support Convergence

- Companies are building out trust platforms.
- PC-based technologies are being ported to support wireless devices.
- Governments developing new privacy and security laws to protect consumers.
- New industry security standards and policies in development.

36

Key Challenges

- Security innovation has not kept abreast with aggressive wireless product innovations.
- Security threat will grow faster as wireless devices continue surpass PC usage on IP networks.
- Industry and governments must work closer on a global basis to develop more protections for consumers.

37

Contribution of Steptoe&Johnson:

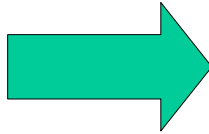
Liability Risks for Security Breaches

38

Why liability? – Answer one



**Something
Bad Happens**



**People Fight
Over Blame
and Financial
Responsibility**

STEPTOE&JOHNSON

Why liability? – Answer two

The major reason companies don't worry about the externalities of their security decisions ... is that there is no real liability for their actions. Liability will immediately change the cost/benefit equation for companies, because they will have to bear financial risks borne by others as a result of their actions.

Bruce Schneier

Testifying before U.S. House of Representatives in 2003

STEPTOE&JOHNSON

Statute and regulation – EU and USA

- EU directives implemented by national law in 25 Member States
- Data Protection Directive (95/46/EC)
- Privacy and Electronic Communications Directive (2002/58/EC)
- Gramm-Leach-Bliley (GLB) Act (1999)
- Health Insurance Portability and Accountability Act (HIPAA) (1996)

STEPTOE&JOHNSON

Statute and regulation – California

- Most important of the 50 states because of size, technology industry and legislative activism
- S.B. 1386 (2003)
 - Requires disclosure of security breach that compromises *unencrypted* personal information of California residents
 - Provides a private right of action
- A.B. 1950 (2004)
 - Requires any business (other than financial or health) that “owns or licenses” personal information of a California resident to “implement and maintain reasonable security procedures”
 - Provides a private right of action

STEPTOE&JOHNSON

Best practices

- Following “best practices” may be the best defence
- Don’t be a “poster child” for bad security
- Example – best practices for patching
 - Implementation of patches provided by manufacturer
 - Timely implementation schedule, taking into account deployment issues
 - Timely replacement of software, particularly if unsupported
 - Implementation of specific statutory and/or regulatory requirements