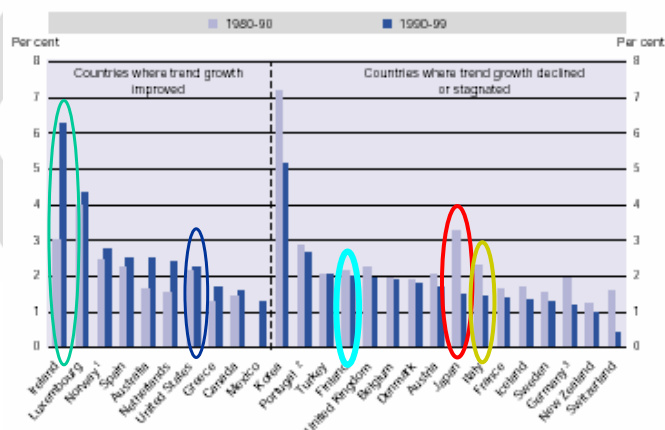


Trust & Security as key Challenges to Promoting ICT and Economic Growth

Presentation by
Nobuo Tanaka
 Director for Science, Technology and Industry
 OECD

at the
 APEC-OECD Workshop on Security of Information Systems
 And Networks
 Seoul, Korea
 September 5-6, 2005

Figure 1.2. Uneven trend growth of GDP per capita
 Total economy, percentage change at annual rate



Note: Trend growth in the 1990s was higher than in the 1980s in several countries: Australia, Canada, Greece, Ireland, Luxembourg, Mexico, the Netherlands, Norway, Spain and the United States. But trend growth declined substantially in Italy, Switzerland, Japan and Korea. The decline in trend growth in Germany is influenced by the unification process.

- 1. Total Norway.
- 2. 1990-98.
- 3. West Germany for 1980-90; Germany for 1991-99.

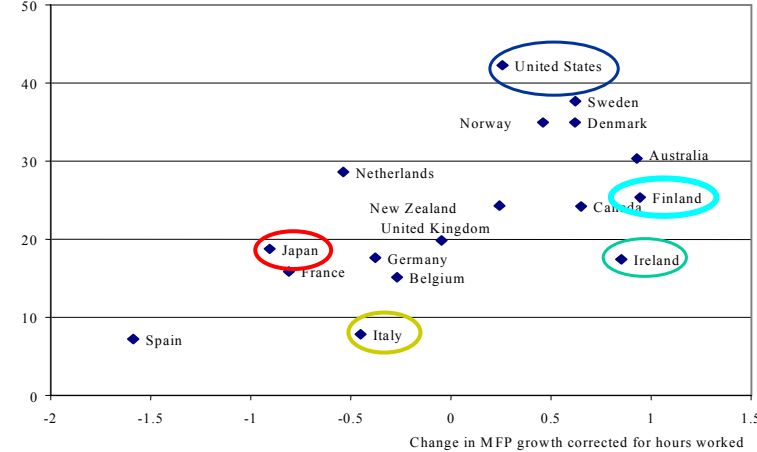
Source: OECD, based on data for the OECD Economic Outlook, No. 68. See Scarpetta et al. (2000) for details.

Source: OECD's Growth Report, "The New Economy: Beyond the hype" 2001.

Winners and Losers

Reason was ICT use: Pick-up in MFP growth and increase in ICT use

Change in PC intensity per 100 inhabitants, 1992-99



Greenspan noticed US productivity growth in late 1990s came from ICT use.

Note: Change in multi-factor productivity growth corrected for hours worked, average 1990s minus average 1980s.

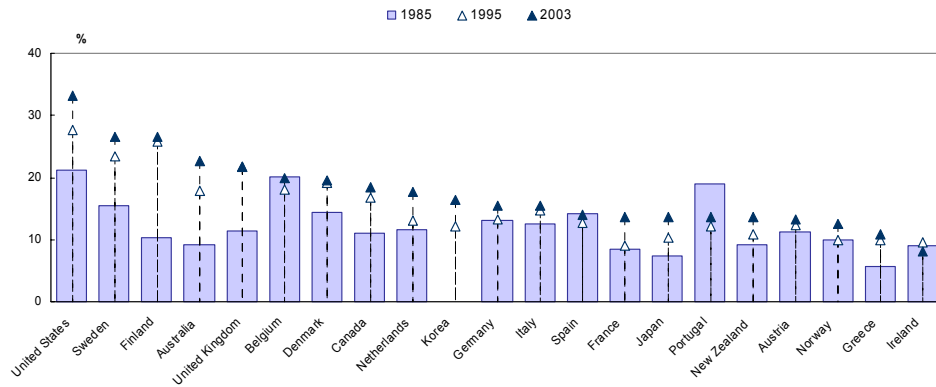
Source: OECD

The main thrust of my presentation focuses on four areas

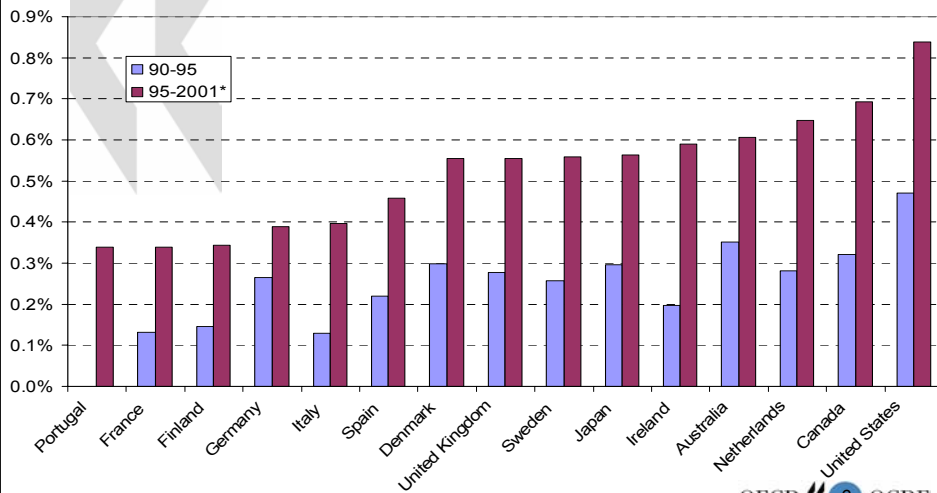
- Firstly, Information Communication Technologies has played a pivotal role in economic growth and productivity.
- Secondly, ICT will continue to play its role but it is under several challenges: globalisation, technological changes and **Trust**.
- Thirdly, governments should design policies that enable ICT to fulfil its potential, and the OECD helps its Members, as well as its key non-members partners do just that.
- Fourthly, what OECD and APEC can do together in the area of **Security and Trust**.

ICT investment has been uneven ...

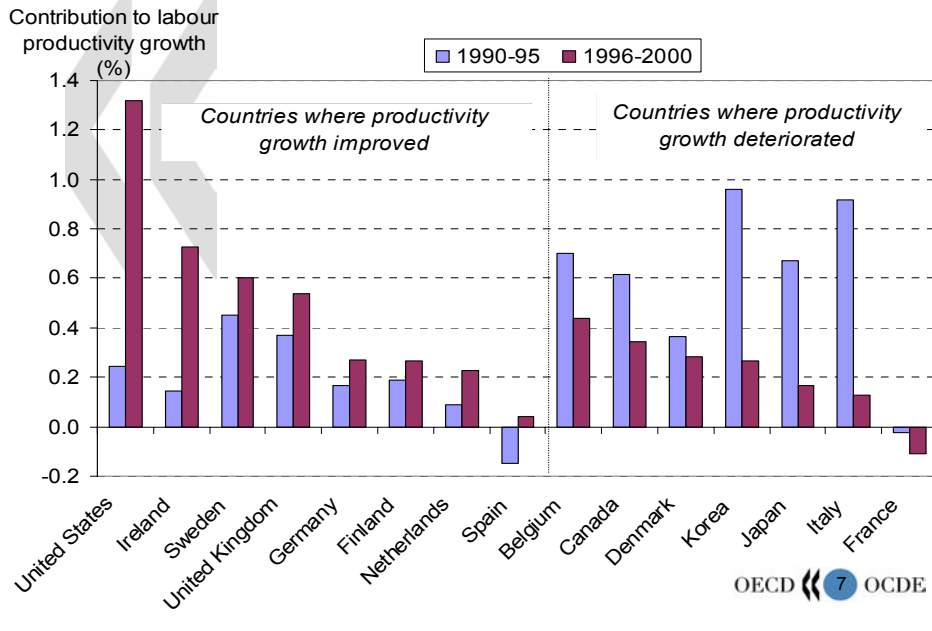
Investment in ICT 1985-2003; as a percentage of gross fixed capital formation



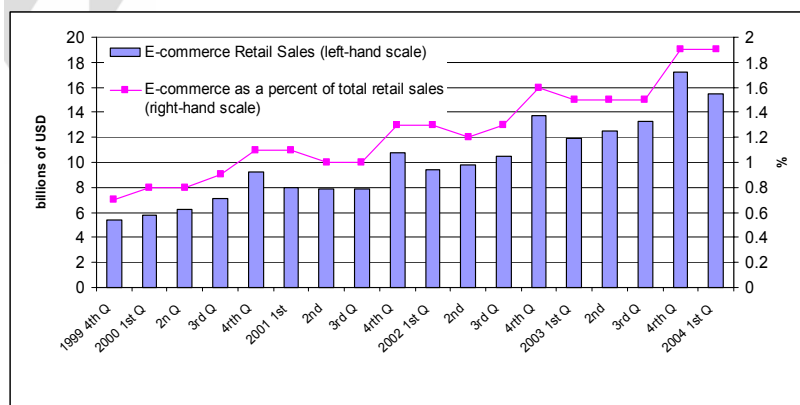
The contribution of ICT investment to GDP is substantial in some countries



Contribution to Productivity by ICT-using services



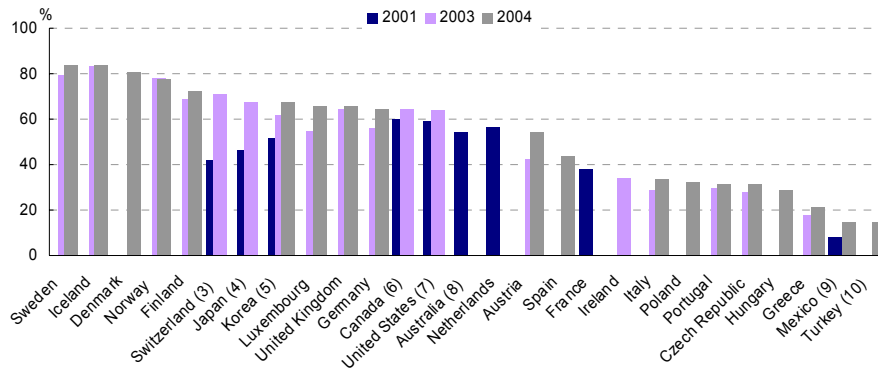
ICT and e-commerce continue to spread estimated quarterly US retail e-commerce sales



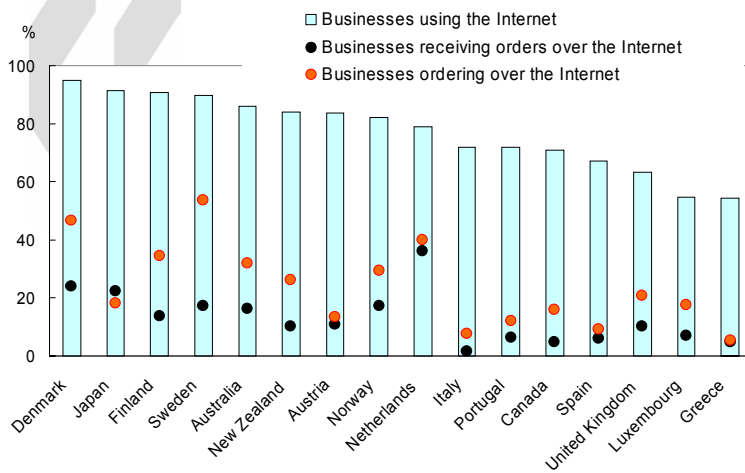
Source: OCED Information Technology Outlook, 2004

Access by Households and Individuals increases

Individuals using the Internet from any location, 2001-2004
As a percentage of all adults



Access to the Internet is high, but real business use still low



However ICT is **NO** panacea and many other factors require policy actions:

- Results from ICT are linked to investment in skills. Hunt for high-skilled workers is getting tougher.
- Organisational and Management change is needed to make ICT work. (firms that are already productive and innovative often get the best returns.)
- The impact of ICT depends on accompanying innovations (co-invention). Innovation-friendly system is needed.
- Scope for experimentation – ease of entry and exit allow firms to test markets and business models.
- Competition in ICT markets and throughout the economy. Global competition and service economy creates complex issues like off-shoring.
- **Demand has been held back by lack of security & trust. TRUST is becoming a major issue.**

Key Policy Messages

To better realise benefits of ICT, Governments should:

- Strengthen competition in ICT goods and services.
- Foster a business environment for effective use of ICT (org. change, skills, innovation, competition).
- Spread the benefits of ICT across the economy.
- **Boost security and trust to enhance usage of ICT.**
- Policies for ICT diffusion and infrastructure development are no longer sufficient; they need to be complemented with policies to remove barriers to demand and effective use of ICT.

Trust & Security are among the 6 OECD Priorities for international co-operation in ICT areas

Six OECD priorities areas:

- **Information Security:** *OECD Guidelines for the Security of Information Systems and Networks*, revised in 2002
- **Privacy:** *Privacy Online: OECD Guidance on Policy and Practice* updated 2003
- **Cross-border fraud:** the OECD released *guidelines* for more effective co-operation in enforcement of laws on cross-border fraud, particularly on the Internet in 2003
- **SPAM:** Today, 60% of e-mail is Spam! a Task Force on Spam to devise a comprehensive response by government, business and civil society to the problems posed by spam
- **Broadband:** *OECD Recommendation on Broadband Development* 2004
- **Digital content:** work ongoing to identify analytical, policy and measurement issues in this complex new area

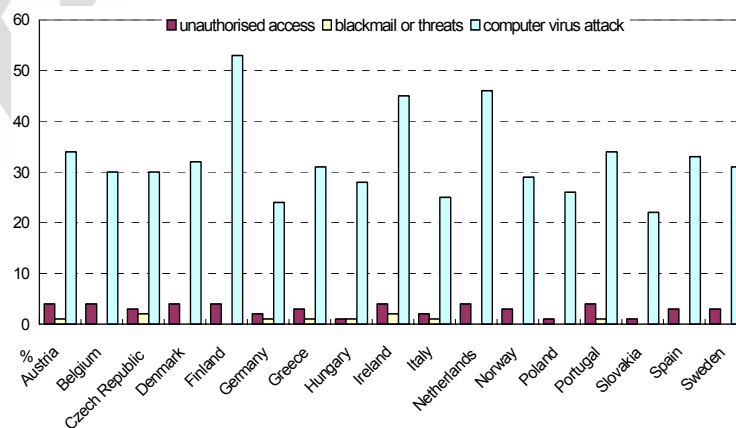
Trust & Security: what is the size of the problem?

- What are the data ?
- OECD work on "Indicators for Trust" aims at measuring the importance of trust online, evaluate the impact of OECD policy in this area, and guide further action.
- An OECD report to be declassified in the coming weeks reviews available official and private/semi-official statistical resources on ICT and Trust and concludes:

"The direct economic costs of phenomena related to trust, such as security and privacy, are growing rapidly. The available evidence all point towards a large increase in e-crime, such as identity theft or online fraud, as being inextricably linked to the rise in ICT use."

Security problems are widespread in enterprises

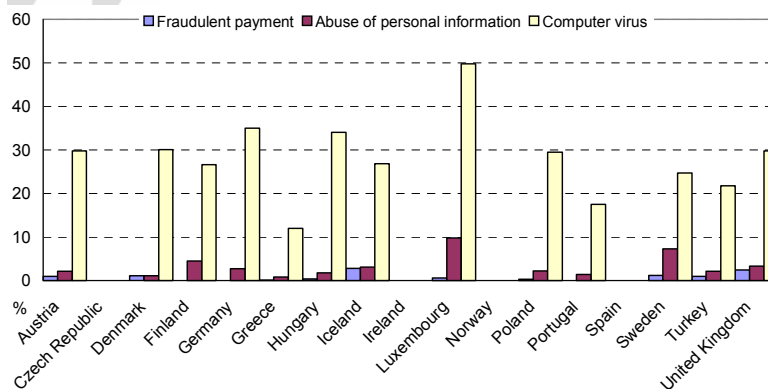
Percentage of enterprises with Internet access having encountered security problems in 2004
Percentage of enterprises with ten or more employees



Source: Eurostat, Community Survey on ICT Usage in Enterprises, 2003, February 2005.

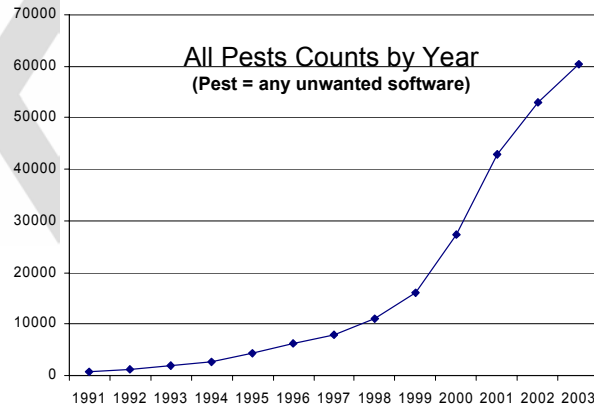
And among individuals

Percentage of individual Internet users having encountered security problems in 2004
Percentage of individuals who used the Internet within the last year



Source: Eurostat, Community Survey on ICT usage in households and by individuals, February 2005.

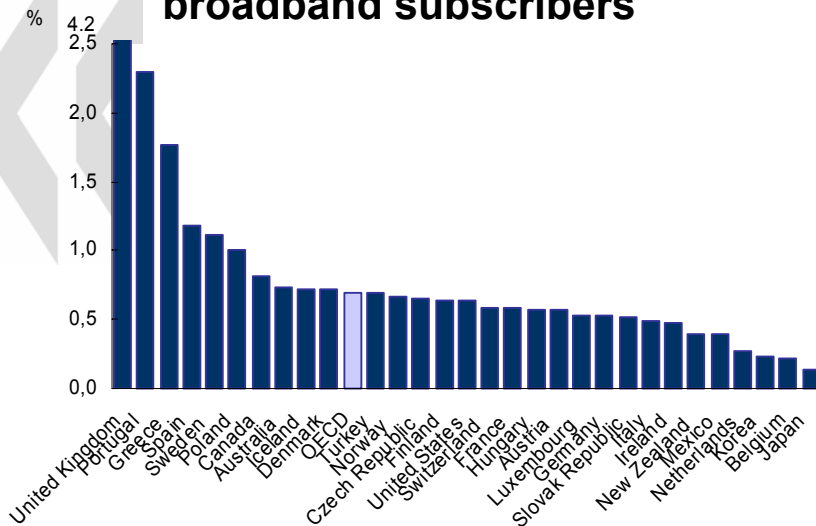
Explosion of malware



Cumulative number of pests categorized as "All Pests".

Source: http://research.pestpatrol.com/Trends/All_Pests_Counts_by_Year.asp

Bot infected computers per 100 broadband subscribers

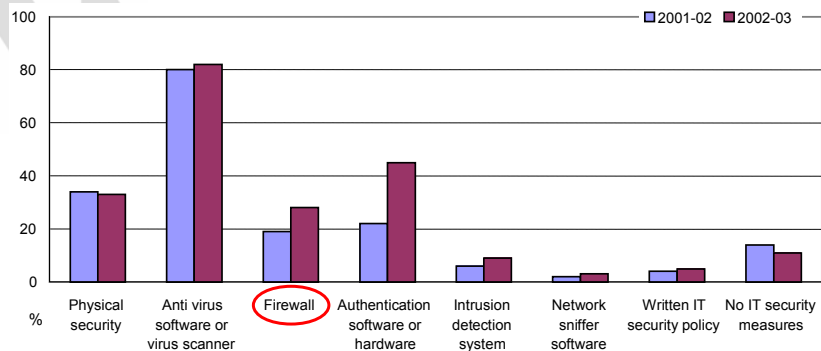


Publication : OECD STI Scoreboard 2005 (forthcoming)

Data Source : OECD, OECD calculations based on OECD and Symantec data, May 2005

Still a long way to go before full adoption of security software by users

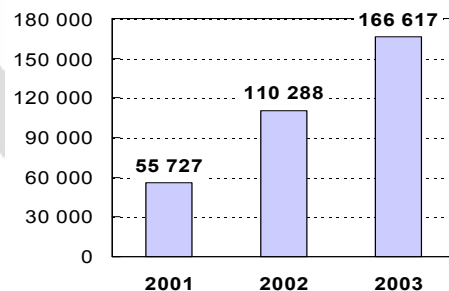
Businesses' security measures in 2001-02 and 2002-03 (Australia)
Percentage of businesses with a computer reporting on security measures in place



Source: Australian Bureau of Statistics, *Business Use of Information Technology*, 2001-02 and 2002-03, Cat. no. 8129.0.

Online fraud is growing

Consumer Sentinel, Internet-related fraud complaints, 2001-2003

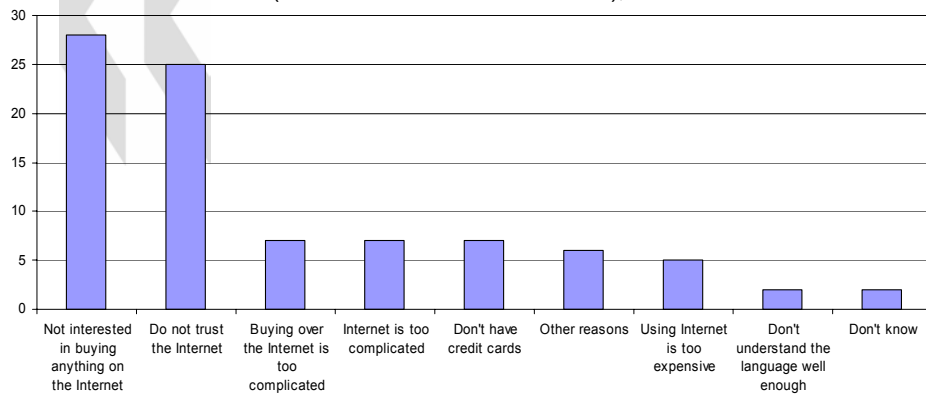


■ internet-related fraud complaints

Source: www.consumer.gov/sentinel/states03/internet_related_trends.pdf, September 13, 2004.

As a result: trust is a barrier to individuals buying online...

Reasons for not buying over the Internet in EU countries (individuals with Internet access), 2003



Source: European Commission, Special Eurobarometer survey on *European Union public opinion on issues relating to business to consumer e-commerce* (Reference: 201 EB60.0), March 2004.

Security is concern #1 for enterprises doing online business, including for large firms

Barrier	Small			Medium			Large		
	2001	2002	2003	2001	2002	2003	2001	2002	2003
Security concerns	13	17	17	13	20	19	11	18	22
Customers not ready	9	10	9	12	16	16	10	19	20
Suppliers not ready	5	6	4	7	9	8	6	12	14
Lack of skilled employees	9	11	11	8	12	8	5	13	8
Concerns about competitors analysing information	5	7	7	9	12	10	5	9	11
Available Internet is too slow	4	5	5	7	7	6	4	3	2
Uncertain about the benefits	8	9	8	7	7	6	3	5	2
Development and maintenance costs too high	11	14	13	10	15	16	6	13	17

Secondary Barriers to E-Commerce, by size of firm, 2001-2003, percent (Canada)

Source: Peters, Catherine and Anthony Nice, 2005, "Barriers to Electronic Commerce in Canada: A Size of Firm and Industry Analysis," Industry Canada, mimeo, presented at OECD WPIE June 2005)

Beyond e-commerce, the lack of security impacts the economy & the society at large

The migration of business, government, and individual's activities to IP-based systems and networks, the technical evolution towards anytime anywhere instant access to systems and networks, and the growing risks to the global IT infrastructure make "that infrastructure itself critical and in the national interest to safeguard".

- The economy in general, including critical infrastructures (communications, energy distribution, financial transactions) rely on the seamless functioning of information systems and networks.
 - In January 2003, the Slammer Worm infected 90% of vulnerable computers worldwide within 10 minutes of its release on the Internet, and severely degraded Bank of America's ATM network (\$ billions damages)
 - In the US, a hacker released intentionally hundreds of thousands of gallons of putrid sludge from the wastewater system
 - 17% of the 100 companies surveyed reported being the target of some form of cyber extortion
- "The IT infrastructure of the US is highly vulnerable to terrorist and criminal attacks" (President's Information Technology Advisory Committee "Cyber Security: A Crisis of Prioritization", Feb. 2005, United States)

Governments need policies. The OECD is assisting them.

- Security & Trust has been a constant strategic priority on the agenda of the OECD since the OECD Turku Conference in 1997
- After 9/11, the OECD adopted the "2002 Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"
- The Guidelines:
 - Promote a "Culture of Security" as a way of thinking about, assessing and acting on the operation of information systems and networks.
 - Provide a general frame of reference to help participants understand security issues.
 - Stress that preserving important societal values such as privacy and individual freedom is essential to achieving a culture of security.
- They call on:
 - Other countries to adopt a similar approach to security.
 - Businesses to build security into the design and use of their systems and networks and to provide security information and updates to users.
 - All individual users to be aware, and to act in a responsible manner by taking preventive measures.
- Other policy work related to trust: 1980 Privacy Guidelines, 1997 Cryptography Guidelines, 1998 Ministerial declaration on Authentication for Electronic Commerce, 2003 Cross-Border Fraud Guidelines

The Security Guidelines had an impact at the regional and global levels...

- The Council of the European Union adopted a resolution "on a European Approach towards a Culture of Network and Information Security" in February 2003.
- At the global level, the OECD Security Guidelines have also served as the basis for the Resolution A/RES/57/239 for "Creation of a Global Culture of Cyber Security" adopted by the United Nations General Assembly in December 2002 and were recognized by the APEC Council of Ministers.
- The ASEM Cyber Security workshop held here in Seoul in June 2005 invited ASEM members to adopt the Security Guidelines as guiding elements for the development of national and international policies.

...and at the national level

- Most countries who replied to the OECD survey have adopted a national policy for information security and use the guideline as a basis for their national framework
- OECD promotes the exchange of best practices and dialogue between governments and with business and civil society. The ICCP WPISP:
 - Organised a OECD Global Forum on Information Systems and Networks Security (Oslo, 2003) with participation from non-member economies
 - Issued two reports on the implementation of the Guidelines in member countries (2003, 2005 - to be declassified in the coming weeks).
- Among the main themes that have emerged from two surveys:
 - **International cooperation** is key and is pursued in various regional fora, facilitating dialogue and exchanges of **best practices**.

Global co-operation is needed

- The information systems and networks to be secured are global by nature. Co-operation is essential for realising a truly global culture of security for information systems and networks.
 - APEC Cybersecurity Strategy is a very important step forward. Like the OECD, APEC remains active in its subsequent work for the implementation of the Cybersecurity Strategy.
 - The OECD-APEC Global Forum on Policy Frameworks for the Digital Economy (Honolulu, Hawaii, January 2003) concluded that:
 - Advancing the creation of a global culture of security was a priority
 - OECD and APEC would co-operate in this area.
- **This workshop is the first joint event dedicated to security of information systems and networks.**

APEC-OECD future co-operation

- Co-operation could come in different forms. **Mutual endorsement** or **promotion** of the other group's achievements may be a constructive way forward that would make best use of the limited resources of the two organisations.
- It is hoped that this workshop will contribute to the exchange of information between the OECD and APEC communities, and be the basis for further co-operation in the area of security of information systems and networks.

Conclusion

Restructuring or Boneyard: The Need for Speed

While **restructuring** our Company in the 1980s, we spent much of our time talking about the accelerating pace of change: in world politics, in technology, in product introduction and in the increasing demands of customers. We don't have to do that anymore. Change is in the air. Newspapers and networks hammer it home daily. GE people today understand that pace of change, **the need for speed**, and the absolute necessity of moving more quickly in everything we do, from inventory turnover, to product development cycles, to a faster response to customer needs. They understand that slow-and-steady is a ticket to the **boneyard** in the 1990s.

"To Our Share Owners" (1990 Annual Report) of GE