Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

26-Feb-2004

English text only

CENTRE FOR CO-OPERATION WITH NON-MEMBERS
DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY

CCNM/GF/KE/DE(2004)1
Unclassified

OECD Global Forum on Knowledge Economy - The Digital Economy

OECD GLOBAL FORUM ON INFORMATION SYSTEMS AND NETWORKS SECURITY: TOWARDS A GLOBAL CULTURE OF SECURITY

PROCEEDINGS

13-14 October 2003
Oslo, Norway

This unclassified document contains the proceedings of the OECD Global Forum on Information Systems and Network Security: Towards a Culture of Security, held in Oslo on 13-14 October 2003. Speakers have been given the opportunity to review their contribution. Comments received have been integrated.

This event is part of the "Global Forum on the Knowledge Economy" managed by the OECD Centre for Co-operation with Non-Members.

This document is also listed as DSTI/ICCP/REG(2004)1 and will be posted on the OECD Web site following the WPISP meeting.

Contact: Anne Carblanc, Tel: +33 1 45 24 93 34, Fax: +33 1 44 30 62 59, anne.carblanc@oecd.org
Sven Moers, Tel: +33 1 45 24 93 65, Fax: +33 1 44 30 62 59, sven.moers@oecd.org

JT00158949

English text only

TABLE OF CONTENTS

OSLO GLOBAL FORUM ON INFORMATION SYSTEMS AND NETWORKS SECURITY

PROCEEDINGS

1. The Norwegian Government hosted the Global Forum on Information Systems and Networks Security: Towards a Culture of Security, in Oslo on 13-14 October 2003. The event was part of the OECD Global Forum on the Knowledge Economy Programme. The Forum attracted some 150 participants.

2. The **objectives** of the Forum were to:

- Take stock of progress made in the national implementation of the Security Guidelines.
- Share information with members, non-members, the business community and civil society.
- Have a forward-looking discussion on expanding the culture of security.

3. Day one concentrated on progress and achievements in OECD member countries. Day two was dedicated to experiences in other fora than the OECD, with perspectives offered from the European Union (EU), the Asia-Pacific Economic Co-operation (APEC), the Global Business Dialogue on Electronic Commerce (GBDe), and in non-member economies.

MAIN POINTS

A global Culture of Security is a key building block for trust online

4. Trust is fundamental for economic growth. In the digital economy, and in the information society more broadly, the security of information systems and networks is essential for building trust. The OECD Security Guidelines were designed to help improve the security of information systems through broadly based cultural change. The development of a culture of security is a collective responsibility to enable trust in the global information society through ensuring the reliability, integrity and sustainable development of information systems and networks.

In a global networked environment, risks, threats and responsibility are shared

5. All participants – governments, businesses and end users – at the national and at the global level have experienced the threats and risks that come with the expanding use of information systems and networks. Recent examples include virus and worm attacks that have rapidly spread over the globe. As the nature of threats is constantly changing, security will remain a challenge that requires a constant co-operative effort of all participants nationally and internationally.

Many valuable and practical initiatives have already been taken to implement the Security Guidelines

6. Many OECD countries have designed information security policies and have initiated awareness raising and education campaigns. They also have implemented response-related initiatives such as the creation of CERTs. Leadership has proved to be important to effectively implement a culture of security: in business as well as in governments, initiatives have been especially successful when the top management level has been involved. Educational initiatives targeting specific populations such as SMEs, end-users or children have also proven successful.

But there is still a long way to go to establish a culture of security

7. At the government level many initiatives have thus far consisted of high-level policy measures, such as national strategies, methodologies, guidance and recommendations. Most of the more practical initiatives have either been in operation for a rather short period of time or are still in the planning phase.

8. Further efforts could be useful in several areas which seem to have up to now received a lower degree of attention, such as sharing of best practices – especially among and with SMEs, building partnerships among participants (public-private partnerships) or the use of existing security standards such as ISO/IEC 15408 and/or ISO/IEC 17799/BS7799.

More action-oriented initiatives will foster the implementation of the Guidelines

9. Sharing best practices and experiences between participants and countries can help them to improve their own initiatives. There is a consensus that feedback from national experiences needs to be shared and the Global Forum was regarded as an important contribution in this respect. However, beyond workshops and surveys which allow for the exchange of general information, in-depth analysis of national policies and specific initiatives taken by OECD countries would provide a clearer picture of the progress made. All participants would benefit from an extended exchange of information which would allow them to reflect on whether their own initiatives are consistent with the guidelines and improve their own efforts as appropriate. There is also a need for initiatives, tools and methodologies for assessing the impact of the measures taken and of the progress made.

Establishing a global Culture of Security requires involving non-member economies

10. All participants acknowledged that the establishment of a culture of security must be global to be effective. Non-member economies are in the process of adopting a similar approach to that of OECD member countries, but have specific needs that should be addressed. Information sharing between OECD member countries and non-member economies about practical initiatives and experiences emerged as particularly important.

REPORT ON THE GLOBAL FORUM[1]

DAY 1: MONDAY 13 October 2003

Opening and Key Note Addresses

11. The Conference was opened by **Peter Ferguson**, Industry Canada, Chair of the Working Party on Information Security and Privacy.

12. In his keynote address, **Odd Einar Dørum**, Minister of Justice, Norway, recalled that if technological advancements result in new benefits, they also bring new threats and vulnerabilities. A dynamic rather than static mindset is required to debate on how to anticipate and address these new threats which may come from unexpected directions. He stressed that social contexts and human aspects are important factors to take into account in this reflection. Mr. Dørum then provided an overview of the measures taken by Norway to promote a culture of security, including the national strategy for information security which is based on the OECD Guidelines. He pointed out training and the creation of a sense of community as important means to ensure readiness and response to security risks. He concluded that an honest approach based on optimism about technology, on acknowledgement of the mistakes made and on discussion about the difficulties encountered was the most effective one.

13. **Herwig Schlögl**, Deputy Secretary-General of the OECD underlined that this Global Forum, which was part of the OECD Global Forum on Knowledge Economy, was an opportunity for member and non-member economies, business and civil society to share experiences while examining progress made regarding the implementation of the Security Guidelines. He highlighted that our dependence on the reliability of people and technology had turned trust into a key issue and provided an overview of other OECD work on trust including the Privacy Guidelines, Consumer Protection Guidelines, Cryptography Guidelines, and work on Alternative Dispute Resolution. He stressed that the OECD had long been successful in helping governments to find common policy approaches and internationally compatible principles, in particular by developing guidelines. As an example, he recalled the gap noted during the 1998 Ottawa Ministerial Conference between governments promoting opposed approaches: regulatory on one hand and market-driven on the other. He noted that OECD's work led stakeholders to ultimately agree on the need for a mix of approaches.

14. Mr. Schlögl pointed out that the Security Guidelines were a key element of trust and had to remain a major area of focus. He called for intensification of the exchanges of experiences between OECD member countries and their extension to other countries and international organisations. In this respect, the endorsement of the Security Guidelines by the United Nations, the European Union and the Asia-Pacific Economic Co-operation (APEC) were a clear encouragement to move forward towards strengthened international co-operation to develop a culture of security across the global information society.

[1] Slides of the presentations are available from the OECD Website at http://www.oecd.org/document/2/0,2340,en_2649_33703_17787394_1_1_1_1,00.html

15. **Oluf Ulseth**, State Secretary for Trade and Industry, Norway, highlighted the importance of Information and Communication Technology (ICT) as a key driver for growth in OECD member countries, transforming business practices as well as governments. In Norway, ICT was also an important driver for change in the public sector which is one of the largest in Europe. He detailed the eNorway 2005 Action Plan which is based on a holistic approach combining efforts towards the development of contents, skills, and infrastructures in order to benefit from ICT investments. He outlined that while citizens asked for new forms of interactions with government, including access to personal files for example, content availability and trust issues turned into key challenges for ICT growth.

16. Mr. Ulseth stressed that the development of a culture of security was a major objective in the Norwegian National Strategy for Information Security, together with the facilitation of secure e-commerce through the introduction of electronic signatures, the establishment of a coherent national policy for the relevant authorities and the co-ordination of their efforts in the field of IT-security. He emphasised the pivotal role of the OECD regarding both the definition of a coherent global approach to the issue of trust and the implementation of the corresponding solutions.

Introductory remarks

17. **Peter Ferguson**, Chair for the Global Forum, welcomed the organisation of this event by Norway and the opportunity for all participants within and beyond the OECD to share information on how they implement a culture of security, and the reasons for success or failure in their specific experiences. He also pointed out the sharing of experience with non-member economies as a major goal for this event.

18. **Hugo Parr**, Chair of the OECD Committee for Information, Computer and Communications Policy (ICCP), recalled the emphasis placed by the Honolulu Conference on the fact that effective ICT policies are important to help ICT use remain a primary driver for economic growth for the next decade. He mentioned trust as a key issue for ICT growth and indicated three tradeoffs to be addressed in this area: the costs of security versus the benefits, security versus user convenience, and security versus privacy.

Session 1: Creating a culture of security for information systems and networks

Round Table on the roles of the participants

19. **Peter Ford**, First Assistant Secretary, Attorney General's Department, Australia, served as moderator for Session 1. He indicated that the focus of the session was on the roles of government, business and end users in relation to the Guidelines; on how they utilised or implemented the Guidelines; and how they could work together. Participants in this session included representatives from government, business and the civil society.

20. He introduced the discussion by highlighting that the 2002 revised Security Guidelines take into account the tremendous changes which have occurred in the ICT environment between 1992 and 2002. He noted that, by promoting the concept of a "Culture of security", the Guidelines were not intended to place security above other values. Instead, the Guidelines called on all participants to consciously consider the security aspects of their activities. He provided an overview of the nine principles of the Guidelines: awareness, responsibility and response, ethics and democracy, risk assessment, security design and implementation, security management and reassessment. Mr. Ford gave a brief overview of the activities for implementing the guidelines in Australia in the framework of the "Trusted Information Sharing Network" initiative.

21. The implementation of the Guidelines in Australia was also based on regular discussions with other countries. From these discussions it seemed that some common characteristics could be identified: A fundamental strategy for creating a culture of security was the promotion of public sector/private sector partnerships in addressing security issues. The protection of national information infrastructures was recognised as being dependent on appropriate international arrangements. Awareness raising was seen as an essential element of protective security arrangements. In some countries sectoral requirements determined the nature of security arrangements in the various components of critical infrastructure protection. Mr. Ford closed his speech emphasising that responsibility for security was shared among all participants and that security is a dynamic process that requires constant readjustment in the light of changes to the external environment.

22. **Tomohiro Innami**, Director, Office of IT Security Policy, Commerce and Information Policy Bureau, from the Ministry of Economy, Trade and Industry in Japan recalled the damages caused by the MS Blaster worm which attacked computers connected to the Internet during summer 2003. This incident was a good illustration of the shared responsibilities of all participants and the need to develop a "culture of security". He provided an overview of the Japanese Information Security Comprehensive Strategy which is consistent with the OECD Security Guidelines, and is based on three pillars: *i)* one should be aware that 100% protection is not possible and that incidents will happen; *ii)* reliance of computer systems and networks on a single operating system or vendor is questionable; *iii)* strategies and budgets should be coordinated to avoid duplication of resources and overlapping strategies. As regards critical infrastructures, Mr. Innami stressed that their protection was a matter of shared responsibility between the public and the private sectors. He outlined the Special Action Plan to Protect Cyberspace adopted three years ago by the Japanese government which promotes information sharing between the public and private sectors and for the establishment of contingency plans.

23. **Andy Purdy,** Acting Deputy Director of the National Cyber Security Division of the Information Analysis and Infrastructure Directorate from the U.S. Department of Homeland Security (DHS), insisted that the creation of a culture of security implies efforts regarding both digital and physical security. He mentioned individual citizens' awareness regarding security as a priority. As regards critical infrastructures, he provided an overview of the measures taken by the US government to protect 14 key areas identified by the DHS, such as banking and finance, chemical industry and information technology. He indicated that the objective was to reduce the warning and response time from four hours to 30 minutes over the next twelve months. He mentioned the creation of a National Computer Emergency Response Team (US-CERT) and outlined that more formal procedures needed to be established in order to ensure that key information is being shared as necessary. He also pointed out the need for information sharing between the private and the public sectors. He mentioned the importance of international co-operation and called for the creation of an international watch and warning network.

24. Mr. Purdy stressed that audit standards to review readiness are necessary and like other kinds of best practices, should be developed in ways appropriate for business as well as for the public sector and made available to both. He emphasised that the measurement of progress made is essential and implies the development and use of methodologies to assess risks to produce visible benchmarks and metrics. He mentioned the need for national cyber exercises for key agencies to test response to cyber attacks. He finally pointed out that the level of security awareness of each individual should be raised up to the point where home users know how to make their system more secure.

25. **Lowell E. Thomas**, Director, Government Plans and Programs, Verizon pointed out that the power outage, the MS Blaster and Sobig worms' attacks and the Isabel hurricane which all struck the US during the same period of time demonstrated very well the interdependence of information systems and the importance of the Security Guidelines' Response principle. Referring to this principle which recommends cross-border information sharing, he drew a distinction between domestic and international information

sharing. Domestic information sharing includes co-operation from companies to companies, from companies to government through Information Sharing and Analysis Centers (ISACs), from governments to ISACs, and from government agencies to government agencies. Regarding international co-operation, he recalled that bilateral and multilateral dialogues had been initiated by the US before 9/11 with participation of industry and had proven to be invaluable. He stressed that cross-border information sharing should begin domestically by building platforms and processes for dialogue involving key sectors.

26. Mr. Thomas finally pointed out that trust and real life exercises are required for information sharing to take place at both the domestic and international levels, and concluded that the OECD guidelines were offering a framework for action to build a culture of security at the global level.

27. **Marc Rotenberg,** Electronic Privacy Information Center (EPIC) executive director and representing the Public Voice coalition (civil society) offered an overview of the work of the coalition, including its co-operation with the OECD on trust issues. As regards the Security Guidelines, he pointed out that they are of common interest for government, business and civil society. However, civil society holds a different position from the other participants for two reasons: *i)* the "awareness", "ethics" and "democracy" principles are considered important principles as security should not be reached at the cost of key political and social values; *ii)* unlike governments and businesses who determine security practices, computer end users do not and should not be expected to have deep technical knowledge, just as car drivers are not expected to have technical knowledge beside steering and braking.

28. Mr. Rotenberg said that the willingness to assess and understand risks before adopting new features is essential for network security. The agreement reached, after a complaint filed by EPIC with the Federal Trade Commission (FTC) concerning the possible impact on security of Microsoft's centralised sign-on service "Passport", has shown that the Government could play a positive role in assessing systems in the private sector, a light form of regulation through oversight that may be more needed in the future. Finally, he listed the three most critical challenges for information security: *i*) how to safeguard digital rights without stifling creativity; *ii*) how to provide security without sacrificing privacy; *iii*) how to promote security without a loss of transparency.

Discussion

29. The discussion mainly focused on issues related to awareness and education, and responsibility.

30. As regards the nature and content of national awareness campaigns and the use of metrics and benchmarks for assessing information security at national level, **Andy Purdy** explained that the message conveyed to individuals through US national awareness campaigns is that home users need to protect their personal information on their machine. Such campaigns also provide practical information to users on how to secure their home systems. In order to develop metrics and benchmarks, the US is seeking involvement from ISPs to measure how many of their users are secure. A partnership with the US Census Bureau will survey 35 000 businesses and 200 000 households every two to three years on their level of cybersecurity preparedness.

31. As regards the relationship between security and responsibility, **Marc Rotenberg** outlined that it is more difficult for the end user to take responsibility for his/her own system where Digital Rights Managements systems take the hardware platforms' security features away from the user and give it to the intellectual property rights owner. Speaking from the floor, **Stephanie Perrin,** President, Digital Discretion Inc., noted that contractual or legal attempts to make individuals responsible may put a heavy burden on the end user and asked how this could be managed. **Marc Rotenberg** spoke in favour of an approach in which the stakeholder who is in the best position to minimise risks carries that burden. For

example, a seller is in a better position to know where products have defects and thus should have more responsibility than users because he has more capability. **Peter Ford** indicated that in Australia these issues are left to courts whose decisions may vary as this is a developing process. Speaking from the floor, Commissioner **Orson Swindle,** US Federal Trade Commission, commented that IT users should be responsible for keeping their computer safe just as automobile users are responsible for keeping their car safe, but that this process will take time even if the IT sector's evolution is faster than the automobile's.

Session 2: Examples of implementation: Case studies and practical guidance

32. **Carol Curd**, CIO for Enterprise Information Security and Privacy and Enterprise Information and Technology, EDS, served as moderator for Session 2. She indicated that the session was intended to reflect as much as possible the views of government, business, and end users/academic/non-profit organisations on methods and priorities for implementing the security guidelines. She explained that the session was divided into four parts: a general introduction to the state of implementation of the security guidelines within OECD member countries; a discussion of the awareness, education and responsibility principles, another on the response principle, and finally a discussion on the security life cycle principles. She mentioned that the speakers were expected to address the broader principles and to illustrate their implementation using case studies and practical guidance.

33. As an introduction, **Anne Carblanc** from the Directorate for Science, Technology and Industry at the OECD gave an overview of the interim results of a still ongoing survey on the implementation of the Security Guidelines by OECD member countries. Consistent with the Implementation plan that member countries had agreed upon in January 2003, a questionnaire had been circulated in July 2003 with 24 questions related to the roles of Governments, business and civil society. By August, responses from 14 member countries had been received.

34. She indicated that the completion of the survey generally demonstrated that responding countries had effectively undertaken to provide leadership in developing a culture of security. Indeed most of the questions asking member countries whether they had or not taken action scored very high numbers of yes. The detailed answers provided illustrative examples of measures or programs of interest for effectively implementing the Security Guidelines. Anne Carblanc stressed that the exercise was also useful in terms of identifying areas which had received a high-level of attention and areas in which member countries could strengthen their efforts.

35. She mentioned, among the main areas for current focus, the development of national public policies; outreach and support activities for other participants (such as CERT-like institutions); awareness raising; and education and training, including initiatives targeting specific populations such as young people, the general public, IT professionals or SMEs.

36. Among the areas having received a lower degree of attention, she mentioned the publication of best practices or recommendations either to foster the development and the exchange of best practices or as an operational improvement for the benefit of all participants; standards and/or the promotion of certified products or selected technologies for IT procurement in order to influence other participants; and the use of international standards.

37. She suggested that more detailed information on current national initiatives to implement the Security Guidelines, measurement of the impact of these initiatives, and sharing of this information would enrich future research on the implementation of the guidelines, contribute to a consistent implementation in member countries and foster the development of a global culture of security. Possible further action by the OECD could include educational country reviews and further co-operation with non-member economies.

Awareness, education and responsibility

38. **Dr. Lorenzo Valeri**, RAND Corporation Europe, outlined the content of the "eAware" research project funded by the European Commission which involved 10 EU members and accessory states. A free guide for structuring initiatives for raising public awareness about information security had been produced out of the project's findings and a final international Conference was to be held on 7 November 2003 in Rome, Italy (see http://www.eaware.org).

39. Key findings from the research were that: *i)* it is important to use a marketing approach for information campaigns to overcome the traditional public antipathy towards technical issues and to persuade the public to care about information security; *ii)* any information campaign should refrain from only conveying a negative message and from making users more scared; *iii)* the campaigns should include information on possible solutions and where they are available to users; *iv)* the message should be tailored to the needs of the targeted audience and to the local environment to avoid failure because of cultural differences; *v)* focus groups and other tools to measure the effectiveness of a campaign should be used.

40. Dr. Valeri indicated that another initiative to raise awareness among experts had resulted in a practical handbook about computer-related crime in the 15 member states of the EU containing information about the forensics and reporting mechanisms in these countries. This initiative targeted CERTs and was based on the CoE Convention on cyber-crime and the Proposed Framework Decision of the EU on attacks against information systems.

41. **Cosimo Comella,** Head of the Technological Resources Department at the Italian Data Protection Authority, gave an overview of initiatives taken by the inter-ministerial committee of the Italian Government to promote a responsible use of the Internet. He stressed that these initiatives, targeted at children, aimed at teaching them how to behave and adopt a responsible behaviour. Indeed, the number of children online in Europe had increased by one third in a year, and many children were visiting the same sites as adults do, running the risk of being exposed to material which is not suitable for them.

42. Mr. Comella indicated that the interministerial Committee – composed of representatives from the Ministry of Education, the Ministry for Technology and Innovation, and from law enforcement agencies and other public authorities in Italy – had prepared a simple guide to the Internet, available from the Italian government portal (www.italia.gov.it), to give parents – regardless of their level of technological knowledge – an introduction to the Internet. Parents could also download the Internet Content Rating Association (ICRA) software to filter inappropriate sites. A simple interactive game taught children how to take advantage of the potential of the Internet while safeguarding themselves from its potential hazards.

43. The Committee had also drafted a co-regulation code together with other stakeholders from the public and the private sectors (including the major Internet Service Providers Associations), the objective being to foster a culture of responsibility of the parties active on the network. The code was currently under review. Furthermore, in order to foster a culture of security, a code of conduct for the public administration was being drafted, with clear rules to teach civil servants and public officials correct use of the Internet and electronic mail.

44. Mr. Comella concluded by saying that Governments alone could not secure cyberspace for children and other users. No strategy could completely eliminate the risks, but the Government could and had to act to promote awareness and to empower citizens and families.

45. **Jeremy Ward**, Symantec UK, reported on a joint initiative of the Business and Industry Advisory Committee to the OECD (BIAC) and the International Chamber of Commerce (ICC). As all business is a matter of trust, security needs to be seen as a business enabler rather than only a business cost. In order to help businesses implement the OECD Security Guidelines, BIAC and the ICC had prepared an international Commentary on the OECD Guidelines aimed at business executives, to help them ask the right questions of their IT department or suppliers. A similar booklet for SMEs will be prepared in due course.

46. He indicated that the booklet contained a more complete explanation of the guidelines, a checklist for businesses with examples of best practice in implementing the Guidelines and links to other standards and regulations (*e.g.* Basel II, ISO 17799). The information provided could be used with employees, shareholders, partners, customers and for a dialogue with regulators. He stressed that it was important to raise awareness about security issues with non-ICT staff in businesses. This will help to ensure that security is seen as everyone's responsibility, not merely that of the IT department. Finally, Dr. Ward outlined examples for the implementation of the Guidelines at the practical level.

47. **Francisco Lopez-Crespo** from the Ministry of Public Administration, Spain, focused on the use of security criteria and of standardisation to give electronic procedures the same legal value as written procedures in the public administration in Spain. Because the "eAdministration" services for citizens require broadly accepted and effective criteria, the Spanish administration had produced a catalogue with legal requirements and matching organisational and technical measures for the design, development, implementation and operation of applications used by the General State Administration bodies in the exercise of their functions. This included the delivery of electronic services and of personalised communication to citizens. The criteria reflected existing security requirements in the Spanish legal framework as well as instruments for the global management of security (*e.g.* ISO/IEC IS 17799). In addition to this, a methodology ("MAGERIT") for risk analysis and risk management had been developed.

48. Mr. Lopez-Crespo indicated that, among other things, the criteria included regulations on security design and implementation, such as evaluation and certification procedures. The criteria aimed at a comprehensive approach to security management and included measures for reassessment and regular upgrades of security measures according to a formal calendar.

Discussion

49. Speaking from the floor, **Peter Ford** asked all three presenters for possible comments on future work, initiatives for best practices and whether further reviews of initiatives might be helpful.

50. **Jeremy Ward** responded that BIAC and ICC would be interested in more details on the needs of specific countries particularly as regards SMEs. He stressed the need to "individualise" the implementation of the Guidelines to reflect the local legal situation in one country. He noted that sharing of information on security incidents among companies was still difficult and would need to be promoted and fostered.

51. **Lorenzo Valeri** stressed that the "e-Aware" project had been focused on the end-user. He noted that however the sharing of information between different countries might be difficult as the "e-Aware" project had shown that solutions that worked well in one country might not work at all in another country. He suggested that governments work more closely with local industry, based on the OECD basic platform. He mentioned that mobile telephony and other mobile services should also be taken into account.

52. Speaking from the floor, **Jeremy Beale**, Confederation of British Industry, insisted on the need to sensitise board members, to involve SMEs, and to bring various efforts together. Regarding awareness initiatives, he thought it necessary to create a "common roof" as there were too many different initiatives.

Response

53. **Peter Burnett** from the UK National Infrastructure Security Co-ordination Centre (NISCC) reported on the UK WARP (Warning, Advice and Reporting Point) programme which is part of a broader information sharing initiative in the UK.

54. The NISCC has developed the WARP concept as a cost-effective alternative to the existing CERTs which can be realised at a fraction of the costs of a CERT and is better suited to the needs of small communities, including SMEs and citizens who were less likely to use CERT services but nonetheless could benefit from CERT-type services and support. WARPs perform some of the tasks of CERTs while not being expected to provide a technical response service to the extent most CERTs do. A WARP provides a filtered warning service by issuing alerts and warnings specifically tailored for its community. It acts as a link to advice and best practice. WARPs gather, sanitize and share incident reports and provide a limited help-desk service for the community, geared to the specific needs and building on the knowledge of the community membership. The WARP concept builds on successful ideas from other sectors (Neighbourhood Watch, Citizens Advice Bureaux). Information on incidents could be anonymised before publication to overcome the reluctance of companies to share information about incidents directly related to them.

55. A "London Connects" WARP had been set up for the London Boroughs. The promotion of information sharing and of WARPs had become a UK policy in the UK Government's Information Assurance strategy.

56. Mr. Burnett recalled that sharing knowledge and information about security incidents helps to build assurance and to develop good practice, and stressed, as regards threat assessment, the need to have information on what is happening in one's own specific sector, and not only on national or global trends or services.

57. **Hiroyuki Takeda**, Director, IT Security Office Information and Communications Policy Bureau, Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan gave an overview of the activities of the Japanese Telecom-ISAC (Information Sharing and Analysis Center). Founded in 2002 as an initiative from the private sector, the Telecom-ISAC was the first of its kind to be established in Japan. Founding members were the seven leading Japanese ISPs. In the future over 100 ISPs were expected to join the organisation. The objective of the ISAC was to collect, share, analyse and provide information on incidents through co-operation and co-ordination among its members.

58. Among the services offered by the ISAC, he mentioned the provision of vulnerability and alert information (since March 2002) and the operation of a portal site. He indicated that the design and implementation of an incident handling system that collects and analyses information on incidents reported by members, as well as of a Wide-area monitoring system aimed at providing a global analysis on ISP security and traffic information (to be monitored automatically by network sensors placed at ISPs spread across Japan) were under way. He also mentioned the objective to further develop the Telecom-ISAC Japan into an ISAC Operation Center.

59. **Stefan Grosse** from the Federal Ministry of the Interior, Germany, reported on the German Mcert initiative. The Mcert-initiative is a CERT directed at small and medium-sized enterprises. It is a public-private partnership project founded by the German ICT association BITKOM, seven industry sponsors and the German Federal Government. At present a test-bed phase with 30 users was in place, and regular operation of the service would start at the beginning of December 2003.

60. He described Mcert as combining security advisories from different sources (the CERT network, the public sector and from industry partners) and processing them into an easy to understand language with added recommendations for action. The objective of Mcert being to provide two types of services, one directed at small companies without an IT department and another for companies with more than 50 employees and an in-house IT department, clients were to receive alert information tailored to their needs based on an IT profile to be created during the registration process. The objective was to have Mcert financed by the founding partners for three years, and then to have the service financed from user fees.

61. Mr. Grosse finally indicated that future activities would include setting up a system for incident reporting and building an emergency response system through which Mcert would arrange for on-the-spot contacts for clients with IT security service providers.

62. **Jinhyun Cho** from the Korea Information Security Agency (KISA) outlined the concepts for the Korean Internet Incidents Response and Support Center to be officially opened by the end of 2003. He recalled that current trends in security incidents include the introduction of hybrid threats integrating hacking, viruses and spam techniques, and that single incidents create increasing economic damage, such as in the case of the "slammer worm" which caused economic damage estimated, for Korea alone, to range up to USD 35 million.

63. He indicated that to improve the existing incident response system, a hot-line on the basis of a Trunked Radio System (TRS) had been established which allows for the timely information of hot-line members on security incidents. For recent incidents, the Korean authorities had improved the timeliness of the release of alerts and warnings.

64. He finally mentioned that the planned Korea Internet Security Center (KISC, to be opened on 17 December 2003) would work on the early detection of incidents on the domestic Korean Internet backbone network and provide for a 24/7 Co-operative Incident Response System. It was to comprise a network monitoring team (monitoring the backbone network and issuing hacking/virus alerts and warnings), an incident analysis and response team (doing research on hacking/virus techniques and response actions) and a response co-ordination team which would co-ordinate the sharing of information and other means of co-operation with domestic and foreign parties.

Discussion

65. Reacting to a question from the audience on how information could be passed on by a WARP, **Peter Burnett** reiterated the importance of keeping the projects small and of sending only pertinent information to users. He indicated that there was an ongoing project in the UK's WARP programme for allowing users to select information for specific environments.

66. Speaking from the floor, **Stephanie Perrin**, Digital Discretion Inc., noted the risk to focus on trust in the security debate while the issue really was about contracts and commitment. **Peter Burnett** took a different view indicating that the UK Government CERT had built up a network of CERTs which it trusted by giving them sensitive information. He insisted on the "give and take" process: we trust your information – you trust our information, and on the risk that, should trust be broken, the WARP or CERT would lose credibility with its customer base and peers, and might no longer be able to function.

Security life cycle

67. **Yih-Jeou Wang**, Head of Division, Ministry of Science, Technology and Innovation, Denmark, stated that national security was not a solely national issue anymore, but needed to be addressed from an

international perspective and required international co-operation. There was a general need for making the use of information and communications technology (ICT) more effective, especially in e-government, and ICT security was a prerequisite for the digitalisation of the public sector. He noted that surveys conducted in Denmark on domestic IT security problems indicated that the public sector had recently been more affected by viruses than the private sector, demonstrating the need to create a trustworthy environment to enable an e-society.

68. Among the areas for action by government, he mentioned the development of an IT security culture at the national level through awareness campaigns, advice and guidance; prevention and restoration through the implementation of common standards, early warning systems and timely emergency planning; targeted development of new knowledge and competencies through research and education. He insisted that the ICT infrastructure had become one of the most important elements to be protected and that it was important to monitor security constantly at the national as well as at the global level: global collaboration and international co-operation played a major role in this. Finally, he recommended that governments enter into a dialogue with industry and develop strong public-private partnerships.

69. **Mikael Kiviniemi** from the Ministry of Finance, Finland, presented the approach taken by the Finnish government with regard to Security management, design and implementation of the OECD Security Guidelines. He referred in particular to the Finnish Government Policy on Information Security, and its Information Security Strategy, Recommendations and Guidelines. He indicated that the Finnish government policy model (*e.g.* administrative and organisational information security or data security) was used by businesses.

70. Among other components of Finlands' Policy on Information Security (in place since 1999), he highlighted the assignment of responsibilities to ministries and government agencies, and the establishment of information security management in the administration. He indicated that enforcement measures had also been taken. As regards information security management, he stressed that all agencies were obliged to take appropriate measures (*e.g.* the development and implementation of a specific security recovery plan), based on Instructions and Guidelines by the Ministry of Finance and on broader obligations in legislation (*e.g.* Data Protection or Telecommunications legislation). Beyond general guidance, the Information Security Recommendations and Guidelines did contain: instructions for specific areas like software development, outsourcing activities, remote work, LANs, assessment of the information security management system and of risks. All guidelines addressed threats, risks and vulnerabilities and most included checklists or offered technical solutions.

71. Mr. Kiviniemi stressed that governments should not over-regulate in the domain of information security, but rather help organisations include security in their processes and invest in the production of recommendations to be used across different sectors. Finally, he recalled that Information Security is a shared responsibility for all participants, not only for ICT staff.

72. **Ralf M. Engers,** Chief Technology Officer, Utimaco Safeware AG, Germany, gave an overview on technological and organisational aspects of secure software development and use, and stressed the importance of independent certification procedures notably to overcome the current difficulties for customers to find the right security products.

73. He explained that the "Common Criteria" for Information Technology Security Evaluation played a major role in this field by harmonising existing national and regional evaluation criteria (like the "Orange Book" or ITSEC) and had been accepted by ISO (ISO 15408). He indicated that the Common Criteria define two types of IT security certifications: Functional Requirements ("what a product does") and Assurance Requirements ("is the product built well and does it meet the purpose?"). Mr. Engers also gave an overview of the different Evaluation Assurance Levels (EAL) in the Common Criteria and the

concept of Protection Profiles and Security Targets. He insisted that security should be built into products "by design" and that thorough testing played a key role in the development of secure IT products.

74. Mr. Engers finally highlighted the need to understand that security is a shared responsibility across a company and across hierarchies.

Ethics and democracy

75. **Georg Apenes**, the Privacy Protection Commissioner of Norway, stated that September 11th 2001 had led, in democratic countries, to a discussion on the right balance between the legitimate need for collective security of any nation or group of nations, and the indispensable human rights securing individual freedom, integrity and dignity of their citizens. However, he noted that, from his point of view, the balance between collective security and individual freedoms had shifted considerably even before September 11th, and that the society was not moving towards a surveillance society, but rather the surveillance society was already there: the means had been invented, technology had been developed and many of the political compromises had been passed in Parliaments before 2001. He recalled that although a set of agreed values was honoured in all liberal democracies, history showed that States, confronting aggression or pressure from their surroundings, experienced challenges of these values. Aggression could force a democracy to accept, through legal and democratic procedures, the suspension of fundamental rights, of the democratic guarantees granted by society to the individual citizen. To any increase of the surveillance and control-level in a society corresponded a decrease of the respected integrity of the individual citizen.

76. As regards the current ongoing security debate, he stressed that the concepts underlying this debate were not clear and highlighted that the setting of the security agenda shifted increasingly from single national initiatives to international activities. While – given the international structure of the terrorism phenomenon – the impact of solely national initiatives might indeed be limited, this had generated another side-effect: national policies (*e.g.* in the Data Protection and Privacy field) could increasingly be influenced by other countries. For example, in Norway, nine out of ten of the past initiatives in the collective security sector had emerged from the international sphere. He also noted that surveillance measures in societies which were largely restricted to criminals, were now being extended to all members of society as a precautionary measure (*e.g.* in the proposals for collecting DNA samples from large parts of the population that had been discussed recently in the UK, Denmark and Norway). He insisted that the presumption of innocence constituted an important building block of a democratic society and should not be given up.

77. Mr. Apenes concluded by recommending that one should bear in mind when designing countermeasures against security risks, that enhanced security measures will likely reduce or minimise security risks, but will not eliminate them totally at a reasonable societal cost; effective solutions require more than enhancing security; they notably require identifying the roots of terrorism.

78. **Marc Rotenberg**, Executive Director, Electronic Privacy Information Center (EPIC), stated that identification was likely to be the most important issue to be addressed ten years into the future. The borders between "physical" and "digital" worlds were already disappearing and the line of where the network ends and the individual begins was blurring. Whereas ten years ago the focus had shifted from stand-alone systems to networks and interconnected devices, the focus today was on technologies to locate or identify items and people, through the increasing use of biometric identifiers (*e.g.* for access to buildings and to networks), or of radio frequency identification (RFID) tags. Other possible applications were emerging such as tracking children in order to deal with child abduction through tags attached to or embedded in bags, bracelets etc.

79. In 1992 the OECD had issued a first version of the Security Guidelines dealing mainly with the security of single computers. In 2002, the Security Guidelines had broadened the perspective to network security. Possibly in 2012, new OECD Guidelines could address the control of identity.

80. In this respect, Mr. Rotenberg highlighted that the main problem of identification occurs when an individual is compelled to identify him/herself. However, possible solutions, including the increased use of privacy enhancing technologies (PETs) can help minimise or eliminate the use of personally identifiable information (PII). Means to authenticate without identifying were already known from the offline world, *e.g.* prepaid telephone cards. David Chaum *et. al*. transferred this concept to the online environment, even if it still proves difficult to implement it in practice.

81. Mr. Rotenberg mentioned other current privacy challenges, such as WhoIs databases (with the publication of personal data on the Internet which facilitates fraud as well as privacy infringements); the various initiatives for retention of traffic data on the use of communications networks that had been created after September 11th (problem of use limitation); and the introduction of additional identification systems (*e.g.* in air travel and for network access; problems of purpose specification and use limitation). He concluded by stressing that these examples constituted similar challenges in many countries, as the new EPIC survey "Privacy and Human Rights 2003" did show.

Discussion

82. Answering a question from the audience on what governments could do to encourage the use of the Common Criteria and what was the greatest barrier against their use, **Ralf M. Engers** noted that barriers were different from country to country. For instance, the "paid consultancy model" common in the UK was not possible in Germany. A weakness was that the strength of algorithms was not evaluated in the Common Criteria. To avoid having to undergo three evaluations it was necessary to either apply the US Federal Information Processing Standards (FIPS) or to create a special profile within the Common Criteria. Nevertheless, the use of the Common Criteria still was the best solution for companies.

83. Speaking from the floor, **Stephan Engberg** mentioned that recent focus group analyses in Denmark indicated a growing distrust between business/individual and government, and asked how this could relate to the ongoing security efforts where trust is the goal? **Marc Rotenberg** noted that one factor could be that decision-making moved increasingly from national governments to international institutions where there was little or no participation of civil society (*e.g.* WIPO). He suggested that a possible task for the OECD would be to act as a forum to re-introduce the participation of civil society in decision-making. **Georg Apenes** added that the media were increasingly setting the agenda for discussion, forcing policy makers to react.

DAY 2: TUESDAY 14 October 2003

84. **Commissioner Orson Swindle** from the US Federal Trade Commission offered a summary of the main results from day one of the Global Forum. He pointed out that the relationship between trust and IT productivity turned the protection of networks into a key factor for economic growth. Above all, he insisted that it was critical to move from awareness to accountability and from there to concrete action.

85. Involving civil society in the process, fostering business leadership at CEO level, measuring the impact of actions taken, and establishing a feedback cycle for the implementation of the Security Guidelines were all critical steps. At a more concrete level, among others, actions to increase computer literacy, assess risks, foster security by design, increase information sharing were important. As regards the relationship between security and privacy, it was necessary to reach a true balance, and several speakers had reminded all participants that ensuring privacy while building a high-level of security was a collective challenge. He suggested that the OECD was uniquely positioned to help achieve these objectives.

86. Commissioner Swindle commended Peter Ford for having identified the need for a global culture of security, and he welcomed progress achieved by all participants in furtherance of this goal. The "Culture of Security" however, was not a destination but an ongoing journey which required a constant effort. Regarding the implementation of the security guidelines by OECD member countries, he called for a shared effort to learn from each other and for progress in outreaching to non-member economies. He recalled the importance of enforcement actions both at the national and international level. He concluded by stating that OECD member countries were at the origin of the Security Guidelines and had to set the example: things change, he recalled, it is time for more action, and we have to persevere.

Session 3: Information systems and network security in a broader context

87. **Keith Besgrove**, Chief General Manager, Regulation and Analysis, National Office for the Information Economy (NOIE), Australia, served as moderator for session 3. He explained that the session was intended to both set the broader context for the development of a culture of security, and be forward looking. Speakers from government and business had been invited to bring this broader dimension to the debate. The discussion would start with a presentation of the initiatives taken by the European Union, APEC, the Global Business Dialogue for e-commerce, and the World Wide Web Consortium (W3C) to develop global frameworks and standards for security. Two business representatives would then highlight the role of technology in supporting information systems and network security and, more generally, trust. Finally, four representatives of non-member economies would provide an overview of their national experience regarding information security.

Global frameworks and standards

88. **Pernilla Skantze** from the European Commission stressed that while security had become a marketing item for telecommunications service providers, there was still a lack of business focus on security in other sectors. To illustrate the clear need for action at the EU level, she mentioned an IDC/Bull survey from 2002 conducted with the IT divisions of 250 European companies with more than 1 000 employees. This survey showed that in 2002, 75% of the surveyed companies did not have an IT security strategy. More striking, 18% of the respondents spent less than 1% of their budget for IT security.

89. Among the activities of the European Union in the area of security, Ms. Skantze first mentioned regulation: the Directive on Electronic Signatures, the new electronic communications legislative framework, and Council Resolutions on Information and Network Security and on an EU approach to a

Culture of Security. A Framework Decision on attacks against information systems implementing and complementing the CoE Convention on Cybercrime was also being prepared. She also indicated that Research and Development for Information Security played a significant role in the EU's 5th Framework Program and was a top priority for the 6th Framework Program. She introduced the soon-to-be-created European Network and Information Security Agency (ENISA) designed to improve the functioning of the Internal Market by helping Member States and the Community to reach a high-level of information security. ENISA would help to prevent and respond to network and information security problems and serve as a centre of expertise. The service was not addressed directly to companies or citizens, but to member states' governments and to the EU institutions. ENISA would have advisory functions, contribute to awareness raising and co-operation, promote risk assessment methods and best practices and follow standardisation efforts, thus contributing to the development of a global approach to information security.

90. Ms. Skantze concluded her speech stressing that information security was an important business enabler. Further co-operation between countries and across sectors was necessary and there was a need to find ways to ensure effective public-private partnerships.

91. **Steve Orlowski**, Chairman of the eSecurity Task Group of the APEC Telecommunications and Information Working Group, reported on recent APEC activities on cybercrime and cybersecurity. In their "Los Cabos Statement", APEC leaders had agreed to have cybercrime legislation in place, and to install national points of contact by October 2003 as well as a procedure for a threat and vulnerability exchange between CERTs. APEC Ministers had agreed to implement the APEC Cybersecurity Strategy.

92. He indicated that the legislation enacted in the APEC member states took into account the CoE Cybercrime Convention. A survey on how APEC member countries had implemented measures against cybercrime had been conducted and a database of legislative approaches had been prepared. The Cybercrime Legislation and Enforcement Capacity Building Project, funded by APEC and the US, had held a Seminar of Experts in Bangkok in July 2003 and had also initiated training courses in APEC member countries. A CERT capacity building project funded by APEC and Australia had held workshops in March and October 2003 (with a follow-up to be held in March 2004). Guidelines for establishing CERTs are being developed and training for establishing CERTs will be conducted in APEC member countries. A network for exchange of information within APEC as well as with the global CERT community will be established.

93. Mr. Orlowski gave an overview of the results of the survey on measures against cybercrime in APEC member countries to which 14 of 21 members had responded. While most respondents mentioned having cybercrime legislation provisions in place as well as provisions to support law enforcement, only half of the respondents had provisions on extradition and mutual assistance. Issues for further work identified through the survey included these two items as well as emerging technologies like wireless access which was not necessarily covered by existing interception legislation.

94. Other areas of activity included work on security and technical guidance, raising of public awareness (*e.g.* through promotion of material such as the OECD Security Guidelines and a website to provide cyber-ethics and cyber-responsibility material and a booklet for SMEs) and training and education (*e.g.* a website of existing training material).

95. **Tomohiko Yamakawa,** NTT DATA Corporation, gave an overview on Public/Private co-operation in Cyber Security from the perspective of the "Global Business Dialogue" (GBDe). Established in 1999, the GBDe is a worldwide, CEO- and board member-driven initiative to develop policies promoting global e-commerce. It is aimed at establishing a permanent dialogue on the appropriate e-commerce framework with policy makers at all levels.

96. Mr. Yamakawa indicated that work on cybersecurity conducted by the "Future of the Internet Working Group" of the GBDe in 2003, included GBDe recommendations for industries on the implementation of a Culture of Security. In these recommendations, cyber security issues had been divided into three categories depending on the respective roles of Government and Industry: *i*) National Security (including combating cyber terrorism, protection of national infrastructure and countermeasures against espionage); *ii)* Public Security (combating cyber crime, prevention and protection from viruses) and *iii)* Security for industries (protection of their own information systems, enforcement of security policy and security management, the development of the security and privacy business as well as research and development on security and privacy).

97. He highlighted that, from the GBDe perspective, the role of business with regard to security included the development of security products and services and sharing of information (*e.g.* with CERTs) as well as establishing best practices. In the privacy field the development of products and provision of services and the implementation of the necessary measures for establishing consumer confidence (through *e.g.* privacy policies, trust marks and other self-regulatory measures) were important. At the same time, it was important that users took appropriate measures to protect their own systems from attacks and unauthorised access in order not to be "reflectors" for intruders. In the future, mixed responsibilities of consumers and industries in the B2C electronic marketplace would have to be considered. GBDe had also been active in fostering and promoting co-operation between the public and the private sector and was in a constant dialogue with governments on a regional level (APEC) as well as on a bilateral level.

98. **Rigo Wenning**, WorldWideWeb Consortium (W3C), briefly presented the W3C which is an organisation of 400 industry members and has developed HTML, XML and other standards. He gave an overview of the security relationships on the Internet. He highlighted that a wealth of standards was in place for securing communications and transactions (*e.g.* XML Signature, XML Encryption, SSL, IPv6, OpenPGP and other cryptographic applications), but unfortunately, none of them were applied on a large scale. Among the issues the W3C had identified in the security area were weaknesses or even the missing of underlying business models. The PKI business model *e.g.* did not work because it also helped business to identify the customer and because the customer paid the service (unlike as with credit cards). In PKI the existing market fragmentation also posed problems. At the same time, a lot of the existing formats and versions were incompatible. On top of that, it had turned out that the security field also was a minefield of patents which were about to become roadblocks for further development.

99. Mr. Wenning mentioned that, as regards trust, there were difficulties to design security functions in a user-friendly way. Any Website from the user's perspective constituted a black box. At the same time, it was difficult to make users familiar with the rather abstract notion of security functions such as certificates. The W3C-developed P3P standard might be helpful here to enhance user trust in electronic activities.

Discussion

100. A question was raised from the audience whether the cyber crime convention of the Council of Europe could be a model for global action which might be needed at the level of the United Nations, and **Steve Orlowski** noted that the convention represented a broad consensus as non-European countries had also participated in the preparation of the convention.

101. To another question from the audience on whether there was a roadmap for the transition from IPv4 to IPv6 and what its relevance with regard to security was, **Rigo Wenning** answered that the transition was an ongoing process and would happen due to the shortage of address space in IPv4. He also indicated that the use of cryptographic models was not mandatory in IPv6.

The role of technology in supporting information systems and network security and trust

102. **François Steiger,** Senior Vice President and General Manager Europe, Middle East and Africa, VeriSign Inc. argued that Cyber Security had become a competitive differentiator. The OECD 2002 Guidelines marked the transition towards the culture of security through, among others, public-private partnerships, a preference for non-regulatory incentives and the recognition of shared responsibilities among government, industry and users. One also had to note the changing nature of networks: networks had become pervasive and were critical to economic and social organisations. At the same time they had become subject to persistent attacks, which were also increasing in sophistication. In this situation security was no longer "optional", and security investments were a prerequisite for business survival.

103. He suggested that a new perspective on Internet security required to shift from "obligation" to "opportunity" as trust was a cornerstone of eCommerce. Because elements of "electronic trust" included authentication, integrity, confidentiality and non-repudiation, authentication methods such as ID and passwords, biometrics, multiple ("n"), factor authentication (*e.g.* tokens, smartcards) played an important role in trust-building. Public key infrastructures (PKI), for example, offered all elements of electronic trust.

104. Mr. Steiger recalled that trust, with respect to the Culture of Security, required shared roles and responsibilities: governments should lead by example in utilising security and trust tools, and provide for a consistent global framework to deter cybercrime. At the same time, national barriers to e-commerce-enabling technologies should be removed. E-commerce participants had the responsibility to deploy appropriate security and trust tools and to support an interoperable standards-based technology environment. Technology producers were to provide tools to government and other participants and commit themselves to advancing technologies to meet evolving threats. He closed his speech stressing that trust was a step beyond security.

105. **Takaaki Matsumoto,** Deputy Senior Executive Manager, Research and Development Headquarters, NTT Data, Japan, indicated that the number of reported incidents in Japan was growing rapidly. At the same time information and network assets had become as important as financial assets. Threats to the Information Society were emerging on the content level (unauthorised network activity), as well as on the network level (conventional computer crime) and on the physical level (physical threats *e.g.* unauthorised intrusion). Information security could however not be achieved by technology alone. There was a need to balance technology on the one hand, and ethics and education on the other.

106. He highlighted that, in order to respond to network threats and create a secure information society, comprehensive "prevention" measures and "enforcement" measures were both necessary. NTT had designed a "Cyber crisis management system" to respond to the need for integrated systems to manage "total security" practices in corporations. This system was linking information centres (to collect information and detect intrusions *e.g.* by application of data mining methods), damage estimating and forecasting systems as well as packet tracing systems on the physical level. Intrusion detection systems and firewalls also played an important role in security concepts, but these technologies had limitations (*e.g.* firewalls cannot block communications for public services and IDS based on pre-registered attack signatures may fail against recently invented malicious attacks). Secure operating systems were also a key element in any security infrastructure.

107. Mr. Matsumoto concluded that a significant number of issues still needed to be addressed at the content level (*e.g.* creation of international frameworks based on the premise that the definition of "harmful content" differs from country to country) and the network level (like the rapid development of technologies for the control of unauthorised access and identification of criminals).

Experiences outside the OECD

108. **Keith Besgrove** highlighted the importance of a dialogue with non-member economies for developing a global culture of security. He asked the presenters to share with the audience the lessons to be drawn from their national experience to ensure the security of information systems and networks, and to indicate in this respect whether and how the OECD could assist their economies.

109. **Husin Hj Jazri**, Director of the National ICT Security and Emergency Response Centre (NISER), Malaysia, provided an overview of the Malaysian experience regarding information security. Malaysia had deregulated the national telecommunications between 1984 and 1993. In 1997 a computer crimes act and a digital signature act had been finalised. In 2000, a security framework including the creation of the National ICT Security and Emergency Response Centre (NISER), a Government ICT Security Division and a Police Cyber Crime Unit had been established. There was also a project for a Personal Data Protection Act. Like other countries, Malaysia today was on the way towards a connected society with ubiquitous computing.

110. He recalled that, at the international level, Malaysia is through NISER a member of the Forum of Incident Response Teams (FIRST, located at the Carnegie Mellon University, USA) and a founding member of the Asia Pacific CERT. He explained that the national Computer Emergency Response Team MyCERT received around 700 cases per year, but as organisations were not inclined to report, the actual number of incidents was likely to be considerably higher. Virus attacks were the biggest issue, followed by spamming. He stressed that it had taken about three months to eradicate the "Code red" worm from the Malaysian networks (the "Blaster" worm) and two months to eradicate the "Nachi" virus.

111. Among the national projects in Malaysia, Mr. Jazri mentioned MyKad, also known as the Government Multipurpose Card (GMPC), which provides PKI-based transactions between the Malaysian public, the government and the private sector through the use of a homogeneous smart card environment. He also indicated that Malaysia was actively involved in increasing the awareness and adoption of Information Security Management Systems (ISMS) and the Common Criteria (CC). A pilot project had been launched to award BS7799-2:2002 certification to organisations in the country.

112. Among the lessons learned from the experience in Malaysia, he highlighted that global co-operation and information sharing were very important areas. For combating computer crime, one of the most important issues was the preservation of evidence. As regards possible support from the OECD for non-member economies, Mr. Jazri indicated that the OECD could help by providing affordable training programmes, and by encouraging the establishment of an international organisation of information security practitioners to ensure that professionalism and ethics are fully preserved.

113. **Prof. Mustapha Amghar** from the State Secretariat in charge of Post and Information and Communications Technology in Morocco gave an outline of the Moroccan experience in e-government. He indicated that electronic administration and electronic trade had begun to develop in Morocco more than four years ago. Currently there were several administrations offering electronic services and some companies active in electronic trade. Public agencies offering e-services included the customhouse, the national social security agency and the Moroccan Office for the Protection of Intellectual Property.

114. He highlighted that studies conducted by the Moroccan Government showed a number of problems with respect to the level of security of the information technology and networks used in the Moroccan Administration. The studies showed that there was a lack of co-ordination and communication between the different institutions. As regards the security level, there was a general unconsciousness of dangers incurred and of how to minimise existing risks (attacks, spam, viruses…). At the same time there was no clear and integrated security policy (*e.g.* security plans, vulnerability, audit, security responsibilities,

ethical code, human resources …). Furthermore, an insufficiency of security devices installed (absence of VPN) was detected. Test and back-up policies were not generalised and there was not enough sensitisation of the personnel to the security aspects. Finally, there was no national entity to ensure the co-ordination, harmonisation and security of the projects related to information systems.

115. In order to respond to these problems, the government had established a national committee on e-government comprised of public and private sector representatives. This committee had defined an action plan to start the e-government project based on two axes: *i)* methodology and technology, *ii)* regulation and legislation. Among the different ongoing projects, he mentioned the creation of a national portal regrouping all electronic services of the administration, the introduction of a secure platform for the communication between administrations based on a virtual private network (VPN), the outsourcing of the administrative electronic services, and information and sensitisation programmes for users of Information Systems to build trust in the use of electronic services. Regulation and legislation initiatives included the protection of intellectual property, measures against cyber crime, regulations on electronic messages and electronic signatures as well as the protection of privacy and personal data. There was also a project for the creation of a certification authority and of a national authority for the security of information systems.

116. Prof. Amghar closed his speech stating that member countries of the OECD could assist Morocco in its efforts by sharing information and experiences, education of national experts on information systems and networks security and through assistance for auditing of the security of institutions. Finally, help would also be welcome to set up a national structure responsible for the security of information systems.

117. **Reza Salim** Associate Director, Bangladesh Friendship Education Society (BFES) stressed that in today's world the right to information has become more and more important: in the information society, the right to information is one of the main human rights that protects and develops human life. However, developing countries were far away from being able to guarantee this right. Limitations in access to information for countries like Bangladesh included that access is not affordable, the inadequacy of the existing infrastructure as well as the non-availability of appropriate education. There was a need for co-operation, collaboration and investment.

118. Challenges were posed by the lack of an integrated computer security system and education about computer security was therefore one of the most important issues. Important next steps for Bangladesh were awareness raising and the provision of appropriate knowledge, as well as the development of security guidelines. Further exploration activities were needed on standards for the security of information systems. In order to realise these objectives, partnership was necessary. The upcoming Global Summit on the Information Society (WSIS) could be used to develop a consensus for a global security policy framework.

119. **Hasan Hourani**, Chief Technology Officer from the Ministry of Information & Communications Technology in Jordan, gave an overview of the activities of his government in the e-government field. He indicated that Jordan had developed a comprehensive IT strategy for the development of the digital economy, and that the Ministry of Information and Communications Technology was aiming at creating a thorough legal, institutional and commercial environment for the ICT sector in order to attract local and international ICT investments. At the same time, the citizen's access to the information and communication infrastructure was to be ensured. The Ministry was also co-ordinating Jordan's e-government Programme.

120. He explained that a legal framework had been put in place to allow for the integration of electronic services in the administrative work in Jordan: the Electronic Transactions Law allows the sharing of information electronically across government departments; it acknowledges electronic messages, contracts, and records as legal documents and allows for on-line payments for government services. The law also recognised electronic signatures and foresaw a certification authority for authentication. He

highlighted that existing e-government services included applications for business registration and telecoms licensing. An additional service for sales and income taxation was expected to be introduced by December 2003. In order to bridge the "Digital Divide" the Jordan government had launched the "Connecting Jordanians" initiative. This included the setting up of "Jordan Information Technology Community Centers" and the reduction of local access rates.

121. Mr. Hourani indicated that the competence for e-government security in Jordan lies with the Ministry of ICT, the Ministry of Justice and the Ministry of the Interior which work closely together. A cyber crime unit had been established in the Public Security Department of the Ministry of the Interior. Up to now, information security attacks in the public sector had only been of minor importance in Jordan. No lawsuits on cyber crime had been initiated so far.

Session 4: Future action to promote a global culture of security

122. **Geoff Smith**, Head, Information Security Policy, Information Security Policy Group, Department of Trade and Industry (DTI), UK, served as Moderator for Session 4. He indicated that the session aimed at facilitating an interactive discussion among all participants on sharing best practices and lessons learned, and at brainstorming on how participants could better work together, including within the OECD, as well as individually, to promote a culture of security.

123. **Geoff Smith** opened the roundtable discussion by asking what the participants understood by a culture of security.

124. Offering a perspective from the end user, **Stephanie Perrin,** President, Digital Discretion Inc., noted that the term "culture of security" did not refer to other important values in our societies. A 'culture of respect' would be a better concept including both respect for security and for individual rights. Following on this remark, **Joe Alhadeff,** Vice President for Global Public Policy and Chief Privacy Officer, Oracle Corporation agreed that a culture of security required that both privacy and security should be taken into account from the very beginning, stressing that if only security issues were being looked at, privacy would not be realised.

125. **Chuan-Te Ho,** Deputy Director, Department of Information Management Research Development and Evaluation Commission, Executive Yuan, Chinese Taipei, representing an OECD Non-member Economy, noted that privacy and security needed to be balanced, and suggested that the OECD Security Guidelines and Privacy Guidelines should be integrated into one set of Guidelines.

126. Further, in support of **Geoff Smith's** indication that the mindset in the Security Guidelines was to achieve both security and privacy, rather than balance them or achieve trade-offs, **Joe Richardson**, U.S. Department of State, recalled the incorporation in the security guidelines of the "ethics" principle which calls for security of information systems and networks to be implemented in a manner that is compatible with the essential values of a democratic society.

127. Referring to the situation before the 2002 Security Guidelines, **Stephanie Perrin** stressed that the 1992 Security Guidelines, which were targeted at IT administrators, had not had much influence. No significant investments had been made, and many products had been put on the market that were not ready and not secure. Therefore, she suggested that the development of a culture of security should aim at creating a "sustainable development of the information infrastructure". This would provide a better indication as to the goals to be pursued as regards security of information systems and networks in a global society.

128. As regards the 1992 Security Guidelines, **Detlef Eckert,** Senior Director, EMEA, Microsoft Europe, noted that the principles had been designed based on the experience and the problems at that time. The beginning of the 1990s had seen a growth of security incidents while there had been an education deficit at the same time, and the 1992 Guidelines had been developed against this background. Now the situation was different and posed new challenges for all participants including industry. He mentioned Microsoft's Trustworthy Computing Initiative as an example of industry response.

129. After stressing that, contrary to the 1992 Guidelines, the revised 2002 Security Guidelines were aimed at a large audience, **Joe Alhadeff** recalled that the new Guidelines offered a possible way to get to a "culture of security", while **Joe Richardson** suggested that the Security Guidelines were more a culture of "be careful" – like we tell children when they go out what to do and what not to do –, and that, as such, a "Culture of Security" was a workable concept. **Chuan-Te Ho** added that as information technology systems had become inevitable for life, so was a culture of security. Ideally, security should be unconscious.

130. At this point in the discussion, **Katarina de Brisis,** Senior Adviser, Ministry of Trade and Industry, Norway, underlined that implementing a culture of security was a collective responsibility and that all participants were "sitting in the same boat" and were responsible for the boat not to sink. All participants were concerned, all needed to contribute. However, it was important to remember that security was not a goal in itself, but that it was essential to support trust necessary for electronic conducting of business. She further stressed that the role of governments was mainly to create appropriate legislative and policy frameworks, facilitate international co-operation and co-ordinate efforts directed at creation and dissemination of codes of conduct, best practices etc. Building on Ms. de Brisis remarks, **Mr. Ho** suggested that because "security" was not just a technical matter, but rather a way to support trust in the e-society, a clear definition would be helpful.

131. Offering another end-user perspective on privacy and trust, **Stephan Engberg,** Founder of Open Business Innovation, pointed to the fact that trust was important but fragile and that distrust was growing among users. He explained that, beyond trust, users wanted to be in control of their data. Focus group analysis in Scandinavia and the United Kingdom showed a growing sense among users of loss of control over their personal data, even moving towards fatalism and social instability. He went on documenting how two major reports on respectively e-government pervasive computing – despite the fact that the analysis section documented otherwise – continued to suggest that end users will accept the growing surveillance and registration. In other words – even when public authorities did the proper socio/economic analysis – it was not translated into sustainable suggestions. Therefore, it was also important to consider security mechanisms vis à vis the control of personal information, as splitting of power between non-related entities, not its concentration in one's hands, is one of the fundamental groundings of democracy.

132. Finally, speaking from the audience, **Marc Rotenberg** remarked that the "culture of security" was too narrow a concept. It had the notion of "defending against attacks" while the threats were broader, thinking of power cuts or hurricanes. Security in a more general sense concerned the maintenance of critical services. He suggested that "reliability" or "integrity" be used instead of "security". He stressed that while infrastructure was becoming more and more important there was a lack of good policy for maintaining this infrastructure.

133. **Geoff Smith** then asked the participants what, in their view, should be the next possible steps.

134. **Katarina de Brisis** suggested that possible ways forward could include the creation of an appropriate framework for international co-operation. Such co-operation should be transparent so that it was easy for interested parties to "join the club". The value of international co-operation would be greatly increased by free exchange of best practices and codes of conduct.

135. **Chuan-Te Ho** suggested to set up a high-level committee on trust in e-society and to convey a clear message to the population about the fact that protection of information systems in a network is as important as developing the network itself. The message should insist on the need to shift the focus from security of products to people's behaviour with respect to security.

136. **Detlef Eckert** suggested that in order to develop the Guidelines, further objectives could be added to the Guidelines which could be measured afterwards, *e.g.* raising awareness required metrics and assessment.

137. **Joe Alhadeff** supported this proposal. It was important that the Guidelines became measurable. The Common Criteria could help evaluate products. But this would cost money and take time. It was important to look at the issue in a holistic manner. In the past the discussion on privacy had focused on the client level, now there was a need to look at the enterprise level as well.

138. **Joe Richardson** remarked that from the results that were available now, no nation had achieved a culture of security. The presentations at the Global Forum showed that it would be useful for the OECD to establish an online mechanism to allow OECD member and non-member economies to access the information available on security and the experience of others. This should be developed as an OECD on-line library. Member countries could make suggestions on useful documents to share. Even seemingly simple things like the identification of points of contact were important to be made widely available. Education and training could be included perhaps to include links to APECs' security training material Website (http://apec.isu.edu).

139. **Stephan Engberg** referred attention to the fact that the EU DG Internal Market (Article 29) and various other entities had recently been trying to promote Privacy Enhancing Technologies. Mr. Engberg commented that in his view the only feasible way to achieve a balance of trust, security and control was moving towards multi-identity based on Privacy Enhancing Technologies – in commercial environments but even and especially in government.

140. **Geoff Smith** concluded the session by a short wrapping-up of the discussion.

141. As regards the definition of a "culture of security", the discussion had highlighted a consensus on the need for a broad understanding of this concept: beyond technical aspects, a culture of security aims at driving a change in risk perception and behaviour of all participants across society and encompasses equally the need for enhanced security and the respect for privacy and other important democratic values. The development of a culture of security is a collective responsibility to enable trust in the global information society through ensuring the reliability, integrity and sustainable development of information systems and networks.

142. As regards next steps to develop a culture of security, the discussion has focused on the need for an appropriate framework for international co-operation among OECD member countries and with non-member economies, for metrics to assess progress in implementing the guidelines, for identification of useful initiatives and best practices and increased sharing of such information between the different partners – where appropriate via a network of "points of contact" – and for further education and training initiatives with a shift in the focus from security of products to people behaviour with respect to security.

Concluding remarks by the Chair of the Conference

143. In his conclusions, **Peter Ferguson** first stated that the objectives of the Forum had been met. All participants had taken stock of progress achieved in implementing the OECD security guidelines, shared

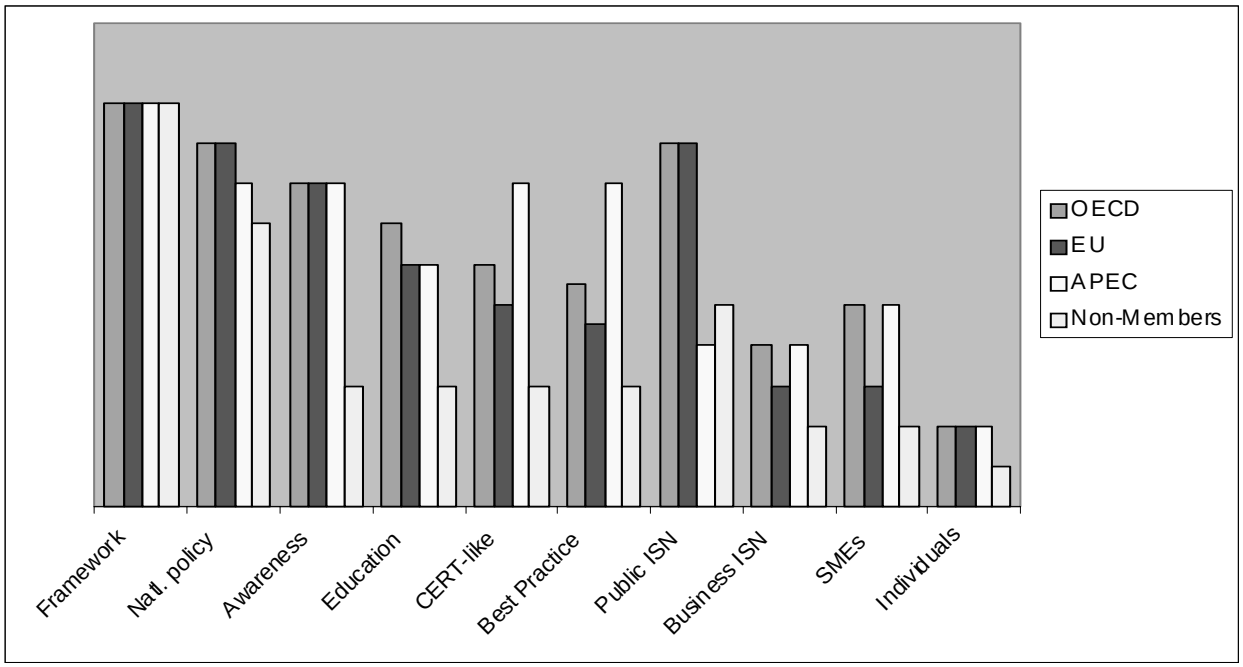
information with OECD member and non-member economies, the business community and civil society, and had a forward-looking discussion.

144. He highlighted that keywords and themes which had emerged throughout the whole conference included, in the first place, "trust" in the global information society – with a constant emphasis on the fact that both security and privacy build confidence, which in turn is a part of trust. "Participation" had also been emphasised by the forum with respect to Civil Society and non-members, though already part of the Guidelines. "Information sharing" was another recurrent theme: sharing of knowledge, information, best practices, and technologies between different constituencies, mindful of cultural differences.

145. There was also a consensus on a culture of information security as a shared public goal to be developed at different levels of government, business, and society. And it had been noted by several that the OECD was a unique place to bring together expertise from and beyond its membership to enhance international co-operation.

146. Peter Ferguson also insisted on the need for further action by all participants to develop a global culture of security. He recalled that State Secretary Olof Ulseth had said in his keynote speech, that when focusing on an international approach to security, OECD is pivotal to reach a global coherent approach, but that execution was key. And Orson Swindle, in his wrapping-up of the first day had concluded that from awareness to accountability and from there to action there was still a long way to go.

147. As regards progress achieved thus far by OECD member countries, the European Union, APEC and non-member economies in implementing information security, Peter Ferguson projected two slides showing a rough attempt by a few experts from these various constituencies to visualise fields in which countries had been especially active. He noted that the graphic showed that the areas which had received most attention up to now were the development of a security framework and a national policy, raising awareness initiatives and implementation of security on public systems and networks. He noted that while the OECD and EU seemed to rank higher in developing a national public policy and implementing security on public systems and networks, APEC seemed to focus more on CERT-like sites and best practices.



Source: OECD Secretariat.

148. Invited to comment on the discussion, the session chairs made the following remarks: **Geoff Smith** stressed that government leadership was key, and that governments should give the example. **Carol Curd** highlighted the importance of the role of business and the need for governments to partner with the private sector. **Peter Ford** supported the idea of measuring improvements and suggested audits as one of the means to achieve this. **Keith Besgrove** stressed the need for further debate about the security objectives to define effective action plans that would take into account the interdependence of all players.

149. Finally, Peter Ferguson offered a summary of the main suggestions for future action that emerged from the forum discussion:

1. Government as well as business leadership is critical to implementing the guidelines and developing a culture of security.

2. The impact of measures for information security should be reviewed.

3. Methodologies (*e.g.* focus groups, interviews, surveys adapted to cultural specificities, etc.), benchmarks and metrics should be developed in order to identify targets to measure progress.

4. Strong public/private partnerships are an effective means for implementing security.

5. Further exchange of best practices is necessary.

6. Further information sharing on security risks and solutions should be organised for a better and more effective response.

7. Industry should be encouraged to further embed security – and privacy - into their hard- and soft-ware, and to find solutions that would, as far as possible, avoid relying on users.

8. Education and training should be provided to non-member economies.

9. Interdependencies between developed and developing countries should systematically be taken into consideration to be more secure together.

150. Peter Ferguson finally thanked the sponsors, hosts, session chairs, speakers and participants for their active input to the conference.

ANNEXE I

OECD GLOBAL FORUM ON INFORMATION SYSTEMS AND NETWORK SECURITY: TOWARDS A GLOBAL CULTURE OF SECURITY

FINAL AGENDA

13-14 October 2003
Hotel Bristol, Oslo, Norway

FINAL AGENDA

DAY 1: MONDAY 13 October 2003

9.00 REGISTRATION

9.30-10.15 Opening and Key Note Addresses

Chair of the Conference: Peter Ferguson, Director, Electronic Commerce Policy, Industry Canada, Chair of the Working Party on Information Security and Privacy

Opening Remarks:

- **Mr. Odd Einar Dørum**, Minister of Justice, Norway
- **Mr. Herwig Schlögl**, Deputy Secretary General, OECD

Keynote Speech: Opportunities and Challenges in Digital Economy: the Importance of Information Systems and Network Security

- **Mr. Oluf Ulseth**, State Secretary for Trade and Industry, Norway

10.15-10.30 Introductory remarks

- **Peter Ferguson**, Conference Chair
- **Hugo Parr**, Chair of the Committee for Information, Computer and Communications Policy

10.30-10.50 Coffee Break

10.50 Session 1: Creating a Culture of Security for Information Systems and Network

Moderator: **Peter Ford**, First Assistant Secretary, Attorney General's Department, Australia

- Presentation of the Guidelines by the moderator

Round Table on the roles of the participants

- Government:
  - **Tomohiro Innami**, Director, Office of IT Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan
  - **Andy Purdy**, Acting Deputy Director of the National Cyber Security Division of the Information Analysis and Infrastructure Directorate U.S. Department of Homeland Security
- Business: **Lowell E. Thomas**, Director, Government Plans and Programs, Verizon
- Civil Society: **Marc Rotenberg**, Executive Director, Electronic Privacy Information Center (EPIC)

11.50-12.20 Discussion

12.20-13.30 LUNCH sponsored by Verizon

13.30 Session 2: Examples of Implementation: Case studies and practical guidance

Moderator: Carol Curd, CIO, Enterprise Information Security and Privacy, Enterprise Information and Technology, EDS

- ***Overview of OECD member countries' implementation plans*: Anne Carblanc**, Principal Administrator, Directorate for Science, Technology and Industry, OECD
- ***Awareness, Education and Responsibility***
  - EU "e-Aware" project: **Lorenzo Valeri**, RAND Corporation
  - "Policies for a Safer Internet: cyber ethics for cyber security – The initiatives of the Interministerial Committee for a Responsible Use of the Internet": **Cosimo Comella**, Italian Data Protection Commission
  - Information Security Assurance for Executives: BIAC/ICC Business Guidance on Implementation of the OECD Security Guidelines in Support of Building a Culture of Trust, **Jeremy Ward**, Symantec UK
  - Criteria of security, standardisation and preservations for full legal value applications in the administrative procedure in Spain: **Francisco Lopez-Crespo**, Ministry of Public Administration, Spain

- ***Response***

  - The WARP Concept (Warning, Advice & Reporting Point) – A UK initiative to establish a 'network' across the UK to provide better & more timely advice & warnings relating to electronic attack, and for receiving incident reports: **Peter Burnett**, NISCC, UK

  - Activity of Telecom-ISAC Japan: **Hiroyuki Takeda**, Director, IT Security Office Information and Communications Policy Bureau, Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan

  - "Best Practice for Computer Warning Networks: Mcert - An existing CERT for small and medium sized enterprises in Germany" A Public Private Partnership Project to secure Germany's IT-Infrastructure. Founded by Germany's ICT-Association BITKOM, seven industry sponsors and the German Government: **Stefan Grosse**, Federal Ministry of the Interior, Germany

  - CERT Integration into Whole Government Activities: **Jinhyun Cho**, Korea Information Security Agency (KISA)

15.45-16.05 Discussion

16.05-16.25 Coffee Break

- ***Security Life Cycle***

  - The changing nature of threats and vulnerabilities, **Yih-Jeou Wang**, Head of Division, Ministry of Science, Technology and Innovation, Denmark

  - Security management, design and implementation: **Mikael Kiviniemi**, Finland

  - Secure software development: **Ralf M. Engers**, Chief Technology Officer, Utimaco Safeware AG, Germany

- ***Ethics and Democracy***

  - Balancing security needs and democratic values: **Georg Apenes**, The Data Inspectorate, Privacy Protection Commissioner, Norway

  - How can improved trust in the new technologies enhance democracy and free speech (to be determined)

17.55-18.15 Discussion

END OF DAY 1

19.30 DINNER hosted by Symantec

DAY 2: TUESDAY 14 October 2003

9.30-9.50 Remarks from Day 1: Commissioner Orson Swindle, U.S. Federal Trade Commission

9.50 Session 3: Information Systems and Network Security in Broader Context

Moderator: Keith Besgrove, Chief General Manager, Regulation and Analysis, National Office for the Information Economy (NOIE), Australia

- ***Global frameworks and standards***
  - European Commission: **Pernilla Skantze**
  - APEC: **Steve Orlowski**
  - GBDe: **Tomohiko Yamakawa**
  - W3C: **Rigo Wenning**

10.35-10.50 Coffee Break

- ***The Role of Technology in Supporting Information Systems and Network Security and Trust***
  - **François Steiger**, Senior Vice President Europe Middle East and Africa, VeriSign Inc.
  - **Takaaki Matsumoto**, Deputy Senior Executive Manager, Research and Development Headquarters, NTT Data, Japan
- ***Experiences outside the OECD***
  - **Husin Hj Jazri**, Director of the National ICT Security and Emergency Response Centre (NISER), Malaysia
  - **Mustapha Amghar**, State Secretariat in charge of Post and Information and Communications Technology, Morocco
  - **Reza Salim**, Associate Director, Bangladesh Friendship Education Society (BFES)
  - **Hasan Hourani**, Chief Technology Officer, Ministry of Information & Communications Technology, Jordan

12.00-12.45 Discussion

12.45-14.30 LUNCH

14.30 Session 4: Future Action to Promote a Global Culture of Security

Moderator: Geoff Smith, Head, Information Security Policy, Information Security Policy Group, Department of Trade and Industry (DTI), UK

Participant Roundtable:

- Government
  - **Katarina de Brisis**, Senior Adviser, Ministry of Trade and Industry, Norway
  - **Joe Richardson**, U.S. Department of State
- OECD Non-member Economy
  - **Chuan-Te Ho**, Deputy Director, Department of Information Management Research Development and Evaluation Commission, Executive Yuan, Chinese Taipei
- Business
  - **Detlef Eckert**, Senior Director, EMEA, Microsoft Europe (*B2C*)
  - **Joe Alhadeff**, Vice President for Global Public Policy and Chief Privacy Officer, Oracle Corporation (*B2B*)
- End user's perspective
  - **Stephan Engberg**, Founder of Open Business Innovation
  - **Stephanie Perrin**, President, Digital Discretion Inc.

16.30-16.50 Concluding Remarks by the Chair of the Conference

17.00 Adjournment

ANNEXE II

FINAL LIST OF PARTICIPANTS

Mr. Audun Petter AANÆS
Ministry of Justice
Oslo, Norway

Mr. Geir AASEN
Enterprise Director
Microsoft Norway AS
Oslo, Norway

Mrs. Inmaculada AGUADO
Chief of Service for International Affairs
Directorate General for Telecommunications and Information Technologies
Ministry of Science and Technology
Madrid, Spain

Mr. Michael AISENBERG
Director of Corporate Government Relations
VeriSign Inc.
Washington DC, United States

Mr. Joesph ALHADEFF
Vice President, Global Public Policy
Chief Privacy Officer
Oracle Corporation
Washington, DC, United States

Mr. Mustapha AMGHAR
Adviser
Expert on Telcomms & Information Technologies
Department of Telecommunications
Rabat, Morocco

Mr. Stefano AMORE
Magistrate-Public Prosecutor
Minstry of Justice
Legislative Department
Rome, Italy

Mr. Georg APENES
Data Protection Commissioner
The Data Inspectorate
Oslo, Norway

Mr. Kamlesh K BAJAJ
Director, CERT-IN
Department of Information Technology
Government of India
New Delhi, India

Ms. Eric BARKS-RUGGLES
Deputy Policital and Economic Counselor
US Embassy in Oslo
United States

Mr. Jeremy BEALE
Head, E-Business Group
Confederation of British Industry
London, United Kingdom

Mr. Kjell BERGAN
Head of Section
Norwegian National Security Authority
Norway

Mr. Laurent BERNAT
OECD, Information, Computer and Communications Division
Directorate for Science, Technology and Industry

Mr. Keith BESGROVE
Chief General Manager
Regulation and Analysis Group
National Office for the Information Economy (NOIE)
Canberra, Australia

Mr. Christophe BIRKELAND
Chief
NSM
Oslo, Norway

Mr. Lars BODSBERG
Research Director
SINTEF
Norway

Mr. Maurizio BONANNI
Engineer
Ministry of Communication
Rome, Italy

Mr. Halvor BOTHNER-BY
Norwegian Telecom & Information Users Association (NORTIB)
Hovik, Norway

Mr. Peter BURNETT
Head of Information Sharing
National Infrastructure Security Coordination Centre (NISCC)
London, United Kingdom

Mr. Dagfinn BUSET
Advisor
Ministry of Justice and the Police
Oslo, Norway

Mr. Daniel CAPRIO
Chief of Staff
U.S. Federal Trade Commission
Washington, DC, United States

Ms. Anne CARBLANC
Principal Administrator, Information Security and Privacy
OECD, Information, Computer and Communications Division
Directorate for Science, Technology and Industry

Mr. A. K. CHAKRAVARTI
Advisor
Department of Information Technology
Government of India
New Delhi, India

Mr. Jinhyun CHO
Researcher
Korea Information Security Agency (KISA)
Seoul, Korea

Mr. Cosimo COMELLA
Head, Technological Resources Department
Data Protection Authority
Rome, Italy

Ms. Stefaniz CONGIA
Office of Service for International and Community Matters
Data Protection Authority
Rome, Italy

Ms. Maureen COONEY
Legal Advisor for International Consumer Protection
U. S. Federal Trade Commission
Washington DC, United States

Mr. Gyorgy CSAPO
Senior Project Supervisor
Prime Minister's Office
Office of Government Information Technology
Budapest, Hungary

Mrs. Carol CURD
Chief Information Security Officer for Client EDS
EDS
United Kingdom

Mrs. Andrea DA SILVA
International Trade Specialist
Office of Information Technologies and Electronic Commerce
US Department of Commerce
Washington, DC, United States

Mr. Shinnosuke DATE
General Manager, Strategic Alliance
Fujitsu Limited
Tokyo, Japan

Ms. Katarina DE BRISIS
Senior Advisor
Ministry of Trade and Industry
Oslo, Norway

Mr. Edgar DE LANGE
Senior Policy Analyst
Ministry of Economic Affairs
The Hague, The Netherlands

Mr. Angel Luis DEL SER VEGA
Technical Service Chief
Ministry of Science and Technology
Madrid, Spain

Mr. Michael DONOHUE
Consumer Protection Policy Analyst
OECD, Information, Computer and Communications Division
Directorate for Science, Technology and Industry

Mr. Odd Einar DØRUM
Minister of Justice
Norway

Mr. Cort Archer DREYER
Adviser
Ministry of Trade and Industry
Oslo, Norway

Mr. Gabriel DUSIL
Senior Director Europe, Middle East and Africa (EMEA)
VeriSign Inc.
Geneva, Switzerland

Mr. Detlef ECKERT
Senior Director Trustworthy Computing
Microsoft Corporation Europe, Middle East and Africa (EMEA)
Diegem, Belgium

Mr. Ernst EIELSEN
Adviser
City of Oslo
Department of Administration Policy
Oslo, Norway

Mr. Stephan ENGBERG
Founder and CEO
Open Business Innovation
Denmark

Mr. Ralf M. ENGERS
Chief Technology Officer
Personal Device Security
Utimaco Safeware AG
Germany

Ms. Grethe FAREMO
Director
Microsoft Norway AS
Oslo, Norway

Mr. Peter FERGUSON
Director, Electronic Commerce Policy
Chair of the OECD Working Party on Information Security and Privacy (WPISP)
Industry Canada
Ottawa, Canada

Mr. Peter FORD
Acting Deputy Secretary
Attorney-General's Department
Australia

Mr. Stein FOTLAND
Sikkerhetskoordinator
Bergen Komune: IT Sekisjonen
Bergen, Norway

Ms. Luisa FRANCHINA
General Director
Ministry for Communications
Rome, Italy

Ms. Liesyl FRANZ
Director, Global Government Affairs
EDS
Washington DC, United States

Mrs. Catherine GABAY
Director, Innovation, Research, New Technology
MEDEF
Paris, France

Mr. Matthieu GRALL
Secrétariat général de la défense nationale (SGDN)
Paris, France

Mr. Filippo Maria GRASSO
Telecom Italia, SPA
Rome, Italy

Mr. Stefan GROSSE
CIIP, CERT, Co-operation with industry
IT Security
The Federal Ministry of the Interior
Berlin, Germany

Ms. Birgitte HAGELSKJAER-NIELSEN
Head of Section
Ministry of Research, Technology and Innovation
Copenhagen, Denmark

Ms. Janne HAGEN
Scientist
The Norwegian Defence Research Establishment (FFI)
Kjeller, Norway

Ms. E. Jane HAMILTON
Manager, Security Policy
Electronic Commerce Branch
Industry Canada

Ms. Chuan-te HO
Deputy Director
Research, Development, and Evaluation Commission (RDEC)
Executive Yuan
Chinese Taipei

Mr. Hassan HOURANI
Chief Technology Officer
e-Government Programme
Ministry of Information and Communications Technology
Amman, Jordan

Mr. Asbjørn HOVSTØ
Manager
ERGO Solutions
Norway

Mr. Tomohiro INNAMI
Director
Office of IT Security Policy, Commerce and Information Policy Bureau
Ministry of Economy, Trade and Industry
Tokyo, Japan

Mr. Eivind JAHREN
Deputy Director General
Ministry of Trade and Industry
Oslo, Norway

Mr. Tobiassen JAN
High Executive Officer
Norwegian NSA
Norway

Mr. Husin Hj JAZRI
Director
National ICT Security and Emergency Response Centre (NISER)
Kuala Lumpur, Malaysia

Mr. Morten Sven JOHANNESSEN
Special Coordinator
Country analysis and social responsibility
Statoil ASA
Norway

Mr. Einar Broch JOHNSEN
Associate Professor
University of Oslo
Department of Informatics
Oslo, Norway

Ms. Heidi KARLSEN
Advisor
Department of Civil Aviation, Postal Service and Telecommunications
Minsitry of Transport and Communications
Oslo, Norway

Mr. Mikael KIVINIEMI
Counsellor
Ministry of Finance
Helsinki, Finland

Mr. Svein KNAPSKOG
Professor
NTNU, Item and Q2S
Trondheim, Norway

Mr. Atsushi KOYA
Chief Engineer
Tokyo Electric Power, Co.
Tokyo, Japan

Mr. Yoshio KUBOTA
Senior Advisor
Tokyo Electric Power, Co.
Tokyo, Japan

Ms. Ilse LANDA
Policy Advisor
Ministry of Economic Affairs
The Hague, The Netherlands

Mr. Jongin LIM
Rector
Graduate School of Information Security
Korea University
Seoul, Korea

Mr. Jannik LINDBAEK
Public Relations Manager
Microsoft Norway AS
Oslo, Norway

Mr. Knut LINDELIEN
Manager
Norwegian Technology Center
Oslo, Norway

Mr. Pekka LINDROOS
Head of Information, Computer & Communications Policy Division
OECD
Directorate for Science, Technology and Industry

Mr. LIU Xinran
Deputy Director
Technology Organization Division
National Computer Network and Information Security Administrative Center
Beijing, the People's Republic of China

Mr. Francisco LOPEZ-CRESPO
Head of Telematics Systems Unit
Ministry of Public Administrations
Madrid, Spain

Mr. Peter LÜBKERT
Head of Client Services and Operations Division
OECD
Information Technology Networks

Mr. Kazuyoshi MAEKAWA
Representative of European Affairs
Fujitsu Ltd.
Belgium

Ms. Jennifer MARTIN
Senior Counsel
Computer Crime & Intellectual Property Section
US Department of Justice
Washington, DC, United States

Mr. Bernd MARTIN
Chief Information Office Austria – Federal Chancellery
Vienna, Austria

Mr. Tor Asmund MARTINSEN
Assistant Director, Head of Security
Directorate of Labour
Oslo, Norway

Mr. Takaaki MATSUMOTO
Senior Executive Manager
Research and Development Headquarters
NTT DATA Corporation
Tokyo, Japan

Mrs. Laramie McNAMARA
Former Commissioner from the Foreign Claims Settlement Commission
United States

Mr. Aled MILES
Vice President and Managing Director for Symantec Northern Europe
Symantec Corporation
United Kingdom

Ms. Patricia MOLL
Government Affairs Manager
Microsoft Corporation
Brussels, Belgium

Mr. Sven MÖRS
Central Department
Telecommunication and Media
Berlin, Germany

Mr. Henning MORTENSEN
Consultant
The Confederation of Danish Industries
Copenhagen, Denmark

Mr. Bill MUNSON
Director, Policy
ITAC
Mississauga, Canada

Mr. Hans Einar NERHUS
Senior Advisor
Ministry of Transport and Communications
Oslo, Norway

Mr. Arne With NORMANN
Senior Security Advisor
Telenor ASA
Lillehammer, Norway

Mr. Brian O'HIGGINS
CTO
Entrust
Ottawa, Canada

Mr. Ove OLSEN
Director
Center for Information Security
Trondheim, Norway

Mr. Loren OLSON
Professor
Department of Mathematics & Statistics
University of Tromso
Tromso, Norway

Mr. Steve ORLOWSKI
Chair
eSecurity Task Group, APEC
Australia

Mr. Hakan OZFIDAN
Computer and Network Systems Administrator
Turkish Prime Ministry
IT Department
Ankara, Turkey

Mr. Hugo PARR
Director General
Chair of the OECD Committee on Information, Computer and Communications Policy
Ministry of Trade and Industry
Oslo, Norway

Mr. Manuel PEDROSA DE BARROS
Director
ICP-ANACOM
Autoridade Nacional de Comunicacoes
Barcarena, Portugal

Mrs. Krisztina PENTEKNE GECSENNYI
Foreign Affairs Official
Ministry of Informatics and Communications
Budapest, Hungary

Ms. Stephanie PERRIN
President
Digital Discretion, Inc
Montreal, Canada

Mrs. Dagmar POPRACOVÁ
Officer Specialist
National Security Authority
Bratislava, Slovak Republic

Mr. Ivan PROCHÁZKA
Head of Department of Foreign Relations
The Office for Personal Data Protection
Prague, Czech Republic

Mr. Donald (Andy) PURDY
Acting Deputy Director
National Cyber Security Dvision
Department of Homeland Security
Washington DC, United States

Mr. Frode REIN
CIO
The Norwegian Parliament, Stortinget
Oslo, Norway

Mr. Joesph RICHARDSON
Senior Foreign Affairs Advisor
Critical Infrastructure Protection Policy
U.S. Department of State
Washington, DC, United States

Mr. Tormod RØNNINGEN
Head of Connectivity Services
Hydro IS Partner
Oslo, Norway

Mr. Marc ROTENBERG
Executive Director
Electronic Privacy Information Centre (EPIC)
Washington, DC, United States

Mr. Reza SALIM
Associate Director
Bangladesh Friendship Education Society (BFES)
Dhaka, Bangladesh

Mr. Carlo SARZANA DI S. IPPOLITO
President Adjoint Honorarie de la Cour de Cassation
Membre du Comité Technique National de la Securité Informatique et des Télécommunications dans les P.A.
Ministry of Justice
Rome, Italy

Mr. Herwig SCHLÖGL
Deputy Secretary-General
OECD

Mr. Lars Bjorgan SCHRØDER
Project Manager
Minstry of Trade and Industry
Oslo, Norway

Mrs. Patricia SEFCIK
Director
Office of Information Technologies and Electronic Commerce
US Department of Commerce
Washington, DC, United States

Mr. Ole Tom SEIERSTAD
Competitve Strategy Manager
Microsoft Norway AS
Oslo, Norway

Ms. Pernilla SKANTZE
Administrator
DG Information Society
European Commission

Mr. Morten N. SKOGVIK
Advisor
Office of Security and Emergency Planning
The Directorate of Labour
Oslo, Norway

Ms. Lusica SLOBODOVÁ
Officer Specialist
National Security Authority
Bratislava, Slovak Republic

Mr. Geoffrey SMITH
Head of Information Security Policy
Information Security Policy Group
Department of Trade and Industry (DTI)
London, United Kingdom

Mr. Terje SOLHAUG
Senior Advisor for Information Security
The Tax Administration
Norway

Ms. Christina SPECK
Senior Advisor
International Communications Policy
National Telecommunications and Information Administration
US Department of Commerce
Washington DC, United States

Mr. Sergio STARO
Deputy Director
Computer Crime Investigative Unit
Ministry of the Interior, Postal and Communication Policy Service
Rome, Italy

Mr. Birger STEEN
General Manager
Microsoft Norway AS
Oslo, Norway

Mr. François STEIGER
Senior Vice President
Europe, Middle East and Africa
VeriSign Inc.
Geneva, Switzerland

Mr. Atsushi SUZUKI
Section Chief of Economic Development
International Affairs Department
Telecommunications Bureau
Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT)
Tokyo, Japan

Ms. Marie SVOBODOVÁ
Senior Counsellor
Ministry of Informatics
Prague, Czech Republic

Mr. Orson SWINDLE
Commissioner
US Federal Trade Commission
Washington DC, United States

Ms. Nóra SYLVESTER
Deputy of Head of Department
Ministry of Information and Communications
Budapest, Hungary

Ms. Asako TAKAHASHI
OECD
Directorate for Science, Technology and Industry
Committee Secretariat

Mr. Hiroyuki TAKEDA
Director of IT Security Office
Information and Communications Policy Bureau
Ministry of Public Management, Home Affaris, Post and Telecommunications (MPHPT)
Tokyo, Japan

Mr. Ichiro TAMBO
Advisor on Science and Technology
OECD
Development Co-operation Directorate

Mr. Dole TANDRERG
Seniro Security Advisor
Telenor ASA
Norway

Mr. Frédéric TATOUT
Responsable Pôle SSI
Ministère de l'Economie, des Finances et de l'Industrie
Paris, France

Mr. Lowel E. THOMAS
Director, National Security and Infrastructure Assurance
Verizon
Arlington, United States

Mr. Torkel THUNE
Managing Director, Services and Security
Stim Computing AS
Oslo, Norway

Mr. Dariusz TORUŃ
Deputy Director of IT and Telecommunication Department
Ministry of Foreign Affairs
Warsaw, Poland

Mr. Kosmas TSIRAKTSOPOULOS
Legal Advisor
Swiss Federal Data Protection Office
Bern, Switzerland

Mr. Oluf ULSETH
State Secretary for Trade and Industry
Ministry of Trade and Industry
Oslo, Norway

Mr. Henrik A. VAAGE
Country Manager
Symantec Norge
Norway

Mr. Lorenzo VALERI
Senior Policy Analyst
RAND
Berlin, Germany

Mr. Pedro VERDELHO
Procurardor Adjunto
Ministério Público
Lisbon, Portugal

Mr. Yih-Jeou WANG
Head of Division, IT Policy Center
Ministry of Science, Technology and Innovation
Copenhagen, Denmark

Mr. Jeremy WARD
Service Development Director,
Symantec (UK) Ltd.
United Kingdom

Mr. Krzysztof WASIEK
Deputy Director of IT and Telecommunication Department
Ministry of Foreign Affairs
Warsaw, Poland

Mr. Shinji WATANABE
Researcher
Research and Development Headquarters
NTT DATA Corporation
Tokyo, Japan

Mr. Rigo WENNING
Privacy Activity Lead
W3C
France

Mr. Johannes WIIK
Agder University College
Norway

Ms. Marianne WILLOCH
Risk Manager
Telenor ASA
Norway

Mr. Tomohiko YAMAKAWA
Senior Researcher
Research Institute for System Science
Research and Development Headquarters
NTT DATA Corporation
Tokyo, Japan
