Informal ICT Management Workshop - OECD, 20-21 October 2004

Workshop Summary

An informal Workshop on ICT Management was organised by the OECD on 20 -21 October at its Paris headquarters. The Workshop focused on three main management issues: Open Source Software, ICT Governance, and ICT Security.

34 ICT managers and directors from 10 member country agencies and 12 international organisations participated in the workshop, in addition to members of the OECD Secretariat - from the ICT Service, the Technology and the Governance Directorates, and the Auditor General - and three independent experts.

Anthony Hutton, the OECD Secretariat’s Executive Director welcomed participants and, along with Guido Maccari, Head of Information Technology and Network Services (ITN), officially opened the Workshop.

Day 1, Session I: Open Source Software (OSS)

This first session was led by Peter Lübker, Head of ITN’s Client Support & Operations. Participants had an opportunity to get an update on what’s happening in the OSS market, share information on their ICT infrastructure and investments, exchange views and experiences on OSS, and on their strategies and plans for the medium term. Representatives of the OECD, the Dutch and French Administrations, and Forrester Research, Inc. made presentations.

Experience/Use of OSS

The majority of participants indicated that their organisations are increasing the number of OSS applications, mainly on the server side (using Linux, Apache, etc.). Little is being done on the desktop. Some organizations and administrations had no experience at all and were looking to this workshop to learn more and to better understand the implications. Others are actively investigating OSS alternatives and setting up pilot projects. One participant stated: “We are not an early adaptor but we don’t want to be the last either”.

Generally, OSS appears to have greatest penetration in central infrastructures. Increasing numbers of servers are running Linux OS (sometimes displacing proprietary UNIX systems) in web applications, in network management and security (e.g., firewalls) systems. A survey from Forrester on the use of OSS in European firms shows that 40% have already implemented OSS solutions and 43% are piloting or considering OSS. Only 17% have no plans yet for OSS.

The French and Dutch administrations appear to lead the way with OSS software in place both at the server and desktop level in several Ministries. The French administration plans to implement OSS in all ministries within a few years. The Korean representatives from the Ministry of Information & Communication and the IT Industry Promotion Agency highlighted their government’s national program to promote OSS throughout the country.

Some international organisations are quite advanced in the adoption of OSS. The Asian Development Bank (ADB) in Manila instituted an open technologies strategy four years ago and now has approximately 60 servers running under Linux. The United Nations Office in Vienna has adopted a mandatory OSS policy for back office operations.
Few institutions have implemented OSS on the desktop. Both the ADB and the UN in Vienna have retained MS/Windows on the desktop. There are however important initiatives underway in the French Administration (Departments of Customs, Interior, Equipment, Gendarmerie, etc.) with the OpenOffice suite installed today on approximately 35,000 desktops, and to a lesser degree in the German and Dutch administrations.

**What drives OSS?**

One participant stated: “It’s very exciting to investigate OSS solutions, but what is driving this, Budget? General Interest? What are the actual business benefits?” Unexpectedly perhaps, lower costs did not appear to be the main driver. Participants who have taken the OSS route agreed that it was difficult to ascertain whether the move has been cost effective. They also noted that strong political support was key to the project’s success.

For many, a strong driver appeared to be the growing dislike of the business & licensing model employed by dominant software vendors, in particular Microsoft. A participant noted that licensing was originally to protect innovation and creation but had now become the “raison d’être” for many companies. Many also resented being “forced” to migrate to updated versions of software with all the associated costs that a migration entails.

Others felt that monies spent on overseas software licenses could be better invested in the region and to developing human capacity. There is a strong driver to boost European and Asian software development and put more competition in place.

Other important drivers were mentioned, including:

- **Interoperability, integration and standardisation.** Greater connectivity and interaction between applications and across networks was considered extremely important. Development of “open standards” was seen crucial by many participants, and more important than OSS itself. For some institutions support for open standards had become a mandatory element of their sourcing strategies. Administrations responsible for maintaining archives for example have to ensure that their records can be read in the future, and thus should be stored in some published format. It was also felt that open standards would be a way to avoid vendor lock-in.

- **Greater transparency, especially in public administrations.** Citizens want to see that their governments make the best use of resources. There is also a question of national sovereignty and increasing concern about governments’ reliance on non-national proprietary software and the public’s ability to access public information.

- **Lesser dependency** on vendors and reducing resources required to ensure compliance with license agreements and better manage upgrades and infrastructure evolution.

- **High costs.** For large organisations or institutions in developing countries, software licence costs can be steep. Administrations that provide software for public use may also aim at low-to-zero cost for their users as an objective. Microsoft in particular was criticised for its aggressive licensing and version support policies adopted some years ago, and a number of organisations had decided to postpone renewal of their contracts with MS as a result.

- **Development of local software industry.** The basic tenets of OSS, namely freely available source code and the right to modify and distribute the resulting software have been recognised in some countries/regions as a means to stimulate the local software industry.
• **Reducing security concerns.** Participants felt that OSS solutions will allow them to see/control what is going on “behind the scenes”. With proprietary software, some participants find it difficult to know what is happening with their own systems (A participant said “I want to know exactly what happens on my own network and be in control of information”)

• **Reducing the complexity** of software sourcing strategy and widening the opportunity for good practices in software solutions.

**Open Standards**

As mentioned earlier, participants felt that open standards are more important than OSS. Without established standards, the introduction of OSS solutions is being slowed down, although it was unclear at to how these standards would be established and which authority would determine software compliance. It was suggested that international organisations should step in and set up an “Open Standards Compliance Authority”.

**Barriers & Challenges to OSS**

Participants felt that there are a number of issues that slow down the adoption of OSS solutions, among which:

• **Lack of a product roadmap.** Software vendors generally have such a roadmap and a strategic vision over the medium term. This is generally lacking in the OSS world, since development is mainly user driven. In an analysis carried out by Forrester of approximately 400 OSS products, 80-90% do not have a roadmap.

• **Licensing/legal aspects.** The plethora of different OSS licences is a cause for confusion. Some organisations are reluctant to explore OSS further because of the uncertainties surrounding rights and liabilities when using or redistributing OSS across the organisation, often world-wide. The form of OSS licences may be incompatible with national laws concerning intellectual property, etc. In France a new OSS licence, CeCILL, has been devised to deal with these issues. A number of guides (EC, FRA, NET) are available to help institutions understand the various licences and to choose the most appropriate one when distributing software to the public domain. Several organisations reported that proprietary software licences and their implications for intellectual property could also be extremely complex.

• **Lack of mature, enterprise-level support and maintenance services.** Traditionally, support for OSS is supplied by the user community. Although this represents a major change, some organisations found that the quality of this support was very good – analysing the capacity of the community to provide support is one important task to be carried out when evaluating an OSS product. And the number of companies providing commercial support is growing - Forrester reported 20-30 of such medium/large companies in Europe.

• **Lack of a robust business case for decision making.** More tangible elements and perhaps more experience are needed to demonstrate the benefits of OSS solutions. Most decisions so far have been made for political reasons rather than real benefits. The OECD was asked if it could help to build a stronger business case for organisations/administrations that do not necessarily have a political mandate to choose an OSS solution.

• **Lack of file conversion tools and interoperability with proprietary software.** Participants were doubtful as to how they would exchange proprietary file formats and Open source documents. Also, many organisations have 10-15 years worth of legacy documents that would need to be converted. Institutions have to communicate and exchange information, both internally
and externally. For example, the OECD Secretariat exchanges hundreds of statistical files every month with national administrations. There are a number of common document formats such as .doc or .xls which are not open standards, but in reality constitute a “standard de fait”; for many organisations it would be very impractical to no longer be able to accept such formats from partners. The same problem exists within an organisation. Tools to convert between proprietary formats and open standard document formats such as OpenOffice are far from perfect.

- **Lack of budget for redevelopment/migration of special applications.** This, in addition to the three reasons above, makes it hard for many institutions, especially international organisations, to justify the investment required for a major change.

- **International Organisations have spent over 1 billion US$** trying to build information management systems, however each organization has chosen different systems and made separate contracts with ERP software vendors. Efforts by top management to agree on a common contractor have failed. How far will organisations and administrations work together to provide common OSS choices and options for all to choose from? Although cooperation in this area has never really worked in the past, the way the OSS web community is shaping up could become a key driver in moving things forwards in more common ways. The OECD and other organisations should discuss this in more depth.

- **Costs.** There is no unequivocal answer to the question as to whether OSS is cheaper than proprietary software. Every case has to be dealt with individually, and there are a number of different methodologies available. Transition, training, support and maintenance costs must be factored in. Where users themselves are impacted, the analysis is more complex. The importance of the cost factor itself is also different from one organisation to another – for some, strategic imperatives take the upper hand. Few organisations had carried out ex-post cost evaluations and more time is needed to appreciate the TCO of any OSS solution.

- **User acceptance.** This can be an important issue for OSS on the desktop, since users are very familiar with MS tools, both in their professional and home environments. This also influences the comparative costs of upgrades/migration, since users often have the latest version of MS software at home before the office environment is upgraded: training costs are thus reduced.

- **User Resistance.** The inverse is also an issue. Although OSS is shedding its hacker image, it is still perceived by some users as a “second-best” product.

- **Education** is also seen as a key challenge -- For example, Microsoft & IBM invest huge amounts in education, familiarising students with Microsoft products and IBM equipment. Education, educational policy and a more strategic approach are necessary if OSS is to move forward.

- **Last but not least, there is a lack of comprehensive and up to date reports** stating the facts and what has been done so far. It is difficult to obtain solid information on where the issues are at a global level on OSS. We are very much at the beginning of a process. Forrester is still struggling to get ongoing and complete figures from North American companies, as it is very difficult to prove ROI and TCO, especially when one does not have correct original data on ICT operating costs. One can measure the cost of acquisition, but not resistance by users, migration costs. Other hidden costs such as re-training of users, conversion of files/applications are difficult to quantify.
**Moving Forward**

In his presentation (below), Peter Lübkert raised the question: how does an organisation make the “right” choice and reduce a complex issue such as OSS to a series of manageable issues that will allow decision makers to move forward. He suggested two approaches, using decision support tools to make a detailed analysis:

- Total Economic Impact (TEI), developed by Giga Research, a subsidiary of Forrester
- Decision Support Matrix (recently used by the City of Munich) which employs a number of weighted criteria against a number of software mixes.

And once the decision has been made to incorporate OSS in an organisation, Forrester recommends building an OSS strategy by:

- selecting domains where you need to introduce open source-based systems
- within each domain, establishing a list of open source components and their area of use and
- selecting the right service provider to assist in deploying solutions.

**Presentations**

**Peter Lübkert (OECD)** described the OECD as having adopted a pragmatic approach on OSS. Several OSS products have been introduced gradually over the 10 years, mainly in back-office applications. This has allowed server consolidation to a mainly Intel-based architecture. Today, 11 OECD servers are in production under Linux. Mr Lübkert highlighted the decision elements key to evaluating software sourcing solutions, distinguishing the technical and strategic elements and the particular requirements of the organisation from purely financial aspects. Criteria other than cost have different weights for each organisation. Quantifying them and then scoring each alternative software solution against the criteria can help provide a rational basis for decision making. Various “decision support instruments” have been developed by a number of institutions. Mr Lübkert concluded by presenting the OSS decision matrix developed by Unilog Integrata for the City of Munich.

**Mark Bressers (Netherlands)** explained the main tenets of the Dutch e-government initiative called OSOSS (Open Standards and Open Source Software program for government). The aim was to improve the availability and accessibility of information, and to render better and more efficient service to citizens by improving interoperability between the (1400) independent national agencies, provinces and local government bodies. The initiative recognises that Open standards and OSS can play an important role in meeting these objectives. A Competence Centre was established to provide technical, legal and organisational advice and assistance. The Centre also plays a pro-active role in raising awareness and disseminating information. Mr Bressers cited a number of OSS implementation examples where hardware and licence cost savings had been realised. He underlined the difficulties experienced in applying more complete TCO methodologies, which were often due to a lack of data on current levels of expenditure. He also mentioned software patents as a big issue both for OSS and ICT vendors in Europe.

**Christian Hardy** of the French "Ministère de l'Economie, des Finances et de l'Industrie" presented a paper showing the strong commitment of the French government to OSS solutions, including on the user's desktop with OpenOffice.org and Windows. A special agency (ADAE), under the authority of the Prime Minister promotes the use of OSS amongst all ministries, as well as ensuring interoperability and common best practice issues. The motivating factors for the French government to replace MS solutions are to:

- Reduce desktop software licensing costs
- Provide the local economy with application development work
• Influence the software market by fostering greater competition between MS and OSS solutions, and hoping that this movement will become Europe-wide.

As of today, there are 35,000 users of OpenOffice.org and over 300,000 are planned for the end of 2005. Many infrastructure servers run already under Linux and a migration to Linux on the desktop is foreseen over the next few years. In parallel to the OpenOffice.org effort, different Ministries have migrated their applications to web-based applications using Zope server, Jboss and Java technologies. This actually requires a tremendous effort because of the important number of unique applications developed at the local Authority level. A major concern is the OSS licensing issue, which could develop over the next few years and create future usage restrictions and cost issues.

**Conclusions and Cooperation**

Many participants underlined the importance of Open Standards as a main criterion for software choice, over and above the issue of OSS. The practical difficulty is that such standards do not exist in all domains, and in particular there are few standards developed today, especially in the public sector. These standards exist in other vertical areas and industries; industry organisations have been established to determine common needs and work effectively with software vendors to address these needs. In the public sector, each institution alone may carry little weight, but together it may become possible to set out common software guidelines and standards that would facilitate procurement to all.

Many participants agreed that international organisations and governments do not have a sufficiently strong lobby or pressure group to influence the market. Organisations and administrations should get organized as a combined group to have more impact on vendors, negotiate licensing modules and obtain the development of features that are best suited to their needs.

It was also agreed that the group should exchange information more regularly and perhaps on a more formal basis. A suggestion was made to form a Working Group that could meet electronically and put forward concrete suggestions on how to move forward. It was also suggested that technical staff from organisations could get together to discuss software solutions.

There was considerable support for the idea of establishing a working group to pursue an exchange of ideas along these lines. To this end, the OECD will make a proposal to set up an OSS Working Group for information exchange among governments and international organisations. We look forward to a positive response from your organisation/administration to this proposal.

**Day 2, Session 1: ICT Governance**

The half-day session was led by Lester Rodriques, Head of ITN’s Corporate Systems & Services. Presentations were given by representatives of the OECD, the Danish administration, the IMF and by Ed Gelbstein.

Mr Rodriques started with a literary definition of “Governance”: “the act, process, or power of governing; exercising authority; the persons, committees or departments who make up a body for the purpose of administering something”. In reality, each ICT department is managed differently in each organization. What then are the key features of these different models? Are some more effective than others at managing ICT in a flat or reducing budget environment? To what extent does ICT governance ensure better service for the client community and cost-effective solutions for the organisation? How relevant are statistics/metrics? How to manage risks? These were some of the questions put to participants – a summary of their comments and responses follows.
Governance Structure

The Chair asked participants whether their CIO sits at the same table with senior/executive management or is s/he just called in to fix problems -- Are ICT managers really in control of governance issues?

- Participants agreed that the business of the CIO should have nothing to do with technical problems or daily business – the CIO should just deal with strategy. Although this view does not appear to reflect the real situation in the majority of organisations.

- However, a minority of participants noted that, in their organizations/administrations, ICT governance is now fully integrated with overall business strategy.

- The ECB representative noted that it benefits from being a new organization and believes that it has a good governance structure in place. The role of their CIO is not seen as head of ICT only. The ECB IT strategy is well aligned with its business and the CIO is involved in determining the ECB strategy.

- One participant stated that “things are on the move” but was not optimistic about high-level involvement in ICT government. Short-term, politically-influenced views often impedes strategy formulation and execution, cited as an example -- funds for an e-government project have just been cut.

How does the CIO get the attention of senior managers?

- A quick survey of participants revealed that six participants think they have a good ICT governance model, 2 participants are “getting there”, 4 participants thought their governance model could be compared to the battleground situation presented in Ed Gelbstein’s presentation.

- Some organizations said that they had hired consultants to propose a governance structure, and had “renewed” their Administration. In some countries, age/generation of administrations seemed to make a difference, with younger Ministers being more aware and in favour of putting IT on the agenda.

- CIOs need to be politicians, educators to educate senior managements and build relationships – start anywhere and convince others. Participants also agreed that IT must align with other divisions/departments to reduce duplication and avoid unnecessary competition.

- One participant said they have support from top management who are conscientious but just have no time, or the inclination for IT. They are often more involved with the political agenda rather than internal management. On the other hand, ICT governance has engaged with business managers who are interested or understand the value of ICT, and with steering groups to deal with specific business issues and projects. But it is often difficult for business managers to commit to savings from ITC investments since there is no guarantee that performance benefits can be delivered.

- As another participant remarked, project financing sources should not be overlooked - whoever has control of funds determines the priorities. Ideally, an independent department for ICT governance should be established, with its own investment budget. This function would liaise closely with business units to monitor demands, and take investment decisions accordingly.

- The IMF has a Board of Governors composed of Finance Ministers, and an Executive Board which runs day-to-day work with the Managing Directors of 24 departments. A Policy Committee
was created in 1997 to oversee IT budget policies. There is a growing consensus that IT management should be separate from the technology function which should remain in IT.

- Regarding the ICT “message”, there appeared to be a clear need to engage senior management and sell them the right messages that would strengthen confidence in the value of ICT. Conversely, an equivalent effort is required to make ICT managers more aware of their contribution to business.

- Broadly, two styles of IT governance were observed: some CIOs focus on running systems and technical strategies, others participate in the business process. CIOs of the second group are more often seen as bringing added value to the Organisation than the first one. The Forrester representative cautioned from seeing the CIO as an extraordinary person, at the risk of irritating other non-ICT executives.

**Resources and Metrics**

- Some organisations have independent committees which decide on investments and allocate funds. For example, the IFC has a capital investment fund which is separated from IT Budget.

- The outsourcing of governance was not seen as a solution – most decisions & principles on the delivery of ICT services should be made internally, and not outsourced. One participant, however, felt that the outsourcing of certain aspects of ICT governance, if well managed, could be included in the overall ICT management strategy.

- It was agreed that it was difficult to establish criteria to measure cost reduction and benefits -- for example, a participant asked “How do you define better economic modelling?” A process is needed to identify, justify and quantify benefits.

- Hidden IT costs should not be overlooked and should be reviewed regularly. Some, however, are less obvious than others. For example, many administrations and organisations rely on “power users” or IT liaisons to provide some support and technical advice – these, it was agreed, should not be considered part of the overall cost of IT, but rather an indication of the penetration of IT in an organisation.

- The Korean participant noted that IT must be considered as a cost-profit centre and charged accordingly to demonstrate its viability. At the ECB, projects are evaluated on the basis of TCO, and all the maintenance costs are budgeted for as part of the TCO. And in order to ensure benefits are delivered, project audits are carried out on an ongoing basis.

**How to strengthen ICT Governance**

A number of practical actions were deemed important to help strengthen appreciation and overall support of IT in an organisation, including:

- Building a strong base with middle management and users, as well as developing a strong relationship with the CEO and senior management.

- Relevance of ICT plans in the political agenda and with policy makers. In Denmark, e-government is the strategic goal which is driving the ICT governance effort. One issue is how to accelerate the process. In Denmark, the appraisal of ICT performance vs. e-government plans are part of the performance management process for senior officials – this is incentivating buy-in at the highest levels.
• In his presentation, the Danish participant further noted the six key components for the alignment of IT with business strategy, as follows:

1. Ensure that IT management and operational management speak the same language
2. Prioritize strategic work
3. Realize that IT is a political deliverable
4. Set out the basic IT governance components
5. Build IT Competence
6. Demand Digital Leadership from middle management

• Need to focus at grassroots level – today’s users are much more aware of the power of technology, they know what they want. The human dimension needs to be considered. It is important to develop and nurture IT champions in business areas, to preserve these relationships and ensure the success of future projects.

• Establish solid links with the user community, and regularly reach out to clients. One organization said that their Help Desk, IT regions, client officer & project managers all collect feedback and input on a regular basis. As not all the new systems wanted by sponsors are automatically wanted by users, it is often important to know what they really want.

• The “balanced scorecard” approach can be an effective method to help define, implement, and align ICT strategies. Scorecards bring consistency to the measurement of ICT based output, and help explain the need for investment in new ICT systems. Along with scorecards, benchmarks should also be regularly employed.

Presentations

Ed Gelbstein – former Director of the UN International Computing Centre, explained that the CIO is expected to possess and display many talents and strengths -- 7x24 endurance and all-around security; full cost control and resource allocation; comprehensive product development, process and project management; people management, vendor management, strategy formulation, etc. These expectations come from the Executive. Ed gave an analogy of IT strategy, metrics and decision-making as an ICT Board game. Assumption: ICT governance is a battleground for bureaucrats and technocrats – and it is never easy.

Svend Olling – of the Royal Danish Ministry of Foreign Affairs, presented the reform of IT in his ministry. Significant savings were realised in last few years by standardising on a single (Windows2000) platform. IT costs per user were cut by 50 per cent. Although staff and communication costs were not factored in to this figure, the staffing of the IT department also was reduced by 14 (It should be noted that in many government agencies, IT staffing are not included in ICT cost measurements, TCO, etc.). The Danish ministry was making regular use of benchmarking, as best practice. However, the reform did not come without a few “bumps”: some of the earlier initiatives lost steam; substantial financial & technological problems were met during implementation; certain business areas had to adapt with extra effort; and there was a sharp increase in WAN costs

Soon Choi – Director of ICT at the IMF presented the Balanced Scorecard methodology. Soon stated that: “Executing an ICT strategy has become the corporate challenge of our times”. He had no doubt that ICT strategy setting has never been more important, but cautioned that only a few of the strategies effectively formulated are effectively executed.

The Balanced Scorecard, developed in the 1990s by Drs. Robert Kaplan & David Norton, is a relatively new approach as applied to ICT management. The Balanced Scorecard approach provides a clear prescription as to what companies should measure in order to “balance” the financial
perspective of ICT. As a management system -- not just a measurement system – it enables organisations to clarify their vision and helps translate strategies into action. A good Balanced Scorecard “tells the story” of the organisation’s ICT strategy.

Among the key objectives of a strategy-focused organization (SFO), that are central to managing value creation, Soon Choi cited: mobilize change through executive leadership; make strategy a continual process and everyone’s job; align the organisation to the strategy; and translate the strategy into operational work plans.

At the IMF, the objectives set out for the IT Balanced scorecard initiative are to:
- Clarify and build consensus around the IT strategy
- Align the IT organisation to the IMF strategic objectives
- Help IT organisation establish and focus on those measures that matter
- Communicate IT strategy & progress to key stakeholders in IMF
- Provide a mechanism that rewards and recognizes contributions made by IT staff.

**Day 2, Session 2: ICT Security**

This half day session on ICT Security followed up from the OECD’s Workshop on Security management held in 2001. The session, led by Ian Hunter, Head of Network Information Systems Division, provided an opportunity for participants to share their views and experiences on security concerns and issues. The chair noted that the objectives of this session were to gain a better understanding of the principal security threats and an insight into what others are doing to counter these threats. Representatives from the Austrian and Swedish administrations, the OSCE, the OECD, Deloitte and Mr. Ed Gelbstein made presentations.

**Overview**

- The majority of organisations/administrations have a security policy or charter in place and take information security very seriously. These can be a combination of staff instructions, sanctions, actions, duties and rights of administrator and users. But even though they may have a policy in place, some participants remarked that their users are not fully aware.
- Most organisations have a security awareness/response team in readiness and the majority carry out security audits. To ensure business continuity, some organisations have disaster recovery plans which they put into action periodically.
- Many organisations use the SecureID device for their remote access. Authentication is just one element – if the SecureID token is lost, one call to the Help Desk can disable access. To avoid the secure ID PIN number written on a piece of paper phenomenon, one organisation recommends that users use their personal bank pin card number which other participants found to be a useful suggestion.
- A majority of organisations employ some form of Email filtering – some will not allow anything in which is not scannable and others quarantine any suspect messages. As one participant noted, this can make the IT department unpopular, but is critical to continuity of service and safeguarding of information. Some organisations are using Open Source email filter systems.
- Less organisations use email encryption, with one organisation imposing penalties on users if confidential information is not encrypted.
- Seven organisations are using instant messaging, which they find is a valuable and appropriate tool, especially for remote offices.
- Participants raised the issue of USB keys/sticks/PDAs etc. and questioned how IT departments can stop information creeping out of IT’s control and out of the organisation. In response, a participant said that they try to offer these services by developing secure extranet facilities, so
users are not tempted to treat information in an insecure way. They have developed services so data can be accessed from all gadgets.

- The Austrian participant noted that their solution has been quite simple regarding remote access. If the user is in a trusted environment then they are provided with a desktop; otherwise, the user has access to terminal server facilities so that the data never goes outside of the organisation in an untrusted environment. They do not mix wireless with internal network.
- The OSCE remarked that their three keywords are: Transparency, accountability, flexibility. They have had much success with policing network access based on good practice – rather than policy: They do not allow foreign devices on the network nor desktops without updated virus protection.
- A participant described to users how security consultants were able to penetrate into his organisation’s system and broke into 14,000 passwords in four hours. He concluded that passwords are fine but they do not make a big difference, even if users are taught good password practices. In fact, one organisation has abandoned use of passwords and login.

**Defining Security Policy**

- The unanimous view was that good security policies should be defined outside of IT operations and in conjunction with the business side. It should not be the same people who design the systems who decide on the policy. The two functions must be separated.
- Participants agreed that asking auditors to help with their security policies would be helpful, and several organisations have already done this. One organisation also included the legal and HR division in the defining process.

**Implementing Security Policies**

- Participants agreed that top management support was essential to be able to implement good and appropriate security and that security policy needs to be discussed at a senior level with auditor and at the organisation governance level, not just IT. As the World Bank stated “It takes a long time to make decisions and choose and implement products, so try to get buy-in for policies”
- Policies must be clear and be monitored/audited for compliance, with clear penalties for non-compliance. As Ed Gelbstein pointed out “if you don’t monitor policies, they are worthless”. He cited the frequently occurring example of staff who leave an organisation, but whose accounts remain active for 2-3 years.
- Several organisations reported that they have mandatory CBT sessions on security awareness with non-attendance being reported.
- The OECD’s Auditor General noted that as the result of several business scandals, where top management used ignorance as a valid defence, the recent Sarbanes Oxley law now punishes top management with up to 10 years prison for unintentionally publishing false information. He said that organisations must have corporate governance, enforced by internal control, which should be addressed in the annual report. Internal control will greatly impact IT and auditors will now also look at the pertinence of policies and not just control activities and information systems. He noted that this is the area requiring most concentration.
**What are we trying to protect, from whom and is it worth it?**

- The OSCE participant commented that the IT community have developed a siege mentality and are busy building fortresses. She pointed out, however, that the police force is to protect but also to serve – a concept which often falls by the wayside. We should not just be building walls but considering different methods for different means. What are we trying to protect, from whom and is it worth it? For example, the OSCE took a different perspective for remote access and looked at what needed to be accessed and what level of protection was required - e.g. low level for mail functionality, medium level for network storage, applications, etc., and high level for ERPs. For wireless, the same question is asked in conjunction with “is it reasonable?” So mobile users are asked: where do they travel, what do they need, and whether they are permanent or occasional travellers. They have developed one open network and one closed.
- Participants noted that information needs to be segregated into classified and protected versus unclassified and unprotected which will help to define what we are trying to protect.

**The human dimension of information security**

- And what about users? As long as they share passwords and pins, what really can be protected? The human factor is not negligible. However, the IT department can do much to raise awareness of clients. Security policy is a little bit like an insurance policy – you gain by not losing. IT departments need to communicate the message that security is everyone’s concern. Security policies are not meant to prevent everyone from doing anything. They are there to make our client’s life easier.
- Correlating the effectiveness of a security policy with user education and awareness, the Turkish participant gave an analogy of fire prevention in buildings – all buildings are equipped for fire protection but who actually knows where the equipment is and how to use it. It is not just a question of technology – the human factor cannot be ignored. How many organisations have readable, understandable security policies? There have to be incentives for getting people to read and understand them.
- Participants agreed that user education is essential. Several organisations have mandatory CB training on security awareness. One organisation noted that it publishes a monthly newsletter which includes security topics with links to security policy.

**Outsourcing Information Security**

- Peter Lübker told participants that OECD has taken a range of measures with no additional resources and asked whether participants had thought about outsourcing certain security measures, such as Email filtering, virus scanning, for example.
- The BEI participant reported that they have successfully outsourced security using two providers and a two layer approach: one external provider takes care of 1st level security and a 2nd onsite provider takes care of the 2nd level. He noted that so far this has been successful since it is easier to be tougher with providers than with employees.
- Another participant questioned whether we can trust outsourcing security? Ensuring that you know the outsourced staff is critical, but just because you know them does not mean they will be reliable. What happens if the outsource company goes out of business? What about the applications, extranets, etc. that have been developed by them?
- The IFC participant remarked that their Help Desk staff are outsourced and asked what is the difference where staff is located? He personally visits outsourced staff every quarter, he needs to know the people and see that they understand he is providing leadership. IFC lawyers ensure they have confidentiality agreements.
• The German participant told participants about a virtual post office project within the government network which combines authentication with mail and mail relay. The work was outsourced to a company which was founded, and is still run, by former hackers.

• Ed Gelbstein recommended a book by the Cutter group called “Divorce and reconciliation strategies for your outsourcer”. He also noted that the UK’s MI5 website has an interesting section on how to manage contractors.

The Internal Threat

• Participants agreed that they are well organised from outside threats, but what do we do against internal threats? The internal threat is real and is the most serious, but are we properly prepared for this type of attack? How do we deal with fraud, backdoor logic bombs, sabotage, and super user abuse? How do we deal with these situations when investigations are costly? And how many of these situations are due to grave stupidity with no malicious intent?

• One organisation reported that it had experienced two of these situations and emphasised that the internal threat is big and very costly.

• It was agreed that what is used is not important per se – but rather how effectively you use it. This factor should be considered in risk assessment and should be combined with physical security, scope, user education and company policies.

The External Threat

• Although governments and international organizations have fairly different IT governance structures, we are all faced with similar IT challenges, security pressures, and at times, have the same threatening groups: anti-globalisation, terrorists, etc.

• Ed Gelbstein added that from cyber crime to cyber terrorism is a small step. He gave the example of water supplies being contaminated by a disgruntled employee.

• Another example was given by the Danish participant of a recent summit in Denmark. Security services received warning of an anti-globalisation attack – they were able to monitor the situation and could identify the perpetrators who were located in Denmark and could act accordingly, but if the perpetrators had been in another country, it would have been different.

• The OECD described a cyber attack on the SME conference in Bologna. The security services were alerted in Italy but, due to various laws, no action could be taken. The cyber threat is worldwide – but there is no worldwide law, there is a need for effective international legislation.

Presentations

Ed Gelbstein presented his vision “Beyond hackers, viruses and worms”. The main points of the presentation were:

• There are 4 separate steps – and only 1 or 2 are in the IT area: - Policies, with penalties for non-compliance; Protective features in systems: e.g. database portioning, strong authentication; Operational administration and monitoring; if you don’t monitor policies they are worthless; Investigation and digital forensics

• Monitoring – we do not have the courage to monitor systems – E-trust. What happens when a user logs on, where, etc?

• Seizure & custody chain – clear procedure needed for seizure and analysis, preservation of evidence, and will it stand up in a court of law?

• Metabolic rate of an organisation is a determining factor in how secure it is, particularly when faced with malicious insiders. Someone inside will know that you are slow and take advantage of this
Reinhard Posch, of the Austrian Administration, presented the Austrian government’s Citizen Card project, its benefits, challenges and techniques.

- The Citizen Card provides Austrians with access to all e-government services with matches “in” and no matches “out”.
- It is not a physical card, but rather a logical one that uses unique information to produce an electronic signature block. It can be used via many types of media.
- One of the primary benefits – apart from being secure – is also that the government can deliver electronic services with no prior contact.

Christopher-Stuart Norman, of Deloitte, recalled that in 1999 he carried out an IT security audit at the OECD as part of the Internal Audit team. That was an IT security audit strictly from the auditor’s point of view. But more generally, how does IT protect itself – and how does it ensure the continuity and integrity of processing? How do regulations impact business?

- Sarbanes-Oxley was the first law to come out. The Enron example: Top management can no longer use ignorance as a viable defence and now has responsibility – 10 years prison if unintentionally publishes false information.
- Organisations must have corporate governance, enforced by internal control, which should be addressed in the annual report.
- Internal control will greatly impact IT: How can IT ensure that what was decided at the top is being applied? Auditors will now also look at the pertinence of policies and not just control activities and information systems. This is the area requiring most concentration.
- IT underlies the whole process of managing business. The COSO framework will play a large part in IT in the near future.
- Control environment: ethics, aim of business “tone at the top”, Risk Assessment (pertinence of), Control activities put in place to control risks. Monitoring of compliance.

Conclusions and Cooperation

- Identity management is increasingly seen as a key element in overall information security management – likely an area of major focus in the foreseeable future.
- One participant pointed out that if you don’t believe in passwords, then you have to change your philosophy. Passwords seem to be a thing of the past – biometrics is the future.
- A participant asked who had attended the recent official hackers’ conference in Las Vegas (www.Defcon.com). He noted that the “bad guys” are really good at sharing information, but organisations are not very good at sharing information. How can we incorporate this culture? He made a suggestion that organisations should employ them to see how they think and operate.
- Participants agreed that there is a failure to facilitate communication between international organisations, and that we should create ways in which we can cooperate and share protected information in a secure manner. There is a long way to go in facilitating the life of our clients – we should share some of our methods.