Information System Security

at the Council of Europe

Laurent Goubeaux
Head of Information System Security
1 Organisation of Information System Security

Information System Security at the Council of Europe (termed as IS Security below) is run by the head of Information System Security, who works in close collaboration with and directly under the head of the Information Technology Department and is responsible for:
- defining and updating IS Security policy
- running regular checks on operational procedures
- raising user awareness of the Security issue on a day-to-day basis
- keeping a watch for departures from and breaches of the rules of use of the Information System
- undertaking risk analyses and audits of the Information System.

2 Security policy

The notion of computer system security encompasses the full range of protection measures against dangers to the IS and it is the starting point for building confidence in the functioning of data and knowledge processing systems.

In an organisation such as the Council of Europe, information is stored, transferred and processed in a great many ways. It may be filed on paper in a hard copy file or on a computer, transmitted by electronic or conventional mail, or simply verbally, and processed manually or electronically. Whatever means of storage, transmission or processing is used, information must be protected against breakdowns in confidentiality, availability and integrity:
- confidentiality guarantees that information will not be disclosed to unauthorised persons;
- availability guarantees the accessibility of information at all times to those authorised to see it;
- integrity ensures the accuracy and completeness of information.

The DIT has chosen the risk analysis method (ISO / IEC TR 13335-1, ISO / IEC TR 13335-2, ISO / IEC TR 13335-3) to manage IS security. Risk analysis takes an analytical approach to risk assessment and identifies possible solutions for the types of risk defined.

The appendix “Risk analysis” explains the method in detail.

3 Operational security

Here we have illustrated this topic with a wall in which each brick is a component of Operational security.
Bricks in the Security wall:

**Technology watching**: keeping up to date with new techniques and technologies in the security field.

**Security policies: ACLs**: lists of rules present on the firewall and the hubs applying the Council’s security policy

**LDAP**: website authentication method for outside visitors with no NT authentication.

**NT Authentication**: authentication method used for information system access from a workstation.

**CERT**: body which issues warnings concerning Internet security vulnerabilities. Similar bodies offering a stronger response are being considered at present.

**Monitoring, supervision**: permits optimum activity administration with fault reporting in the event of a breakdown.

**IDS**: Intrusion Detection System, real-time surveillance of attacks coming via the Internet.

**Anti-spam**: stops individuals taking over the coe.int domain in order to send advertising or prohibited mail.

**URL Filtering**: makes it possible to control access to certain sites not connected with work. Staff attempting to access such sites receive an on-screen warning.

**IP Filtering**: means that only the ports to and from the Internet which are necessary will be opened.

**Viruswalls**: E-mails are automatically filtered to delete viruses coming in from outside (200 per month on average).

**Firewalls**: the basic protection tool between Intranet and Internet.

**Proxies**: these not only enhance Internet access performance but also log activities and provide a single Internet access point. All Council of Europe staff appear as one and the same person to the outside.

**Unserviced sockets**: sockets not in use are not systematically serviced, above all for security reasons. Many outsiders move around on our premises. If an unused socket is serviced, one of them could plug in a laptop PC and gain access to the network and therefore to our Information System.
**VLANS:** thanks to virtual local area networks, network architecture can be divided into autonomous zones. However, these zones can communicate for the provision of services such as e-mail and the Web.

**Switched Ethernet:** this technology is used to segment the network, providing protection against network "sniffing" and also enhancing network performance.

**Back-up power supply:** the components making up the infrastructure are powered by alternating current. In the event of a power failure, they are automatically switched to back-up batteries.

**Geographical and equipment redundancy:** the equipment making up the IT infrastructure is split between two geographically separate rooms. In most cases, each department is served by two machines, located in each of the rooms.

All these bricks go to make up the virtual wall separating in-house facilities from the outside. This presentation also highlights the fact that, against all expectations, the danger lies much more within (80% of threats) than outside (20%).

### 4 Raising awareness of Security

Awareness-raising is crucially important for IS Security, and at the Council of Europe it is taken very seriously. Above all it is an ongoing dialogue with users who must be convinced of the need for IS Security or understand the issues at stake.

Regular reminders are given of the Secretary General’s Instruction no. 47, which governs the proper use of the Information System. It sets out in detail the rights and obligations of users and the obligations of system administrators to ensure that everyone is provided with the best possible level of security. This Instruction differs from the earlier charter in that it forms part of our regulations and makes users liable to sanctions if they repeatedly abuse our computer facilities. It is no longer a code of conduct but a set of official rules.

New security awareness events are run each year, and these have included a Security clip in 2001 and a quiz in 2002. News items are published on the Council of Europe Intranet portal every month.
Appendix: Risk analysis

The notion of computer system security encompasses the full range of protection measures against dangers to the IS and it is the starting point for building confidence in the functioning of data and knowledge processing systems.

In an organisation such as the Council of Europe, information is stored, transferred and processed in a great many ways.

It may be filed on paper in a hard copy file or on a computer, transmitted by electronic or conventional mail, or simply verbally, and processed manually or electronically.

Whatever means of storage, transmission or processing is used, information must be protected against breakdowns in confidentiality, availability and integrity:

- confidentiality guarantees that information will not be disclosed to unauthorised persons;
- availability guarantees the accessibility of information at all times to those authorised to see it;
- integrity ensures the accuracy and completeness of information.

These three principles must be respected at the level of the Council's Information System.

IS security is not a state to be attained but a constant drive for progress in a context of perpetual change. Aware that zero risk is extremely difficult and costly to achieve, the DIT has opted for a risk reduction approach to managing security, known as risk analysis.

Risk analysis takes an analytical approach to risk assessment and identifies possible solutions for the types of risk defined.

It is based on three elements: descriptive analysis of the risks present, specification of criteria for describing risks and risk evaluation.

Risk reduction measures are categorised in terms of likely causes or possible consequences of an incident, giving five scenarios:

- for deep-rooted causes (natural exposure, culture, appeal, targeting etc) structural measures are deployed, influencing the actual structure of the IS and its environment to avoid certain threats or limit the damage;
- for immediate causes (accident, error, malicious acts etc) there are either dissuasive measures which, in the case of human threats, deter individuals from carrying out attacks, or preventive measures to stop damage or prevent an attack from reaching IS resources;
- technical consequences (deterioration of resources) are covered by protection measures which do not prevent deterioration but at least limit its extent;
- functional consequences (damage to or malfunctions of applications) are dealt with by palliative post-deterioration measures which limit the consequences in-house and restore damaged resources to their initial state;
- definitive consequences (losses) require recovery measures aimed at partial loss compensation through loss transfer to a third party, insurers or damages won in court cases where the cause was someone seeking to cause harm.

There are arrangements covering each risk and measures are applied according to its classification.