Among the things a company can do and should do is get themselves a respectable IT security system, all the better if this system is designed and fit for an international information security standard. **BS7799:2** is a British Standard Institution standard used mainly among the firms based in the EU. It is one of the security standards acceptable for implementation according to the recommendations for banks under Basel II protocol which sets up risk standards for EU-based banks, and it is one of the steps toward the federal security Sarbanes-Oxley certification for companies on US stock exchanges.

Up until now it used to be just a buzzword used in different seminars and discussion panels during recent years, yet as of May 2005, CS Computer Systems, Zagreb-based system integrator and a long-time security solution provider for some of the largest public and private companies in the country, has received an official BS7799 certification from DNV auditors as a **first Croatian company to achieve this level of security protection**.

ISO17799 vs. BS7799
People often talk about BS7799 and about ISO17799. What is one and what's another, is this same thing? ISO/IEC17799 is Code of practice for Information Security Management, a group of best practices gathered among industry specialists but it yet has to be adopted as an official standard. BS 7799-2:2002 Specification for Information Security Management is an international standard according to which you can certify your own organization and protect your confidential and proprietary information.

What exactly is BS7799 and what can its implementation do for security of my information?
BS7799 contains 127 controls which are designed to cover ten different areas of information security, including physical security, internet access, attacks form inside, business continuity, screening policies etc. By implementing the standard, a set of policies and procedures is defined which uniquely define and describe the setup within the organization, all in accordance with the security norm guidelines.

What kind of business can benefit from such a certification?
Any business is suitable for BS certification. However, most likely to green light such a project will be telecoms, banks, insurance companies, state ministries plus whoever has secret information they want to shield from mishaps. Among more known clients of BS7799 certification are Sony research center, Vodafone, Singapore telecom, Citibank, Unicredito bank is starting their own project, plus several Croatian companies have made preparations for their upcoming certification.

What would be the four key breakdown points of such a project?
The most likely four issues where a BS7799 project might break down and never get finished properly are as follows:

- Customer must make a firm definition of what kind of data they wish to protect by acquiring the certificate
- The customer's board of directors must fully back up this project to stand any chance for success

- It must be made available to hold interviews with the key information system users in order to get necessary business info regarding the information flow and protection
- The IT system should not be kept secret, but opened up for discussion and change, should it be necessary

Just how radical changes will I have to do on my IT system to get certified?

It depends on:

- Type of information one wishes to protect
- Physical location of the critical information
- Current level of protection

How much can all this cost me?

1. Consultation work
2. Possible costs of hardware or software replacement/upgrades
3. System maintenance
4. Audit and certification costs

Unrealistic expectations

No security project will ever guarantee you that your information is 100% safe. What BS7799 can do for you is make a comprehensive fix up of you security system, fully document all procedures and policies of the protection system thus allowing for allocation of responsibility, it detects attack not only from outside but from inside as well, gives you tools to further analyze and improve after a security incident occurs, and it can give you a confidence boost before your customers, press and the board.

Keeping your certificate

Your audit is done once a year, plus there is a recertification audit after each three years. What is important to remember is that there needs to be a good maintenance contract in place in order to accommodate any changes which might occur on the system in-between audits.

What can I do for your business regarding BS7799 certification process?

- Project design for security system assessment and evaluation, including the definition of security unconformities
- Additional control implementation for fixing up all detected unconformities, through the expertise and knowledge of our engineers who daily work with technologies of Hewlett-Packard, Cisco, Microsoft, Checkpoint, TrendMicro, Websense, RSA Security etc.
- Security policy and procedure documentation production
- System maintenance 24x7x365, health checkups, remote online monitoring, up to two-hour response time, daily/weekly and monthly reports