INFORMATION SECURITY

In recent years, an increasing number of countries have enacted legislation governing the protection of personal data held by commercial companies. To the extent that personal data relates to information about employees, current and potential customers, suppliers and business partners, these laws cover a wide spectrum of issues, including;

- Security measures taken to protect personal data.
- International data transfers – data cannot be transferred to other countries that do not provide an adequate level of protection.
- Existence of procedures to ensure that data is accurate and up to date.
- Control over third parties processing data on behalf of other organisations.
- Monitoring and recording of employee communications.

More recently, legislators have become increasingly concerned with the possibility of global markets being seriously disrupted due to the failure of key IT systems or networks due to criminal or accidental acts. Consequently, there is now a clear drive by regulators both in the US and Europe to focus on broader information security issues, especially in the finance sector. In October 1999, the US Congress enacted the Gramm-Leach-Bliley Act. Although primarily concerned with the re-organisation of the US banking system, following repeal of Glass-Steagall, the Act contained specific provisions relating to protection of personal information and fraudulent access to financial information.

On the basis of Gramm-Leach-Bliley, the main US regulatory Agencies (Office of the Comptroller of the Currency, Federal Reserve, Federal Deposit Insurance Corporation, Office of Thrift Supervision) issued joint standards, **"Interagency Guidelines Establishing Standards for Safeguarding Customer Information"** (IGESSCI) relating to administrative, technical and physical safeguards for customer records in financial institutions.

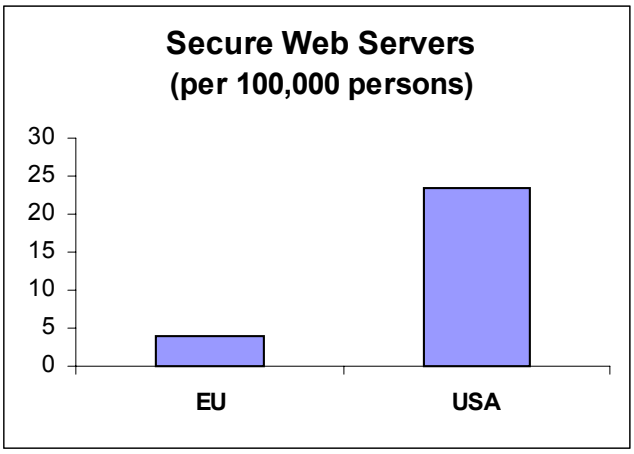
The new standards (*which are effective 1 July 2001*) go significantly further than anything previously issued and address in some detail aspects such as :

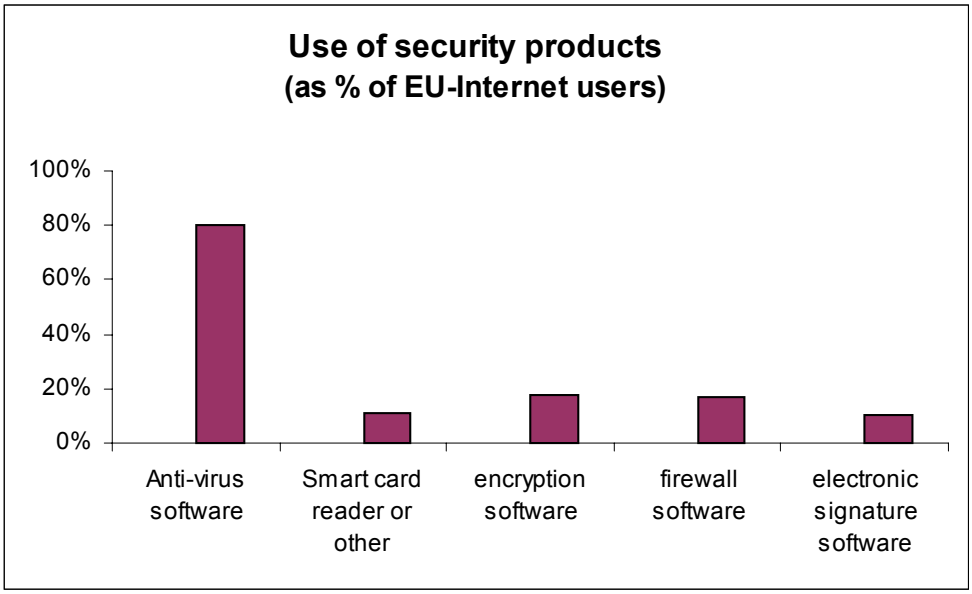
- Access restrictions on customer information systems including controls to prevent employees from providing customer information to unauthorised individuals.
- Encryption of electronic data customer information, including whilst in transit or in storage on networks or systems to which unauthorised individuals may have access.

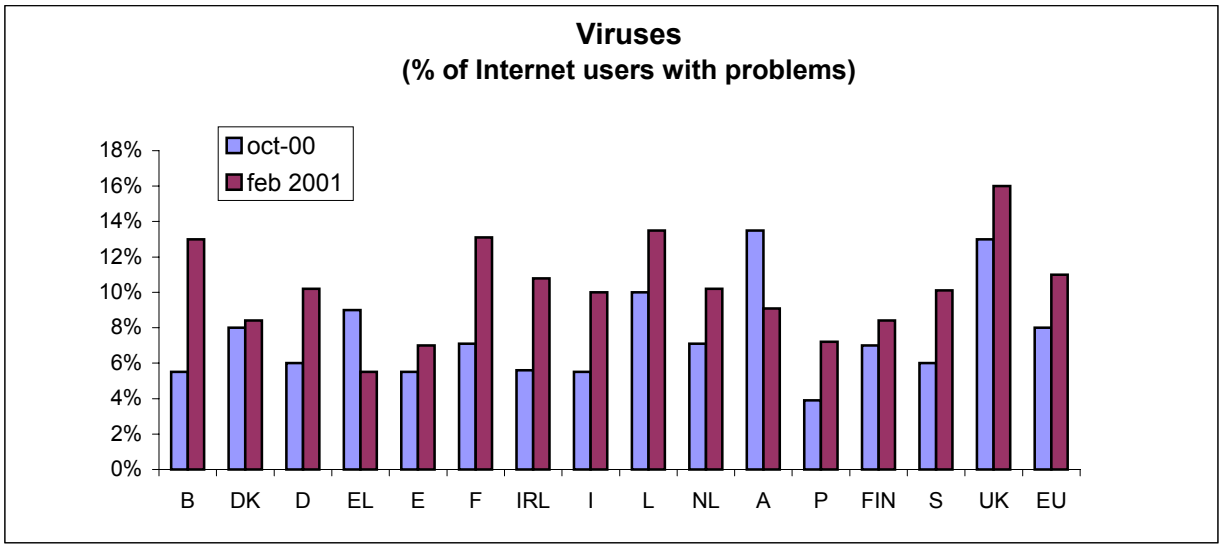
- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer data.
- Monitoring systems and procedures to detect actual or attempted attacks or intrusions into systems.
- Measures to prevent against destruction, loss or damage to customer information due to potential hazards such as fire and water damage or technological failures.

Whilst companies that have entities that may be subject to regulation by one of the above named US agencies should ensure they comply with IGESSCI, they should be aware that things are also moving in Europe.

The Stockholm European Council (23-24 March 2001) concluded *"the Council together with the Commission will develop a comprehensive strategy on security of electronic networks including practical implementing action*". In response the Commission has now issued a working document to member states **"Network and Information Security: Proposal for a European Policy Approach"**. This paper addresses issues relating to Availability, Authentication, Integrity and Confidentiality of networks and information systems within the EU. In so doing, it provides some significant statistical information that shows that Europe lags well behind the US in information security as shown below :







Although the EU document is essentially a discussion paper it does outline a number of proposed actions that are designed to drive market forces to increase investment in security technology or security practice. Further, the Commission recognises that there is a need to improve the functioning of the existing legal framework. For example, whilst the following regulations exist they are rarely invoked :

- Art 4 Directive 97/66/EC – providers of a publicly available telecommunications service are obliged under EU law to inform subscribers of breaches of security and any remedies, including costs involved.
- Art 17 Directive 95/46/EC requires IT processors and controllers implement appropriate and organisational measures against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

- Directive 97/33/EC and 98/10EC require that Member States take all necessary steps to ensure the availability of public networks in the event of catastrophic breakdown.

In conducting risk surveys, the findings of FLUX Consultancy in the last 2 years would tend to confirm the concern of regulators. Key issues we have identified repeatedly, relate to :

- Lack of internal IT security policies and guidelines
- Poor administration of logical access control to systems
- Extensive and uncontrolled access by third parties (e.g. consultants to client data)
- Absence of any contingency plan testing
- Lack of encryption of electronic data customer information, whilst in transit or in storage.

Further, few if any organisations appear to be aware of their responsibilities under national or EU legislation in the area of IT security.

It follows that the concern of FLUX today is not so much that companies are condemned for a regulatory violation, but that they are held civilly liable for negligence. In this context, we believe that there is now sufficient legislation and codes of conduct (e.g. ISO /IEC 17799 or US FFIEC standard on IT security) to clearly define best industry practice for IT security management. With the increasing criticality of IT services for clients, in the event of loss, we believe service providers are increasingly leaving themselves open to claims for legal damages if they cannot prove that they have adhered to best industry practice in IT security.

In the context of the foregoing, the EU document on Network and Information Security raises the issue of liability in these terms *"On the cost side, market actors are not responsible for all the liabilities related to their security behaviour. Users and providers with low levels of security do not have to pay third party liability. This is like a careless car driver who is not held liable for the costs that occurred as a result of his accident."*

Looking forward, FLUX is convinced that commercial organisations will have to invest more time and money in information security if they are to avoid costly and damaging law suits. If you need to be convinced just try and assess how much information leaves your company everyday via uncontrolled email attachments.

PATRICK MAUGHAN
email : maughan.patrick@fluxrisk.com
tel : 0032.2.725.11.79 - fax : 0032.2.725.17.47
FLUX RISK SERVICES SA
16 Av de la Sablière,1160 BRUSSELS – BELGIUM
http://www.fluxrisk.com