Security as a legal obligation.

About EU legislation related to security and Sarbanes Oxley in the European Union.

By Edwin JACOBS, Company Lawyer[1], Associate researcher at the Interdisciplinary Centre for Law and Information Technology (ICRI) ' IBBT - University of Leuven

Web: ICRI website
Web: ISABEL website
Email: edwin.jacobs@law.kuleuven.ac.be

Brief Biographical Description: see Brief Biographical Description Edwin Jacobs

Abstract

Since the Sarbanes-Oxley Act there is a worldwide focus on security issues in general. This new focus seems to emphasise that security is a new kind of legal obligation. However, security is already a legal obligation for all EU companies since the early nineties. On top of that, in electronic banking there is a whole range of legal obligations in some way related to security, that were already (and remain) applicable, notwithstanding a possible application of the Sarbanes-Oxley Act on some EU companies. The criterion of what can be 'reasonably expected' as 'bonus pater familias' from service providers, but equally also from their customers, becomes increasingly important.

1. Introduction

Security can be considered as a legal obligation for companies. 'The problem is made worse by the Internet's internationality. No uniform system of law or policing can patrol it. The merchants, like the cannon-carrying merchant ships of two centuries ago, must provide security themselves. The more secure people can be in their transactions, the larger those transactions will be and the more profitable the Internet will be as a business medium.'
In the present paper we give a high level overview of the legal sources, applicable in the EU, imposing such an obligation and we examine the criteria that shall be used for judging a company that is in breach of its security obligation.

2. Security as a legal obligation

2.1. Sarbanes-Oxley and 'corporate governance'

Today, security is often associated with the requirements introduced by recently enacted legislation such as the US Sarbanes-Oxley Act (hereafter 'SOX'). This was enacted as a consequence of the financial scandals concerning Enron, Arthur Andersen and Worldcom. It is based on a bill introduced by senator Paul Sarbanes and congressman Michael Oxley and applicable to companies registered with the U.S. Securities and Exchange Commission (SEC). SOX directly affects mainly, but not exclusively , US companies. Only about 500 non-US companies have a quotation on the NY stock market. SOX is also important for EU subsidiaries of US multinational companies and questions can be raised about the compatibility with private international law (which is out of scope of the present short paper). They were required to comply with SOX from 15th July 2005. However, on 2nd March 2005, the US Securities and Exchange Commission (SEC) extended this deadline by one year until the fiscal year that ends after July 15, 2006. The fiscal year of many companies runs in parallel with the calendar year. Consequently, they will need to be SOX-compliant by 31st December 2006, including testing their control regulations for effectiveness.

The Sarbanes-Oxley Act contains 69 sections, mainly about financial control, quality of the accountancy records and procedures, independence of the auditors, etc. The most often quoted provision however, is Section 404. Under section 404 of Sarbanes-Oxley, the company's management is required to file a report that contains the following:

- a statement of management's responsibility for establishing and maintaining adequate internal controls over financial reporting;

- an assessment by management of the effectiveness of the company's internal controls as of the end of the company's most recent fiscal year, including a statement as to whether the controls are effective;

- a disclosure of any "material weaknesses" in internal controls that management has identified;

- a statement identifying the framework used by management to evaluate the effectiveness of the company's internal controls; and

- a statement that the accounting firm that audited the company's financial statements has issued an attestation report on management's assessment of the company's internal controls.

In the EU the general topic of 'corporate governance' has been taken up and translated into a number of non-binding codes and guidelines. The Basel II agreement in the financial sector and the Belgian 'Code Lippens' are examples of this evolution.

The need for compliance with the Sarbanes-Oxley Act, and certainly the attention paid to SOX also in the European press together with the attention for corporate governance, has led to a renewed focus and awareness regarding internal control, audit, procedures, and ICT security, not only as a tool for obtaining good corporate governance and internal financial control but also ICT-security as a goal as such (against hacking, phising, pharming, viruses etc.), because a breach of ICT-security could easily also cause a breach of internal (financial and reporting) control.

2.2. Legal security obligations in case of personal data processing

The emphasis in popular press on SOX and the 'corporate governance' codes of conduct should not make us forget the already existing EU legislation in the field of security. Already in 1995, the EU introduced the Data Protection Directive. This Data Protection Directive imposes an explicit obligation for adequate security on every company that processes personal data (data about physical persons, such as names, addresses, financial data, etc.). Pursuant to this obligation, the controllers and processors of such personal data should take 'appropriate' security measures. 'Appropriate' or 'adequacy' in this context is measured according to four criteria:

- the measures should be 'state-of-the-art'

- the nature of the data has to be taken into account (stricter for financial data, health data, etc. compared to mere contact data

- the measures should be in line with the potential risks (financial institutions are often a target for hackers)

- the investments have to be proportional to the potential of the controller or the processor.

2.3. Legal security obligation for publicly available communications services

As far as companies (e.g. possibly also some banks) provide publicly available communications services (e.g. via public websites) over public networks (internet, mobile payments via cellular phones etc.) there are similar legal security obligations that are contained in the EU Electronic Communications Directive. The obligation is very similar to the one described above in the context of the Data Protection Directive.

3. General duty of care in case of a professional service provider in the financial sector

3.1. The concept of general duty of care

The presence of specific legislation related to security and risk management should not make us forget that every person (so also customers of on line services!) and every company have a general duty of care. If the lack of appropriate security measures leads to damages for third parties, the liability of the company which omitted to apply best practices in this field (and hence to behave as the 'bonus pater familias') will automatically be involved. Contrary to the specific legal security obligations described above in the specific laws, the general liability can to a certain extent be reduced by liability disclaimers that have to be carefully drafted.

3.2. Role of service level agreements, industry standards and best practices.

A prudent and professional ('bonus pater familias') financial institution or payment system should have service level agreements (SLA) with its key suppliers in order to control as much as possible the adverse effects of system failure for its customers. Complying with industry standards (or even having their own standards as high as the best practices in the industry) also contributes to being a 'bonus pater familias' service provider. This does not mean that such service providers are automatically bound by an obligation to achieve a precise result about security (e.g. offer a continuous or security 'breach less' on line service) towards their customers; it remains an obligation of 'best effort', but a 'best effort' of a high and professional level.

Financial institutions that outsource certain activities are often obliged to conclude SLA's with their suppliers. This obligation is imposed by the national authorities exercising prudential control on credit institutions and investment firms in the EU member states. The Basel Committee on Banking Supervision wrote a paper called 'Risk Management Principles for Electronic Banking'. The starting point is that the rapid development of e-banking capabilities carries risks as well as benefits and that such risks must be recognised, addressed and managed by financial institutions in a prudent manner according to the fundamental characteristics and challenges of e-banking services. These characteristics are: the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of open electronic networks, the integration of e-banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology. To facilitate such adaptation of risk management principles, the Basel Committee presented a document 'Risk Management Principles for Electronic Banking'. It is expressly emphasised that 'These Risk Management Principles are not put forth as absolute requirements or even 'best practice.' because (1) setting forth too detailed risk management requirements could be counter-productive, taking into account the rapid evolution of technology in e-banking, and (2) each bank's risk profile is different. Therefore the risk management principles and sound practices described in the document 'Risk Management Principles for Electronic Banking' are meant as tools by national (prudential) supervisors.

4. Some specific legal issues related to secure electronic banking

4.1. Liability under Electronic Transfer of Funds legislation

Being an issuer of an instrument for the electronic transfer of funds (e.g. credit card, debit card), implies all responsibilities (also regarding security) and liabilities mentioned in the EU Recommendation 97/489/EC of 30 July 1997 concerning transactions carried out by electronic payment instruments and in particular the relationship between issuer and holder, and the corresponding national legislation in the EU member states.

4.2. Anti money laundering legislation

The European Directive of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, applies to financial institutions and i.a. describes legal requirements regarding identification (and thus security of all stakeholders) of their clients.

4.3. Impact of possible application of consumer legislation.

When offering services to consumers (i.e. B2C, as opposed to merely professional customers in B2B), this entails the application of the consumer legislation. Recent changes to consumer regulations result in the expansion of the scope of these regulations, especially in the financial sector. E.g. the EU Directive for Distance Marketing for Financial Services and the European Commission Communication on application of the e-commerce directive to financial services may also become relevant.

5. Security obligations of customers of e-banking or other electronic services in general

No matter how secure and sophisticated a (financial) service provider's security may be, caution is still recommended for all customers. It is reasonable to expect a degree of 'common sense' and vigilance from customers, certainly from professional customers in B2B. The criterion of the 'bonus pater familias' also applies to customers, at home and at work. They are also subject to an obligation of a general duty of care. Appropriate internal security policies should exist at the customer side. Customers working in an on line environment, be it for e-banking or other electronic services in general, should have a secure pass words policy, keep virus scanners and firewalls up to date, and inform the service provider (e.g. bank) and/or authorities immediately when they suspect a security breach (e.g. coming from phising, hacking etc).

6. Conclusion

Security is a legal obligation for all service providers, not only those subject to SOX or to specific security legislation. Customers that use the services also have certain legal obligations to protect their own security.