Niklaus Blattner: IT in the financial sector - aspects of regulation and supervision

Summary of a speech by Mr Niklaus Blattner, Vice-Chairman of the Governing Board of the Swiss National Bank, at 8. Berner Tagung für Informationssicherheit (8th Conference on Information Security), Berne, 29 November 2005.

The complete speech can be found in German on the Swiss National Bank's website (www.snb.ch).

* * *

The completeness, integrity, traceability and constant availability of data that has been securely processed are essential in order for the financial system to function smoothly. The Swiss Federal Banking Commission (SFBC) supervises banks and securities dealers domiciled in Switzerland. Its microprudential supervision focuses on the individual financial institution, in particular with regard to the protection of creditors and investors. By contrast, it is the task of the Swiss National Bank (SNB) to contribute to the stability of the financial system, i.e. it is engaged in macroprudential oversight.

Banking legislation provisions governing the IT organisation requirements of a financial intermediary do not explicitly address the topic of information security, but rather focus on the notion of "proper and rightful conduct of business". For the SFBC, information security is merely one concern among others. In one of its circulars it has, however, addressed several critical areas in greater detail, e.g. on the topic of external data management and outsourcing. The SNB's mandate is limited to the payment and securities settlement systems. In its oversight function, the SNB focuses on systems which might constitute a potential threat to the stability of the Swiss financial system.

The SNB's objectives with regard to information security include the following: security policy and organisation, physical and staff security, system operation, system development and maintenance, communication and information exchange and – last but not least – business continuity management. Similar to the SFBC, the SNB basically pursues a dualistic approach, i.e. it relies primarily on the results of internal and external audits.

Any supplemental, cross-system measures must be jointly coordinated and synchronised by all the major players. The steering group "Business Continuity Planning" (BCP), headed by the SNB, assumes this function and examined the business continuity plans developed in the individual companies. The report reveals that a great deal of progress has been made with regard to the BCP efforts of the systemically relevant infrastructures and their major participants. Moreover, the report contains concrete requirements for the different players and identifies room for improvement in various respects. One measure, which has meanwhile already been implemented, concerns the creation of an alarm and crisis organisation that spans the entire financial sector.

The final conclusion that can be drawn is that it is the responsibility of the individual company to ensure information security. Regulation, oversight and supervision play only a secondary role. Information security deserves to be accorded appropriate priority by every board and every management, regardless of whether the company is a global player or a small savings bank.