It's the economy, stupid*

BANKING SECRETS

"Skyfall" is the name of the new James Bond film that arrived in cinemas in November. This genre cements the image of discreet banking with regular reliability. We as bank clients would fall out of the sky, too, if we were aware of the dangers to which our financial data could be exposed; that is if it is not adequately protected.

by Casha Frigo Schmidiger, Publicist

Deep trusting relationships are crucial not only with commercial banks. As super banks, the central and national banks are all the more exposed to high risks worldwide. They are the supreme guardians of monetary policy. As such they must keep price levels and monetary values stable and provide funds for the financing activities of commercial banks. They form the backbone of a national banking system.

In many countries, the departments of the central bank are spread across several parts of the country for historical and political reasons. The network connections between the regionally separate departments consist of in-house networks with redundant structures. Gigantic volumes of data are involved in the data exchange of the national bank with its different branches but also with the different commercial banks in the country and with international bodies such as the European Central Bank ECB or the World Bank. IT systems often determine the sequence of important business processes. "Big data" represents one of the most daunting challenges of the future. Both banks and national banks will have to tackle it. The volumes of data created in the future will significantly surpass the huge volumes already existing today. However, financial institutions are still largely unclear on how they will record, process and, above all, protect this flood of data.

Money, the lifeblood of an economy

Data security is a subject that will increasingly concern the financial industry in future. After all, the industry is facing mounting pressure from criminal forces and from future trends such as intelligent digital networks, to say nothing of targeted attacks out of the vast endlessness of cyberspace. For instance, Gauss, a virus "related to" Stuxnet, has already infected more than 2,500 computers in banks in Israel, Lebanon and Palestine. Anyone who succeeds in manipulating the payments of a major bank or the data flows of a central bank damages an entire economy. Once the flow of money is shut off, there is not much more you can do.

However, one falls far short if one blames the banking industry for being insufficiently security-conscious and depicts it as sweeping security problems under the rug. Central banks in particular are putting security issues at the top of their agendas. This prioritisation is evident from an excerpt from a job ad published last August: "As an IT security architect, you bear professional responsibility for the IT security architecture. You formulate concrete specifications for the chief information security officer for IT and devise pertinent approaches. You are responsible for detecting weaknesses in IT security and for determining appropriate actions to reduce the identified risks."

It would be wrong in information security to focus solely on technologies and processes, known as logical security. The latter is only as effective as the weakest link in the chain and human beings are still that weakest link. One cannot come to grips with information security with technologies alone. This fact has to be made perfectly clear. Everything must be done organisationally to ensure that data does not end up on the wrong track.

So, what can a central bank do to protect its information?

Comprehensive information security – a two-point programme

1. **People, process, technology: organisational, physical and logical security in triad**

   As explained above, the implementation of information security entails much more than merely installing hardware. It also involves numerous services ranging from a status-quo analysis to life cycle management. Information security is implemented as a logical project process comprising four phases:

   The first phase, **security assessment**, is similar to a SWOT analysis. In it, the assessors evaluate the strengths and weaknesses, the opportunities and risks of the previous information security strategy. To this end, they take stock of and check the people, processes and technology involved. A strictly technological assessment is not sufficient and does not show the whole picture. The employees' security awareness is also critically examined in light of the major danger posed by human beings.

As regards the **technology** used, the Crypto assessors check to see what kind of security architecture is in place (firewalls, encryption, etc.). This check involves participation by ethical hackers as well as social engineering or phishing attacks on site. **The main processes** in the organisation are also scrutinised as part of this assessment. Does the organisation cope effectively with the critical parameters? Are there internally defined procedures on matters such as how to deal with a loss of data?

Once the security requirements are clarified, one proceeds in a second phase to devise technical **security architecture** for maximum security tailored to customer needs and the basic conditions involved. This architecture includes a zone and zone-transition system for the different security levels in the network.

Security as a continuous improvement process

Phase three consists of **realising and defining a process.** This phase entails adapting procedures and roles based on various best practices and implementing a process framework tailor-made for the customer.

Regular audits required

Security is only as good as the security practices actually applied. To ensure optimum information security, regular checks must be conducted of organisational and technological measures to minimise and decimate risk. Phase four of consulting by Crypto AG involves **controlling**, i.e. a concise measurement of the actions adopted.

2. Highly vulnerable backbone for data transmission

Central bank data is subject to maximum security requirements by legislators and the bank's customers, the commercial banks. The storage area network infrastructure underlying data exchange consists of several physically and geographically separate parts. Data is transported over optical-fibre connections known as interswitch links. Even today in 2012, they are easy to tap and attack. As protected zones, storage centres are usually secure enough for data to be exchanged in plain text between the individual storage areas. However, if links are run externally over publicly accessible territory, i.e. optical fibres, high-security encryption of the data flow is mandatory. Even the enormous transmission capacity of 10 gigabits per second provides security in appearance only. Not a single byte "can hide in the crowd" even at this high data throughput. Each data packet, no matter how quickly it is sent, has a destination address and a source address following precisely defined structures (frames). Seamless high-security encryption of all information sent is the only means of effectively countering modern attack methods. The HC-8555 Gigabit Ethernet Encryption from Crypto AG is the world's fastest encryption unit and delivers powerful Ethernet link encryption.

The famous quote* by Bill Clinton's campaign director James Carville used in this article's title takes on a deeper meaning: "It's the economy, stupid. The economy is what determines a country's prosperity." And it is the central banks that guarantee the stability of a currency. A crucial pillar such as national monetary policy is not publicly negotiated. Thanks to data encryption and seamless control of people, processes and technology, financial strategies are treated confidentially and guarantee a country's prosperity. ■