Digital revolution creates achilles heel for Swiss bank secrecy

February 14 2010, by Alix Rijckaert

The digital revolution is turning into the achilles heel of Swiss banks, according to security and banking experts quizzed about recent stolen data turning up in the hands of neighbouring countries.

The digital revolution is turning into the achilles heel of Swiss banks, according to security and banking experts quizzed about recent stolen data turning up in the hands of neighbouring countries.

CD-ROMs, USB sticks and even mobile phone cameras have become handy options for disgruntled or ambitious staff to copy computer data on thousands of clients when a few years ago a cumbersome paper trail was needed.

Swiss banks built much of their recent reputation around a legal obligation to maintain secrecy on their customers' banking affairs --

criminal cases aside -- including from the taxman, whether in Switzerland or abroad.

But preventing one-off leaks, which can have much a bigger scope than before, is becoming a conundrum.

Banks are "big consumers of Information Technology" and have to "square the circle" to counter the threat, Gregoire Ribordy, director of network security firm IDQuantique told AFP.

Measures are available, such as minimising the extent of information open to client advisers, automatic access restrictions, multiplying the number of people needed to unlock encrypted data, or prohibiting USB keys and CD-ROMs at the workplace.

Nonetheless, "information has to circulate so that people can do their jobs," said Ribordy.

Yet, even a miniature camera on a cellphone is enough to take a snapshot of data displayed on a computer screen, he pointed out.

The 1934 law on bank secrecy was specifically designed to discourage staff from leaking client data to foreign powers by making it a criminal offence, but that was in the era of hand or type-written ledgers and punch cards.

In 1996, a private security guard became a whistleblower by recovering documents from the shredding room of UBS bank in Zurich to reveal details on hidden Holocaust-era accounts.

But little has filtered on the exact origins of a CD-ROM with stolen Swiss bank data German authorities recently said they were ready to buy for 2.5 million euros in a crackdown on tax-dodging German taxpayers.

A spokesman for the Swiss Bankers Association, Thomas Sutter, acknowledged that the case "is not a good thing for the financial centre."

The German case emerged just months after French authorities picked up a CR-ROM with raw data taken by a former employee of HSBC Private Bank in Geneva, Herve Falciani, allegedly with details on some 3,000 clients.

And in 2008, an anonymous whistleblower sold data on thousands of clients at Liechtenstein banks, helping Germany investigate suspected tax evasion by business executives, sports stars and entertainers.

In the French case, Falciani was a computer expert at the bank.

While in recent years public attention has focused on external attacks by hackers or thefts exploiting Internet Banking, IT security specialist Jerry Krattiger told Le Temps newspaper that about 70 percent of leaks were by insiders.

Hans Geiger, of the Swiss Banking Institute at Zurich University, said there was generally a "high probability" that such leaks would emerge from the IT or computer department.

"I think they are always within the bank or from a service provider to the bank," he told AFP.

"They don't walk away with data or info about two or three clients, they walk away with CDs with hundreds of thousands of clients."

"There is no absolutely safe way," he added.

Another way for banks to tackle the whistleblowing threat is to foster trust and loyalty among their staff, according to Arturo Bris, professor of

finance at IMD business school in Lausanne.

Human resources also have a crucial role to play in detecting "suspect behaviour, an employee who is frustrated or faces personal problems" and therefore more likely to be tempted by data theft.

"The bigger the group, the more difficult it is to find the rotten apple," Bris added.

Switzerland's two biggest banks, UBS and Credit Suisse, declined to discuss their security arrangements but insisted that security for private clients was a major priority.

Geiger said banks relied on "a real internal police force," including IT specialists.

While information technology is of "strategic" importance, Krattiger regretted that it was a largely "hermetic world" for senior executives and directors.

Meanwhile, the very same managers hold the purse strings, but security is not a revenue generator, Ribordy noted.