Wake-up calls on rogue traders keep ringing, but who's answering the phone?

Leon Gettler – The Age Newspaper, Australia
February 2, 2008

IN THE fallout from Societe Generale's $8 billion implosion, Lyndon Nelson, the head of risk at Britain's market regulator, Financial Services Authority, told reporters that the scandal was a "wake-up call" for banks.

Hardly. The sad fact is, there have been many wake-up calls. Often, it's a similar story of traders playing the odds. And unfortunately, those calls are likely to keep coming. Examples include the foreign exchange trades that cost NAB $360 million in 2004, the result of poor supervision, inadequate internal controls and a culture focused on good news and profits.

Then there was Nick Leeson's $US1.3 billion derivatives-trading losses in 1995 that all but wiped out Barings Bank, the bank that funded the Napoleonic wars and was subsequently sold to Dutch banking and insurance group ING for £1.

Or Yasuo Hamanaka, Sumitomo's chief copper trader. Known as "Mr Five Per Cent" because of the share of the copper market he was believed to control, Hamanaka engaged in a decade-long manipulation to corner the market in the 1990s, ultimately costing his employer about $US2.6 billion.

Then there were the wrong-way bets in 2006 that cost US hedge fund Amaranth more than $6 billion. Amaranth, whose name means "unfading flower" in Greek, made billions the year before betting on natural gas. After hurricanes Katrina and Rita triggered a spike in energy prices, it cleaned up. But, eventually, prices began to fall. Amaranth essentially doubled its bets as gas prices continued to plummet, turning the unfading flower into a shrivelled-up trader.

Or the collapse of Long Term Capital Management in 1998. Put together by people with Nobel prizes in mathematics, who were considered to be geniuses, LTCM went broke and nearly brought down the financial system when its models, which ruled out the possibility of large deviations and took on a monstrous amount of risk, failed to take into account the unknown force of the Russian debt default.

Not to mention Toshihide Iguchi, a former car salesman who rose to become one of Daiwa Bank's senior US executives and who, in 1995, was discovered to have hidden more than $1 billion in trading losses over 12 years.

John Somerville, the head of KPMG's performance risk and compliance practice said the "wake-up calls" don't seem to work. The big problem is that the qualities that make a fantastic trader can also make a chillingly competent fraudster.

"It seems to be a very similar story every time," Mr Somerville said.

Part of the problem, he said, might be the gulf that exists between traders and the people supposed to be supervising them.

"When you are in a world where you are paying your front-end people, your originators and traders, lots of money and you don't pay your back-office people as much, you get a serious disconnect in capabilities," Mr Somerville said. "The people at the front end are going to be sophisticated and the guys at the back end will be process driven. So would they have the nous, the knowledge and insights to ask the questions they need to?"

Another problem, he said, was corporate memory. It did not last forever, and some organisations tended to repeat mistakes. Studies had shown that corporate memory ran to about seven years.

"All the banks went through the NAB saga. They all did a fair bit of work on whether they would be exposed to something like that and what they needed to tighten up their control frameworks. But how real is it seven years on? Does it still have the same level of attention, scrutiny and focus?"

Former Sydney detective Paul Curby, the founder and managing director of the Insight Risk Group in Singapore, a fraud risk advisory business, said all financial institutions, including Australian banks, were vulnerable. The same patterns, he said, just kept repeating. "I have done work all around Asia. I have done work in Europe with different financial institutions and with different multinationals and pretty much it's very similar. People are people wherever you go."

"Unfortunately, the larger the organisation is, you might find that something important might come to someone's attention but it is not acted upon because they believe someone else should be looking at it."

There were no foolproof systems, he said, but even the most skilled fraudsters eventually came unstuck. What organisations needed to do was put in place preventive measures. And they needed to know the right questions to ask.

"When we go into organisations, we stress-test the controls and look for frauds which will succeed within the institution's control environment," Mr Curby said.

"What had this trader been doing compared with the other traders, for instance? There must have been signals earlier on that were either ignored or not properly followed through.

"They should be looking at this guy's open positions (where instead of buying one market and selling another, the trader buys one market and then doesn't balance it by selling the other), his margin account, how many open positions this trader has compared to other traders and how many trades was he doing compared to other traders exercising similar trades.

"They are the sorts of things organisations should look at to see whether your star performer is actually a star performer or whether he or she may be trying to manipulate the system."

Another method was to make sure that the traders took time off from the office. During that time, there would be absolutely no contact with the office.

"Data has shown that in the past fraud has been uncovered where an employee has gone on leave and someone has occupied that position and has discovered something unusual and started digging around and found more than meets the eye.

"In banks, they call it block leave and it varies from organisation to organisation. In some, you may have to hand in your BlackBerry and you're not allowed to do emails. When you are on your block leave, you are uncontactable, you can't influence or authorise any transaction. You are removed, so to speak."

A full-scale probe into a bank's systems costs anywhere from $50,000 for a week's work to $150,000 depending on the size of the department.

On the other hand, Mr Curby has gone into banks and found $1 billion at risk. "The $50,000 for a week's work plus reporting is a rounding error for a bank," he said.