FT.com FINANCIAL TIMES
TECHNOLOGY
Digital Business

Lessons from SocGen: Internal threats need to become a security priority

Print

By Geoff Nairn

Published: February 11 2008 10:18 | Last updated: February 11 2008 10:18

The staggering €4.9bn ($7.1bn) loss incurred by a rogue trader at **Societe Generale** has repercussions that extend far beyond the rarefied world of derivatives trading – notably concerning IT security issues that affect many organisations.

Richard Stiennon, an IT security consultant, says: "The **SocGen case** is a classic internal one, carried out by a knowledgeable insider and, technically, it would have been very easy to detect."

Nevertheless, Jérôme Kerviel, a junior trader on SocGen's equity futures trading desk in Paris, managed to hide his trades for almost a year before being discovered last month.

He was helped by his intimate knowledge of the bank's control systems and procedures and by vulnerabilities in IT security.

"You can always rely on the IT guys to leave a gaping hole for an insider to exploit," says Mr Stiennon, who previously worked as a "white hat" hacker for PwC.

Mr Kerviel had spent five years working in middle-office functions before being promoted to the front office.

Bob McDowell, senior analyst with TowerGroup, the financial services consultancy, says: "It is relatively unusual for people to move from the back office to the front office in an investment bank and someone like that should be not be allowed to run large positions."

Mr McDowell also points out that Mr Kerviel was not working in a customer-facing business but on the proprietary trading desk which is subject to "less onerous procedures", partly because the money at risk is the bank's own.

Financial firms have spent huge sums on IT systems and procedures to comply with regulatory regimes such as Basel II, ITIL and Sarbanes-Oxley in recent years. In theory, they have an armoury of technology ready to catch any trader who strays.

SocGen itself had built a sophisticated risk management system for its derivatives trading operation. The system, supplied by US vendor Algorithmics, was designed to measure the external risk of a counterparty defaulting on a deal. But a greater danger was lurking within SocGen; risk management systems are not designed to spot "rogue traders".

"This was a surveillance problem not a risk management problem," says Simon Asplen-Taylor, head of regulatory services at Detica, an IT consultancy.

Even the rules-based surveillance systems widely used in investment banks would have struggled to flag Mr Kerviel's behaviour as suspicious, because he appeared to be staying within his daily trading limits.

A recent survey by CERT, the IT security programme run by Carnegie Mellon University, shows that corporate IT security strategies remain heavily focused on protecting business from external threats such as hackers, even though the insider threat is getting worse – 27 per cent of incidents involve insiders.

For this reason, analysts stress the importance of enforcing internal procedures and security systems.

For example, Mr Kerviel was able to log on as someone else, allowing him to bypass his trading limit by "taking [trading] positions using the machines of colleagues at the same time and in full sight of all," as he says in his statement to police.

"It's human nature for people to share passwords," says Mark Fullbrook, manager of UK-based IT security firm Cyber-Ark.

But this becomes a more serious problem when traders are able to access systems in the back-office. "It should not be possible for someone in the front office to access client-opening and interdealer systems," says Mr McDowell.

Security experts say such problems can occur when old log-ins are not cancelled and are especially serious if they include "privileged user" log-ins. These powerful passwords are normally restricted to IT staff, as they provide a "back door" into systems and allow the holder to access and change data.

Keeping log-ins and access privileges up to date as employees join, leave or move is a chore for corporate IT departments and the potential security loopholes created by inefficient manual processes has led to the growth of dedicated solutions for "leavers and joiners", such as Quest Software's ActiveRoles Server. For managing privileged user passwords, Cyber-Ark has Digital Vault software.

Single sign-on is a related technology that seeks to eliminate the risks arising from users needing multiple passwords to access different systems. Vendors in the SSO market include **Entrust**, **IBM** and **Citrix**.

Passwords, by their very nature, provide only limited protection against internal attacks. More robust protection can be obtained using authentication technologies such as biometrics.

Today, laptops and computer keyboards often come with built-in fingerprint scanners. But investment banks are not big fans of biometrics, despite the obvious benefits. Mr Stiennon says: “The problem with using biometrics or any other control technology in the dealing room is the ‘push back’ you get from the traders.”

Nevertheless, Mr McDowell believes the SocGen case will force investment banks and other organisations to look again at using biometrics.

There are many other technologies to help businesses protect themselves from internal threats. But they must go hand-in-hand with strict supervision and procedures.

As Mr Kerviel told the police himself: “The techniques I used were not at all sophisticated, and in my opinion, any correctly conducted control should have been able to detect these operations.”

.....

Security checks

• Be aware of the areas in which staff have worked
• Do not rely on risk management systems for internal security
• Enforce procedures
• Ensure log-ins and access are up to date as staff move/leave
• Prevent multiple sign-on

Copyright The Financial Times Limited 2010. Print a single copy of this article for personal use. Contact us if you wish to print more to distribute to others.

"FT" and "Financial Times" are trademarks of the Financial Times. Privacy policy | Terms
© Copyright The Financial Times Ltd 2010.