

## **Preventing Fraud Through Improved Access Management** ***Idan Shoham, M-Tech - 19 Feb 2008***

The recent debacle at Societe Generale highlights how a breakdown in internal controls can trigger massive losses in financial institutions, and presumably other types of organizations.

While public disclosure of exactly what happened at Societe Generale is understandably limited, it appears that one trader was able to execute a series of massive transactions and hide them by turning off or manipulating surveillance systems, which would otherwise have flagged the transactions for further review. There is speculation that the trader was able to do this by combining previous knowledge of the surveillance applications with passwords borrowed from coworkers.

So what can we all learn from Societe Generale's painful experience?

Clearly there are organizational lessons such as issues related to separation of duties, staff training and so forth – but we'll leave those for another day (not least, because this author is a technologist, not an HR expert!).

Secondly, there are several obvious technological lessons to pay close attention to. Had certain solutions been deployed at Societe Generale, this devastating trading incident would probably have been prevented.

Here are three things that organizations should do to protect themselves against this kind of problem:

\* Policies:

Organizations should identify toxic combinations of privileges that should never be assigned to a single user. Automation can be used to monitor actual user privileges and raise an alarm if a single user is inadvertently assigned such a combination.

\* Periodic audits / privilege recertification:

As employees change jobs, their IT access requirements constantly change. Users ask IT to "fix the problem" when they cannot access needed applications, and as a result users collect privileges "like lint."

Periodic reviews of user privileges by managers and application owners enable organizations to spot excessive or obsolete rights and ask that they be removed. This sort of review can identify problems that automated policies never do, because it is just too hard to define an exhaustive set of policies.

\* Change passwords:

It sounds simple, but if every user's passwords change regularly, then it's just too hard to share passwords. Most passwords should expire every three months or so, but passwords to sensitive applications should expire monthly, at the very least.

Unfortunately, changing passwords too often negatively impacts users, who have trouble remembering them, and might respond by writing them down (bad!). Automation can help here too: password synchronization can reduce the number of passwords that users must remember simultaneously and single sign-on can make it possible to change passwords very often (e.g., daily) while eliminating the need for users to remember and type them manually.

So how would these measures have helped Societe Generale, and more importantly - how can they help your organization? If internal controls were bypassed by sharing passwords, then regular password changes would have made this more difficult. If internal controls were violated by a trader having too many privileges at the same time, then either policies regarding segregation of duties or periodic reviews would have caught this toxic combination and alerted IT to correct it. In any case, the trader in question would not have been empowered to bypass controls.

All of this is a bit abstract, so let's map it to identity and access management products that your organization can purchase and deploy:

- \* Policy enforcement is the job of a user provisioning system.  
Example: ID-Synch from M-Tech.
- \* Periodic audits are the job of an "audit compliance" product.  
Example: ID-Certify from M-Tech.
- \* Password synchronization is the job of a password management product.  
Example: P-Synch from M-Tech.
- \* Periodically randomizing sensitive passwords can be handled by a privileged password management product.  
Example: ID-Archive from M-Tech.