

## COMPUTER SECURITY FOR BANKING AND FINANCIAL DATA

# Legal governance versus internal security

Cases of lost data or excessive rights affecting business transactions are increasingly more numerous, with consequent damage for the affected companies. Effective measures exist but they are not implemented, either by ignorance or due to underestimation of the risks.

*Didier ASSANDRI\**

Recent affairs have drawn the public's attention to the consequences of data loss, and people have realized that lots of information can now be copied or moved thousands of kilometres away within seconds. But we should not forget that back in 2008, the KfW Bankengruppe in Germany transferred €300 million to Lehman Brothers the same day it declared insolvency; the bank argued at that time it was an accidental transfer, but one could argue that financial transactions are a fundamental element of banking. In another recent case, the Société Générale lost €4.9 billion on uncontrolled trading activities.

These affairs are interesting because they force us to be concerned with safety of information and data protection. Indeed companies are often ignorant of the dangers they incur, or in the best case, inefficient against the potential risks. Unfortunately one often needs a consequent disaster, which can reach amazing sums without counting the damage to the company's image, to set up adequate solutions.

But first of all, what are the reasons for these data leakages, which cause so much damage? From the known cases, one can draw the following conclusions: the major part of data losses are due to careless employees or happen by accident; for many leaders, board members and managers, electronical data processing remains an impenetrable and unknown world; the monitoring and control of IT staff is a major element of the risk management; the monitoring and control of Business Processes



*Didier ASSANDRI, Managing Director, SOLVIS Ltd.*

requires continuous attention; the quantity of data which can now be stored on portable media, (PDA included), is such that companies have difficulty controlling their data flow.

At the same time, banks and financial companies are so focused on following the letter of the law in order to pass audits (either internal or external), that they lose sense of the original intent of the regulation. They are compliant but data security is still weak, due either to ignorance or resignation.

### **Separate the legislature from the executive**

There is one step, however, which is valid for either internal or legal compliance: the segregation of duties. This could be com-

pared to the separation between the legislature and the executive in politics. An administrator should not be able to give access to whomever he wants, and at the same time a trader should not initiate a transaction and being able to authorize it by himself. But besides the human factor that people normally do not like to be controlled, the main difficulty remains to reconcile business and IT: to make financial transactions, banking secrecy, discretion and business agility rhyme with active directory, groups, forests and user permissions.

There is no magic here; we have two different worlds that need to communicate and this might well turn out to be an opportunity for RBAC solutions. What is RBAC? Role Based Access Control, sometimes spelled ABAC for Attribute Based Access Control, is a technology which speaks business language in the User Interface (UI), and which is able to deploy all the necessary information to the technical systems for authorization of access. The most sophisticated systems are able to display in real-time who has access to what, either for data access or business transaction authorization. Such a system can even be proactive by automatically blocking all transactions when it detects an anomaly between the current status and the desired status of rights and accesses.

### **Why is RBAC essential for banks and financial institutes?**

RBAC, or whatever name this technology will have in the future, is essential because it bridges the gap between legal governance, what is needed to be compliant with regulations, and internal governance, where business, ethical and security rules are defined. With RBAC companies will not only

be compliant, but they are then able to verify this anytime by accessing reports which reflect the current situation. It also removes the complexity of IT access rights for the business, leaving a clear picture which should reflect the desired state. I want to illustrate this with two pictures. In the first figure, you have a representation of access rights for a given department. It does not matter what “A, B and so on” are; assume these are the rights to certain activities. As you can see, it is quite difficult to find out exactly who has access to what.

Now, the next picture represents the same organisation where the access and permissions rights have been consolidated with an RBAC approach. As you can see, the picture looks quite different. It is now obvious that any member of the “Accounts Payable” group will have access or rights to D, E, F and G; those members where the title is “Accounts Payable Clerk” will have access to A and those where the title is “Sr. Accounts Payable Clerk” will have access to B and H. The three employees which show additional rights have then either supplementary rights to their current function or ... it is a mistake, in which case a corrective action needs to take place. Now rename A, B, C, D and the like with Ledger accesses, Clearing authorisation, Marketing or HR files and the picture becomes even more complete.

More important, the corrective action can be taken directly by the Manager of the Accounts Payable group. He doesn't need IT to do the changes. He has full control over persons having access to his area of responsibilities. He is compliant and access to his department's data is under control.

### Why is RBAC not commonly used?

RBAC, as such, is relatively new and has greatly improved over the years. Some auditors already make use of some functionalities of such a solution to perform their controls but they take it back with them after the audit. Banks and financials institutes could greatly improve their data security by implementing a fully-fledged RBAC solution and using it on a daily basis, but such projects require 3 major conditions to succeed: First, management attention: if the board itself doesn't push for such a protection, little will happen. It is the board's responsibility to ensure that the intellectual

Figure 1 - A typical company access rights landscape

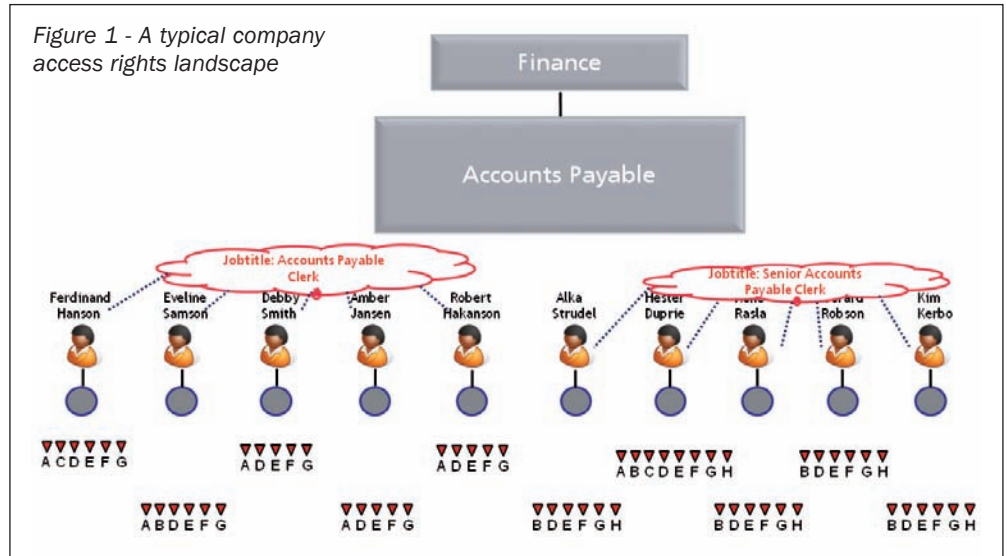
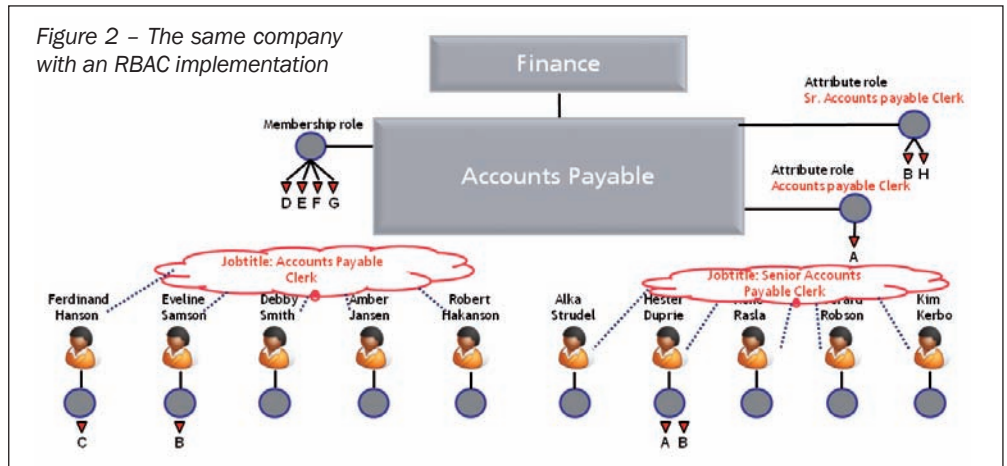


Figure 2 - The same company with an RBAC implementation



property of a company is protected, in order to ensure the sustainability of the activities, but how many board members have a technical background? Second, make sure the business managers sit at the same table as the technicians. You cannot offer a business solution which has only been thought through by technicians. In the best case, it will not be used; in the worst case it will endanger the business. Third, you need a project manager who really understands what RBAC is and how it works: sometimes it is even better to use the services of a person external to the organisation, even if the rest of the project is done internally. This person will tend to be neutral to all parties and prevent the pitfalls of such a project driven by just one person's experience.

Finally leaders and managers should remember that governance has to be a means to increase data security within a company, but it should not define the whole

of the enterprise security, because often governance recommendations are only the minimum standards and some industries require higher level of protection; banks and financial institutes belong to this category.

This level of protection has become even more critical now, since the risk of criminal indictment from any bank employees willingly breaching bank secrecy laws is largely compensated by the financial incentives and the protection offered by some sovereign nations in exchange of sensitive client information.

Opportunity makes the thief, and if these opportunities are made more difficult by establishing effective structural solutions, the bank and financial institutes will have completed the duty of due diligence they have towards their customers. ■

D.A.

\*Managing Director, SOLVIS Ltd.