Zero Tolerance for Sensitive Client Data

Private Banking and security in the cloud

For wealth management and private banking companies, data security and privacy have always been a top priority. Some senior managers may remember the days when client data was locked up in a standalone database with no connection to any other system in the bank. Those days are over. With rising IT and operations cost, tougher regulations, and ever more demanding clients, banks are under pressure to adopt new operations models and new technologies.

Enter cloud computing: while the majority of wealth management and private banking companies are still hesitant, some have started to think about using cloud computing and hosting data outside their data centers. Not too long ago, according to a senior banker, such considerations would have been vehemently rejected due to security concerns. What has changed?

Firstly, there is a political and social trend towards more transparency. Government and financial-market authorities demand that banks become more transparent. Banks have to disclose detailed client data and client financial data. If they don't comply, they face hefty fines and are accused of unethical behavior. The pressure to disclose client data may well influence the banks' attitude towards data security and confidentiality.

Secondly, advocates of cloud computing claim that, from a security and privacy point of view, there is no difference between outsourcing and using the cloud. They stress that banks have practiced outsourcing for years, with offshore companies all over the world having access to the banks' client data. For them it is evident that banks have accepted the potential security risks that are inherent in this kind of working model.

And finally, as the technology matures, providers and users are getting more experienced with different cloud environments and with managing cloud security. Cloud providers are enhancing their security infrastructure, trying hard to keep pace with the ever more sophisticated techniques of hackers and cyber criminals. These efforts strengthen the trust of banks in cloud environments.

Given this growing confidence in cloud computing, private banking companies need to think about new strategies for data security and privacy. They will not be able to adopt cloud computing pervasively anytime soon; strong regulations as well as unresolved legal and regulatory issues will prevent that. But they should start working on solutions that use cloud technology without compromising data security and privacy.

The silver bullet is to adopt a zero-tolerance solution for sensitive client data. Don't let any sensitive client data leave your premises. This approach segregates sensitive from non-sensitive client data, and keeps the former in a locally controlled area. Sensitive client data typically include client-identifying data such as name, address, relationships, and affiliation. Non-sensitive client data comprise cash and security positions,

instructions, orders and trades. A code acts as a kind of gate keeper to the sensitive client data. It is this code only that is known outside the locally controlled area.

The rationale for the approach is that the majority of processes in a bank do not need sensitive client data. Portfolio management systems, for example, verify asset allocations, evaluate, simulate, and rebalance portfolios, and can generate orders without needing to know the client who owns the portfolio. Client-identifying data are only required at the touch points with the client. These touch points include e-banking, client relationship management and financial advisory, client contact and communication logs, and client reporting. All processes to and from these touch points need the specific code to interact with the client-identifying data. Large banks have been using this segregation approach for processes that cross divisional boundaries such as trade execution.

When fully implemented, this approach would allow banks to move non-sensitive data to a hybrid, or eventually a public cloud environment without compromising clients or business units. Concern for data breaches would rest with the client-identifying data that is locally controlled, while the rest of the data may literally be anywhere, anytime.

Conclusion

Cloud computing is on the rise for banks including wealth management and private banking companies. Like companies from other industries, they are turning to the cloud for more flexible, more agile, and less costly IT and operations models. For security and privacy-conscious companies, however, the cloud, and in particular the public cloud, is a risky place. Even if providers continue to invest in best-of-breed security tools, they will not be able to prevent data theft and cyber attacks. Stricter security measures may even backfire as they slow down performance and slacken business processes, thereby tempting people to bend the rules.

If the banks cannot fully protect the data once they have left their premises, the best strategy is to reduce the amount of sensitive data in the cloud. A feasible approach is to segregate sensitive from non-sensitive client data, letting the latter take advantage of new technologies and operations models but keeping the former safe in a local environment. The effort to implement this approach across all front-to-back processes is substantial, but the resulting segregation would optimally prepare a bank for cloud adoption.