

P E R S P E C T I V E

Information Rights Management
Solution: Securing Information Exchange
in Outsourcing Arrangements



YOUR INNOVATION PARTNER

The data leakage menace

Data theft perpetrated by a Bank of America employee about a year ago is making news these days, with the Bank only now informing customers whose accounts may have been compromised. The errant employee leaked customers' data including their name, address, Social Security number, bank account details, and account balances to a gang of fraudsters, who used the information to steal from hundreds of accounts. This is one more entry in a long list of similar incidents that have occurred at different banks all over the world to dent the confidence of customers.

That's not all. Leaked data is powerful ammunition for competitors, as it gives them information about their rivals' satisfied and dissatisfied customers, and brings untapped opportunities to light. Hence, financial services firms, which are in possession of a wealth of sensitive customer data, make prime targets for fraudsters.

To support their growing business, banks and financial institutions have progressively extended their own networks within the home country and overseas. Along with scale, banks' vulnerability to data theft has grown, made worse by their practice of outsourcing several activities, from call center to form filling to bulk printing to third party vendors in order to balance the workload and save money on routine account maintenance activities, which were becoming increasingly expensive to support in-house.

Although outsourcing has decreased operating expenses and improved bottom-lines, the incidence of data leakage at the vendors' end has badly dented customer confidence. This negative sentiment is amplified by widespread media coverage of financial irregularities perpetrated through the misuse of leaked data.

A study of data breach in the United States over the past several years reveals that external agents masterminded most incidents, followed by insiders. Interestingly, misuse of privilege data topped the list of threats.

Protective measures taken by banks

Over the years, financial institutions have taken several measures to secure the data that is

exchanged with their outsourcing vendors. Yet, sensitive financial information does make its way to the black market, with potentially disastrous consequences – competitors can gain access to trade secrets, customers might be defrauded and sue the bank in turn, and banks' reputations might be irreparably damaged.

Naturally, bank Chief Information Security Officers (CISO), vendors and customers are concerned about the risk of data leakage inherent in outsourcing arrangements. This is how banks and vendors have responded to the above challenge so far.

Strengthening physical security: Data centers are provided 'fortress-style' security, with extensive checks on the movement of personnel and material at entry and exit points.

Protecting documents: Typically, when banks outsource bulk printing of statements/ demand drafts, scanning of cheques, creation of marketing collateral or similar activities, they send the password protected data files to the vendor on digital media. The vendor organization's authorized employees, who have been given the password, open the files and process them as required. The risks are obvious – assuming that the package is not pilfered in transit, once the documents are opened at the vendor's end, they are laid bare to unscrupulous employees, who can steal the information and pass it onward.

Building private networks: Some institutions have circumvented these issues by building private secure networks to transmit data files to their vendors. While this takes care of the 'lost in transit' problem, it does not protect open files from being misused. Therefore, banks have started to add a second layer of security in the form of data encryption. While these safeguards are superior to mere password protection, they come at a hefty price, one that not all institutions are willing or able to pay.

IRM: A new solution to an old problem

Since quite a while, data security technology vendors have been working on a new offering in the form of an "Information Rights Management (IRM) Solution." As its name suggests, this solution enables financial institutions to control the rights to digital information that leaves their

organization for further processing. Thus, a bank (or creator of a file) can specify who may read, edit or print a file, on which machines it may be accessed, how many times it may be used, or how long it must last before à la “Mission Impossible”, it self-destructs.

The special thing about an IRM solution is that it can make two systems located in two totally disparate environments talk to each other in such a way that a level of security and trust is maintained between the two. Herein, the systems within the bank and the vendor organization are bonded with a security policy such that the files generated by the bank’s source system may only be used on the vendor’s destination system and that too as stipulated. The encrypted files exchanged between the two systems contain a complementary policy, which decides other attributes like digital fingerprints, accessibility, validity etc. Once the files’ validity runs out, they can either self-destruct or exist as encrypted information impervious to misuse.

Another advantage of the IRM solution is that it maintains detailed records of activity related to protected files over their entire life cycle, which is very useful during audit.

The IRM solution provides the same degree of security as a private network at a fraction of the cost. In addition, it provides a greater degree of control to the originator of the information (files).

That being said, the scope of IRM also extends to the exchange of documents between financial institutions and customers or financial institutions and other agencies such as research and analyst firms. Banks need to protect documents sent to customers because data leakage could have serious consequences including the violation of customer privacy. Documents exchanged with analysts usually contain rich corporate and financial information, that is neither available freely nor free of cost, and hence must be safeguarded.

Today, these exchanges are protected at the document level, either with a password or a hardware dongle that must be inserted into the computer where the document is to be opened. The former method is vulnerable to hacking as

well as inconvenient for users, whereas the latter is expensive.

An IRM solution can circumvent all these limitations. When installed in the destination computer system, it embeds certain software in it, so that the user can open a password-protected document straightaway. A point to note is that this document can neither be opened on any other device, nor by anyone other than the intended recipient. If multiple banks were to accept the IRM solution, it would enable the user to open protected documents sent by each.

By deploying this solution, banks can reap several benefits. For one, they can safeguard data that is exchanged outside their security perimeter. Two, they can save the cost of setting up expensive private networks or providing security hardware for individual computers. Last but not least, they can restore customer confidence.

IRM challenges and opportunities

- Currently, IRM solutions are limited to servers and computer systems. Going forward, they must be rendered capable of protecting documents stored on portable devices, on the Internet and in the cloud.
- In a win-win arrangement, IRM solution and core banking technology vendors can integrate their solutions together to offer a readymade protection facility to documents generated on standard banking platforms.
- Similarly, IRM solutions can be integrated with document management systems, which are extensively used these days.

Industry response

Sensing a winning proposition, several vendors have started to explore the IRM space, to join the likes of Microsoft, Liquid Machines, Oracle and Seclere Technologies.

The financial services industry, however, has been slow to adopt; and only a few institutions have piloted a solution. Awareness of IRM technology is mostly restricted to CISOs, who

are convinced of its merits. Their viewpoint is yet to take root within the larger banking organization, where questions about regarding the wisdom of investing in technology to support activities as 'trivial' as printing. They only need to consider that the outsourcing vendor of a global banking major paid over 4 times the cost of an IRM solution in punitive damages when their data defenses were breached.

What could be a greater argument in favor of IRM adoption?

Reference:

2010 Data Breach Investigations Report, Verizon in Co-operation with United States Secret Service, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Author

Arindam Ray

Principal Consultant –
Finacle Solution Architecture and Design
Infosys Limited



YOUR INNOVATION PARTNER

PERSPECTIVE

Universal Banking Solution | System Integration | Consulting | Business Process Outsourcing

Infosys Limited

Plot No. 44, Electronics City, Hosur Road, Bangalore - 560100. India
Tel.: + 91 80 28520261, Fax: + 91 80 28521747, e-mail: finacleweb@infosys.com
www.infosys.com/finacle

Join us on Twitter, LinkedIn and Finacle Whiteboard at www.infosys.com/finacle/networking.asp

*COPYRIGHT NOTICE: Copyright ©2011 Infosys Limited, Bangalore, India. ALL RIGHTS RESERVED.
Finacle logo is a registered trademark of Infosys and Infosys acknowledges the proprietary rights of the trademarks and product names of other companies mentioned in this document. Infosys believes the information in this publication is accurate as of its publication date; such information is subject to change without notice.