

Banks and data leak prevention

Contacts:

Bob Tarzey
Quocirca Ltd
Tel +44 1753 855794
bob.tarzey@quocirca.com

Clive Longbottom
Quocirca Ltd
Tel +44 118 948 3360
clive.longbottom@quocirca.com

Banks are an obvious target for data thieves—how can they be stopped?

The financial services industry deals with a commodity that is primarily electronic—money. Consequently it spends more per employee on IT than any other industry. Despite this, there is a worrying tendency for information that should be confidential to end up in the public domain. Why is this and what can be done?

BRIEFING NOTE:

This briefing has been written by Quocirca to address issues faced by financial services organisations with regard to data loss.

The report draws on Quocirca's knowledge of the technology and business issues faced by banks and other financial services companies and provides advice on the approaches that can be taken to prevent data leakage.

During the preparation of this report, Quocirca has spoken to a number of end users, service providers and vendors and is grateful for their time and insights.

Quocirca would like to thank Symantec for its sponsorship of this report.

- **The financial consequences of data theft for banks are direct and indirect**
When a customer's money is stolen electronically, the onus is on the bank to compensate. The bank can also face fines if the loss is caused by careless data management on its part and publicity can lead to brand damage.
- **Banks have to share data and it is often not a bank itself that is responsible for data leaks**
Consumers get caught unawares by email scams, businesses are careless with customer information and public sector bodies, with which banks are obliged to share information, have proved to be reckless in the way they handle data.
- **Banks need to review their IT infrastructure**
Ultimately, for thieves to achieve their goals they need access to financial services and products that the banks have ultimate control over. Strict management and auditing of all IT assets is essential.
- **The software development process needs rigorous quality control**
Examples are on record of backdoors being built into banking systems by rogue developers. Testing and auditing must be exhaustive and carried out using dummy, not real, customer data.
- **Processes need to be well defined and audited**
The way in which data and transactions are handled internally needs to be governed by strong processes. Those responsible for weak processes or those who ignore strong ones must face the consequences.
- **Education and awareness needs to be driven by banks**
Banks need to keep up awareness campaigns for consumers and encourage best practice amongst their business customers to prevent data leakage.
- **The level of potential risk is not going to decrease**
New financial products, such as e-wallets and the continuing growth of internet shopping and other online services, will mean more and more opportunity for would-be thieves. In order for this growth to continue, people need to have more confidence in the way their financial data is being managed.

Financial services, IT and data security

Financial services organisations (including banks, insurance companies, building societies and so on, but referred to from here on as just ‘banks’) spend more on information technology (IT) per employee than those in any other industry. Some



estimates suggest it is more than double that spent in the utility, telecoms and public sectors.

There are a number of reasons for this, but the most obvious is that banks deal with a commodity that is primarily information—money, represented electronically. Every bank employee is an IT worker and every customer has to interact with banks electronically at some level—be it a consumer withdrawing cash from an ATM or a business managing a new share issue; in banks the use of IT is pervasive. Retaining existing and attracting new customers requires a high level of confidence in the security of a bank’s operations and this must include IT.

With all this electronic interaction comes risk. Most thieves are after one thing—money—and targeting banks is obvious because there is no intermediate commodity to be sold to get their hands on it. Why go to the effort of stealing alloy wheels off a car and selling them to raise money when, with someone’s credit card details, a thief can start spending straight away? Why set up a drug smuggling network when, by using a botnet and well crafted phishing emails, people will just send you the details to access their bank account of their own free will?

What’s more, whilst many industries can keep their interaction with customers and partners to a reasonably small number of trusted entities, banks cannot. The very nature of the services they provide means the widespread sharing of confidential data. When a retailer loses a set of credit card transactions, it is the bank’s money that is at immediate risk, not the retailer’s goods. When the banking details of citizens are lost by tax collection agencies, again it is the bank’s money not the government’s that is at risk.

Worst still, sometimes such details are being passed from one organisation to another without the bank even being involved, such as the high profile case in November 2007 where the UK’s tax collection agency (HMRC) lost the details for paying child benefit to millions of UK families in an internal data transfer on a disk. The data was not encrypted, the only security being a password

which a persistent hacker could probably work around.

The obvious downside for banks is money lost through theft, but it goes beyond this. There is compensation to be paid to customers who may become victims through no fault of their own and fines may be incurred for regulatory breach. Then there are indirect costs—such exposure can cause customers to desert and share prices to drop, leading to further financial loss and brand damage: a real worry, especially for a trusted high street bank. Customers may lose confidence in transacting electronically and revert to more costly to-service branch visits. Furthermore, data security breaches are likely to become even harder to cover up as disclosure laws tighten across Europe.

Infrastructure, processes and awareness

The financial services industry provides the oil that makes the global economy work, yet however much it spends on IT, the exposure to risk is always going to be there because of the open interaction with customers that is required and the easy pickings this can provide for thieves. However, it is not all gloom; there is plenty that can be done.

There are three areas for action—infrastructure, processes and awareness. The last of these must include educating the bank’s employees alongside customer awareness campaigns.



Within the bank, there is a reasonable amount of control in all three areas. On the inside, many banks are rationalising their data centres, consolidating their server and storage assets to improve utilisation and make security easier to manage. Better asset management leads to better auditing and an enhanced capability to respond to regulatory requirements. Outside of the data centre, greater control can be exercised over end-users through the use of end point security software on PCs and mobile devices. The imperative for doing this should not be in doubt—in February 2007 a laptop PC with 11 million customer records on it, entrusted to an employee of the Nationwide Building Society, was stolen from their home; Nationwide was fined £980,000.

Banks can implement internal processes and be strict about ensuring they are followed. Rules can be applied to sensitive content—not allowing it to be printed, copied or sent as attachments to emails. On the people side, banks are free to put

their own employees through intensive education and penalise those who ignore security advice or fail to follow well-defined procedures. However, it is after data has left the relatively secure environs of the bank's own infrastructure that some of the worst leakages occur. The problem includes both consumer and business users.

Getting consumers on side

Consumers are more likely to be on the same side as banks. After all, it is in their own interests to protect their own data, but many consumers are still easily duped and end up giving away enough personal details to provide thieves with direct access to their bank accounts. This includes both web- and email-based scams and the variety of techniques used, and communication channels exploited, is continually growing. Banks constantly remind consumers about the dangers but even the most savvy may be taken in by an innovative new threat.

Brand protection vendor, MarkMonitor (a Symantec partner), reports that UK banks lost £33.5M in 2006 through phishing alone, although it believes figures will be down for 2007 as banks make better use of technology and processes to avoid attacks.

For direct access to their own accounts most banks are now turning to strong authentication requiring consumers to identify themselves with more than just a password. There are a range of techniques—some requiring physical devices such as USB tokens and some based on multiple levels of soft authentication. Examples are 'Verified by Visa' or new schemes like the one being piloted by the credit reference agency Experian, based on Microsoft CardSpace. Such techniques certainly improve matters, but nothing is foolproof and strong authentication alone does not reduce the need for improvements elsewhere.

The bigger problem—business users

Business users are a bigger problem for a number of reasons. First, those handling sensitive financial data do not have the same level of personal interest in protecting data as consumers. Second, whilst an individual giving away their own details puts just one set of accounts at risk, cases involving data leakage by organisations usually involve the details of many customers, perhaps thousands or millions. Thirdly, whilst banks can impose processes and education on their own staff, such processes will often be more lax in other organisations, especially in the public sector (to which many banks are required to provide wide ranging information).

Banks can issue all the advice they like but, even though the actual situation will vary a lot, it must be assumed that the infrastructure, processes and employee practices will be of a lower standard in the organisations they have to deal with. One of the biggest problems arises when banks are required to send data off-site, especially to public sector organisations.



Where there is no choice, encryption of data is paramount, and when data is just required for statistical purposes it can often be anonymised. All too often, data is being transferred on disks when sending it electronically is a more secure option—network transmissions cannot be lost in the post and data is less likely to end up in the wrong hands. There must be processes in place for authorising such movements and making sure they are secure. It is not enough to blame a junior employee for losses incurred in this way; accountability must be upwards. Where practical, the use of web-enabled applications is far better; data need never actually "leave" the data centre but is just viewed as required in a web browser (most online banking works in this way).

Data leakage—recent issues

Unfortunately such lapses still seem to be fairly routine. In June 2007 a disk with 62,000 customer records was lost by HBOS en-route to a credit reference agency and the data was not encrypted. In November 2007 a disk was lost being transferred from the UK's HMRC to Standard Life Bank; HMRC refused to say if the data was encrypted or not "for security reasons". In both cases the problem seems to have been loss rather than theft but the reputations of the banks and the agencies were badly damaged, and the disks are still at large and therefore the customers' data is still at risk.

Another less obvious area of data leakage is when organisations are developing applications that handle financial data. Deployed applications may be very secure having undergone extensive testing by development and quality assurance teams but software development projects often involve contractors or may be outsourced entirely to a third party. Real data should never be used; most banks are more than happy to provide valid dummy data and they should make sure this is widely publicised to their customers. Beyond this, organisations need to be on the guard for rogue developers. A breach by TS Ameritrade, which it admitted to in May 2007 and had allowed the leakage of credit card details over a number of

years, was down to backdoor access created by a programmer.

When banks are communicating with customers they can still assert a level of control, limiting data that is sent to an essential minimum and insisting on secure processes for communication. However, there is still a big problem area externally, which is the greatest area of exposure for banks. Many external organisations accumulate financial data about their customers and handle it in ways that would horrify even the most lax of banks. The good news is that regulation is increasingly forcing better practice and punishing those who do not adhere.

The payment card industry

The payment card industry (PCI) has defined strict standards about how retailers and other organisations handle credit card customer and transaction information. These days it is possible to take credit card payments without storing any sensitive data—the payment card companies provide proxy servers for taking payments that meet PCI requirements. With valid credit card details changing hands for as little as a couple of Euros it is in the PCI's own interest to tighten things up as much as possible.



Data protection acts (DPA) require better handling of electronic data of all sorts and punish those that fail. Appalling examples of the way governments have been handling their citizens' financial information may prove harder to rein in, but the unwelcome publicity following such breaches and disciplinary action taken against some of the individuals responsible may improve practices. Bizarrely, the UK government faces prosecuting its own HMRC department for the breach of its own DPA in November 2007; although a government fining itself does not make sense—heads need to roll instead. HMRC has since admitted that the leakage was due to broad “systemic failure”; i.e. poor processes.

The risk from external organisations

Banks will always have only limited control over the practices of external organisations. If banks have done all they can to secure their own infrastructure and processes and ensure that the interactions they have with their consumer and business customers are as secure as can be, then,

when sensitive finance details end up in the wrong hands due to careless practices of third parties, the information leaked should become less and less useful to those that wish to exploit it.

The level of risk is not going to decrease any time soon. According to the Office for National Statistics, in the UK alone the value of business transacted online increased by 29% to £130 billion during 2006. New financial products will provide new areas for thieves to exploit. For example, experiments are underway with “electronic wallets” such as Barclaycard OnePulse, O2's Wallet (based on its mobile phones) and extensions to the use of Transport for London's Oyster Card scheme. Consumers want the convenience of such products and businesses want the benefit of the efficiencies but all need to be increasingly aware of the risks and how to avoid them.

Banks alone have the ultimate responsibility for who is able to authorise transactions of any sort. They can control access through better managed infrastructure and processes and ensure better awareness among employees and customers. Unfortunately, banks will always have to share the details of their account holders externally and there will continue to be breaches through the carelessness with which those details are handled. Only tight security and practices at the core can render such information useless to all but the rightful users.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information and interactions by delivering software and services that address risks to security, availability, compliance and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

About Quocirca

Quocirca is a perceptual research and analysis company with a focus on the European market for information technology and communications (ITC). Quocirca reports are freely available to everyone and may be requested via www.quocirca.com.