Conserving customer value: Improving data security measures in business

Received (in revised form): 2nd July, 2008

Adrian Gregory

is Managing Director of DQM Group, a data value management specialist providing solutions that monitor, protect and facilitate the databases of leading commercial data owners such as publishers, credit and marketing information companies.

Keywords security, fraud, identity, data, compliance, trace

Abstract British private and public sector organisations face an enormous security challenge in today's data-rich society. The causes of security breaches are varied and prevention has, until now, been largely unregulated. This paper looks at the security and accessibility of data sets, investigates where threats to security come from, what can be done to prevent security breaches and what can be done if a breach occurs. It also looks at industry regulation, compliance and the likely move towards compulsory notification of security breaches.

Journal of Database Marketing & Customer Strategy Management (2008) **15**, 233–238.

doi:10.1057/dbm.2008.20

IDENTITY FRAUD — THE BACKGROUND

ID theft has become a serious issue. One need only look at the figures: back in 2005, *Which?* reported that a quarter of UK adults claim at some time in the past to have had their identity stolen or know someone who has fallen victim to ID fraud; fraud prevention service Cifas has reported increasing cases of ID fraud since 1999 when 9,000 cases were identified, compared to 77,500 in 2007;¹ and a study by online identity management firm Garlik² estimated that ID thieves were defrauding more than 100,000 Britons a year, and predicted this would increase to 200,000 by 2010.

So why is ID fraud increasing so dramatically? According to Cifas, the police investigate less than 1 per cent of identity fraud cases, and figures from KPMG reveal that just 200 fraud cases came to court in 2007.³ Until recently there has been

insufficient deterrent to criminals in the UK, with sentences tending to be relatively light. Furthermore, it is difficult to recover the money taken by the fraudster or even to gain compensation from them. The implementation of The Fraud Act 2006, however, may herald change. The new legislation, which came into force in January 2007, is intended to cover a multitude of fraud situations and aims to make the investigation and prosecution of fraud in the UK easier.

Another factor is the rapid growth of online shopping. According to CardWatch, card-not-present (CNP) is the most popular form of identity fraud in the UK, while figures from APACS show a 74 per cent growth in CNP since 2003.⁴ The problem with this kind of fraud is that neither the card nor cardholder is present during a transaction, making it more difficult to verify identity. The online world in the

Adrian Gregory
DQM Group Limited
Tel: +44 (0)870 242 7788;
Fax: +44 (0)7798 705858;
URL: www.dqmgroupp.com

form of social networking sites is another area at risk to ID theft. Security company Sophos claims⁵ four in ten users freely divulge private data to strangers on Facebook and pundits claim members may be putting too many details about themselves online, which fraudsters could use to steal someone's identity.

ID fraud can occur for any number of reasons: physical theft of an individual's credit card, passport or such like; incorrect disposal of documents containing sensitive information; phishing, whereby a fraudster attempts to acquire usernames, passwords or credit card details, by posing as a trustworthy entity in an electronic communication; and hacking. But, thanks to recent high-profile cases splashed across the news, the method most prominent in the public eye at the moment is, perhaps, the occurrence of data losses or breaches among private or public sector organisations. A whole host of situations involving human interference might be to blame for this; from something as simple as an employee losing their work laptop to a more sinister stimulus such as an employee being blackmailed by criminal elements to obtain customer data. The recent shocking revelation that the personal details of 25 million recipients of child benefit had been lost by HMRC brought the issue to the fore. Indeed, this was not a one-off example of data security inadequacy and represents just the tip of the iceberg. Last year, to give just a few examples, 15,000 Standard Life customers were put at risk of fraud after a courier lost a computer disk containing personal information; Newcastle City Council admitted that personal data and payment card details of up to 54,000 local residents had been downloaded from an insecure server to an IP address outside the country, nine NHS trusts admitted to losing the personal details of more than 160,000 patients and Nationwide was fined nearly £1 million by the Financial Service Authority after a laptop containing

customer account details was stolen from an employee's home.

The consequent financial loss in the aftermath of ID fraud is astronomical. A 2007 Experian⁶ study claimed that, on average, each identity fraud in the first half of the year involved the loss of £680, while Cabinet Office figures⁷ from 2006 reveal that identity fraud cost the economy £1.5 billion in 2005. Corporate identity fraud is estimated to cost in excess of £50 million a year. These figures could be much higher given that undetected fraud is not recorded. Indeed, over £1 billion of fraud came to court in 2007 according to KPMG Forensic's Fraud Barometer — the highest value since 1995 and the second highest in the 20-year history of the Barometer.

TACKLING THE PROBLEM

Tackling the problem is no easy task. The government is planning the introduction of ID cards, which other countries have found to offer a more secure form of identification than many of those available today. Furthermore, the introduction of an ID card would likely involve a central ID database, which financial services companies could use to verify the status of an ID card. Cifas is lobbying for the release of death records, which would help alert lenders if they received an application for credit from someone who was recorded as deceased (Home Office figures suggest impersonation of the dead is growing at a rate of 60 per cent a year). On an individual level, more care needs to be taken when disposing of documents containing sensitive information. According to MEL Research,⁸ 18 million households regularly throw out sensitive financial documents without shredding. Leading UK organisations, including Royal Mail, Cifas, the FSA, City of London and Equifax, launched National Identity Fraud Prevention Week three years ago, a nationwide awareness campaign to

help protect individuals and their businesses from identity fraud.

The private sector is making huge investments in fraud prevention. Front-line staff are being trained to spot false identity documents. Thorough checks are made on applications for financial products — for example, proof of name and address, photo identity, electoral roll, payment history and fraud databases are all checked and verified.

Where data security breaches are concerned the issue is, perhaps most importantly, being addressed almost exclusively from the point of view of stopping data leaving the organisation through, or to, an unauthorised party. Firewalls and encryption routines help prevent illegal access to sensitive information. The problem with this approach — while absolutely necessary — is that such measures cannot protect against computer theft, loss/theft of data on physical media or loss/theft of physical records. Moreover, although escalation procedures once a breach has occurred can minimise the impact of identity fraud, it cannot help trace the fraudsters.

Organisations of every kind keep records on their clients and customers, which is vital for a whole array of business practices such as sales activity, marketing campaigns and customer service. Transactional processes such as billing, credit and finance requirements all involve maintaining detailed personal records. The need for more sophisticated methods of tracing fraudsters and data thieves has never been greater.

Most institutions have already put tight internal measures in place, but all too frequently these measures do not pay attention to the eventuality of a breach. Most companies would be appalled to find their customers were contacted inappropriately by rogue traders with, at worst, fraudulent intentions. Unfortunately, these breaches are all too often a result of human intervention. For larger list owners,

the consequent recovery of a client's marketing communications would typically run costs into hundreds of thousands of pounds or euros, not to mention the subsequent chaos for customers and employees alike.

Yet, as has already been mentioned, the security and accessibility of data sets is frequently viewed as a purely internal issue. If an organisation were to admit that it had experienced a breach of its data security, that might open it up to potential legal liability as well as exposure of its reputation. So most keep quiet if it happens. Even the requirement of the Data Protection Act 1998 to keep personal data secure has tended to be viewed as an entirely internal process.

One consequence of this inward focus has been a lack of clear ownership and specified processes to deal with data security. Often the issue is handled within IT departments rather than as a stand-alone function.

Abuse of this 'out of sight, out of mind' attitude has therefore been relatively easy. It is an uncomfortable fact that most breaches of data security are carried out by an organisation's own staff, including its director and senior managers. Research by KPMG Forensic found that the typical company fraudster is a trusted male executive who gets away with over 20 fraudulent acts over a period of up to five years or more.

Significant changes in the broader culture across commerce and the public sector — and especially among data subjects — mean that 'laissez faire' is no longer an acceptable attitude. Growing legal pressures, from industry-specific regulations to international laws, now mean that every organisation that has data needs to be sure it is holding on to it. Indeed, leading brands are becoming increasingly aware of the damage security breaches can do to their image. As a result, data security is moving from an IT discussion to the boardroom, not least

because the brand is often the most highly valued asset on the balance sheet.

TRACK AND TRACE

Data security can never be 100 per cent. We have established that somehow, somewhere, data will leak (or be stolen) from the tightest of security systems. Therefore, there is a significant need to widely implement measures for tracking and tracing identity thieves and fraudsters once a breach has occurred. There are various means of doing so, whether electronic or physical. However, all involve the use — in one way or another — of ‘seed names’. Seed names are agents or identities that appear to be real customers, but have in fact been inserted into the database to obtain a view of any unauthorised use of record.

These undercover agents then log and report all approaches received by mail, telephone or email. This can also then be compared with any parties known to have rented the list, and the terms of their licence, so that cases of abuse can be spotted and policed. This kind of tracking activity allows a company to be aware of any data abuse before customers have a chance to complain, thus potentially preventing any loss of reputation and damage to brand.

The whole direct marketing industry uses such ‘sleepers’ as standard practice to guard against unauthorised use of commercial mailing lists. Now corporations and government bodies are beginning to adopt the same approach in order to monitor data abuse. Even in the early stages of such techniques in the wider commercial and public sectors, there have been cases of pre-emptive discovery, where unauthorised data usage (in fact data theft) has been identified, which would have otherwise lain undiscovered.

Yell, the international FTSE 100 directories business, is one company whose customer database is a fundamental asset. Its

business data lie at the heart not just of its traditional printed products, such as its Yellow Pages directories, but also its rapidly developing online classified directory service Yell.com.

Yell invests in data tracking to spot any abuse of its intellectual property rights, and its directories and website clearly state that the Yell products and services should not be used for activities such as the compilation of databases, directories and lists or for telemarketing or direct mailing purposes. Any abuse of their data by third parties, including marketers, runs the risk of undermining the relationship they have with their advertisers and the trust they have in them and their products and services. So policing usage of data is absolutely critical.

Both data owners and corporate marketers have a vested interest in preserving the quality of lists. One important factor in the process is to ensure that lists and data are only used in strict accordance with their licensing terms, so that the receptiveness of people on those lists to marketing offers is preserved. By applying these unique identifiers they can be shown to relate to a specific data set, creating an audit trail and evidence of any data loss. This is necessary within corporations, because a customer record often exists in various places (marketing database, customer service records, transactional records, billing, etc) and it is critically important to be able to spot exactly *where* a leak has occurred. If all consumer-facing industries introduced compulsory seeding of their customer databases to allow for tracking of violations in the use of those data, consumer confidence in the protection of their personal data would be less of an issue.

An additional attraction of implementing such track and trace measures is that organisations are finding it inspires an overhaul of general data management and quality standards — in other words,

improved standards of compliance with data regulations. By compliance, a number of different things are meant. Do the data an organisation holds comply with relevant legislation, such as the Data Protection Act or the European Directive on Privacy and Electronic Communications? Have the data been 'fairly collected' and applied only to the purposes for which it was originally requested? There are a host of such literal compliances to think of. Secondly, are the data clean, accurate, up-to-date and comprehensive? Directing bills to the wrong address or sending direct mail to dead people will have implications in terms of both legal liability and brand damage. Thirdly, who is responsible for the data, its integrity and quality, and its management? Who do they report to? Where does that responsibility end up at board level? Because if something goes wrong, responsible parties need to escalate action to redeem the situation. Finally, and most importantly, are the data doing what they should? Can the right people get at it easily to perform their roles? Is it analysable to produce meaningful business insights? Is it integrated within key business processes?

This understanding of current data standards, and how they need to be improved to comply with current usage and security regulations, can affect the valuation of a firm, either for investors or for potential acquirers. This is the product of the last ten years' growing culture of CRM. Firms have recognised the importance of being able to identify, value and manage each individual customer. To do so requires the building up of individual data on each customer, often through loyalty schemes — the number of which has more than doubled in the last decade.⁹ The corollary of this is a concern on the part of potential acquiring companies to audit and understand that all those customer data are properly collected and otherwise compliant. If not, then acquiring companies

will not be prepared to pay premium price for acquisition targets.

Typically, when consultants are hired to investigate the risks and exposures to a company's database they check that it complies with the Data Protection Act, the European Directive on Privacy and Electronic Communications, The Direct Marketing Association Best Practice and Information Security Best Practice (based on ISO 27001 standards). The database might then be subjected to a data hygiene and quality assessment that analyses standards in terms of factors such as people and businesses that have moved location, people who have died, firms that have ceased trading, duplicate records, out-of-date or inaccurate records, incomplete records and market coverage.

The resulting analysis can then be transformed into actionable strategies to manage the company's databases for efficient and effective business value development in order to deliver substantial gains in the short, medium and longer term.

NOTIFICATION REQUIREMENTS

Finally, notification of data security breaches is likely to become a legal requirement. In the US, in 2002, California became the first state to pass a Notice of Security Breach law requiring any organisation that suffers a breach of its data security and the loss of personal data to disclose this fact and to offer assistance to the data subjects affected. A further 33 states have since implemented similar legislation.

Some European Union (EU) states have similar laws in place, though not currently the UK. However, the introduction of the E-Commerce Directive 2006 has created a new regulatory framework for electronic communications networks and services. The objective of this framework is to protect citizens and businesses within the EU when they are using e-commerce.

To meet the terms of the directive, the UK's Information Commissioner drew up new proposals affecting internet service providers and network operators. These require the notification, to the national regulator, of any security breaches involving the loss of personal data. The regulator must then decide whether it is in the public interest to inform the general public of the breach. Notification to the customer is also required where any breach of data security leads to the loss, modification or destruction of, or unauthorised access to, personal data.

While not yet implemented, these requirements are likely to come into force before 2010. They create a new climate of opinion and a legal background that is likely to lead to pressure for the same standards to be applied by all data owners, whether using electronic networks for data transmission or not.

CONCLUSION

UK public and private sector organisations are holding an increasing volume of data on customers and citizens. If such organisations are to continue to be allowed to use this information to improve customer service, they also have to take on the responsibility of keeping it safe and secure. The exposure

of 25 million personal records every year¹⁰ to potential theft and fraud is already unacceptable. In addition, individuals themselves must become more responsible about the way they keep and dispose of their personal records. For organisations to concentrate only on internal systems security is not enough. Equal attention needs to be given to ways of tracking and tracing abusers and fraudsters after a data breach has occurred, so that the perpetrators might more frequently be brought to justice. Only by removing the criminal element from the picture can the tidal wave of identity fraud be turned back.

References and Notes

- 1 CIFAS. (2008) 'Is identity theft serious?' www.cifas.org.uk/default.asp?edit_id=561-56.
- 2 Garlik. (2006) 'UK cybercrime report' www.garlic.com/cybercrime_report.php.
- 3 KMPG Forensic. *Fraud Barometer* — also all further KPMG Forensic references.
- 4 Sources: www.cardwatch.org.uk and www.apacs.org.uk.
- 5 Sophos (2007) 'Facebook members bare all on networks' 2 October. www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html.
- 6 Experian (2007) 'Victims of Fraud Dossier' Part III. www.experian.global-pressoffice.com/show_docs.cfm?dtype=IP.
- 7 Cabinet Office (2006) 'All party briefing — Identity fraud' London School of Economics, London.
- 8 MEL Research (2005) 'Bin raiding'.
- 9 GI Insight (2008) 'Loyalty leap'.
- 10 DQM Group (2006) 'Fraud fright'.