Data theft leads to PR nightmare

Organisations may have good internal security practices, but can they be so sure about third party processors? **Eugene Oscapella** finds that there can be serious implications when business partners suffer a lapse in security.

January can be brutally cold in Canada. But an information management company and some of its major customers in one of the country's coldest provinces – Saskatchewan – experienced chills for another reason. In mid-January, a hard drive containing personal information on up to one million Canadians disappeared from a secure area of the information management company, ISM Canada, a member of the IBM Global Services consulting group. The 30-gigabyte hard drive was not particularly valuable as a piece of computer equipment – perhaps worth only a few hundred dollars – but reports suggested that the personal records it contained could be an identity thief's dream.

CLIENTS FEEL THE FALLOUT

Among the data kept by ISM were insurance records for one of Canada's largest insurance companies – Co-operators Life Insurance. Records of 180,000 of its clients may have been contained on the hard drive. Several Saskatchewan government agencies also entrusted personal information about provincial residents to ISM. A Canadian mutual fund company, Investors Group, reported that the hard drive held account information for two-thirds of its one million clients.

Within days, Co-operators advised policyholders by letter that personal information about them may have been on the missing hard drive. Among the possible pieces of information were name, address, beneficiary (for pension clients), date of birth, social insurance number and pre-authorised chequing information (including bank account numbers) and employer's name. Although banking information was not connected with some names and addresses, a company spokesperson said it would not be impossible to put the two together.

The letter cautioned that identity theft might be possible with the loss of this information: "Given the potential serious consequences, we urge you to be vigilant and to review and verify all your bank accounts, credit cards and any other financial transactions and to be aware of the heightened possibility of other unauthorised use of your personal information."

A few days after the letter was released, and amidst claims that this amounted to Canada's greatest privacy disaster, the chief executive officer of Co-operators Life Insurance was seen apologising to the company's customers at a press conference broadcast on national television.

> The chief executive officer of Co-operators Life Insurance was seen apologising to the company's customers at a press conference broadcast on national television.

FIRMS FACE COSTLY LEGAL ACTION

To add to this corporate misery, a class-action lawsuit was launched in early February. The suit named ISM and several of its clients, including the Saskatchewan government and Co-operators. The suit claimed that the defendants violated customer privacy, were negligent in securing confidential information and notifying the public about the lost hard drive.

Within a few weeks, local police arrested the alleged culprit, a high-tech employee who may have merely wanted the hard drive to add storage space to his computer. However, police did not know whether the personal information from the hard drive had been passed on to anyone else.

MINIMISING THE RISKS

Data protection and security experts have suggested what might be done to prevent such losses of data. The consensus? It is hard to protect against dishonest employees (or contractors), although vigilance in selecting personnel is important. However, two security measures, used together, could help to frustrate would-be identity thieves. The first involves splitting a database – for example, keeping names on one database, and other personal information on another. The second involves encrypting the data. And finally, corporate security policies are a must, even if only because they force companies to contemplate the unthinkable.

Meanwhile, the scale of potential identity theft incidents continues to grow. Canada's *National Post* newspaper reported on February 19th that an unauthorised intruder gained access to a database belonging to a company that processes transactions for merchants. The intruder had access to Visa, MasterCard and American Express account numbers from clients in several countries. As many as eight million account numbers may have been compromised overall.

Dutch industry faces tougher privacy sanctions

The Dutch privacy authority has started to clamp down on breaches of the Personal Data Protection Act. But how do Dutch enterprises and privacy activists feel about this law, its implementation and enforcement? **Joe Figueiredo** reports.

The first group of over 200 Dutch organisations have received warning letters from the College Bescherming Persoonsgegevens (CBP), the Dutch Data Protection Authority, reminding them of their reporting obligations under the Wet Bescherming Persoonsgegevens (WBP), the Personal Data Protection Act, and warning non-compliant organisations of a possible fine of up to €4,500.

Notification requirements

The WBP, which became law on September 1st 2001 (replacing the Wet Persoonsregistraties (WPR), the Personal Data Registration Act) requires Dutch organisations to notify the CBP immediately of their intention to collect and process personal data. They have to provide the authority with information such as the reasons for collecting and processing personal data, and the type of data-security measures in place. Notification details are stored in a public register and made readily accessible through the CBP's website. When the WBP was enacted, organisations were given a year to resubmit notifications that were required under the old WPR, but had become obsolete under the new act.

Enforcing these notification procedures requires the CBP to identify violations. "By analysing past and present notification statistics, we can identify, with some certainty, particular groups of organisations not fulfilling their notification obligations," says Gert Onne van de Klashorst, CBP's public relations officer.

According to a CBP investigation into how the privacy act is working in practice, too many organisations are failing to comply with the notification rules. It reports serious violations among both the public and private sectors.

Unfair and unfriendly

VNO-NCW, the Confederation of Dutch Industry and Employers which represents 80 per cent of the Dutch business community, has raised objections to the warnings. "Our members, including some 15 trade associations, were apparently selected on the basis of some sort of statistical analysis, and not on individual proof of non-compliance. Besides, the number of notification exemptions under the WBP could also account for the decrease in the number of notifications," says Bart Rijgwart, VNO-NCW's adviser on information technology policy, including data-security and privacy issues. The number of notifications has in fact dropped from around 70,000 under the previous act, to around 25,000 under current legislation.

> Many organisations are failing to comply with the notification rules.

On the law itself, Rijgwart feels that its 'legalese' makes it too complex for smaller businesses (without legal expertise) to understand. Notification requirements are also too encompassing and increase administrative work. Rijgwart recommends restricting notification to cases where there is an identifiable and significant risk to privacy. Furthermore, the VNO-NCW cannot find any visible evidence from the way the WBP is implemented and regulated that notification procedures help protect data and privacy.

Maurice Wessling who heads Bits of Freedom, a Dutch privacy and citizens'-rights group, agrees on this last point, but for a different reason: "Citizens, indeed, have the right to know where and how their personal details are being used, and by whom. However, unless the CBP has the means to enforce the law more aggressively - current fines, for example, are not proportionate to the offence and would hardly impact a large business financially - the effectiveness and value of notification could be argued."

Nevertheless, the CBP, which seems bent on continuing with its crackdown on Dutch organisations that breach the privacy law, has scheduled further actions for later this year. "Although we are focusing on notification offences this year, we continue to look at material breaches of the law," says van de Klashorst of the CBP. "Part of our work is case-based, where we investigate complaints brought by individuals, but we are also proactively discussing privacy and other issues with organisations and have planned investigations."

And it looks like the CBP has its work cut out. "The fact that only a hundred privacy officers—most of them in the non-commercial sector—have been appointed in the two years since the WBP has been law, demonstrates the lack of seriousness and enthusiasm shown by Dutch organisations to this law," complains Maurice Wessling.

AUTHOR: Joe Figueiredo is a Netherlands-based business & technology writer specialising in information and communications technology (ICT), and new media. His details can be found at: www.fits.scarlet.nl.

European Parliament condemns airline data deal

The European Parliament has waded into the debate on transferring airline passengers' details to government authorities in the United States. **Eugene Oscapella** reports.

In a starkly worded resolution passed on March 12th – one containing several statements of "regret" (relatively strong language in the realm of diplomacy) - the European Parliament criticised both the European Commission and the US over an "agreement" on the transfer of airline passenger information to US authorities. The resolution was passed by an overwhelming majority – 414 in favour, 44 opposed.

Under the US Advanced Passenger Information System (APIS), airlines arriving in and departing from the US are required to transmit information about passengers and crew to a centralised database operated jointly by US Customs and the Immigration and Naturalisation Service (*PL&B Int*, Feb 2003 p.8-11).

However, at the Parliament's plenary session in Strasbourg on March 12th, Frits Bolkestein, head of the European Commission's Internal Market division, stressed that there was no agreement as such, but rather two documents – a joint statement in mid-February by senior Commission members and representatives from US Customs explaining the outcome of their talks, and a second document in early March from US Customs containing undertakings about the handling of sensitive data.

A Commission explanatory document ("FAQ") about the issue explains that, for airlines established in and operating flights from EU countries, the US Customs and Border Protection Bureau (CBP) gained access to the Passenger Name Record (PNR) data of transatlantic flights as of March 5th.

Bolkestein said: "There have been discussions; the US side have given certain assurances. This is the first step in a process. Both sides are committed to finding a more legally secure solution in due course."

Despite this explanation, the preamble to the European Parliament resolution argued that the US Administration has interpreted what it called the interim "agreement" so as to impose, under threat of severe penalties, direct access to computerised reservation systems and, in particular, to the PNR data. This, said the preamble, can be linked with personal information, including sensitive information as defined in Article 8 of the EU Data Protection Directive.

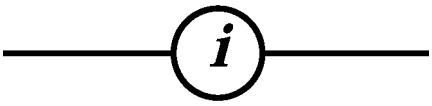
The preamble further noted the "doubts and concerns that have been expressed by the national authorities concerning the legitimacy of this demand, including its legitimacy under US law, and in particular about its compliance with EU data protection legislation." It mentioned the risk that reservation system databases may become *de facto* data-mining territory for the US Administration, noting that this could affect between 10 and 11 million transatlantic passengers each year.

> "This is the first step in a process. Both sides are committed to finding a more legally secure solution in due course."
>
> - **Frits Bolkestein, European Commission**

The strongly critical tone of the preamble continued apace in the main text of the resolution. The resolution "regretted" the Commission's failure to assume its responsibilities with the necessary diligence. Those failures, it said, included not verifying whether there is a real basis in US law to justify access to reservation systems data, delaying the assessment of US legislation under Article 25 of the Data Protection Directive (regarding transfers of data outside the EU), and omitting to provide information to the public "who should be the first to know what is being done with information about them."

The resolution noted in particular the dilemma that the current situation posed for airlines. Using an analogy uncharacteristic of formal resolutions, it spoke of airlines being caught "between a rock and a hard place." "If they follow Community law," said the resolution, "they are liable to US sanctions...If they give in to the US authorities' demands, they fall foul of the data protection authorities." The resolution noted that this also creates difficulties for the national data protection authorities, which are obliged to enforce the Community rules.

The resolution did not rest simply with criticising the Commission. It called for the Commission to remedy the situation by securing the suspension of the effects of the measures taken by the US authorities pending the adoption of a decision regarding the compatibility of those measures with Community directives. It further called on the Commission to examine the problems raised in the resolution and reserved the right to examine the action taken before the next EU-US summit. The resolution directed the President of the European Parliament to activate procedures with a view to determining whether an action may be brought before the European Court of Justice.



FURTHER READING: European Parliament resolution on data transfers by airlines to the US (B5-0187/2003): http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm#apis