# GMAC laptop theft highlights gaps in offsite security

GMAC Financial Services were at the centre of a serious privacy incident last month after compromising around 200,000 customer accounts. **Alan Pedersen** asks whether better security practices could have avoided embarrassment.

In March, an employee at GMAC, the credit lending arm of General Motors, had two laptops stolen from the locked boot of their car. According to *Information Week*, which broke the story, details on around 200,000 customers were stored on the laptops, containing a veritable treasure trove of information for ID fraudsters - names, addresses, dates of birth, social security numbers, and credit scores.

Stolen laptops are, of course, an inevitable risk for companies keen to promote flexibility and mobility in their workforce. Replacing stolen hardware is an inconvenience, but compromising the customer data stored on hard drives can have huge implications for a company's reputation - especially one that operates in the financial services sector. In GMAC's case, it appears there was a major failing in security. A spokesperson for the company told *Information Week* that although the laptops were password-protected, no encryption was used.

As a result, GMAC was forced into sending out letters to affected customers warning that their details may have been compromised and recommending they place a fraud alert on their credit files. The spokesperson said that the company would be reviewing its security policies and was now prohibiting employees from storing 'certain' information on laptops.

The fact that the laptops were only password-protected is somewhat surprising and bucks the trend among financial services companies, which traditionally tend to be more security-savvy than those in other sectors.

Experts agree that if you are taking valuable data outside the bricks and mortar safety of the office environment, you are going to need something a little stronger than a password. Protecting information on your laptop with a password is about as safe as, well, locking it in the boot of your car.

Replacing stolen hardware is an inconvenience, but compromising the customer data stored on hard drives can have huge implications for a company's reputation.

## Assessing the risk

Yag Kanani, partner in charge of information security services at Deloitte & Touche, said that remote security policies should be based around a risk assessment framework. "Companies need to look at what the risks are and what the business impact would be if that data fell into the wrong hands," he said.

For customer data stored remotely on laptops or PDAs, Kanani said encryption is the best practice approach, although the overheads involved can put companies off. "A lot of organisations instead tell their users not to store sensitive files on their laptops, rather than encrypting files." But the problem with this kind of policy, he explained, is that a lack of awareness or just straightforward refusal to follow the rules can create gaps in compliance. "Awareness is a big issue, I seldom see good awareness programmes within organisations," he explained. "Even if you do these things at an optimum standard, you still have to protect against a disaffected employee who might try to steal data."

## Encryption

Andrew Beard, advisory services director at PricewaterhouseCoopers, said that businesses are using different methods to encrypt customer data. "In many cases, organisations are taking the approach that everything is encrypted by default. There are other methods that allow you to create virtual drives and just encrypt the data on those drives." The latter option, he said, enables better performance for laptops, but there is a trade-off on security in that all data is not automatically encrypted. "The downside is obviously that as an organisation, you're passing control to your users and relying upon them to make that decision."

## Don't get complacent

All large organisations handling customer data will have security policies and procedures in place. But perhaps the GMAC incident serves as useful warning that companies should not be sitting back too comfortably. While compliance gaps can easily occur, the security breaches that may arise as a result are not so easy to clean up.

# ISPs win file-sharing privacy case

**Eugene Oscapella** reports on how Internet service providers (ISPs) are successfully playing the privacy card in an attempt to avoid disclosing the identities of customers engaged in online file-sharing of copyrighted music.

A March 31st decision of Canada's Federal Court has stressed privacy concerns in refusing to order several ISPs to disclose the identity of 29 customers who allegedly infringed copyright laws by illegally sharing music files online.

The plaintiffs, a coalition of major Canadian record labels, had wanted the names to enable them to sue individuals it claimed were frequent online music sharers. The record labels said they were unable to determine the name, address or telephone number of the Internet users, as the file sharing software they were using allowed them to operate under pseudonyms.

All of the parties to the motion agreed that ISP account holders have an expectation that their identity will be kept private and confidential. Customers' expectation of privacy was based on both the terms of their account agreements with the ISPs and with Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA). They also agreed that PIPEDA allows ISPs to disclose personal information without consent under a court order.

The Court rejected the application for an order to disclose for several reasons, among them that downloading a song for personal use does not amount to a copyright infringement under current Canadian law (in early April, the federal government announced its intention to draft an amendment to outlaw such downloading). However, the Court gave several justifications relating to data quality and processing for its refusal to grant the order:

- There was no evidence explaining how a pseudonym was linked to a given IP address. It would be irresponsible for the Court to order the disclosure of the name of the account holder of that IP address and expose this individual to a lawsuit by the plaintiffs.

- The information being sought was not routinely kept by the ISPs and would need to be specifically retrieved from their data banks.

Customers' expectation of privacy was based on both the terms of their account agreements with the ISPs and with Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA).

- Delays by the industry in seeking access to the information made it more difficult to retrieve and more unreliable; it might be impossible, due to the passage of time, to link some IP addresses to account holders.

- At best the ISPs will generate the name of the account holders, but they can never generate the name of the actual computer users.

Broader privacy concerns were also central to the Court's decision, but Federal Court Justice von Finckenstein acknowledged the limits to the protection offered by privacy legislation. It was "unquestionable but that the protection of privacy is of utmost importance to Canadian society...However while the law protects an individual's right to privacy, privacy cannot be used to protect a person from the application of either civil or criminal liability."

Justice von Finckenstein concluded that the plaintiffs had not made out a *prima facie* case (including a causal link between pseudonyms and IP addresses). Nor had they established that the ISPs are the only practical source for the identity of the pseudonyms or that the public interest for disclosure outweighs the privacy concerns in light of the age of the data.

The court concluded that under the circumstances, given the age of the data, its unreliability and the serious possibility of an innocent account holder being identified, privacy concerns outweighed the public interest concerns in favour of disclosure.

The decision was consistent with an admittedly unscientific online poll conducted in February by Toronto's *Globe and Mail* newspaper. Only 12 per cent of respondents thought that ISPs should be required to turn over to the music industry the names of ISP customers who swap songs.

Representatives of the Canadian music industry have now filed an appeal against the judgment.

The Canadian Federal Court's response, however, was not unique. In December 2003, a United States appeal court ruled that the recording industry could not rely on the subpoena provisions of the Digital Millennium Copyright Act to compel ISPs to disclose the names of subscribers whom it had reason to believe were infringing its members' copyrights.

FURTHER INFORMATION: For a copy of the ruling, see: www.fct-cf.gc.ca/bulletins/whatsnew/T-292-04.pdf