



## Data theft highlights user-privilege flaws

By: Kathleen Lau

ComputerWorld Canada (05 Jul 2007)

A recent data security breach of 2.3 million customer records from a U.S. financial processing company brought into question the seeming lack of control organizations have over so-called power users in the enterprise, IT security experts said.

Fidelity Information Services has reported a data breach through its Tampa, FL.-based subsidiary Certegy Check Services Inc. An investigation into the incident has revealed it was committed by a senior-level database administrator at Certegy, who likely stored data on a device and subsequently walked out the door with it.

Information included names, addresses, phone numbers, bank account and credit card information, which was then sold to a data broker, who in turn sold it to marketing firms.

Internal data theft is a "hot topic" in the IT industry not just because of legislation and privacy concerns, but from a governance standpoint as well, said Tom Slodichak, chief security officer at WhiteHat Inc., a Burlington, Ont.-based IT security provider.

Traditionally, he said, companies were primarily concerned with external threats like malware, but that focus has since shifted.

"Now, the flip side of the coin is a lot of attention is being paid to human policies and also technological controls that would prevent the removal of information," Slodichak said.

Another Canadian security expert hypothesized that "iPod slurping" could have been what enabled the database administrator to steal such massive amounts of Fidelity data.

A handheld iPod drive with the capacity to download up to 80 gigabytes of data can easily be connected to the USB port of a computer on a network, explained Eugene Ng, vice-president of technical services at NCI Secured Intelligence in Mississauga, Ont.

"It takes maybe 15 minutes to fill up 80 gigabytes; you stick it in your pocket and walk out the door," he said.

Most companies don't have good governance control over their database administrators because of the high-level privileges required to do their job, said Francis Ho, executive committee member of the Federation of Security Professionals.

"It's difficult to protect against that kind of attack because database administrators have access to everything in the database," Ho said.

Ho suggests companies can encrypt their database and increase access monitoring as a risk mitigation measure. This can, however, present some tradeoffs to work performance, he added.

Just earlier this year, authorities were investigating a possible customer data breach at the Canadian outlets of clothing retailer Club Monaco, which was alerted of the incident by a third-party payment processor, according to news reports.

It's not known to date whether the alleged breach was caused by an insider or by an external hacker.

Slodichak doesn't believe such crimes are due to lack of awareness as cybercrime reports have consistently

relayed that 70 per cent of security threats are internal – some malicious while others purely of human error. It's merely an issue of putting policies into practice, said Slodichak, who believes there were multiple opportunities to prevent the breach from happening.

"Although the probability of actually preventing one of these against a determined malicious individual is low," he said.

He suggests implementing the right technology to track suspicious behaviour.

"If someone is going to start stealing large amounts of personal data, then that implies there is some sort of technological conveyance, whether it's sent out as a spreadsheet via e-mail to a personal account, or on a memory stick," Slodichak said.

According to Ng, some companies are looking into ways to control the types of devices employees plug into their computers. One such measure is by using software that is centrally managed by the IT department and pushed out onto user desktops, giving IT better control of what gets into a user's machine.

Policies are then enforced alongside the technology, he said, some dictating only a mouse and keyboard may be plugged into a USB port. Very often, multimedia devices are banned.

Corporate-issued devices are often the solution, Ng added, especially given the increasing affordability of the hardware and ability to encrypt stored data to protect against theft or loss.

Besides educating users about handling privileged data, Slodichak, recommends also enforcing policies with disciplinary action.

According to Ho, Canadian businesses would be kept "more honest" if legislation were enacted, such as that in California requiring companies to report data breaches. It is, however, unlikely the same law will cross north of the border, he added.

"While these legislative and regulatory themes have helped the security industry, it's only going to get better over time," said Ho.

NCI's Ng believes that mandatory disclosure regulations are thrusting the issue of data breach to the forefront. "Years ago, if a breach happened, everything was brushed under the covers."

Copyright © 2007  
ITworldcanada.com