

The Complete Buyers' Guide for Identity Management

Keeping It Simple: Sun's Pragmatic Approach to Identity Management

Sun OpenSSO Enterprise for Access Management, Federation, and Secure Web Services – Webinar

Sun Open Source Identity Management Guide

COMPUTERWORLD Security

Print Article Close Window

Insider at Cal Water steals \$9M and runs

Money back but case highlights threat within

Jaikumar Vijayan

May 22, 2009 ([Computerworld](#)) On the night of April 27, hours after he had resigned from his job as an auditor at the California Water Services Company, Abdirahman Ismail Abdi used his still active electronic key card to get into the secured facilities where he used to work.

He then allegedly gained access to computers belonging to two senior executives in two separate buildings at the utility to initiate and confirm three wire transfers totaling more than \$9 million, to an account in Qatar.

Early the next day, he put his wife and children on a flight to Frankfurt, Germany, and then attempted to deposit a check made out to CWSC totaling more than \$25,000, which he had apparently stolen, into his bank account in the U.S.

On May 1, with federal authorities hot on his tail, Abdi canceled a reservation he had on a flight out of San Francisco to London, and then over the next few days somehow managed to flee to Canada where he remains at large. The money itself, however, has since been recovered.

The attempted theft, as described in court papers filed in the U.S. District Court for the Northern District of California, is the latest example to highlight why security analysts say insiders pose a bigger -- though often underestimated -- threat to corporate assets than external attackers.

Earlier this month, Wilbur Fondren, deputy director for the U.S. Pacific Command (PACOM) Washington Liaison Office was [charged with conspiracy](#) for selling classified government information to a Chinese agent.

Fondren is alleged to have gotten at least some of the information from a classified government computer using his top secret clearances and access.

Last August, Rene Rebollo, a former financial analyst at Countrywide Financial Corp., [used his access to corporate databases to steal personal information about customers](#) which he then sold to information brokers.

Most notoriously, last July, Terry Childs, a former network administrator for the City of San Francisco's [allegedly locked access to a critical FiberWAN city network for days](#) by resetting administrative passwords to its switches and routers, and then refusing to divulge the new passwords.

Security analysts have cautioned about insider risk for some time, but an increase in incidents highlights the continuing challenges companies face in dealing with the issue. A recent survey by SailPoint Technologies of 125 large companies found that eight out of 10 of the businesses were concerned about insider threats.

At the same time, about 57% of the respondents said they did not have the visibility they needed across their networks to prevent insiders from abusing their access. Less than two in 10 felt they had the controls needed to deal with insider threats.

BlackBerry® Professional Software

Get started now ▶

BlackBerry

The latest incident highlights some of those issues. The fact that Abdi was able to access his company's secure facility after he had resigned points to a lack of "leaver" or termination controls, said Brian Cleary, vice president of products at security vendor Aveksa Inc. Such controls require a full understanding of the access rights that a particular user has and on creating a process for removing that access across a multiple applications, he said.

It is also unusual for an auditor to have access to a funds transfer system in the manner that Abdi appears to have, Cleary said. According to the court documents, Abdi used two different password-protected computers, located in two separate buildings, to initiate and confirm the money transfers. It is unclear from the court documents whether Abdi stole the passwords to the computers or he had some kind of legitimate access to the systems.

However, a well-implemented access control system would have allowed the water company to grant access to applications based only on need, and it would have been able to monitor, track and log that usage, Cleary said. "The business risk from insider access that is inappropriate or misused is very real and can create serious operation impacts," Cleary said. "This problem is very pervasive within organizations as they don't have the visibility and control over user access."

One big challenge companies face with insider threats is achieving the right balance of controls, said John Pescatore, an analyst with Gartner Inc. "Any security approach that falsely blocks legitimate user action will quickly be turned off," he said.

"If insider actions are legitimate 99.9% of the time and some insider threat detection systems is 90% accurate then for every 10,000 user actions there will be 10 malicious activities but there will be 1,000 alarms," out of which 991 are false alarms, he said.

From a business perspective, such a security control "is often worse than the problem," Pescatore said.

Cal Water spokeswoman Shannon Dean said the utility couldn't discuss the case because of the ongoing investigation. But she said it is because the company had the appropriate financial controls in place that the fraud was detected and the wire transfers were intercepted before any funds were lost.