

## **New Data Loss Highlights Problems With Contractors and Laws**

John Girard, Avivah Litan

A troubling new California data security breach demonstrates the urgent need for enterprises to require more rigorous security practices from outside contractors, and for a comprehensive federal data breach disclosure law.

## NEWS ANALYSIS

---

### Event

On 30 January 2008, media reports stated that California state government officials have acknowledged that more than 400 candidates for state employment have been notified that highly sensitive data related to their applications has been lost. The data, which included psychological evaluations of applicants for positions as police and corrections officers, was contained on a notebook computer that was stolen from a psychologist — an outside contractor — vacationing in Mexico. A government spokesperson stated that the computer was protected by a password and that the data could not be easily read.

### Analysis

The critical need to secure the sensitive data stored on workstations, and particularly on notebook computers and other mobile devices — through encryption or equally strong compensating methods — has been well understood for at least a decade. Nonetheless, reports of massive data security breaches continue to appear in the media with disturbing frequency. Gartner receives many inquiries from enterprises that are still struggling with legitimate barriers to internal implementations of data protection measures. However, there is absolutely no reason that an outside contractor working with highly sensitive data cannot be compelled to follow rigorous data protection practices (certainly more rigorous than ensuring that data cannot be easily read). Outside contractors work at the pleasure and discretion of the employer and are not bound by terms that apply to in-house employees. Minimal acceptable data protection practices can therefore easily be written into every contract for outside contractors — and enterprises must do so.

This data security breach also highlights the inconsistencies in state disclosure laws in the U.S. and the need for an overarching federal breach disclosure law that would simplify enterprise compliance. Most state laws are modeled after the California law that came into effect on 1 July 2003, which specifically excluded medical information — such as psychological evaluations — from the types of personal information covered. (Some states, Arkansas among them, have chosen to include medical information.) The covered entities also vary from state to state, ranging from persons or enterprises that conduct business with the state to the more comprehensive category of data collectors that handle nonpublic information. A federal disclosure law should make compliance simpler and more effective, even in cases that do not extend, as this one does, beyond U.S. borders.

### RECOMMENDATIONS

---

- **Enterprises that allow outside contractors access to sensitive data:** Negotiate all new contracts, and renegotiate any contracts in progress, to require contractors to: use encryption or equally strong compensating security methods; strengthen accountability for external access, including methods for authentication; and provide an enumerated list of systems, procedures, commands and files related to the contracted work.

### RECOMMENDED READING

---

- "Security Consequences for Employee-Owned IT" — Enterprises can mitigate the security challenges of employee-owned IT by basing implementation choices on risk and manageability. **By John Girard**

- "Data Loss Could Have Huge Impact on U.K. Banking Industry" — A data loss by the U.K. tax agency could prove enormously expensive for the country's banks. **By Avivah Litan**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

## REGIONAL HEADQUARTERS

---

### Corporate Headquarters

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### European Headquarters

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### Japan Headquarters

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### Latin America Headquarters

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509