Learning from Losses:  
Wandering Laptops Should Teach Lessons  
by M. E. Kabay, PhD, CISSP-ISSMP  
Associate Professor, Information Assurance  
Norwich University, Northfield VT

Just recently I was updating some lecture materials for an upcoming course and needed some recent examples of losses of control over data. I ran across some excellent reporting by Ashlee Vance of _The Register_ and I think readers will enjoy reading his work.

* * *

ERNST & YOUNG LOSES LAPTOP COMPUTERS WITH CUSTOMER DATA

Mr Vance wrote that the international consulting firm Ernst & Young lost a series of laptop computers in early 2006. In February, the firm grudgingly admitted that a laptop with confidential customer data – including the SSN of Scott McNealy, CEO of Sun Microsystems – had been lost or stolen in January. [http://tinyurl.com/qxjz7](http://tinyurl.com/qxjz7) McNealy reported that his identity had in fact been compromised. Then a March report in the Miami Herald stated that some Ernst & Young auditors went to lunch on Feb 9 – leaving their laptop computers in a conference room in the office building where they were working. Two men stole four of their laptops. E&Y declined to issue a public statement about these breaches of security, although when pressed, they did assure the public that “password protection” sufficed to compensate for loss of control over the data. [http://tinyurl.com/laj8c](http://tinyurl.com/laj8c)

On March 15, Vance wrote that E&Y had lost yet another laptop computer – this one stolen in January from an employee’s car. It contained financial and tax records compromising the security of “thousands” of IBM employees and ex-employees. Once again, the company refused to issue a public statement about the theft and informed the potential victims of identity theft two months after the incident. [http://tinyurl.com/hltf6](http://tinyurl.com/hltf6) On March 23, Vance found out that E&Y had admitted to BP that 38,000 employees were included in the January laptop theft. [http://tinyurl.com/oayw3](http://tinyurl.com/oayw3)

FIDELITY INVESTMENTS LOSES LAPTOP WITH CLIENT DATA

Ashlee Vance, scourge of careless laptop users, reported on March 22 in The Register that Fidelity Investments had announced the loss of a laptop computer containing detailed HP retirement plan data for 196,000 HP employees, including names, addresses, salaries and SSNs. In contrast with the disgraceful performance of Ernst & Young, Fidelity announced the loss relatively quickly and cooperated fully with the trade press. In addition, the data on the laptop were encrypted. [http://tinyurl.com/kyj3p](http://tinyurl.com/kyj3p)

The same article reported that Ernst & Young were rolling out encryption software for their corporate computers. At last.

On 24 March, Vance reported that the _reason_ a Fidelity employee was carrying 196,000 records about HP employees on a laptop was… wait for it… as part of a demo intended to

***

So aside from nominating Ashlee Vance for a journalism award, what can we learn from these unfortunate circumstances? Nothing particularly new, but perhaps readers will appreciate having fresh examples with which to enliven security-awareness and policy discussions where you can raise the following points:

* Think about whether specific data _ought_ to be on laptop computers at all in their raw form; would anonymized versions be just as good (e.g., for demos)?

* Confidential data on corporate computers should be encrypted using whole-disk or partition-level encryption (not file-by-file encryption) with appropriate provisions for key escrow or key recovery procedures in case the user forgets the key or leaves the organization (or this plane of existence).

* Passwords alone are an inadequate form of protection for confidential data.

* Every organization should have a computer security incident response plan in place to handle potentially embarrassing cases such as data loss or loss of control over confidential information. Honesty, forthrightness, openness, clarity, and truth are not just for girl scouts – they will largely prevent embarrassment and humiliation when the truth eventually comes out.

***


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.