VAnishing Confidence

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In this brief series of articles, I’ve been recounting the tale of data losses at the Department of Veterans Affairs (VA). The next column will be the last in the series.

On Monday, August 7, 2006, Secretary Nicholson announced that a Unisys subcontractor working for the VA offices in Philadelphia and Pittsburgh had reported that his desktop computer was missing. The computer contained PII for 18,000 and possibly up to 38,000 veterans.

A week later (August 14), the VA announced that it would spend $3.7M on encryption software and would encrypt data on all the department’s computers and external data storage media or devices. Installation would be Friday Aug 18th.<

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002447&taxonomyId=17

In mid-September, the stolen Unisys desktop computer with VA data was located and a temporary employee working on subcontract to Unisys was arrested and charged in the theft.<

http://www.infoworld.com/article/06/09/15/HNunisyscontractor arrested_1.html

In October 2006, the Congressional Committee on Oversight and Government Reform published a report on data losses in US government agencies since January 1, 2003.<

http://oversight.house.gov/story.asp?ID=1127 > There were 788 incidents in 19 agencies – in addition to hundreds of incidents at the VA. The report’s findings included these bald assertions:
1. Data loss is a government-wide occurrence. . . .

2. Agencies do not always know what has been lost. The letters received by the Committee demonstrate that, in many cases, agencies do not know what information has been lost or how many individuals could be impacted by a particular data loss. Similarly, agencies do not appear to be tracking all possible losses of personal information, making it likely that their reports to the committee are incomplete. For example, the Department of Justice reports that, prior to the May 2006 Veterans Administration data breach, “the Department did not track the content of lost, stolen, or otherwise compromised devices.”

3. Physical security of data is essential. Only a small number of the data breaches reported to the Committee were caused by hackers breaking into computer systems online. The vast majority of data losses arose from physical thefts of portable computers, drives, and disks, or unauthorized use of data by employees.

4. Contractors are responsible for many of the reported breaches. Federal agencies rely heavily on private sector contractors for information technology management services. Thus, many of the reported data breaches were the responsibility of contractors.
Alas, the best-laid plans of VA administrators gang agley, and on October 31, 2006, VA officials informed 1,400 veterans that their PII had been lost on unencrypted data disks sent by mail from the VA clinic in Muskogee, OK on May 10, June 10 and July 10 were lost. A spokesperson for the hospital explained the three-month delay as being due to the “wait for officials in Washington to approve the wording of the letter.” Approval arrived October 26th. There was no explanation of why the data were unencrypted nor why two additional disks were mailed out after the May 10 disk was lost. A report on this incident dated Nov 3, 2006 by Rick Maze in the _Federal Times_ <http://www.federaltimes.com/index.php?S=2331714> also indicated that a laptop computer from the VA hospital in Manhattan was stolen on September 8 from a computer locked to a cart in a locked room in a locked corridor – and that the data on the stolen machine was deliberately not encrypted despite policy because “a decision had been made not to encrypt data being used for medical purposes.”

And more was to come in February 2007, but that’s for next time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 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.