The VA Data Insecurity Saga

by M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA & CTO – School of Graduate Studies
Norwich University, Northfield VT

The following summary of an specific case of management failures will serve to help readers think about the management responsibilities for information assurance.[1]

Announcement Without Taking Responsibility

In March 2007, *Network World* writer Jon Brodkin wrote an excellent analysis of ten letters informing victims of data theft or loss of control of personally-identifiable information (PII) that their data might be compromised.[2] He pointed out that almost all of the letters failed to express any responsibility for the loss of control over data stored on unencrypted disks that were lost or stolen or for poorly-secured Web sites that posted PII without protection or with poor protection. Perhaps staff attorneys warned the public relations officials to avoid any implication of responsibility to avoid contributing anything that would exacerbate their liability in potential lawsuits. Passive voice is often used to shift responsibility from specific agents to the great gaseous cloud of the unnamable and unblamable. The classic example is, "Mistakes were made."

In 2007, the following letter was sent to physicians affected by a security breach

> DEPARTMENT OF VETERANS AFFAIRS
>
> 1615 Woodward St.
>
> Austin, TX 78772
>
> -----, MD
>
> Dear -----, MD:
>
> I am writing to you, as the Director of the Veterans Integrated Service Network (VISN) 7 in Atlanta, Georgia, to inform you that I have been notified that a portable computer hard drive used by an employee of the Birmingham Veterans Affairs (VA) Medical Center is missing. This portable hard drive was used to back-up information contained on a VA employee's office computer, related to research projects with which the employee was involved. A file on the portable hard drive included information from the Unique Physician Identification Number (UPIN) Directory dated 2004, which includes demographic information and identifiers, such as the UPIN, dates of birth, state license numbers, business addresses, and employer identification numbers (EIN). In the case of your information, we believe the EIN was your Social Security Number. This file was obtained by VA from the Centers for Medicare & Medicaid Services (CMS) for the purpose of conducting research on veterans' health care.
>
> The Birmingham VA Medical Center has conducted extensive physical searches and has involved local police and Federal investigative resources, and a reward is being offered;

however, the hard drive remains missing. To prevent further security breaches or losses, we have taken immediate measures to protect the integrity and security of all personally identifiable information including prohibition of the use of external drives and the required encryption of personally identifiable information when authorized distribution is required.

An independent risk analysis was conducted as required by law, and risk mitigation recommendations are being implemented immediately. VA will contact you shortly by mail to offer a credit monitoring service at no cost to you. In the mean time, one precaution we recommend is for you to request a free credit report from one or more of the three national credit bureaus by calling the toll free number 1-877-322-8228. The credit bureaus may also be contacted at:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-916-8800

More information about credit protection, including placing a "fraud alert" on your accounts, is available by calling the Federal Trade Commission at its toll free number, 1-877-438-4338, or by visiting its website, http://www.ftc.gov/

If you have questions concerning this letter, the Birmingham VA Medical Center has established a dedicated call center to answer your questions. Please contact us toll free at 1-877-xxx-xxxx from 6:00 am to 9:00 pm CT, or e-mail us at < address suppressed > .

We at VA take information security and privacy very seriously. We apologize for any inconvenience or concern this situation may cause, but we believe it is important for you to be fully informed of any potential risk to you.

Sincerely,

[digitized signature]

Lawrence A. Biro
Network Director, VISN 7

Initial Problems

On May 3, 2006, a career civil servant at the Department of Veterans Affairs (VA) violated official policy by taking computer disks containing personally identifiable information (PII) about 26.5 million veterans home with him. The disks were stolen from his home.[3] Two weeks after officials learned of the theft, the VA disclosed the incident to the public and set up a Website and an 800-number to provide veterans and with information and a channel for reporting possible identity theft.[4]

The USA.gov Website put up a page called "Latest Information on Veterans Affairs Data Security"[5] with answers to frequently-asked questions; the VA itself also continued issuing press releases.[6]

In early June 2006, the VA announced that the stolen data might include PII about up to 1.1M active-duty troops, 430,000 members of the National Guard and 645,000 members of the reserves.[7] Reactions from a coalition of veterans groups was immediate: they launched a class-action lawsuit demanding full disclosure of exactly who was affected by the theft and seeking $1000 in damages for each victim.[8]

The VA struggled to cope with the bad publicity and potential legal liability resulting from the May theft. On May 26, 2006, Secretary of VA R. James Nicholson issued a Directive to all VA supervisors in which he wrote, "Having access to such sensitive information brings with it a grave responsibility. It requires that we protect Federal property and information, and that it shall not be used for other than authorized activities and only in authorized locations. As managers, supervisors, and team leaders it is your responsibility to ensure that your staff is aware of and adheres to all Federal and VA policies and guidelines governing privacy protected material. I also expect each and every one of you to know what sensitive and confidential data your subordinates, including contractors, have access to and how, when and where that data is used, especially in those cases where it is used or accessed off-site."[9]

On May 30, 2006, the VA fired the analyst "response for data loss" and announced changes in the administration of information security in the organization.[10] The press release made no mention of who was responsible for allowing anybody to store unencrypted PII on VA computers or media.

Coincidentally, at the end of May, the Government Accountability Office (GAO) issued a report: "GAO-06-612: Homeland Security: Guidance and Standards are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts."[11] The report specifically named the VA as requiring "guidance and standards for measuring performance in federal government facility protection."

On June 21, 2006, the VA announced that it would provide free credit monitoring for everyone affected by the data theft in May.[10]

But worse was yet to come.

Systematic Management Failures

On June 14, 2006, Linda D. Koontz, Director, Information Management Issues and Gregory C. Wilshusen, Director, Information Security Issues of the Government Accountability Office of the United States offered testimony before the Committee on Veterans' Affairs, House of Representatives. The GAO report on their analysis and recommendations later appeared as GAO-06-866.[12] Highlights of their analysis included these comments:

> For many years, significant concerns have been raised about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information, including sensitive personal information. Both GAO and the department's inspector general have reported recurring weaknesses in such areas as access controls, physical security, and segregation of incompatible duties. The department has taken steps to address these weaknesses, but these have not been sufficient to establish a comprehensive information security program. For example, it is still developing plans to complete a security incident response program to monitor suspicious activity and cyber alerts, events, and incidents. Without an established and implemented security program, the department will continue to have major challenges in protecting its information and information systems from security breaches such as the one it recently experienced.

Two related reports appeared about a week later with specific comments about the May 2006 data breach[13] and about the overall challenges facing the VA and the Department of Defense (DoD) in protecting personally-identifiable information (PII) of active-duty and retired military personnel.[14]

At the end of June 2006, the laptop and external hard drive stolen on May 3 from the consultant's home were recovered. Forensic examination suggested that the data had not been accessed. This good news suggested that the disaster might blow over.

It was not to be.

The Inspector General (IG) of the VA, George Opfer, released a report on July 11 severely criticizing senior managers of the VA for their lackadaisical response to the original theft of unencrypted PII. The inadequate data security policies had not yet been corrected.[15] VA Secretary James Nicholsen responded to the IG's report with assurances that the agency had "embarked on a course of action to wholly improve its cyber and information security programs."[16]

Continued Problems

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 being Friday Aug 18th.[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.[18]

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.[19] 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 oft 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*[20] 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.

Analyses and Responses

On Friday, February 2, 2007, Secretary of Veterans Affairs Jim Nicholson announced that a VA employee in the VA medical center in Birmingham, AL had reported an external hard drive as missing on January 22nd. According to Rep Spencer Bachus (R-AL), the backup hard drive contained personally identifiable information (PII) on up to 48,000 veterans – and despite VA regulations promulgated in 2006, as many as 20,000 of those records were not encrypted.[21] A week later, the VA admitted that the hard drive actually contained PII about 535,000 patients and 1.3 million doctors.[22] It was that loss that led to the letter quoted in the first section of this section.[23]

A few weeks later, the Government Accountability Office (GAO) released the closest thing to an exasperated blast of exasperation I think government workers are capable of: in testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives on February 28, 2007, GAO Director of Information Security Issues Gregory C. Wilshusen presented a report entitled "Veterans Affairs Needs to Address Long-Standing Weaknesses."[24] The summary on page 2 of the PDF file include this commentary:

> For many years, GAO has raised significant concerns about VA's information security—particularly its lack of a comprehensive information security program, which is vital to safeguarding government information. The figure below details information security weaknesses that GAO identified from 1998 to 2005. As shown, VA had not consistently implemented appropriate controls for (1) limiting, preventing, and detecting electronic access to sensitive computerized information; (2) restricting physical access to computer and network equipment to authorized individuals; (3) segregating incompatible duties among separate groups or individuals; (4) ensuring that changes to computer software were authorized and timely; or (5) providing continuity of computerized systems and operations. The department's IG has also reported recurring weaknesses throughout VA in such areas as access controls, physical security, and segregation of incompatible duties. In response, the department has taken actions to address these weaknesses, but these have not been sufficient to establish a comprehensive information security programs. As a result, sensitive information has remained vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure. Without an established and implemented security program, the department will continue to have major challenges in protecting its systems and information from security breaches.

In early March 2007, the VA reacted to the January 22nd loss of the portable hard drive. Chief Information Officer (CIO) Robert Howard promulgated a policy restricting the use of portable data storage devices. Only flash drives smaller than 2 GB – and only those issued by the VA's CIO office itself – would be permitted on the VA network or computers. Encryption would be used throughout the system, just like the assurance issued in August 2006 about spending $3.7M on encryption tools.[17] In addition, the CIO announced sweeping changes in security administration, with promotion of five deputy CIOs to the rank of assistant secretaries for the following functions: application development, information security, operations and maintenance, resource management and strategic planning.

As of late May 2007, federal agencies announced that they would stop storing Social Security Numbers and other PII wherever possible.[25]

ENDNOTES

[1] This paper is based on a series of articles published in *Network World Security Strategies* in 2007.

[2] Brodkin, J. (2007). "Deep regrets, from TJX to ChoicePoint, about data leaks." *Network World* (March 14, 2007). http://www.networkworld.com/news/2007/031407-wider-net-apologies-letters.html?page=1

[3] Gross, G. (2006). "U.S. agency loses data containing 26 million IDs." *Network World* (May 22, 2006). http://www.networkworld.com/news/2006/052206-us-agency-loses-veterans-data.html?brl

[4] Gross, G. (2006). "Lawmaker calls on VA head to resign after data theft." Network World (May 25, 2006). http://www.networkworld.com/news/2006/052506-lawmaker-calls-on-va-head.html?inform

[5] US Government Veterans Information "Lastest Information on Veterans Affairs Data Security." http://www.usa.gov/veteransinfo.shtml

[6] Using keyword "data" in the search field at http://www1.va.gov/opa/pressrel/index.cfm provides a reasonable chronology.

[7] US Department of Veterans Affairs (2006). "Secretary Nicholson Provides Update on Stolen Data Incident: Data Matching With Department of Defense Providing New Details" (June 6, 2006). http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1134

[8] Associated Press (2006). "Data on 2.2M active troops stolen from VA." *USA TODAY* (June 7, 2006). http://www.usatoday.com/news/washington/2006-06-06-veterans-data_x.htm

[9] US Department of Veterans Affairs (2006). "Directive by the Secretary of Veterans Affairs R. James Nicholson To All VA Supervisors on Information Security." (May 26, 2006). http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1128

[10] US Department of Veterans Affairs (2006). "VA Secretary Inserts New Leadership in Policy & Planning Office." (May 30, 2006). http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1129

[11] US Government Accountability Office (2006). "Homeland Security: Guidance and Standards are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts." Report GAO-06-612 (May 2006). http://www.gao.gov/cgi-bin/getrpt?GAO-06-612

[12] US Government Accountability Office (2006). "Veterans Affairs: Leadership Needed to Address Information Security Weaknesses and Privacy Issues." Report GAO-06-866T (June 14, 2006). http://www.gao.gov/cgi-bin/getrpt?GAO-06-866T

[13] US Government Accountability Office (2006). "Information Security: Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs." Highlights of GAO-06-897T http://www.gao.gov/highlights/d06897thigh.pdf

[14] US Government Accountability Office (2006). "Information Technology: VA and DOD Face Challenges in Completing Key Efforts." Highlights of GAO-06-905T http://www.gao.gov/highlights/d06905thigh.pdf

[15] Department of Veterans Affairs Office of Inspector General (2006). "Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans." Report No. 06-02238-163 (July 11, 2006). http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf

[16] Associated Press (2006). "Personal data for 38,000 veterans missing, VA says." USA TODAY (August 7, 2006). http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-08-07-veterans-data_x.htm?csp=34

[17] Gross, G. (2006). "VA to spend $3.7M on encryption tools: The move follows the theft of a VA laptop in May." *Computerworld* (August 14, 2006). http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002447

[18] McMillan, R. (2006). "Unisys contractor arrested in VA theft: Investigators do not believe 21-year-old suspect sought agency's data." *InfoWorld* (September 15, 2006). http://www.infoworld.com/article/06/09/15/HNunisyscontractorarrested_1.html

[19] Waxman, H. A. (2006). "Committee Report Finds Data Breaches Throughout Federal Government." *Committee on Oversight and Government Reform, 110th Congress* (October 13, 2006). http://oversight.house.gov/story.asp?ID=1127

[20] Maze, R. (2006). "VA reports two more data security lapses." *Federal Times* (November 3, 2006). http://www.federaltimes.com/index.php?S=2331714

[21] Broache, A. (2007). "Hard drive vanishes from VA facility." *C|Net News* (February 5, 2007). http://news.com.com/2100-1029_3-6156386.html

[22] Keizer, G. (2007). "Lost VA hard drive may have held 1.8M IDs: Initially, the agency said just 50,000 were potentially affected." *Computerworld* (February 13, 2007). http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011218

[23] Kabay, M. E. (2007). "PIIssed off yet?" *Network World Security Strategies* (June 12, 2007). http://www.networkworld.com/newsletters/sec/2007/0611sec1.html

[24] US Government Accountability Office (2007). "Information Security: Veterans Affairs Needs to Address Long-Standing Weaknesses." Report GAO-07-532T (February 28, 2007). http://www.gao.gov/new.items/d07532t.pdf

[25] Vijayan, J. (2007). "OMB sets 120-day deadline for Fed breach-notification plans: Agencies have the summer to develop and implement first phases of policies." *Computerworld* (May 29, 2007). http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9021544

