A Stolen Laptop at the Department of Veterans Affairs: The Worst Data Theft Ever?

CASE STUDY

The Department of Veterans Affairs (VA) is responsible for dispensing federal benefits such as healthcare, burial, disability compensation, and pensions to U.S. military veterans and their families. It serves roughly 63 million people who are eligible for benefits.

On May 22, 2006, the VA revealed that a laptop and disks containing the personal electronic files of 26.5 million military veterans had been stolen from the home of a longtime Veterans Affairs employee on May 3. The employee, a data analyst, brought the materials home in order to work on a project from his residence in Aspen Hill, Maryland. At that time it was believed that the analyst had done this without authorization. The data stolen included names, social security numbers, and birth dates of veterans who were discharged from the military starting in 1975. Also involved were files of veterans who were discharged earlier and later filed claims with the VA. The stolen data were not related to health records or financial information, but they were not encrypted.

The VA announced that it could find no evidence suggesting that the stolen data had been used illegally. The department went on to assert that the perpetrators of the burglary might not even know what they possessed or how to use it. Jim Nicholson, Secretary of Veterans Affairs, wrote a letter to the veterans whose data were potentially exposed, advising these veterans to be "extra vigilant" in monitoring their bank and credit card statements. The VA set up a call center and a Web site to field queries from veterans. In the first few days after the theft was announced, the VA received over 100,000 calls to its toll-free information line.

The theft of the VA data occurred at a time when the nation's confidence in the security of personal data was at an all-time low. Security breaches at ChoicePoint in February 2005 and at CardSystems Solutions the following June had shaken the belief that companies entrusted with sensitive personal data could adequately protect them. ChoicePoint, the world's largest commercial data broker, failed to properly screen its customers, enabling thieves to gain access to the personal data of over 150,000 consumers. At CardSystems, a payment processor that handles transactions for major credit card companies, a hacking incident compromised the credit card accounts of 40 million consumers. In the wake of these and other scandals, a number of states enacted laws to compel organizations that process private data to inform consumers when their data have been compromised. Though Congress has debated a number of similar bills, it has been unable to come to a consensus on the issue, so no federal statute exists.

With 26.5 million records exposed, the VA breach was the second largest such case after CardSystems and the largest unauthorized disclosure of social security identification data. Such data are particularly useful to anyone intent on identity theft because they are used for accessing credit reports, bank accounts, and credit card accounts.

The acting VA inspector general reported to Congress that his office had been concerned with the department's security controls since 2001. The inspector general had concluded that the operating system, password system, and detection alerts were all vulnerable to security breaches. The leadership of the VA was more seriously called into question for the way it initially responded to the data theft. The department did not report the incident to law enforcement until two weeks after it found out about it. Officials from the Justice Department and the Federal Bureau of Investigation (FBI) felt that the delay may have inhibited their ability to perform a thorough investigation and solve the case.

The VA did not initially offer a statement explaining why it waited before informing law enforcement or the public. Nicholson himself did not learn about the theft until 13 days after it occurred. It was unclear how many people knew about the theft before Nicholson did, and who eventually made the decision to tell him.

When the burglary occurred, the data analyst informed his supervisors, but they did not tell the inspector general's office right away. VA Inspector General George Opfer became aware of the issue as a result of office gossip. The inspector general's office was only able to begin an investigation on May 10 because one of its employees heard discussion about a burglary during a regular meeting. In testimony before Senate and House panels investigating the

breach, Opfer revealed that the employee whose house was burglarized had been routinely transporting the data to his home for three years, unbeknownst to his supervisors. The data analyst was placed on administrative leave for the investigation. He was not thought to have broken any laws.

According to Opfer, a 2004 audit of the VA included recommendations to centralize IT security programs, to ensure that employee job descriptions contained proper rules about what data they could access, and to complete work on intrusion detection systems, infrastructure protection actions, and better access controls. None of these recommendations were fully implemented.

Two former CIOs from the VA, John Gauss and Robert McFarland, appeared before the House Committee on Veterans' Affairs and offered opinions on how to improve information security at the department. They agreed that centralized management of all IT programs and activities was paramount. McFarland noted that decentralized management is deep-rooted at the agency, making it resistant to change. Gauss cited such "cultural impediments" as reasons why he was unable to institute central management of IT at the departmental level or a strong information security program during his tenure. Gauss wanted to introduce a horizontal structure that would be less susceptible to delays, budget overruns, and performance failures.

Both former CIOs stressed that the VA CIO and the chief information security officer needed to have greater direct authority to enforce security policies and mandates. They agreed with the recommendation of Committee Chairman Steve Buyer that the CIO be raised in rank to undersecretary and the chief information security officer be raised to the assistant secretary level. McFarland left the agency in April 2006 when he became frustrated with the implementation of a new "federated" IT management system whose purpose was to reduce costs and make the department more efficient.

Nicholson approved the reorganization in October 2005, enabling the VA to divide its IT operations into two domains. Congress also passed a bill that gave a single executive control over all of the department's IT spending. The VA planned to merge the two IT domains to finally centralize IT programs and activities completely. McFarland testified that such a consolidation was the only hope for ensuring a secure IT environment.

These actions were of little consolation to veterans. Five veterans' groups came together to file a class-action suit against the federal government in response to the burglary and the delayed actions of the VA in its aftermath. The suit required the VA to provide full disclosure of which veterans were affected by the theft and asked for damages awards of $1,000 for each—a potential payout of $26.5 billion. Language in the complaint accused the VA of disregarding the privacy rights of veterans and "recklessly failing to make even the most rudimentary effort to safeguard" their personal information.

The VA consulted credit-monitoring services to plan assistance for those that might be affected—a list which had grown to include as many as 50,000 Navy and National Guard personnel. The Bush administration later asked Congress to approve a $160.5 million package to cover the cost of free credit monitoring for all of the veterans and military personnel whose records were in the stolen database. In the weeks following the disclosure of the breach, the VA also announced that the stolen data included disability codes and, perhaps, phone numbers and addresses.

The VA finally had some good news in late June 2006 when the stolen laptop and storage media were recovered. Initial forensic analysis indicated that the database had not been accessed since the date of the theft, but further tests would determine if the data had been duplicated or accessed in any way. Nicholson said that law enforcement officials had told him that there was reason to be optimistic that the data had not been utilized. Lawmakers, while pleased with the progress of the investigation, were not prepared to let the VA off the hook. Representative Lane Evans, the ranking Democrat on the Veterans Affairs Committee, summed up their feelings by stating, "Today's announcement does not relieve the Department of Veterans Affairs from fixing its broken data security system and failed leadership."

The leadership of the agency was again called into question when the Veterans Affairs Committee revealed that documents obtained from the VA showed that the data analyst did have authorization to take home a laptop and use a software package to work with the data. The Associated Press detailed three such documents dating back to 2002. The documents respectively authorized the analyst to use at home special software designed to manipulate large amounts of data, to access the social security numbers of millions of veterans, and to remove a laptop and other accessories from the VA building for outside work. The documents weakened the agency's defense that it had security policies in place, but the employee violated the policies. Nonetheless,

Nicholson had by this time decided to fire the employee, a decision which the analyst formally challenged.

On August 5, 2006, authorities arrested two teenagers from Rockville, Maryland, for the theft of the laptop and hard drive. They were charged with first-degree burglary and theft over $500. A third suspect, a juvenile, was also facing charges. The burglary was committed randomly and the teenagers did not realize what data were on the stolen equipment until the case gained notoriety.

With that chapter of the case closed, Congress and the VA itself could turn their full attention to what went wrong and how to prevent it from happening again. Those goals were made all the more urgent just a few days after the arrests when the VA announced that a desktop computer containing the personal information of 38,000 veterans was missing from an office of Unisys Corp in Reston, Virginia. The VA had subcontracted Unisys to perform insurance collection tasks for VA medical centers in Pittsburgh and Philadelphia. The computer may have contained records of patients' names, addresses, social security numbers, dates of birth, insurance company names, billing information, dates of military service, claims data, and medical information. The data were not classified, nor were they encrypted—the contract did not require encryption. The VA teamed with Unisys to notify the veterans who might be affected and offered them credit-monitoring services. Unisys could not immediately determine whether the computer had been stolen or simply misplaced. The company was reviewing security tapes, records, and logs as well as conducting interviews in its quest to resolve the issue.

Sources: Hope Yen, "Veterans' ID Theft May Be Largest Ever," The Associated Press, accessed via Forbes.com, May 23, 2006; David Stout and Tom Zeller Jr., "Vast Data Cache About Veterans Is Stolen," *The New York Times*, May 23, 2006; David Stout and Tom Zeller Jr., "Agency Delayed Reporting Theft of Veterans' Data," *The New York Times*, May 24, 2006; David Stout, "Veterans Chief Voices Anger on Data Theft," *The New York Times*, May 25, 2006; Hope Yen, "VA Breach Discovered Through Office Gossip," The Associated Press, accessed via Washingtonpost.com, May 25, 2006; David Stout, "Veteran Data Was Removed Routinely, Official Says," *The New York Times*, May 26, 2006; Hope Yen, "Veterans' Groups Sue Over Data Theft," The Associated Press, accessed via Msnbc.com, June 6, 2006; Jaikumar Vijayan, "IT Centralization at VA Key to Security, Former Agency CIOs Say," *Computerworld*, June 29, 2006; Christopher Lee and Zachary A. Goldfarb, "Stolen VA Laptop and Hard Drive Recovered," *The Washington Post*, June 30, 2006; Brian Westley, "2 Teens Arrested in Theft of VA Laptop," The Associated Press, accessed via Yahoo News, August 5, 2006; Linda Rosencrance, "Update: Another VA Computer Missing," *Computerworld*, August 8, 2006; and Larry Greenemeier, "No More Excuses," *Information Week*, May 29, 2006.

CASE STUDY QUESTIONS

1. List and describe the security weaknesses at the Department of Veterans Affairs.
2. What management, organization, and technology factors contributed to these weaknesesses?
3. How effectively did the VA deal with these problems?
4. What solutions would you suggest to prevent these security problems?