The New Atlantis
A Journal of Technology & Society

Cyber-Insecurity

Computer Theft Puts Veterans' Data at Risk

On May 3, 2006, some time between 10:30 a.m. and 4:45 p.m., a burglar pried open a window in a house in Maryland. He left with some coins, a laptop, and an external hard drive—not a bad haul, but nothing spectacular. Yet a few weeks later, this incident led to congressional hearings and front-page articles in newspapers across the country.

The house belonged to a man who worked as a data analyst at the U.S. Department of Veterans Affairs (VA), the government department responsible for administering pension and health benefits for the nation's veterans. The stolen hard drive contained the names, Social Security numbers, and birthdates of 26.5 million veterans, and the burglary put all those people at risk of credit card fraud and identity theft if that data fell into the hands of someone who knew how to exploit it.

In light of the potential threat, the department's dawdling after the burglary is astonishing. The VA inspector general did not learn about the theft until a week later, through a casual comment made by another VA employee. Nearly another week went by before the Secretary of Veterans Affairs, Jim Nicholson, was informed on May 16. And six more days elapsed before the incident was announced to the public on May 22.

As the press began to investigate the story, the scope of the data breach became clearer—and more troubling. The hard drive also contained information on veterans' spouses; it contained

Copyright 2006. All rights reserved. See www.TheNewAtlantis.com for more information.

some phone numbers and addresses; it contained information on veterans who participated in chemical testing programs during World War II; and it contained (potentially embarrassing) information on the disability status of veterans. Later it was revealed that the hard drive had data relating not just to veterans and their families but also to men and women in the service today—in fact, it contained personal information about the *vast majority* of active-duty military personnel as well as over a million members of the National Guard and Reserve.

The bureaucratic chaos within the department, both before and after the public revelation, is almost incomprehensible: communication was nonexistent, internal tension was rampant, and there was an utter failure to recognize the magnitude—both practical and political—of the problem. Crucial days passed before the start of a serious investigation to find out even the most elementary facts, like how many veterans were affected. After mind-boggling confusion about who was in charge of the data analyst, his supervisor finally "admitted that he had no idea what projects the employee was assigned, nor did he have any understanding of the size or contents of the databases with which the employee routinely worked," according to a report from the VA inspector general. By July, the data analyst was fired, and two VA officials quit over the incident.

At a hastily convened congressional hearing, Secretary Nicholson testified that the data analyst had been routinely working on such sensitive data at home since 2003 without official authorization. While VA regulations require that employees "safeguard an individual against the invasion of personal privacy," according to the department's inspector general, there was no clear VA policy "that specified how protected information not maintained on a VA automated system should be safeguarded, particularly when it is removed from the workplace." The employee never asked anyone's permission to take the data home to work after-hours, and apparently no one was aware he had it there. While the inspector general notes that the employee was a "dedicated individual who worked long hours and produced meticulous work," earning an "Outstanding" in his most recent performance appraisal (the highest possible rating), the employee unquestionably exercised poor judgment in bringing the data home.

In the wake of the security breach, the VA sent letters to all of the veterans believed to be affected, warning them to keep an eye out for "suspicious activity regarding [their] personal information," presumably by monitoring their bank and credit card statements. The department later offered free credit monitoring for one year to the millions of affected individuals. Secretary Nicholson ordered that each of the VA's 235,000 employees complete the department's annual privacy and cybersecurity-awareness training by the end of June. He also convened a task force charged with compiling

Copyright 2006. All rights reserved. See www.TheNewAtlantis.com for more information.

an inventory of all VA staff who need access to sensitive data and recommending broader privacy improvements.

It seems clear that the VA needs a thorough overhaul of its cybersecurity policies. In March 2006, two months before the current incident, the House Committee on Government Reform issued its annual computer security report card, giving the VA an "F." (From 2001 to 2005, the committee gave the VA an "F" four times and a "C" once.) Months earlier, in late 2005, the Government Accountability Office (GAO) noted in a report that the VA's senior cybersecurity official had no one directly or indirectly reporting to him, "raising questions about this person's ability to enforce compliance with security policies and procedures and ensure accountability for actions taken throughout the department. The more than 600 information security officers in the VA's three administrations and its many medical facilities throughout the country were responsible for ensuring the department's information security, although they reported only to their facility's director or to the chief information officer of their administration."

Of course, while this specific lapse brought the VA into the searing public spotlight, it is worth noting that the department is not alone in its inattention to cybersecurity. The same committee that gave the VA an "F" has given the federal government as a whole a "D+." And the GAO reported last year that "pervasive weaknesses in the twenty-four major agencies' information security policies and practices threaten the integrity, confidentiality, and availability of federal information and information systems.... These weaknesses put federal operations and assets at risk of fraud, misuse, and destruction. In addition, they place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption."

The government, of course, is by no means the only entity at risk of losing citizens' personal data; there have been numerous examples of credit companies and data brokers exposing millions of people's private information due to lax cybersecurity practices. ChoicePoint, a data broker, accidentally revealed the financial data of 163,000 people, resulting in 800 cases of identity theft. LexisNexis, another data broker, accidentally revealed personal data for about 310,000 people. Citigroup reported the loss of data for about 4 million people less than two weeks before MasterCard International reported the exposure of data for 40 million customers. All of those incidents were from just 2005.

The VA episode fortunately ended with a whimper: The laptop and hard drive were found (thanks to a tipster), and FBI computer-forensics experts were able to determine that the VA databases were likely never accessed. If the burglar, or the laptop's eventual recipient, had been sufficiently savvy to recognize the value of the data on

Copyright 2006. All rights reserved. See www.TheNewAtlantis.com for more information.

the hard drive and had been able to find a buyer—or if the data had been more critical, perhaps revealing veterans' health records—the situation could have been much worse for millions of veterans. Next time, it might be.

Copyright 2006. All rights reserved. See www.TheNewAtlantis.com for more information.