Securing Those That Served: Safeguarding the personal data of American Veterans

Billy David Cullins

Angelo State University, Center for Security Studies
ABSTRACT

American Veterans comprise a growing segment of society that requires non-traditional protection for personal data and information. As the Department of Veterans Affairs (VA) and the Veterans Benefits Administration (VBA) modernize, a review and reminder of past data breaches and compromises is pertinent to a conversation of increased budgets, technological advances for VA facilities, tighter personnel controls, and removal of antiquated systems from VA centers.
From the time of the American Revolutionary War brave men and women have offered
their lives in sacrifice and service to the United States of America and the Constitution of these
United States. These men and women form a small but distinctive sector of the population we
refer to as Veterans. By statute, a veteran is defined as a “person who served in the active
military, naval, or air service, and who was discharged or released there from under conditions
other than dishonorable” (Moulta-Ali 2014).

The United States Veterans Benefits Administration (VBA) and Department of Veterans
Affairs (VA) are tasked with the gathering, storage and fortification of sensitive information for
millions of past and present veterans, as well as their dependents (Affairs 2013). This
information, however, is not being safe-guarded and multiple examples of personal information
being compromised exist in many areas of the VA. This historical record of losing data, along
with the migration of more services that have traditionally been face-to-face government
functions, such as applying for disability and compensation, become online functions, it is vital
to the security of millions of veterans and their dependents that every effort is made to educate
and inform digital users of VA services on how they can protect themselves while utilizing the
online services offered.

EARLY CONSOLIDATION EFFORTS

In reaction to the vast numbers of returning service members post-World War II (WWII),
The War Department acknowledged that a cohesive system to store the millions of paper
personnel files for all military agencies existed. In 1946 President Harry S. Truman issued
Executive Order 9784—“Providing for the More Efficient Use and for the Transfer and Other
Disposition of Government Records” (Peters and Woolley n.d.). Executive Order 9784 directed
that, among other things:

The head of each agency shall establish and maintain an active continuing program for
the effective management and disposition of its records. Agencies shall retain in their
custody only those records that are needed in the conduct of their current business, and
except as herein otherwise provided, shall promptly cause all other records to be offered
for transfer to the National Archives or proposed for other disposition in accordance with
law.

In the years following Executive Order 9784 a string of minor consolidations of federal
records occurred, but each branch still maintained separate repositories. Then in 1951 Secretary
of Defense George C. Marshall made a successful proposal to the General Services
Administration (GSA) to take custody and consolidation of former Department of Defense
(DOD) civilian employee records. However, the GSA lacked a large enough facility to store
these records. That would change at the onset of the Korean War when the decommissioned
Goodfellow Ordnance Plant in St. Louis, Missouri, home of the Department of the Army’s (DA)
record repository was re-activated to manufacture ordnance, requiring the DA to re-locate all of
its personnel records. The following years saw a series of consolidations and interim storage
facilities for military records until 1958 when Congress appropriated funds for a consolidated facility to store the nearly 400,000 cubic feet of records that had been accumulated from the various services and other government agencies.

In 1961, at a cost of $5.6 million dollars, The National Personnel Records Center (NPRC) was built in St. Louis, MO and became the fundamental storehouse for all federal military and military civilian employee records (Administration n.d.).

NPRC FIRE OF 1973

Assuming enough had been done, not much thought was put into the physical security of those records until July 12, 1973 when a calamitous fire at the NPRC destroyed roughly 16-18 million Official Military Personnel Files (OMPF) (Stender and Walker 1974). The resultant investigation found that, in addition to the sheer volume of paper data stockpiled at the NPRC, an estimated 55 million personnel records, little attention to fire suppression had been paid while establishing the NPRC. Additionally, while the NPRC had been constructed with room enough for 400,000 cubic feet of records, nearly twice that amount was being stored (Ibid, 37). The 1976 loss of records was the largest loss of federal military records until a careless analyst compromised the personal information of nearly 26.5 million veterans in May of 2006.

MAY 3, 2006

On May 3, 2006 the home of an east-coast based Veterans Affairs employee was burglarized and a laptop and external hard-drive containing unencrypted information, including names, social security numbers and disability ratings relating to an estimated 26.5 million veterans was stolen (U. D. Affairs, Veterans Affairs Data Theft 2006). The ensuing Department of Veterans Affairs Office of Inspector General’s (OIG) report entitled “Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans” found that, not only did the employee not have appropriate authorization to be in personal possession of the information, but that glaring oversights in information security within the VA had been noted for years and ignored. One statement in the OIG report read:

For the past several years, we have reported vulnerabilities with information technology security controls in our Consolidated Financial Statements audit reports, Federal Information Security Management Act audit reports, and Combined Assessment Program reports. The recurring themes in these reports support the need for a centralized approach to achieve standardization, remediation of identified weaknesses, and a clear chain-of-command and accountability structure for information security. Each year, we continue to identify repeat deficiencies and repeat recommendations that remain unimplemented. These recommendations, among other issues, highlight the need to address security vulnerabilities of unauthorized access and misuse of sensitive data, the accuracy of position sensitivity levels, timeliness of background investigations,
and cyber security and privacy awareness training. We have also reported information technology security as a Major Management Challenge for the Department each year for the past 6 years (General 2006).

This loss of data prompted stricter controls and measures suggested by the Office of Inspector General but still records continued to be lost. As recently as 2013 a box of personal medical records relating to nearly 20 veterans was found in the attic of a deceased Centerville, OH man who had previously been employed as a registered nurse at a Dayton, Ohio Veterans Affairs facility (Barber 2013). These glaring oversights in physical security, along with recent efforts to minimize the staffing at many VSO’s across the country while dealing with an increase in returning combat veterans with complex medical, emotional and physical issues has seen the roll-out of many websites that veterans and their dependents are being directed to for services. These sites, designed to streamline the application, review, issuance and administration of benefits and services are just as vulnerable as physical records.

MOVING INTO THE DIGITAL AGE

In January of 2014 an internal memo generated at the Corporate Data Center Operations (CDCO), a public-private Franchise Fund data center located in Austin, Texas reported that 20 separate users of the VA’s e-Benefits website portal were unable to access their own information but had full access to the information of other veterans. (U. D. Affairs 2013). e-Benefits, a joint DOD and VA web-based computer portal was launched in early 2013 “to try and address its (VA) notorious and persistent benefits claim backlog affecting hundreds of thousands of veterans” according to VA Secretary Eric Shinseki (Wood 2013).

In response to the growing backlog of benefit applications and claims of mishandling of information, the House Committee on Veterans Affairs heard testimony from Jerry L. Davis, former Deputy Assistant Secretary for Information Security Office of Information and Technology, U.S. Department of Veterans Affairs. While speaking before the committee in 2013, Mr. Davis stated:

In nearly 20 years of building and managing security programs across government and private industry, I had never seen an organization with as many unattended IT security vulnerabilities. Upon my arrival in late August 2010 I inherited the results of more than 15 continuous years of an unattended and documented material weakness in IT security controls. This material weakness included more than 13,000 uncompleted IT security corrective actions. These 13,000 security corrective actions would require more than 100,000 sub actions to fully remediate and manage IT security vulnerabilities and improve the VA security posture (Davis 2013).

This information is shocking and reveals that, not only do veterans have to worry about the physical loss of their records due to the sheer volume of records held by the VA or
carelessness by VA employees, but the potential, and demonstrated, breach of their information on VA websites and servers.

THE FUTURE AND VETERANS’ DATA

Simply put, the VA has a demonstrated record of not safely or properly assuring the physical or cyber-security of data entrusted to its care. While efforts have been made to ensure that access to websites containing personal or veteran specific information have been tightened, to include the introduction of complex passwords often requiring users to enter as many as 14 characters including a combination of uppercase, lowercase, special characters and numbers that must be changed every 90 days, it simply isn’t enough. As lately as February of 2014 a draft report from the VA's Office of Information & Technology Risk Management Team was leaked and acquired by CNBC. This report indicated that "The VA cannot ensure the safety and privacy of Veteran and employee healthcare, benefits, and financial information. The VA is non-compliant with its own privacy and security policies and with Federal laws and regulations" (Gusovsky 2014).

The future is inexact and, as the VA begins the tedious task of transferring all of its paper records to digital formats while concomitantly working to reduce the estimated 300,000 backlogged claims for compensation, pension or disability it will become critical for users of the various emerging VA web-based interfaces to become acutely aware of the VA’s history of data loss while looking ahead at personal security measures that can be taken to protect individual identity (Emmons 2014). It’s important that each and every user of any VA website work to secure their own data by following the guidelines set forth in password structure, ensuring that access to these sights is done on a secure network and, preferentially on a single-user machine (i.e. personal computer). Additional measures such as running routine and regular computer scans to ensure the integrity of one’s own system to check for malicious software that might attempt to compromise personal information will greatly reduce the incidents of data theft from personal networks.

No one step can be taken to definitively protect the information stored by the Department of Veterans affairs. It’s clear that, regardless of how cautious the VA is protect data, human error and sheer negligence will often prevail. However, as more veterans return home and more strain is placed on a system that already services nearly 23.4 million veterans, it is imperative that effective, accountable and assured methods for data storage and Information Security are implemented quickly before another 25 million veterans lose trust in the system they fought, and earned a right to be a part of (U.S. Department of Veterans Affairs 2009).
References


