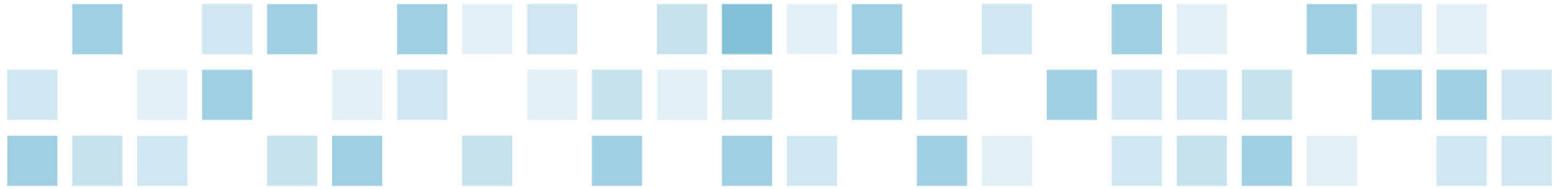


Testimony Before the Committee on Veterans' Affairs, House of Representatives

Legislative Hearing on H.R. 571, H.R. 593, H.R. 1015, H.R. 1016, H.R. 1017, H.R. 1128, and H.R. 1129



Statement of Daimon E. Geopfert

Principal and National Leader of Security and Privacy, McGladrey LLP

March 19, 2015

Background

Mr. Chairman and Members of the Committee, thank you for the opportunity to discuss the Department of Veterans' Affairs (VA) Office of Information and Technology's (OIT) management of its information security programs. My name is Daimon Geopfert, and I was asked to speak today as a veteran, as well as a security expert with experience in both the government and corporate worlds. I have 15 years of experience with the Department of Defense (DoD) including 12 years active duty Air Force, officer and enlisted, as well as three years as a defense contractor building Security Operations Centers (SOCs). While on active duty I was a communications specialist, an agent with the Air Force Office of Special Investigations (AFOSI), and an IT specialist within the Air Intelligence Agency.

Since leaving the DoD, I have spent the last eight years as a security consultant, initially with a "Big 4" firm and now as a principal with McGladrey LLP, serving corporations ranging from the Fortune Top 10 to the middle market, as well as federal, state, and local government entities. I have conducted hundreds of security assessments and breach responses in my career within networks of almost every size and composition. My specializations include ethical hacking, security monitoring, digital forensics, incident response, and malware analysis. Like many of my peers, I have also received a letter from the VA notifying me that the organization failed to protect my personal information.

Purpose

I am here today, quite simply, to make a call for accountability, and to draw attention to the continued need for the VA to resolve and strengthen their information security capabilities. Men and women in the armed services are held to account for almost every action they perform or fail to perform, and they expect the same mentality to apply to those people and entities that control critical aspects of their lives, such as their sensitive medical records or personal data. These veterans have a justifiable expectation that the VA will be held to account for its performance in the

same way that they would have been. However, all indications are that the VA has failed in this duty. What is most frustrating for veterans is that this is not a singular instance of failure, but rather a long-running, systemic version of failure of technologies, processes, and leadership. When veterans were in uniform, this level of non-compliance with their expected duties would not have been tolerated. Passing legislation such as “HR 1017 – The Veterans Information Security Improvement Act” would provide a detailed roadmap for the VA to follow in addressing these issues.

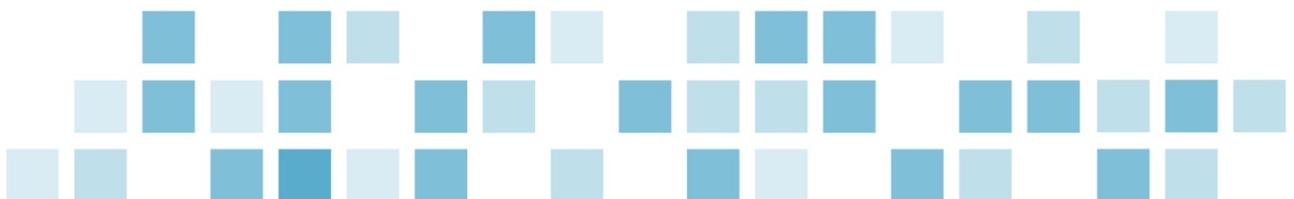
VA History

The VA has a widely reported history of non-compliance with regulations such as FISMA and HIPAA. Testimony by Mrs. Sondra McCauley, currently the Assistant Inspector General for Information Technology Audits at the Department of Homeland Security Office of Inspector General, before this Committee in November of 2014 stated that the VA has had 15 straight years of material weaknesses within its information systems controls with a total of 35 significant findings in the prior audit, five of which are unresolved from previous years. [1] It has been reported that, after the most recent audit, this timeline now spans 16 straight years of material weaknesses. These reports documented an extensive list of weaknesses and vulnerabilities within thousands of systems and applications, as well as within required core security processes and competencies.

The VA’s own internal risk assessments state that a data breach of its primary VistA system is “practically unavoidable” and would result in exposure of “financial, medical, and personal Veteran and employee protected information” with “no way of tracking the source of the breach”. [2] This risk was noted as being from the point of view of an average user, but it also applies to hackers or rogue users. A primary goal for any hacker gaining access to a target environment is to stop looking like a hacker. Hackers want to acquire valid credentials and fade into the background so that their activities look like those of an approved user; therefore, the moment they gain access to any user system these “unavoidable” vulnerabilities are now available to them.

Based on many of the VA’s public comments, reports, and testimony, the focus of its efforts to protect VA systems seems to have been on managing attacks by foreign adversaries at a nation-state level. This is understandable because the VA network can be used as a stepping stone into other DoD environments using direct exploitation or “watering-hole” style attacks that have been utilized against high-tech and financial industries. However, while this focus on foreign adversaries is critical, almost any advanced skill or technology that is exclusively in the realm of nation-state level actors very quickly makes its way into the hands of criminal attackers focused only on monetary gain. In addition, as has been pointed out in numerous security research papers, there is ample evidence showing that nation-state level hackers often end up working on personal projects for their own gain. It is naïve to assume that these individuals would not utilize the skills, tools, and access granted to them during their day jobs to gather sensitive data for their own enrichment at a later time.

In a recent interview Stephen Warren, the VA’s Executive in Charge and Chief Information Officer, stated that physical loss of data and user error were the VA’s most significant risks, accounting for some 98 percent of known security incidents. [3] Some of the most significant findings for the recent VA audits center around the concepts that VA security procedures are lacking in auditing,



logging, and monitoring of the environment, making it highly likely that the VA would not have the capabilities to know that it has suffered a cyber-breach. [4] The OIG identified, and the VA stated in recent testimony, that its networks contain unknown and unmonitored systems and network connections, which would undo almost any effort to deploy effective monitoring. [1] In this same vein, CIO Warren stated that the VA has no evidence to show that data had been exfiltrated after a recent breach, but extensive reporting indicates that the VA would most likely not have the capability to prove, or even know, the truth of such statements. To support this point, it should be noted that CIO Warren later qualified his statements with a specific example of foreign infiltrators known to have extracted materials out of the VA environment, but because of the lack of logging by the VA and the use of encryption by the adversaries the contents of that data are unknown. Scenarios such as this allow the VA to continue to state that the organization is unaware of any theft of data by hackers, but it is likely a factor of the apparent lack of monitoring capabilities rather than the success of any prevention efforts.

Corporate Comparisons

These widely known and extensively reported issues would simply not be tolerated in the corporate world, largely because of the existence and enforcement of explicit legislation and industry standards. If examinations of a commercial organization produced results similar to those identified within the VA, the organization would be rated at the lowest levels of maturity for security governance, grossly out of compliance, and at a critical risk of suffering a breach. An organization in the private sector with this history would face substantial fines and penalties in addition to suffering reputational impact resulting from public scrutiny. There is little doubt that in the corporate world, the officers and directors of such an organization would face serious personal consequences.

It should be noted that the VA is understandably struggling with legacy systems, massive quantities of sensitive data, high levels of interconnections with other entities, and any number of technical and architectural issues. These are significant, often overwhelming issues; however the VAs corporate peers often operate under the same conditions and are expected to perform.

The Office for Civil Rights, the Health and Human Services (HHS) division responsible for enforcing the Health Insurance Portability and Accountability Act (HIPAA), has been levying fines of millions of dollars on companies for issues ranging from exposing the private health information of only a few hundred or thousand individuals to events that violated required controls but were not shown to have actually resulted in lost data. An investigation showed that the VA committed over 14,000 HIPAA violations over a three-year span, but that must be caveated because the same investigations showed that approximately only one out of every 365 violations was actually reported to OIG. [5] This likely makes the VA the largest HIPAA offender in the U.S., for which it has never been fully held to account. Would the FFIEC-OCC tolerate this from a bank? Would the SEC tolerate this from a broker dealer? Would State Attorneys General tolerate this from anyone under their purview without harsh civil or criminal repercussions? If the answer to those questions is “no,” then the veteran community is reasonably curious as to why the VA is held to a different standard.

The VA is, for all practical purposes, exempt from many of the legal penalties that force its corporate peers into compliance, and the results of this situation are self-evident. HR 1017



provides the VA with governance mechanisms to address this issue. I understand that there is a competing Bill – HR 1128. However, on review it is clear that it provides high level requirements that will not provide the detailed instruction needed for VA to address its longstanding information security weaknesses. HR 1128 simply adds additional general requirements to the existing list of 'general' requirements. The trend within other industries is the shift from general to specific security and privacy guidance. The recent shift from the Payment Card Industry (PCI) 2.0 standard to the 3.0 standard is an example within retailers, and the SEC's OCIE cyber security initiative is an example within the broker dealer space. It is time to provide a clear and concise set of requirements to the VA in order to provide the appropriate guidance, structure, and oversight necessary to break this cycle of non-compliance.

Impact to Veterans

While most of the testimony to this point has been on the various issues with the VA environment, it cannot be forgotten that the true risk in this scenario is to the health and well-being of generations of veterans. The most obvious risk is identity theft, which results in enormous financial and mental stress. It goes without saying that introducing any type of additional stress into this population could be extraordinarily damaging. Many of the individuals that would be affected by a data breach within the VA are already at heightened risk because of a variety of injuries—both physical and mental.

By the VA's own estimation, 22 veterans a day take their own lives because of a complex set of physical, mental and financial conditions. While it might sound bombastic to tie identity theft to suicide, it is a fairly straightforward scenario. Many of the veterans interacting with the VA are already under immense pressure from transitioning to civilian life while dealing with a variety of mental and physical conditions, which often impacts their personal finances. For a veteran in this situation, waking up one morning to find out that someone has fraudulently opened a \$50,000 home equity loan without his or her knowledge would be devastating.

Organizations like the VA will often state that it cannot be proved that data stolen from its environments led to identity theft, but this is a symptom of the nature of identity theft not a demonstration of a direct relationship. The repercussions of having personal data stolen might not materialize for years, and when an individual does become aware that something is wrong, it is essentially impossible to specify the source of the leak.

The VA often contains "full identities" of individuals: information such as a veteran's or dependent's name, address, Social Security Number, phone number, and other items that can be used to prove someone's identification. This type of data is the premier target for hackers. If someone steals your credit card number, it can be cancelled. If someone steals your identity, they can impact your financial safety for essentially the rest of your life.

While this is the most obvious risk, it is not the exclusive one. What if beyond identity theft, some actor managed to perform a mass alteration or destruction of medical records out of sheer malice? Do you think this would be beyond the pale for various hacktivist groups or hacking crews that claim allegiance to various countries or terrorist groups? It could conceivably disable the entire VA infrastructure, interrupting services to millions of veterans. It would be a direct, highly visible strike against the U.S. veterans that fought them.



This is not an outlandish scenario. In fact, the capability to do this was demonstrated by the recent data manipulation scandal and the review of the affected systems. If such data alterations were available to standard users, they are available to attackers.

Conclusion

The men and women who have served our country, as well as their dependents, deserve and expect to have their welfare protected by organizations like the VA that play such a critical role in their lives. This legislation is sorely needed, and would be one of the first of its kind to provide such detailed, prescriptive guidance. The protection of the personal information of veterans should be a bipartisan issue, so our community hopes that this will be quickly passed and enforced. For more than a decade, the capability of the VA to protect the sensitive data of veterans has been in question with well-documented, significant, systemic, long-running failures. While legislation and standards already exist that provide high-level guidance on how this data should be protected, this history of non-compliance demonstrates conclusively that a new approach is necessary. Targeted, appropriate legislation is needed to force compliance and provide veterans and their families with the security they deserve. This legislation should explicitly require proper preventative, detective, and corrective controls, along with required reporting and oversight. The VA, and the bodies that oversee it, have an obligation to veterans to finally take decisive actions demonstrating their resolve to do the right thing.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other Members of the Committee may have.



Works Cited

- [1] S. F. McCauley, "Testimony - VA'S LONGSTANDING INFORMATION SECURITY WEAKNESSES ARE INCREASING PATIENT WAIT TIMES AND ALLOWING EXTENSIVE DATA MANIPULATION," 2014.
- [2] "ERM-20130702.005R-OIS.001 - VistA Anonymous User Access," 7/2/2013.
- [3] M. S. Warren, "VA's Longstanding Information Security Weaknesses Continue to Allow Extensive Data Manipulation," 2014.
- [4] V. OIG, "Department of Veteran Affairs - 2013 FISMA Audit," 2013.
- [5] C. Prine, "Privacy breaches in VA health records wound veterans," Pittsburgh Tribune-Review, 2013.

The views expressed herein are those of Mr. Geopfert, and are not necessarily those of McGladrey LLP.





Daimon E. Geopfert

National Leader, Security and Privacy Consulting
Technology Risk Advisory Services
McGladrey LLP
Chicago
daimon.geopfert@mcgladrey.com
312.634.4523



Summary of Experience

Daimon Geopfert is a Principal with the risk advisory services group at McGladrey LLP. He specializes in penetration testing, vulnerability and risk management, security monitoring, incident response, digital forensics and investigations, and compliance frameworks within heavily regulated industries. Daimon has over 20 years of experience in a wide array of information security disciplines. He serves as the firm's national leader for the security and privacy practice, responsible for the development of the firm's overall strategy related to security and privacy services and applicable methodologies, tool kits and engagement documentation.

Daimon is a regular presenter for organizations such as Information Systems Audit and Control Association (ISACA), InfraGard, the Certified Fraud Examiners and SC Magazine's World Congress. He has been quoted in a variety of publications, including The Wall Street Journal, Fortune Magazine, The Washington Post and the Kansas City Business Journal.

Representative Experience

- Information systems security assessment
Daimon has served as the manager and lead technician for security assessments performed on some of the largest corporations and government entities in the world. He has designed and implemented testing frameworks and methodologies used to properly capture and communicate the technical, operational and regulatory impact of identified security weaknesses.

Daimon's experience in this area includes analyses and reviews of the following:

- Security testing across the enterprise: network, host, application and database
- Wireless, Voice over Internet protocol (VoIP), cellular, modem/telco assessment
- Security operations structure and effectiveness
- Social engineering testing, including phishing/pharming, phone and physical
- Corporate security policies and procedures
- Application secure architecture and coding analysis



- Incident response, forensics and security monitoring
Daimon acts as the lead developer for McGladrey's forensic and monitoring service offerings, and has designed and deployed incident response and security monitoring programs within several highly regulated clients. These frameworks are based on customized versions of National Institute of Standards and Technology (NIST) SP800-81, ISO 18044:2004 and the SANS IR 6 Step. Daimon previously served as a special agent with the Air Force Office of Special Investigations – Computer Crimes Investigations, as a researcher with the CIA's Directorate of Science and Technology, and deployed and ran Security Operations Centers for the Department of Defense (DoD).
- Security program management
Daimon has managed and performed a myriad of security program engagements across a variety of industries. The purpose of these projects was to assist organizations in deploying efficient, manageable and cost-effective solutions and processes that would address the wide ranging business and regulatory aspects of IT security. Daimon has deep experience in Payment Card Industry (PCI), HIPAA/Health Information Technology for Economic and Clinical Health (HITECH), FFIEC/Federal Deposit Insurance Corporation (FDIC), Federal Information Security Management Act (FISMA), NIST SP800 series, ISO 2700X, National Information Assurance Certification and Accreditation Process (NIACAP)/DoD Information Assurance Certification and Accreditation Process (DIACAP), American Electric Reliability Corporation(NERC)/Critical Infrastructure Protection (CIP), EU Data Privacy Directive, and various state security and privacy laws.

Professional Affiliations

- Information Systems and Controls Association (ISACA)
- International Information Systems Security Certification Consortium (ISC)²
- FBI InfraGard, Michigan Chapter—Member, Presenter, Speaker Committee
- The SANS (SysAdmin, Audit, Networking, and Security) Institute
- The Ethical Hacker Network

Professional Certifications

- Certified Information Systems Security Professional (CISSP)—(ISC)²
- Certified Information Security Manager (CISM)—ISACA
- Certified Information Systems Auditor (CISA)—ISACA
- GIAC Certified Incident Handler (GCIH)—The SANS Institute
- GIAC Certified Reverse Engineer of Malware (GREM)—The SANS Institute
- Certified Ethical Hacker (CEH)— EC-Council

Education

- University of Michigan, Ann Arbor, Michigan, Master of Science in Computer Science
- United States Air Force Academy, Colorado Spring, Colorado, Bachelor of Science in Computer Science
- Numerous technical and industry courses and seminars

