HealthCare.gov: Consequences of Stolen Identity

Testimony of Michael Gregg before the US House Committee on Science, Space, and Technology.

Rayburn House Office Building, Room 2318

January 16, 2014

My name is Michael Gregg and I am the CEO of Superior Solutions, Inc., a security assessment firm which performs security assessments, penetration tests, and audits. Superior Solutions helps companies secure critical assets as well as works with organizations after security breaches have occurred to determine what happened to prevent future breaches.

I have more than 20 years of IT security experience. I also work with organizations such as ISSA and ISACA to help educate security professionals. I have authored more than 15 books on IT/cyber security. I have taught for Villanova University and other educational institutions. I have also served as an expert witness. My testimony is divided into three parts. I have done so as I believe these are the three critical areas the committee should consider.

- How might HealthCare.gov be hacked?
- Why does HealthCare.gov need to be reviewed by an independent 3rd party?
- What would be the result of HealthCare.gov being exploited?

How might HealthCare.gov be hacked?

My analysis of the HealthCare.gov website was gathered from passive analysis of readily available information and my personal knowledge of web applications and web design. Under no circumstance did I or any employee of Superior Solutions conduct any type of "hacking" efforts or attempt to exploit any weaknesses in the HealthCare.gov website.

While functionality has been the main focus thus far in the scrutiny over the HealthCare.gov website, my concern is that a much bigger issue is looming in that individuals enrolled at the HealthCare.gov website could have their personal information and/or medical records stolen.

My concern is that the HealthCare.gov website is a major target for hackers who are looking to steal personal identities. Although HealthCare.gov doesn't store this information directly on the website, it only links to it through a maze of third-party government sites such as the Internal Revenue Service, Department of Homeland Security, Social Security Administration, Department of Veterans Affairs, and others. While there are many ways that the HealthCare.gov website may be hacked, I have described five potential ways that this could occur:

1. Code Injection Attacks - When a website is poorly designed, it's often vulnerable to what is referred to in the security industry as “injection attacks.” This means a hacker can go onto the website and write malicious code which he/she then tricks the website into accepting and running as its own code. One of the most widely used code injection attacks is SQL injection. The best example of poor input validation is the fact that some 834 files are corrupted and are unusable when passed to insurance companies. The transport of this data via Electronic Data Interchange (EDI) might be targeted when being passed back to the insurer and being mapped to the Qualified Health Plan (QHP). Such errors point to the fact that input is not being handled correctly.

2. Cross-Site Scripting - This attack can occur when a hacker goes in and (as in cases stated above) tricks the website into accepting malicious code through an input field such as a web request or form field. The next time a person visits the site, a cross-site scripting attack will run against their web browser, stealing saved passwords, cookies, or other sensitive information from the user.

3. Insecure or Weak Authentication - Websites that are poorly designed often struggle with inadequate “authentication” and “session management” - these are important security features that, when done right, protect the integrity of your account. When they are weak or inadequate, a hacker can impersonate users and take over their accounts.

4. Clickjacking - In this type of attack, hackers take advantage of poor security on a website to slip invisible frames over seemingly innocuous items or features on a webpage such as an entry form, a video, or a “like” button. When individuals click on this button (for instance, “submit form”), they're actually clicking on the hidden link slipped over the real web page, so their information is redirected to a malicious website or sensitive information is stolen.

5. Sensitive Data Exposure - Websites that are not properly secured can leak sensitive data or fail to properly encrypt it. We've seen this before even with well-designed commercial websites and mobile apps. For example, the site does not properly encrypt its users’ passwords or transmits information in clear text. Twitter and Gmail used to have this problem before they switched to default SSL encryption for all users. In the case of HealthCare.gov, the real risk is likely to be in how it relays data back and forth between the various third-party websites it is linked to (e.g., IRS, Veterans Affairs, etc.) and how well it encrypts those communications.

Why does HealthCare.gov need to be reviewed by an independent 3rd party?
While the types of attacks previously discussed may sound foreign to many, the threat is real. HealthCare.gov has a large attack surface that is very complex and that makes it very hard to secure. Why does the site need an external review? Let's start with certification and accreditation. With my expert knowledge of certification and accreditation, I find it hard to believe that during the release and update to the

HealthCare.gov website, that all the requirements of FISMA, FIPS 199, and FIPS 200 were properly completed. Even if, for the sake of argument, we assume such testing was performed, this is not enough when we are talking about the potential loss of millions of individuals' personal information.

The website itself is large. HealthCare.gov is reported to be about 500 million lines of code. This pales in comparison to others such as Microsoft Windows. Windows 8 is reported to be no more than 80 million lines of code. Microsoft has spent almost 30 years attempting to secure their operating systems. It's illogical to believe such a large site such as HealthCare.gov, could be secured in such a short period of time. To believe that this has occurred would mean that the contractors responsible for the development of this site have been able to do what no other major company (Microsoft, Apple, Facebook, and Google) has ever accomplished.

It's considered a "security best practice" that the individuals that write the code and develop the site are not the same individuals that test the security features of the site. Think of it as "separation of duties."

When a large application or website is reviewed, it is typically performed in one or more of three ways. These three categories include: audits, vulnerability assessments, and penetration testing.

1. Audits - Reviewing a checklist of criteria of things that should be completed. As an example, credit card numbers should be encrypted.

2. Vulnerability assessments - Typically software packages that perform scans looking for common problems, misconfigurations, and missing patches/updates. As an example, using a software tool such as Nessus or Retina.

3. Penetration testing - This type of assessment examines what an insider or outsider can access, how that can be leveraged, and what would be the resulting impact. Typically, organizations bring in external, third parties to perform these types of penetration tests. Such tests are much different than certification and accreditation testing in that they examine the site in much the same way as a hacker would.

All three are required for a well developed, robust application.

What has been reported is that currently, the HealthCare.gov website is only being scanned and patched after problems are discovered. As an example, Mr. David Kennedy, previously testified that he had found issues and reported them to the site administrators to be addressed. Such an approach is detective in nature. Think of it in this way, the site administrator must find and secure all problems yet a hacker only needs to find one vulnerability to exploit the site. Hackers now work in organized groups out of places such as Russia and Eastern Europe. Should these hackers find problems in the site, they *would* *not* report them. Such information would be used to exploit HealthCare.gov and expose US citizens to undue risk.

What would be the result of HealthCare.gov being exploited?

There are two areas of concern if/when hackers exploit HealthCare.gov which include loss of personally identifiable information (PII) and healthcare information. If these attacks were to occur, they could be devastating. Just consider the following attacks and the number of personal information lost:

- Adobe - 38,000,000 accounts exposed
- Sony - 77,000,000 accounts exposed
- T.J. Maxx - 94,000,000 accounts exposed
- Target - 120,000,000 accounts exposed
- Heartland - 130,000,000 accounts exposed

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

A successful attack against HealthCare.gov could expose many more individuals than the exploits previously listed. It could very well be the largest ever. Some might argue that if HealthCare.gov is vulnerable, why hasn't it already been exploited? One reason is timing. Hackers have shown that they have the patience and fortitude to spend a considerable amount of time waiting if there is a big reward. Since the deadline for open enrollment is not until March 31, 2014, hackers would be foolish to exploit the site now. Think of how many social security numbers a breach of the HealthCare.gov website might offer cyber criminals at that time.

Some of the items that an individual might have to deal with as a result of identity theft:

- Reduced credit ratings - An individual’s credit rating can be seriously impacted by identity theft.
- Increased difficulty obtaining loans - A theft flag can be added to your credit report which means that you must take additional steps to prove you are the person you claim to be.
- Criminal issues - An identity theft might result in someone using your identity and being arrested or charged with a crime. The victim might be identified with traffic tickets or even criminal charges that are hard to disprove.
- Emotional impact - Dealing with identity theft can be time consuming and emotionally draining. Victims may also be denied employment or forced to deal with collection agencies.

While these items are a scary thought, the second real threat is healthcare/medical identity theft. Such attacks are on the rise. A study by the Ponemon Institute found that a whopping 94 percent of polled healthcare organizations have suffered “data breaches” that exposed patient records. This is a 65 percent increase since 2010-2011. Backing up this study is a 2012 report from the U.S. Department of Health's Office of Civil Rights, which found that in just three years nearly 21 million patients became the victims of medical record data breaches.

Losing a patient's medical record puts a person at risk of identity theft, medical identity theft, and other crimes. Why would hackers target personal health records? Why, because these records are seen as the latest gold mine to organized cybercrime. Medical records can contain social security numbers, birth dates, information about someone's family members, and billing information that could include credit card numbers. Electronic medical records can potentially allow hackers to spoof personal identities and wreak havoc in the lives of many. Medical records are just like any other hacking target in that it can offer a payout or financial reward.

Such information is targeted by hackers. As an example, here are just a few of the medical record hack attacks from 2012:

- 780,000 patient records stolen from Utah Department of Health
- 315,000 records from Emory Healthcare
- 228,000 records from South Carolina Department of Heath
- 116,000 records from Alere Home Monitoring, Inc.
- 102,000 records from Memorial Healthcare System Florida

What might be the result of medical record or health care information being stolen from the HealthCare.gov website? Some possible scenarios include:

- Not getting hired for a job - Some companies check medical records.
- Getting the wrong treatment - If someone has had treatment under your identity, you could receive the wrong medication.
- You are denied life insurance - Someone using your stolen identity may have been treated for AIDS or cancer.

Some real life examples include:

- A woman in Utah was contacted by the state's child protective services unit and told that they were going to take her children away because her newborn baby had tested positive for methamphetamines.
- A pilot from Colorado was billed $41,000 for surgery by a Denver hospital despite the fact that he had not ever been in that particular hospital. He then spent years disputing the charges and nearly filed for bankruptcy because of it.
- A hacker demands 10 million dollars for 8 million patient prescription records stolen from the Virginia Department of Health Professionals in 2009.

Source: http://www.megapath.com/megapath/assets/File/PDF/WhitePapers/WP_MedIDTheft.pdf

In the end, the most frustrating aspect of medical record theft is that patients feel powerless to stop it.

Closing

When my organization builds applications, we bring all the people together: end users, developers, and security professionals so that security can be built in to the design from the point of inception. The HealthCare.gov website was designed and built quickly without the oversight for security that is required. As a result, this site offers hackers a substantial payday if/when they are able to breach the security of the site. There are many ways in which this might be accomplished such as cross site scripting, SQL injection, URL misdirection, etc. Regardless of how this is accomplished, the end game is the same, in that it will result in a massive loss of personal information.

Hacking has become “big business” today. The era of lone hackers in their basements targeting websites has passed. Today, hacking a site such as HealthCare.gov offers organized crime groups, rogue nation states, and even terrorists a huge potential reward. This problem can be addressed by bringing in a team of external security consultants to review the security of the site and make an independent assessment of its current state. I ask this committee to consider the importance of this activity before it is too late. As Winston Churchill stated, “*I never worry about action, but only inaction.*”

Thank you for allowing me the opportunity to be here today. I look forward to your questions.