eHEALTH INITIATIVE
Real Solutions. Better Health.

House Committee Science, Space, and Technology: "*Is My Data on Healthcare.gov Secure?"*

On Tuesday, November 19th, the House Science, Space, and Technology Committee hosted a hearing to investigate the security standards and technical measures that should have been established during the implementation of HealthCare.gov. The panel of witnesses included:

- Mr. Morgan Wright, Chief Executive Officer, Crowd Sourced Investigations, LLC
- Dr. Frederick R. Chang, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Southern Methodist University
- Dr. Aviel D. Rubin, Director, Health and Medical Security Laboratory Technical Director, Information Security Institute, John Hopkins University (JHU)
- Mr. David Kennedy, Chief Executive Officer, TrustedSEC, LLC

Chairman Lamar Smith (R-TX) began the hearing with his opening statement followed by a statement from Ranking Member Eddie Johnson (D-TX).

Background

Since the rollout of HealthCare.gov on October 1st, there have been number of security concerns and risks surrounding the system. The information available on the website is one of the largest collections of personal data that is intertwined with multiple external networks. According to documents provided by the Department of Health and Human Services (HHS), a full security testing was never conducted prior to the rollout of the website. There are speculations based on the testimony before the Homeland Security Committee that hackers may have already attempted to attack the system. Under the Federal Information Security Management Act (FISMA), it is the federal agencies responsibilities to ensure private records are sufficiently protected against potential security breaches and identity thefts. The purpose of this hearing was to examine the threats surrounding the website and of its vulnerabilities to hackers and cyber criminals.

Witnesses

Morgan Wright, CEO at Crowd Sourced Investigations, LLC, testified before the committee about his concerns and analyses of the potential security threats to HealthCare.gov. Mr. Wright explained there are approximately over 500 million lines of computer code making up the system. Since October 1st, there were reportedly approximately 500,000 visitors on the website. Mr. Wright explained while Facebook uses just 20 million lines of code, the website attracts 727 million active users since September 2013. He used this comparison in order to demonstrate the highly complex system of HealthCare.gov website. Mr. Wright highlighted four critical issues related to the security risks of HealthCare.gov. First, there was a lack of end-to-end security testing. The inability to conduct a complete assessment of the website creates significant security risks. Second, user account creation and registration were required in order to review the various health insurance options. Mr. Wright explained that it creates a norm to provide personal information upfront in order to view their options for a health care plan. This further creates fraudulent websites and scams that heighten identity theft and data compromises. Third, cybersquatting and domain name confusion is a security risk. If a consumer accidently visits the wrong website, their information may be compromised since the individual unknowingly provided their personal data to a deceptive website. Fourth, the insider threat is always a factor when dealing with sensitive information. Mr. Wright explained that health care navigators are hired without any background checks. This raises security and privacy concerns for the consumers.

Dr. Fred Chang, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security at Southern Methodist University, shared his concerns of the security measures with HealthCare.gov. Mr. Chang explained that technology has evolved significantly and cannot underestimate the current cyber system. He further explained that as a software system becomes more complex, there will be number of flaws which are exploited by cyber criminals and thefts. This inevitably leads to security breaches and increases systems vulnerability to hackers. Mr. Chang shared three types of security risks associated with HealthCare.gov. First, the number of fake websites has increased since the launch of HealthCare.gov website. This creates major security issues and identity theft problems if consumers unknowingly share their personal information to fake websites. Second, completing an online application that requires sensitive information is risky. Mr. Chang acknowledged that it is convenient and the American people already engage in wide variety of online transactions. However, there are always security risks when providing sensitive personal information online. Third, security risks from complex software such as HealthCare.gov are increased due to flaws and vulnerabilities of the system.

Dr. Avi Rubin, Health and Medical Security Laboratory Technical Director of Information Security Institute at Johns Hopkins University (JHU), shared his insight on security issues surrounding the HealthCare.gov website. Mr. Rubin explained launching a large software program such as HealthCare.gov takes multiple steps. He said it was not a surprise when there were numerous technical problems with the rollout of HealthCare.gov. There is more vulnerability in a system depending on the systems complexity. Mr. Rubin explained that security must be the foundation of a system when building a large program such as HealthCare.gov. Security features and standards will be difficult to adjust and to monitor once the system has been built. There are greater risks to high profiled websites such as HealthCare.gov.

Mr. David Kennedy, Chief Executive Officer of TrustedSec, LLC, testified before the committee about the security issues related to HealthCare.gov website and of its lack of ability to protect personal information. Mr. Kennedy explained that TrustedSec has not directly hacked into the website but assessed that there are critical security risks based on identified exposures. He further explained there is public information available that shows how the website is integrated with federal and state departments. In consequence, this heightens security risks for the website. Mr. Kennedy explained today's technology has advanced and evolved quickly. He said there are websites that are more difficult to hack into because of their high security measures. The purpose of establishing security on a website is to monitor and to protect sensitive information, detect the flaws, and fix them in a timely manner. However, HealthCare.gov website has many security issues that need to be addressed immediately. Mr. Kennedy explained HealthCare.gov is vulnerable to several security issues because it is integrated with number of state and federal sites and third parties. The infrastructure of the website is complex. Its vulnerability and exposure can directly affect involving third parties. Mr. Kennedy earlier in his testimony described himself as a 'White Hat' hacker. Mr. Kennedy explained that a hacker can extract as many as thousands of information on the website using various codes. Mr. Kennedy showed the committee members that there have been many attempts to extract and to hack into the system using the search bar located in the website.

Questions and Discussion from the Committee Members

Chairman Lamar Smith (R-TX) asked if the HealthCare.gov website can be fixed or if it should be started over. Mr. Smith further asked what would be the real dangers and impact if hackers were successful in attacking the website. Mr. Wright explained from a technology industry point of view, it would be easier to start over rather than attempting to fix the number of problems the website presents. Mr. Wright said the software system should have been built around security as the foundation for the software program. Mr. Kennedy acknowledged his confidence that the website has been hacked. He explained personal information such as social security numbers, age, and etc. are prone to be retrieved by hackers. Fraudulent activities are likely to be seen with a complex system such as HealthCare.gov. The website is integrated with other trusted infrastructures which could allow hackers access other sensitive personal information. Mr. Chang explained identity theft will become an issue; fraudulent tax returns among other identity theft issues will be seen. Mr. Wright explained the website is the largest collection of personal information. There are unknown threats with high profiled system such as HealthCare.gov.

Ranking Member Congresswoman Eddie Johnson (D-TX) asked if the health care industry lagged in technology compared to other industries. Mr. Rubin responded health care seems to be far behind when it comes to technology and security standards. The lack of technology advancement is especially evident in hospitals and in operating rooms. Mr. Rubin stated health care information technology has a lot to learn in order to improve on its security measures.

Vice Chair of the Committee Dana Rohrabacher (R-CA) expressed his concerns for the security measures surrounding personal information on HealthCare.gov. He asked if sensitive information were being hacked and if there were attempts from other countries as well. Mr. Kennedy responded there are patterns of inconsistency around security. There are ways to prevent these security breaches. However, it will be difficult since security was not the foundation when establishing the HealthCare.gov website. He explained there are possibilities of hackers from other countries. There are organized crimes that happen purely for financial reasons.

Congresswoman Suzanne Bonamici (D-OR) explained the ACA is not solely based on the website. She said the functionality of the website is not the biggest concern for the American people. Accessibility to health care coverage is the main concern for most Americans. In efforts to address those issues, there are several avenues in order to obtain a health care plan. The process to gain access to health care coverage should be easy for the American people. She explained there have been many concerns with the Data Service Hub storing personal information. Ms. Bonamici asked if the hub stores any medical records. Mr.

Rubin responded that the hub is used to verify the provided information and it does not store any personal data.

Congressman Randy Neugebauer (R-TX) asked if there were any security risks for allowing health care navigators to be exempted from a federal background-check. Mr. Chang responded that identity theft is possible and personal information will be at risk. Mr. Neugebauer asked if HealthCare.gov website operates differently compared to other websites. He further explained that there are many ecommerce website builders available to develop a website yet the administration built a new system from scratch. Mr. Wright explained there are accountability issues and exposure of civil litigations. The legal ramifications are not as strict under government's work. There is more flexibility under the federal sector compared to the public or private industry. Mr. Wright said that the administration has immunity from many of the accountabilities that private sector do not have.

Congressman Ami Bera (D-CA) acknowledged that the rollout of the website has not gone smoothly. In contrast to HealthCare.gov, California's health insurance exchange website asks for basic information before it allows the consumer to view their options. He explained this features makes the website more secure. Mr. Bera suggested that fake websites and false URL addresses needs to be identified and to shut them down immediately. Also, he asked the committee to determine which states have not enforced a federal background-check on navigators. Mr. Bera explained that navigators should be required to undergo a background-check. Mr. Bera asked the panel of witnesses if HealthCare.gov website was secure and if they would advise the American people to use it. There was a unanimous no within the witnesses. They all agreed there were security risks and not to use the website yet.

Congressman Chris Collins (R-NY) asked a series of yes or no questions to the panel of witnesses. There was a unanimous 'no' among the witnesses to the following questions: would the witnesses have launched HealthCare.gov on October 1st, if anyone would have signed off on the front-end requirement as complete, is the website secure today, and will the website be secured on November 30th. Mr. Collins asked if the witnesses would recommend for the website to be shut down until it is verified and secured. Mr. Wright, Mr. Chang, and Mr. Kennedy agreed. Mr. Rubin responded that he needed more information.

To download the witness testimonies and view a recording of the hearing, click here.