Enter Search Keyword

Home

U.S. Senate Committee on Commerce, Science, & Transportation

Home / Hearings

Hearings

Mar 26 2014

Protecting Personal Consumer Information from Cyber Attacks and Data Breaches

Thune Data Breach Hearing Statement

Ranking Member, U.S. Senate Committee on Commerce, Science, and Transportation

WASHINGTON, D.C. — U.S. Senator John Thune (R-SD), Ranking Member of the Senate Committee on Commerce, Science, and Transportation, will submit for the record the following prepared remarks at today's "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches" full committee hearing:

Thank you, Chairman Rockefeller, for holding this afternoon's hearing on data breaches and protecting consumer information. Protecting consumers from identity theft, fraud, and financial harm is certainly a goal that all of us on this committee share.

I am glad that representatives from Target and the University of Maryland accepted our invitation to be here today to tell us of their recent and well-publicized breaches. While the forensic investigations into these incidents are still ongoing, it is clear that millions of individuals have unfortunately been affected. I look forward to hearing about what lessons Target and the University of Maryland have learned from these breaches and what additional steps they are taking to prevent them in the future and to better safeguard individuals' personal information.

Yet data breaches clearly are not unique to Target and the University of Maryland. A data breach report from Verizon found there were more than 600 confirmed data breach disclosures among private and government entities and at least 44 million compromised records in 2012 alone.

While we are here today primarily to discuss data breaches in the private sector, we can't forget that the U.S. government also holds immense amounts of consumer financial data and personal information. It is estimated that the federal government spent more than $14.6 billion on IT security in fiscal year 2012, but it is not immune to cyber attacks and data breaches. In 2012, federal agencies reported more than 22,000 data breach incidents – a number that is more than double what was reported in 2009.

In addition, a recent report by the Government Accountability Office – the government's watchdog – identified several instances where federal agencies failed to notify affected individuals, even when the breach was determined to have a high risk of harm.

Breaches of personal information can affect individuals in many ways, ranging from the inconvenience of having a credit card replaced, to the harm of identity theft where a criminal runs up large debts or commits crimes in the victim's name. When there is risk of real harm stemming from a breach, we need to make sure that consumers have the information they need to protect themselves.

That is why I support a uniform federal breach notification standard to replace the patchwork of laws in 46 states and the District of Columbia. A single federal standard would ensure all consumers are treated the same with regard to notification of data breaches that might cause them harm. Such a standard would also provide consistency and certainty regarding timely notification practices, which benefits both consumers and businesses.

I also want to ensure that businesses appropriately secure information and are not burdened by outdated or ill-suited security requirements, but rather are provided with the flexibility to develop effective and innovative tools to secure the information they are entrusted to protect.

For these reasons, I cosponsored S. 1193, the Data Security and Breach Notification Act of 2013, with Senator Toomey and a number of my colleagues on the Committee. This bill would require companies possessing personal data to notify consumers in a timely manner if their information has been unlawfully taken.

Mr. Chairman, I know you have also introduced legislation on this topic, and I look forward to working with you and our colleagues as we consider how best to promote the security of personal consumer information and ensure appropriate breach notification.

Of course, we should acknowledge that this issue is not a new one. The committee reported data breach legislation in 2005, and again in 2007, but finding broad agreement on the path forward has proven difficult. We should heed the testimony of Mr. Wagner and not allow the perfect to become the enemy of the good.

Our recent experience advancing legislation on the role of the National Institute of Standards and Technology in the identification of voluntary best practices and standards for cybersecurity gives me reason for optimism. And I was pleased to see that several of the witnesses today have highlighted the good work done by the National Institute of Standards and Technology in this regard.

As we've noted in the past, legislation is also needed to enhance information sharing of cyber threats, with liability protections. While not every data breach occurs because of a cyber attack, timely information sharing of cyber threats is key to preventing and responding to cyber attacks – whether it is a breach of consumer data, theft of intellectual property, or an attack on critical infrastructure.

So, I look forward to learning more about the new partnership between the merchant and financial associations that will focus on sharing more information on cyber threats and improving technology to protect consumers. I also hope Visa and Target can elaborate on the work they are doing to identify and prevent payment card fraud resulting from the recent breach, so that the payment system is more secure and consumers are better protected.

I also look forward to hearing from Chairwoman Ramirez, of the Federal Trade Commission about the work the agency is doing on enforcement and education to protect consumers from identity theft and fraud. I also know that the Secret Service and the Federal Bureau of Investigation, in partnership with industry and government partners, are working hard to detect and prosecute cybercriminals and fraudsters. So, I hope our witnesses can share their experiences – good or bad – working with federal agencies on our shared goal of safeguarding consumers' personal information.

Thank you again, Mr. Chairman, for holding this hearing, and I look forward to hearing from our witnesses.

###

Return to Hearing

Browse by: March 2014 GO

Filter by: -- Congress -- -- Types -- GO

03/26/14 -	**Current record**
03/13/14 -	**The U.S. Aviation Industry and Jobs: Keeping American Manufacturing Competitive**
03/12/14 -	**Postponed: Executive Session**
03/06/14 -	**Enhancing our Rail Safety: Current Challenges for Passenger and Freight Rail**

Home About Hearings Subcommittees Oversight & Investigations Press Room Majority Minority Contact
Privacy Policy