Written Testimony of Ravi Pendse, Ph.D.
Vice President and Chief Information Officer
Brown University Cisco Fellow
Professor of Practice, Computer Science and Engineering

Before the U.S. Senate Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
"Getting it Right on Data Breach and Notification Legislation in the 114th Congress"

February 5, 2015

Executive Summary

With an ever-increasing collection of databases, the impact of "big data" on privacy, and the monetary value of personal data used for identity and financial theft, today's America is in need of sound and achievable legislation around data security, privacy, and the notification of consumers after a data breach. Such legislation would benefit all U.S. citizens as well as the organizations collecting and protecting their data.

National legislation governing data breaches will have many advantages over existing state laws and reduce the burden that these dissimilar state laws place on complying organizations. While it's necessary for us to pursue centralized standards, it's important to produce legislation that accommodates organizations of all sizes. In addition to laws regarding data breaches, we should create incentives for proactive measures to reduce the likelihood of breaches, one of the most important being the development of a trained cybersecurity workforce through education and training.

Introduction

Good morning Chairman Moran, Ranking Member Blumenthal, and distinguished Members of the Committee. Thank you so much for the opportunity to testify today about the data breach and notification legislation, it is truly an honor.

I want to commend you for investing your valuable time to discuss this important area of cyberinfrastructure and protection. As younger citizens get online in schools leveraging the power of the internet to learn and create knowledge, your work on this legislation will be critical to protect our youth. As the amount of data continues to increase exponentially, primarily driven by our mobile and highly connected lifestyle, your work on this legislation will be critical to protect our netizens. As internet-connected devices on the "Internet of Things" increase in number from 10 billion to a projected 50 billion by 2020, impacting our economy by as much as $19 trillion, your work on this legislation will be a critical catalyst to empower connected innovation and wealth generation. As connected robots and 3-D printing fundamentally change how we manufacture goods and manage our supply chain, your work on this legislation will be critical to supporting next-generation innovation and our leadership in the world.

My name is Ravi Pendse. I have the privilege and honor to serve as the Vice President and Chief Information Officer at Brown University. I am a Brown University Cisco Fellow and a senior member of IEEE. I am also a faculty member in both Computer Science and Engineering. My area of expertise and research is in the "Internet of Things", cybersecurity, and aviation network security; I also teach classes in these fields. Currently, I am teaching a class called "Internet of

Everything" so your work on this legislation is critical to many young people I interact with each day who I know will change our world for the better.

Thank you again for the opportunity to provide written and verbal testimony relative to a uniform federal law concerning the definition, protection, and notification of the personally identifiable information of consumers. This is a necessary and extremely relevant topic in our hyper-connected world. The Privacy Rights Clearinghouse reports that there have been over 932,700,000 records compromised in over 4,450 U.S. breaches since April 2005. Countless high-profile security breaches have appeared in the news in the last year. My university witnesses an average of 30,000 attempted attacks each day.

As long as there is a black market for the sale of personal and financial data, and these breaches are attainable, the attacks will continue. At the same time, we are living a mobile and highly connected lifestyle, American children are getting online at a younger age, and ten billion of our household devices are connected to the internet. This ubiquity of connectivity makes sound security principles and postures a necessity. We, as individuals, enterprises, and a nation, must continue to focus on this area for the protection of our consumers and national security.

Background

Security breach notification laws have been written in most U.S. states since 2002. The first such law, California SB 1386, became the de facto standard for all states nationwide. Since then, other states have been more descriptive in their remedies, making each, in effect, a standard as they appear.

Forty-seven states (including Rhode Island, where Brown is located), the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches involving personally identifiable information. Many of these state security breach laws have provisions regarding which entities must comply with the law; how "personal information" is defined (such as name combined with Social Security number or driver's license number); what constitutes a breach; how, when, and to whom a notice must be sent; and which situations are exempt (such as a breach of encrypted information). No two are exactly alike.

As a university with students from all 50 states, we are impacted by them all. Maintaining the necessary standards for each state has been not only onerous, but also difficult to completely and legally address. This can create a barrier for small, innovative organizations lacking the expertise or legal team to address the specifics of state laws.

Breach notification is a national issue, and the definition of entities, timing, and requirements should not be left to the individual states. Of course, the state Attorney General would have the ability to protect the citizens of their jurisdiction and make claims as such. Having one standard

for this conduct would be beneficial to those who protect the information and respond when a security incident occurs.

Recommendations for Cybersecurity Breach Legislation

A single national legislation governing data breaches should be established to replace disparate state laws. This legislation should…

1. ...define the rules and actions that are required in the case of a breach, including the method, speed, delivery, and content of notifications.

2. ...adjust for the size, nature, and scope of both the breach and the organization. For example, a hard time limit for breach notification may be unattainable for small organizations, nonprofits, and educational institutions without skills in deep forensics and data science. A tiered approach based upon the severity of the breach and size and designation of the organization would make compliance achievable to all.

3. ...be compliant with current national legislation (such as HIPAA, GLBA, and HITECH) and prevent the possibility of conflict with other federal laws.

4. ...mandate that organizations disclose what happens to customer data. Consumers appear to be happy to give away their data (and their privacy) to services including social media sites for the sake of convenience. A requirement to inform consumers how their data and information will be used is a relevant response to this changing landscape of data exchange.

5. ...define expectations of security for organizations collecting and storing personally identifiable data. Given the highly publicized breaches that have occurred in the past twelve to eighteen months, it is apparent that even many larger enterprises do not provide necessary security. No matter what the size of the company, certain expectations of security should be defined when data is collected and stored.

6. ...create incentives for the formation of industry forums such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). Such forums provide an opportunity to share threats and approaches within an industry.

7. ...consider compliance with the accepted framework by the National Institute of Standards and Technology (NIST), or any framework that meets or exceeds the NIST standards, in order to establish the baseline against which to audit.

8. ...most importantly, provide measures or incentives that establish education to better combat breaches. It is important for us to develop cybersecurity expertise within the U.S.; our national security cannot be offshored. Cisco's 2014 Security Report estimated a global shortage of more than a million security professionals. While efforts like the

National Initiative for Cybersecurity Education (NICE) have attempted to address this shortage, the numbers and expertise of available professionals are still lacking. Cybersecurity programs should be encouraged both in K-12 and higher education. A K-12 program would prepare students to protect themselves as well as join the workforce. Incentives for the expansion of certified cybersecurity programs in higher education, including emerging graduate programs, could make a more immediate impact on the size of the workforce. Similar to the Teach for America program, we could create a conduit for trained security graduates to enter the workforce by establishing a loan forgiveness program dependent upon a designated amount of years in the profession.

Conclusion

We must continue to work on multiple fronts to mitigate the impact of data breaches. Legislation that sets national standards will provide clarity for organizations and balanced protections for all U.S. citizens. As this is a global problem, we must continue to leverage and maximize resources whenever possible to understand and detect persistent threats.

I would be supportive of an effort to create a single, national law around data security and breaches; a national law will remove the undue burden of complying with forty-seven disparate state laws. However, we must be careful to avoid a "one size fits all" model that could be impossible to attain for small organizations, nonprofits, and education. Established tiers of responsibility and compliance levels may better serve all, while legislating a single set of standards that can be embraced and addressed successfully.

In addition to reactive legislation around the handling of data breaches, we need to be proactive. I strongly recommend incentives for proactive measures to reduce the likelihood of breaches, one of the most important being educational initiatives to develop a trained cybersecurity workforce. From additional Americans with forensics expertise to an engaged and educated nation of consumers, we should remember that people provide one of the most critical lines of defense.