OPENING STATEMENT

Ranking Member Dan Maffei (D-NY)
Subcommittee on Oversight
Committee on Science, Space, and Technology

"Can Technology Protect Americans from International Cybercriminals?"

March 6, 2014

Cybercrime occurs on a daily basis. Widespread breaches, like the recent data breach at Target, affected up to 110 million people by exposing their personal data and credit card information. Smaller breaches can still have serious economic consequences. Last year, hackers with reported links to Al Qaeda engaged in hacking the phone systems of small businesses in New York, including in my district in Syracuse, New York. One of the companies hacked, an Albany-based dry cleaner, halted plans to expand in Syracuse because they were struggling to pay the $150,000 phone charges they incurred as a result of this attack. This particular breach resulted in more than 75,000 minutes of overseas calls to Zimbabwe, Bosnia, the Congo, Libya and the Maldives.

Last year alone half a **billion** records of personally identifiable information, including names, emails, credit card numbers and passwords were leaked through data breaches according to an IBM cyber-threat report. But many breaches go unreported. Others go undetected. The full scale and consequence of cybersecurity threats cannot be accurately assessed.

When cybercriminals obtain credit card information on tens of millions of consumers from a retail establishment we all end up paying. Retailers have to pass along the costs for these security incidents through increased prices as a result of fraud, enhanced security upgrades, and potential litigation costs. When foreign governments infiltrate our government agencies, it jeopardizes our national and economic security. When an individual employee at a university, hospital or insurance company steals the digital data of students, patients or clients to engage in identity theft, there are real consequences for Americans.

I do not believe there is a silver bullet to preventing cyber-threats or eliminating the inadvertent disclosure of personal privacy-related data. Technology alone cannot protect us. This is a multi-faceted threat and requires a multi-pronged response. A combination of corporate awareness, federal policies, the proper implementation of security standards, employee and consumer training, and due diligence along the chain of information play a critical role in confronting this growing cyber menace.

There are some technical solutions that can certainly help in countering this threat. The migration of so called E-M-V chip cards in the U.S. and the use of "chip and PIN" transactions can play a role. While this will help counter fraudulent person-to-person transactions, they will not stop all fraudulent transactions, like online sales where a card is not present. Online retail sales in the U.S. alone are expected to grow from $231 billion in 2012 to $370 billion by 2017, making online financial transactions an even more appealing avenue for cybercriminals.

Standards are another technical solution that can play a key role in helping secure IT systems against a wide-range of cyber-threats. The National Institute of Standards and Technology recently released its "Framework for Improving Critical Infrastructure Cybersecurity." This guide can help federal agencies and private industry alike implement reliable and robust IT networks that are as safe and secure as possible.

I am concerned however, that industry is not doing enough to protect itself and to protect ***our*** data from these various cyber threats. The Payment Card Industry (or PCI) has its own Security Standards Council and we have a witness from the council testifying here today. His testimony clearly says – quote: "the PCI Standards are the best line of defense against the criminals seeking to steal payment card data." While the efforts of the industry to police itself are laudable, a recent 2014 report by Verizon called the "PCI Compliance Report" found that only 11.1 percent of the payment card industry companies that it surveyed in 2013 were "fully" compliant with the PCI "Data Security Standard." This was a decline of nearly 50 percent from the 2010 Verizon "PCI Compliance Report" that showed 22 percent of companies in the Payment Card Industry surveyed in 2009 were "fully" compliant with this standard.

It is unclear why the application of these industry endorsed standards has declined but it is a troubling trend. This is particularly troubling since even the PCI Security Standards Council has said that they have seen a correlation between successful cyber-attacks and the lack of compliance with its standards. We need to figure out a way to either incentivize industry to act or to mandate a requirement that they must act.

It is important that we explore these issues to help understand what the private sector is doing to protect consumer data and how we can be effective partners. But I think it is equally important to understand what the commercial market is doing ***with*** consumer data.

We are all sharing more data with more sources all the time. As we share more personal data the opportunities for that data to be stolen, sold or lost escalates. We provide detailed financial data to our banks. Our local grocery store knows the food we eat, the beverages we drink and the toothpaste we use. Facebook knows who we associate with, our favorite movies, books and vacation spots. Google Maps knows where we've been and where we're going. How private industry maintains this data, for how long and how securely is important to every consumer, including me. I hope that Mr. Brookman, a consumer privacy expert from the Center for Democracy & Technology, and one of our witnesses here today, can offer some suggested guidance on how Congress should be thinking about these issues that affect the privacy and security of all of us.

I look forward to hearing from our witnesses and I appreciate the Chairman calling this hearing today. I yield back.