NEW YORK STATE SENATOR

Terrence Murphy

Looking for the facts beyond Equifax: Senators Murphy & Croci host public hearing on cyber-security

TERRENCE MURPHY October 27, 2017

ISSUE: **EQUIFAX BREACH**, **CYBER SECURITY**, **CYBER CRIMES**

New York, NY - Imagine you are about to retire. Then one day you wake up and all your personal information, your social security number, birth date, addresses, even your driver's license number, have been stolen. The hackers who have that information now have control of your life.

That nightmare became a reality on September 7, 2017, when Equifax, one of the nation's

three major credit-reporting agencies, announced that hackers had breached their security systems. The personal information of 145.5 million Americans was exposed, including credit card numbers for 209,000 people. It was the equivalent of giving criminals carte blanche to make purchases in consumers' names, open credit cards, take out loans - and even drain their bank accounts.

Equifax may have left stunned consumers cutting up their credit cards, but Senator Murphy, acting in his capacity as Chairman of the New York State Senate Standing Committee on Government Operations and Investigations, and Senator Thomas Croci, who serves as Chairman of the New York State Standing Committee of Veterans, Homeland Security and Military Affairs, responded to citizen's cries for help, hosting a public hearing on October 24 at the New York State Senate Hearing Room in Manhattan. The goal of the hearing was to examine the state of cyber-security in New York and suggest steps the State can take to take to better protect its citizens. Senators Murphy and Croci were joined at the hearing by fellow State Senators and committee members Martin Golden, Elaine Phillips, David Carlucci and Brad Hoylman.

"There have been two significant breaches in recent months. Suddenly, thousands of people's credit card, social security and bank account information were out there for the taking. My office received dozens of calls from concerned constituents looking for assurances that we could protect their personal information. Today, we hope to find answers that will help solve this important issue," said Senator Murphy. "We have the opportunity to be proactive and make New York a national leader in cyber-security. This hearing is not an indictment. We are not here to prosecute Equifax or interrogate any of the experts sharing information with us. We do have a responsibility to hold bad actors accountable. But the purpose of this hearing is to help lawmakers determine the best course of action to protect the citizens of this State. I want to let the people of New York know that this committee is

fully engaged and will continue this examination."

"I want to compliment Senator Murphy and my Senate colleagues for conducting a hearing to bring together expertise from different sectors to address this State's cyber-security challenges and the effects it has on its residents," said Senator Croci. "The take away from the Senate's efforts and this hearing was universal, that government, business, local municipalities and everyday New Yorkers need to collaborate and share information to come up with solutions to protect our personal information and our residents from cyber-attacks."

Senator Golden said, "The digital world, including the Internet, is the crime scene for the 21st century. Victims are everyone - not just individuals, banks, retailers, but also utilities, government, corporations, health care, education, and everyone that relies on electronic database and management systems. New York's computer laws were written decades ago. They are antiquated and must be updated. They do not reflect the severity of cyber-crimes and the magnitude of the harm to victims. We need to pass a comprehensive cyber-crime bill to provide our law enforcement community the needed tools to arrest and punish cyber criminals. I want to thank Senator Murphy and many of my colleagues who continue to work on cyber security legislation to protect the citizens of this great State and City."

"Cyber-terrorism continues to be one of the most serious threats to both our national security and personal privacy," said Senator Phillips. "With the world shifting into a digital era, nearly everything we do is connected to the internet and our computers: banking, communication, shopping, transportation, and even our medical records. Incidents like the recent Equifax breach only reinforce the vital importance of cyber-security and the need for consumers to be better educated and more responsible for protecting their personal information."

More than a half dozen experts attended the hearing, which included discussions and oral testimony on topics such as the danger facing New York State and its commercial enterprises from cyber-attack; information on current best practices to prevent, respond or recover from a cyber-attack, and solutions that the State, local governments and businesses can use to meet the challenge of providing effective cyber-security.

Speakers included Eric Ellman, Senior Vice President, Public Policy and Legal Affairs, Consumer Data Industry Association; Mary Kavaney, Chief Administrative Officer, Global Cyber Alliance; Michael Kaiser, Executive Director, National Cyber Security Alliance; Rich Mahler, Vice President, Finance and Administration, Revolutionary Security; Peter Morrison, Senior Director of Security Management, CA Technologies; Dr. Steve Chapin, Professor of Engineering and Computer Science, Syracuse University, and Dr. Austen Givens, Professor of Cybersecurity, Utica College. Written testimony was provided by Dr. Shiu-Kai Chin, Professor of Electrical Engineering and Computer Science at Syracuse University; Roger Parrino, Commissioner, Division of Homeland Security and Emergency Services, State of New York, and New York State Police Superintendent George Beach II.

In his testimony Michael Kaiser stated, "We cannot forget about our most vulnerable populations. Increasingly, older adults are becoming the targets of online scams. More than 38% of all U.S seniors say someone has tried to defraud them online. We have seen a jump in tech support scams, tax scams, Ransomware, false debt collection emails, and sweepstake scams directed at seniors. Young people must also be engaged in learning online security as early as possible. Teens have expressed interest in phishing, website security, and creating better passwords. Learning how to prevent identity theft, malware and staying secure online have become top concerns for both parents and teens."

Mary Kavaney offered the assistance of Global Cyber Alliance (GCA) in helping to improve

the cyber-security posture of New York State and its business community. "Small and medium business owners all too often do not understand basic cyber-hygiene. What to do, how to do it, and how to afford it are serious and pressing issues for government and business alike. GCA was created to identify systemic global cyber risks, develop solutions for those risks or leverage existing solutions, and then measure the effectiveness of those solutions. These tools are shared free and globally. I would like to continue to work with your committee to help improve the safety and security of New York State."

Dr. Givens has been researching public-private sector cooperation and collaboration in homeland security for the past six years. "Based upon my research in this area, I am convinced that public-private sector partnerships are indispensable for effective cyber-security in New York State," said Dr. Givens. "In my view, the best way to accomplish this is through the use of incentives. It has been said that 85% of critical infrastructure in the United States, including information technology infrastructure, is owned or managed by business. That fact alone means that government should work with the private sector in the cyber-security arena. For example, New York can provide firms with generous tax breaks for computer hardware and software that are consistent with the state's cyber-security goals, or guarantee businesses low-interest loans to invest in their own security measures. I also believe it is in the best interests to provide support for institutions of higher education. These institutions can play an indispensable role in expanding our state's pool of cyber-security experts."