NEW YORK STATE SENATOR

Michael F. Nozzolio

What Can Be Done to Prevent Cyber Attacks in the Future?

MICHAEL F. NOZZOLIO July 28, 2015

Cyber crime and cyber terrorism are currently the fastest growing threats to individuals in the United States. Statistics show that cyber crime has now surpassed illegal drug trafficking as a way for criminals to profit. Our digital infrastructure is being compromised every day and as such, it has never been more vital to protect ourselves and our personal information from the threat of cyber attack. With several recent high profile breaches in both the public and private sectors, those in power must be held accountable and reaffirm their commitment to protecting our invaluable information. We must alter the course of the cyber security epidemic by treating it for what it really is, an imminent threat to the safety and security of ourselves, our State, and our Nation.

According to a recent study conducted by the Ponemon Institute, each data breach costs companies $3.5 million on average, at a cost of about $201 per record. The study also found that 42 percent of data breaches were caused by malicious or criminal attack, 30 percent by human error, and 29 percent by system glitch. The common thread between these causes? They are preventable.

Earlier this year, my colleagues and I in the Senate held a Joint Committee Hearing on Cyber Security. During the hearing, we examined New York State's current cyber security infrastructure; cyber security in retail, financial, and other commercial sectors; technical solutions to cyber crime; and legal responses to cyber criminal activity.

In the Senate, we also enacted a number of bills to address cyber security concerns directly, while the Assembly failed to recognize the importance of this legislation to crack down on cyber terrorism and its rapidly expanding threat to our State's security and finances. The legislation would establish tougher penalties for cyber-related crimes, create cyber security programs to identify potential risks and threats, and require the state to perform a comprehensive review of all its cyber security measures every five years. If signed into law, these measures would have enhanced New York State's cyber security and helped to protect our citizens' personal information, while strengthening penalties for those found guilty of cyber crimes. Most importantly, we could have established the New York State Cyber Security Initiative to ensure that our State has a proper cyber security defense system in place. Currently, we have no concrete recourse on how to deal with the issue of cyber attack.

The New York State Attorney General also proposed legislation this year, strengthening New York's Data Security Act, which is disturbingly behind the times when it comes to the very real threat of a compromised digital infrastructure. Any law we have on the books dealing with this issue is reactive in nature. The law only requires that a company provide notice to consumers and the New York Attorney General's office if there is a breach of private information, such as an individual's name in combination with a Social Security Number, driver's license, bank account, or credit card number. In an effort to protect our private information, the Attorney General's proposed legislation includes a number of protocols to be established, and requires the adoption of model data security procedures.

We need to be proactive. We need to anticipate what could happen if our data security is undermined and stop it from occurring. In a report released last year, the NYS Attorney General's office found that security breaches reported by businesses, nonprofits and governments in New York more than tripled between 2006 and 2013, exposing 22.8 million personal records of New Yorkers in nearly 5,000 incidents.

It is important to remember that anyone could be the victim of cyber attack. We must educate ourselves on how to protect our information at home through regularly checking credit and bank accounts, utilizing virus protection, using only credible, verified & protected websites, and knowing how much information on ourselves is actually out there. We can advocate for more stringent cyber security laws but we need to understand the issue and protect ourselves.

Each cyber attack threatens our National Security and compromises our digital infrastructure. We must deal with this issue promptly and diligently in order to protect our State and Nation from what could be devastating consequences in the future.

This column concludes a three-part series on cyber security, focusing on how this issue affects our daily lives and our personal confidential information, as well as the economy of our Nation and our National Security.

###