NEW YORK STATE SENATOR

Michael F. Nozzolio

Recent Cyber Attacks Pose Even Greater Risk to Our National Security

MICHAEL F. NOZZOLIO August 27, 2015

Cyber crime and cyber terrorism continue to be the fastest growing threats to individuals in the United States. The latest cyber attack involving the Joint Chiefs of Staff at what was thought to be the ironclad Pentagon, changes the game and should have us all deeply concerned for the National Security of the United States.

With our digital infrastructure so vulnerable to attack, it is more vital than ever that we protect ourselves and our personal information from the very real danger of hackers. Recent high profile breaches have been emblazoned on our television and computer

screens only to have those in power reassure us that the breaches have been dealt with and our information is again protected.

Over the last year we've seen hackers infiltrate private companies like Home Depot and Target, and government agencies like the Office of Personnel Management (OPM) and the Internal Revenue Service (IRS). The cyber security epidemic is an imminent threat to the safety and security of ourselves, our State, and our Nation. One notable similarity between the hacks is that those in power have grossly downplayed each violation's severity and scope. The Joint Chiefs of Staff breach just reiterates our vulnerability.

It should come as no surprise that the federal government in Washington, DC, has downplayed the range of several cyber attacks including May's breach of the IRS. Recent reports revealed that there were 220,000 additional incidents where data was breached, along with 170,000 failed attempts by third parties to gain access to taxpayer data. Using the federal IRS agency's online transcript services, hackers attempted to gain access to thousands of taxpayers' private information. Originally, the federal government claimed that the tax return information for 114,000 taxpayers had been illegally accessed and 111,000 unsuccessful attempts were made by third parties. What's more, 15,000 fraudulent tax returns were processed during the 2015 tax filing season. This IRS revelation is only the beginning.

Recently, another cyber security breach came to light that is perhaps the most dangerous yet. In July, the unclassified email system for the Joint Chiefs of Staff was infiltrated, affecting 4,000 military and civilian personnel who work for the Joint Chiefs of Staff. Russian hackers are suspected of coordinating the cyber attack through social media accounts, using a method known as *phishing*. Phishing relies on the receiver opening attachments in their email that look very similar to most ads for products or services. Once the receiver opens the attachment, it is laced with malware or malicious software, used for the sole purpose of gathering sensitive information. While it remains unclear whether the attack was sanctioned by the Russian government, it should have us all very concerned.

While the information stolen in the Pentagon hack appears to be unclassified, the hack, however, lends itself to some very serious questions: How could this have happened if proper cyber security measures were in place? What if the hack had occurred on the classified email server? What if the cyber attack was indeed sanctioned by the Russian government? Although the Pentagon held courses on email security *after* the attack, why weren't Joint Staff employees aware of the dangers associated with opening suspect emails *prior* to the attack? Had Joint Staff employees been informed of the dangers prior to the attack, perhaps the breach could have been prevented, as it was due mostly to human error. The data hackers were able to procure may seem arbitrary but that information, which included details on planning, schedules, and personnel, could have exposed classified information if pieced together properly.

In response to the attacks, the claimed unclassified email server was represented by the Obama administration to be shut down immediately after the breach was discovered, and the Defense Department has started the arduous process of sifting through the forensics of the attacks. These steps may be necessary but they are certainly not enough. Protecting our National Security is imperative and we cannot afford to wait until hackers are able to gain access to our classified servers. Confidential information in the wrong hands could be devastating. As a Nation, we must develop a comprehensive plan to protect our country from the very real and equally terrifying threat of cyber attack before it is too late.

###