NEW YORK STATE SENATOR

Michael F. Nozzolio

What Can the Recent Cyber Security Attacks Teach Us?

MICHAEL F. NOZZOLIO July 15, 2015

Our digital infrastructure is under attack. With hackers from around the globe, and most recently reported, China, developing more sophisticated methods to infiltrate even the most advanced and secure systems, we as individuals and as a Nation have never been more vulnerable to cyber security breaches.

According to a recent poll conducted by *The Rochester Business Journal*, fifty-five percent of those polled were increasingly concerned that a major cyber attack could pose a serious threat to the economy or national security of the United States. Even more alarming is that forty-four percent have experienced a cyber security breach on a personal level or through their place of employment. Overwhelmingly, seventy-three percent of those polled believe a large-scale cyber attack on the United States by another country should be considered an

act of war.

If the recent examples of cyber attacks in this country have taught us anything, it is that the number and frequency of attacks will only increase if the issue is not addressed immediately. In the past, many of us believed that the issue of cyber security was one that did not affect us directly or we could avoid if certain precautions were taken. Now, a simple trip to the ATM, filing our taxes online, filling out employment forms, or even checking out at the grocery store can change the trajectory of our finances and personal sense of security in mere seconds.

In the last few months alone, there have been several high profile cyber attacks affecting millions of individuals across the United States. First, an attack on the United States Internal Revenue Service and most recently, a breach of the United States Office of Personnel Management (OPM), possibly by hackers from China.

According to federal authorities, the data breach at OPM occurred in June, compromising computer systems and possibly resulting in the unauthorized transfer of sensitive data such as the Social Security numbers of more than 22 million current, former, and retired employees—not the four million, as was originally disclosed by OPM. Federal hearings on the security shortfall recently brought to light one indisputable fact: OPM was not adhering to their very own security best practices, and as a result, they left the agency exposed, making it a veritable playground for hackers. Private companies have been fined for security breaches while OPM did not hold itself to even its own standards. Last week, after weeks of passing blame and shielding the public from the real scope of the hack, OPM Director Katherine Archuleta was forced to resign her post. Even the Internal Revenue Service (IRS), has found itself a victim of cyber attack due to lapses in protocol and as a result, hackers were able to procure 100,000 tax returns and request 15,000 fraudulent refunds. These agencies are responsible for protecting and preserving the public trust and have failed. They must be held accountable.

Department Store Target’s 2014 security breach compromised the private banking information of nearly 70 million customers. Many of us had our lives temporarily disrupted as a trip on our way home from work to pick up necessities, turned into a flurry of phone calls and disputed charges. In spite of taking the necessary precautions to protect our personal information, a simple purchase at a retailer we believe to be credible can

completely dismantle our trust and destroy our finances. One of the most discernible differences between the Target and OPM hacks is that those in power took responsibility and admitted that more could have been done to thwart the attack from the beginning.

These recent, large-scale attacks on cyber security have shown us that even those entities we thought to be impermeable against attack are only as secure as the practices and procedures they adhere to. Each attack has taken money away from the United States economy and compromised our national security. According to the Center for Strategic and International Studies, cyber crime has cost the U.S. economy roughly $445 billion a year--$160 billion lost by individuals and $285 billion lost by companies. With our safety and our livelihood at risk, necessary actions must be taken to strengthen cyber security procedures in both the public and private sectors.

This column continues 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. We will discuss in the next column, how we can protect ourselves and our Nation from any current or future cyber attacks that threaten the very foundation and safety of our sovereign Nation.

###