Preventing Cyber Attacks Requires a Cooperative Approach

by **Al Berman** | July 30, 2015 2:07 pm | 0 Comments

Al Berman, President, DRI International

High-profile data breaches at Target, Home Depot, Sony, JP Morgan, the U.S. Office of Personnel Management, and even the recent “impact team” hack of the Ashley Madison website with its 37 million members have put cyber attacks on the front pages and in the national spotlight.

The apparent ease of penetration and inability to identify threats has created a new industry for hackers who can extort, compromise, sell, and even destroy data without ever leaving the comfort of their homes. The lack of coordination between the public and private sectors creates an environment that is highly susceptible to attacks from both internal and external environments, and as the frequency of these attacks shows, there are very few, if any, who are truly safe from online digital attacks.

With the great variation that exists among private-sector industries, data security measures taken by one industry may not meet the needs of another. To address the issue of cyber threats and other security risks, the private sector relies on the ability to obtain information (while maintaining anonymity) from similar organizations. These Information Sharing and Analysis Centers (ISACs) are created by industry groups with the goal of advancing the physical and cyber security of the critical infrastructure of North America, and have proven vital in identifying threats.

ISAC members come from industries ranging from financial services to utilities to automotive. Recently, the automotive industry ISAC recognized an issue with hackers’ being able to penetrate the networks that operate key components of an automobile. What started out as remotely unlocking car doors by imitating the frequencies of car door remotes became more intrusive and dangerous after the recent demonstration of hacking that took control of a Jeep. To address this issue, the Automotive ISAC members began working to address this issue and create a more secure network for vehicles.

This private-sector action was followed last week by the introduction of a bill in the U.S. Senate that would direct the National Highway Traffic Safety Administration and the Federal Trade Commission to establish federal standards for automobile cyber security.

The role that government can and/or should play in protecting data held by private organizations is a touchy issue. While the federal government may prosecute those who violate laws, it is not responsible for the cleanup of individual data breaches.

That isn’t to say that the government isn’t taking steps to address the issue of data security and cyber attacks. In addition to the Senate bill, the Comprehensive National Cybersecurity Initiative established a framework for creating a more secure cyber environment. It sought to establish a set of major objectives: establishing a defense against immediate threats, enhancing the security of supply chain vendors, expanding education and research, and creating strategies to deter hostile and malicious activity in cyberspace. And in April, less than a year after signing the DATA Actinto law, President Obama launched a new sanctions program to target individuals and groups outside the United States that engage in malicious cyber attacks. The executive order authorizes the Treasury Department to freeze the assets and bar the financial transactions of entities engaged in

Related Stories

How to Manage Big Data’s Big Security Challenges.
Read the story »

Symantec Exec: Use Big Data to Improve Enterprise Security.
Read the story »

Top 5 Enterprise Security Risks.
Read the story »

Cyber Security Skill Shortage: A Case for Machine Learning.
Read the story »

cyber attacks.

Legislation like the Senate bill to improve the security of automobile systems is important, as the hacking of cars is certainly a problem, but the need continues to exist for more overarching cyber legislation. Consider the risk to financial systems or, even more fundamental, the power grids and the damage that would be caused by a cyber attack. A recent report by the University of Cambridge Centre for Risk Studies and Lloyd's of London created a scenario of a cyber attack blacking out New York City and Washington, D.C. It estimated the impact on the U.S. economy at upwards of $1 trillion.

Therefore, rather than focusing on a single area like automobile security, it is more important to create an overall strategy that protects the entire critical infrastructure and associated resources.

Businesses and industry take certain measures to protect their data. Measures such as encryption and bio identification (fingerprints, retina scan, voice prints) provide more security at the level of the individual business. At the industry level, companies often cooperate to create standards that enhance security. Some industry standards actually provide rewards for securing data and networks. Organizations that meet the Payment Card Industry Data Security Standard (PCI-DSS), for example, receive a discount on fees paid to credit card companies. This discount can amount to millions of dollars for merchants and service providers that take payments from credit card customers and is a powerful incentive to be more secure.

Unfortunately, these measures and the public and private sectors acting independently of each other are not going to solve the problem. We must expand on efforts like the Comprehensive National Cybersecurity Initiative, mentioned above, which was a government action informed by the involvement of representatives from the private sector. An integrated sharing of information between the public and private sectors to identify threats quickly and eliminate perpetrators' ability to carry out these attacks will slow the spread of cyber terrorism.

Alan Berman, president of DRI International, is a Master Business Continuity Professional (MBCP), an NFPA committee member, a member of the ASIS BCP technical committee, a member of the Committee of Experts for ANSI-ANAB, a former member of the NY City Partnership for Security and Risk Management, and the co-chair for the Alfred P. Sloan Foundation committee to create the new standard for the U.S. Private Sector Preparedness Act (PL 110-53). Over a career that has spanned 25 years, he has served as a President and CIO for a major financial institution, National Practice Leader for Operational Resiliency for PricewaterhouseCoopers and Global Business Continuity practice leader for Marsh.